DARI MATERI YANG TELAH SAYA BERIKAN, SILAHKAN MASING MASING KELOMPOK MEMILIH TOOLS IT AUDIT YANG ADA PADA WEB YG TERLAMPIR ATAU REFERENSI SENDIRI.

JELASKAN FUNGSI DARI TOOLS TERSEBUT DALAM IT AUDIT, DAN PENJELASAN SINGKAT TTG TOOLS TERSEBUT

MALTEGO

HARLI SEPTIA FANI (182420122)
PUTRI ARMILIA PRAYESY (182420125)
DEVIAN SAPUTRA (182420128)
I MADE HARYA WIJAYA OKA RAFFLESIA (182420129)
PUTRI ELEINA NURRAHMA (182420138)

MALTEGO

MALTEGO INI DISEBUT **OSINT** (**O**PEN **S**OURCE **I**NTELLIGENCE **G**ATHERING) SEBUAH ALAT UNTUK MELAKUKAN *FOOTPRINTING*, DIGUNAKAN UNTUK MENGUMPULKAN INFORMASI SEBANYAK MUNGKIN DENGAN TUJUAN FORENSIK, *PEN TESTING*, ATAU *ETHICAL HACKING*. APLIKASI YANG DIGUNAKAN UNTUK MEMETAKAN JARINGAN KOMUNIKASI YANG BERADA DI INTERNET TUJUANNYA ADALAH MENGUMPULKAN INFORMASI TENTANG TARGET DAN MENAMPILKAN INFORMASI TERSEBUT DALAM FORMAT YANG MUDAH DIMENGERTI, MEMVISUALISASIKAN INFORMASI TERSEBUT KE DALAM SEBUAH FORMAT GRAPH, SANGAT COCOK UNTUK *LINK ANALYSIS* DAN *DATA MINING*.

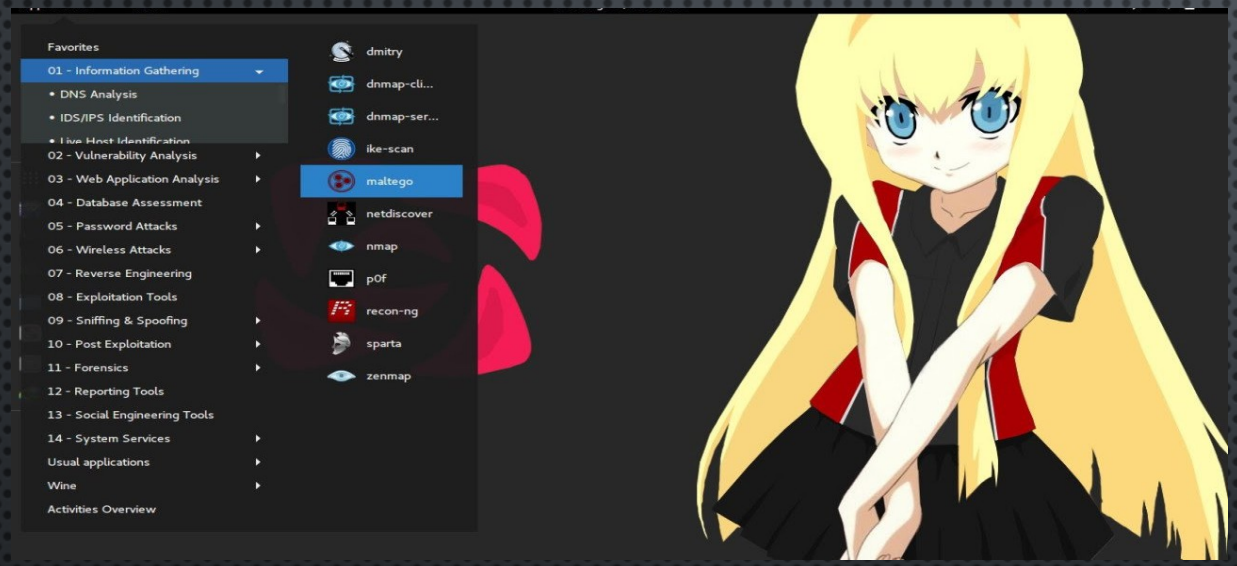
FUNGSI DARI MALTEGO ADALAH MEMUDAHKAN SESEOORANG YANG MENCARI INFORMASI TENTANG APA YANG MEREKA SELIDIKI ATAU MEREKA INCAR SEBAGAI TARGET, CONTOH KETIKA SEORANG MENCARI INFORMASI DARI SEBUAH DOMAIN MENGGUNAKAN MALTEGO, MAKA MALTEGO AKAN MENAMPIKAN BEBRAP INFORMASI SEPERTI BERIKUT:

- BLOCK IP HOSTING
- DOMAIN REGISTE
- EMAIL USER & ADMIN
- PHONE NUMBER
- PETA JARINGAN

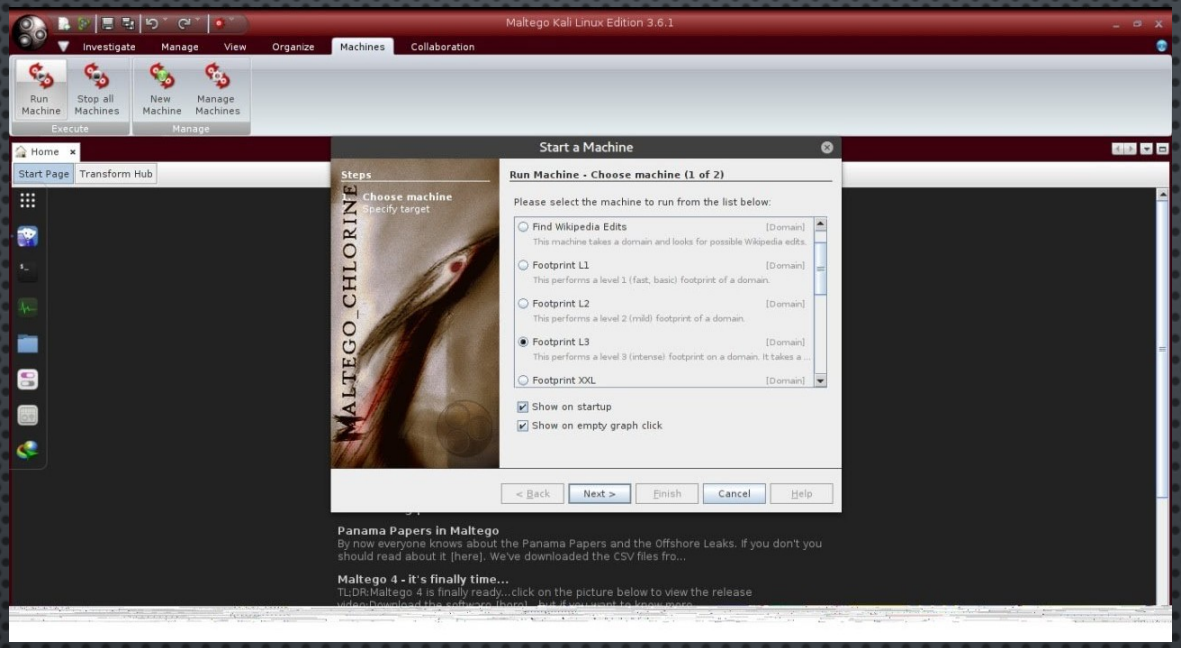
MALTEGO DIBEDAKAN MENJADI VERSI KOMERSIAL (COMMERCIAL EDITION) DAN VERSI GRATIS (COMMUNITY EDITION). VERSI GRATIS YANG TERSEDIA DI KALI LINUX HANYA DAPAT MENAMPILKAN MAKSIMAL 12 HASIL TRANSFORMASI, SEBAGAI SEBUAH FRONT-END UNTUK SERVER OSINT, MALTEGO VERSI GRATIS HANYA DAPAT MEMAKAI LAYANAN SERVER MILIK PATERVA. KARENA VERSI YANG DISEDIAKAN OLEH KALI LINUX ADALAH VERSI GRATIS DARI MALTEGO

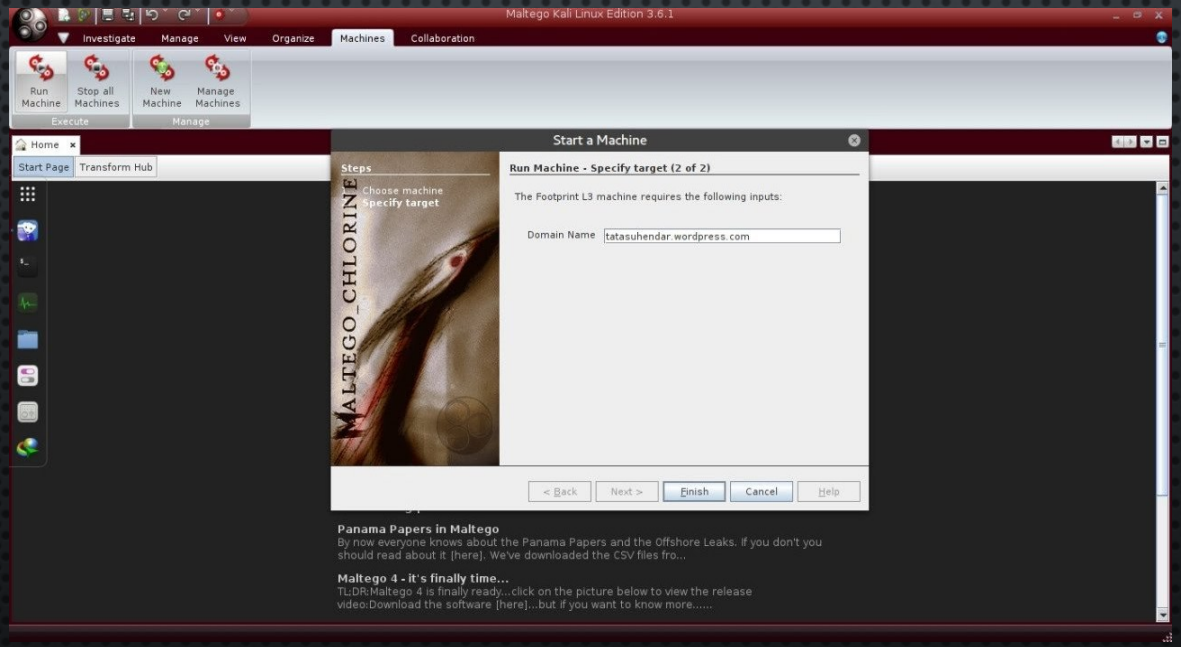
TAHAPAN DALAM PENGGUNAAN MALTEGO

1. BUKA MALTEGO PADA KALI LINUK ANDA, ADA DI MENU INFORMATION GATHERING > MALTEGO

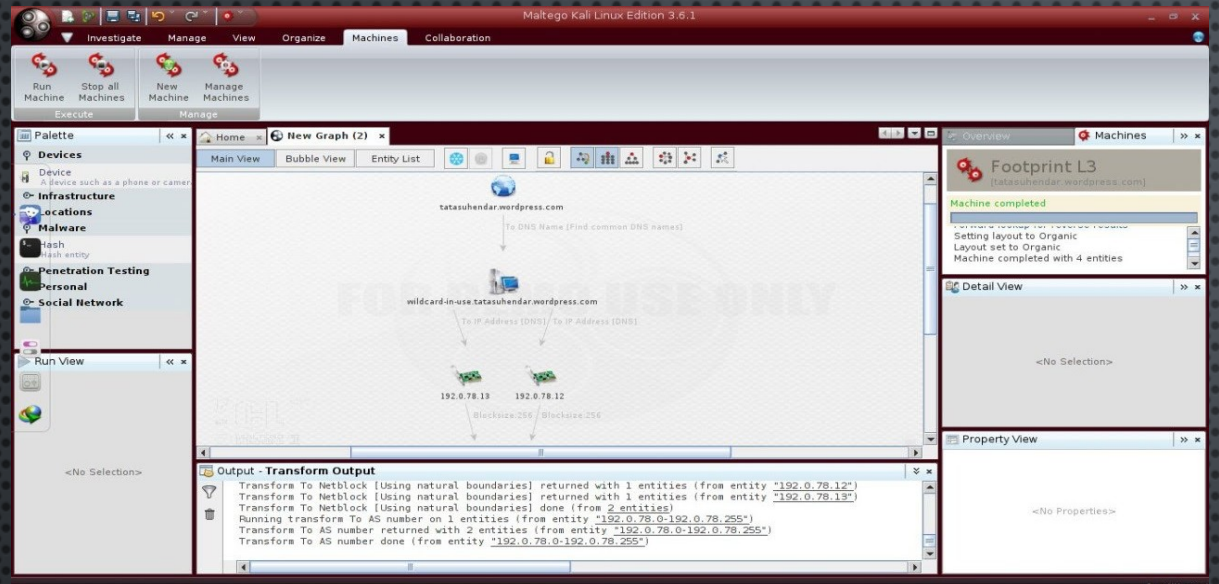


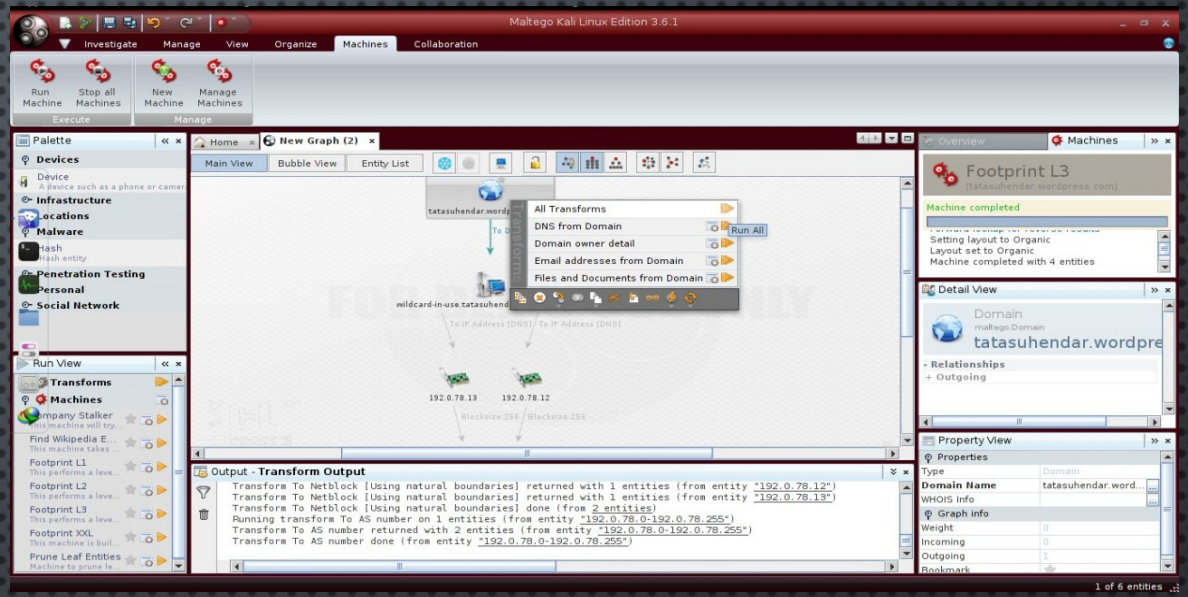
2. LOGIN DENGAN EMAIL DAN PASSWORD YANG TELAH TERDAFTAR
3. SETELAH SELESAI LOGIN MAKA AKAN MUNCUL DIALOG START A MACHINE, PILIH FOOTPRINTING L3 LALU DI STEP KEDUA KITA HARUS MAMASUKAN DOMAIN ATAU LINK WEBSITE TAGE


Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a ...
Footprint XXL [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release

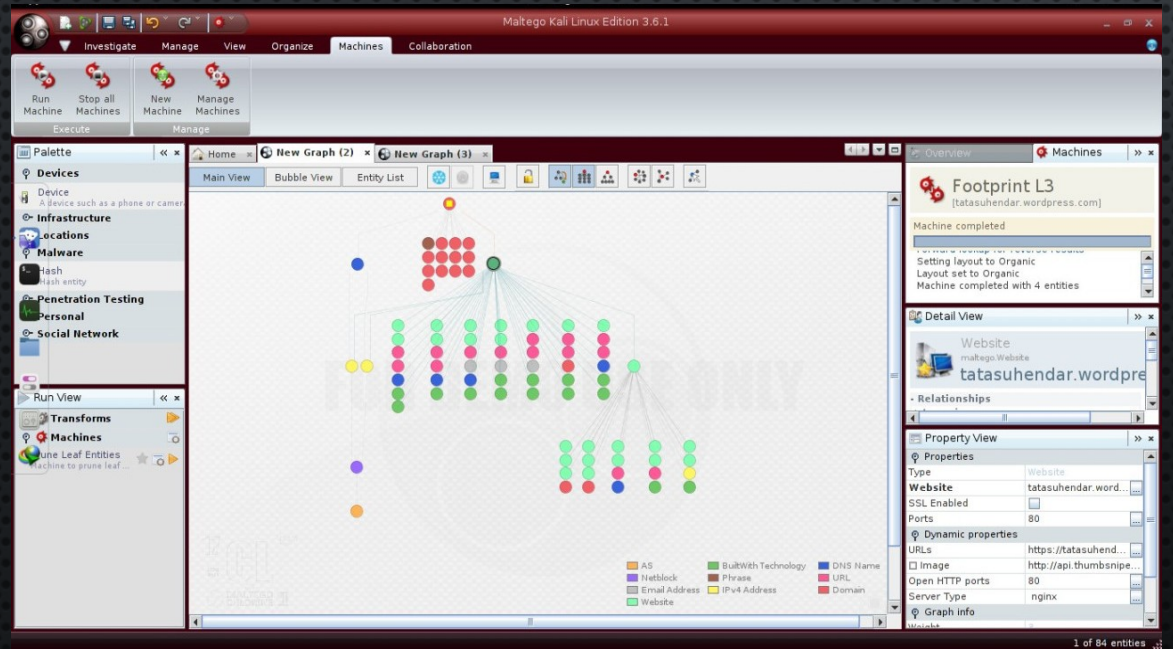

Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Specify target (2 of 2)
The Footprint L3 machine requires the following inputs:
Domain Name
tatasuhendar.wordpress.com
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more.....

4. TAMPILAN AWALNYA KURANG LEBIH SEPERTI INI, DAN DISINI KITA BISA MENGGALI INFORMASI DARI TARGET DENGAN KLIK KANAN PADA WEB TARGET DAN RUN ALL TRANSFORMS

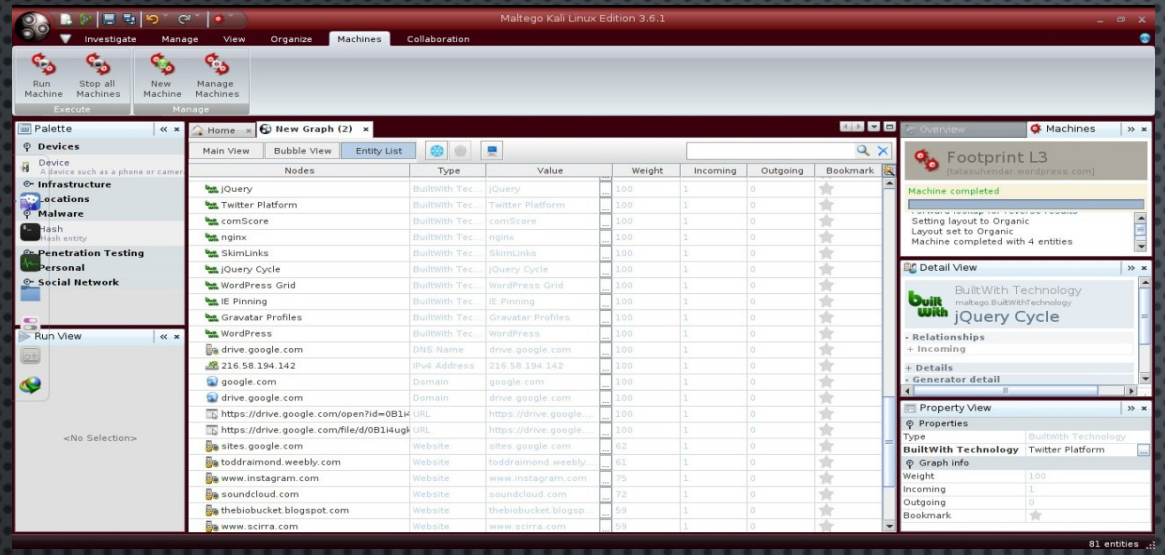




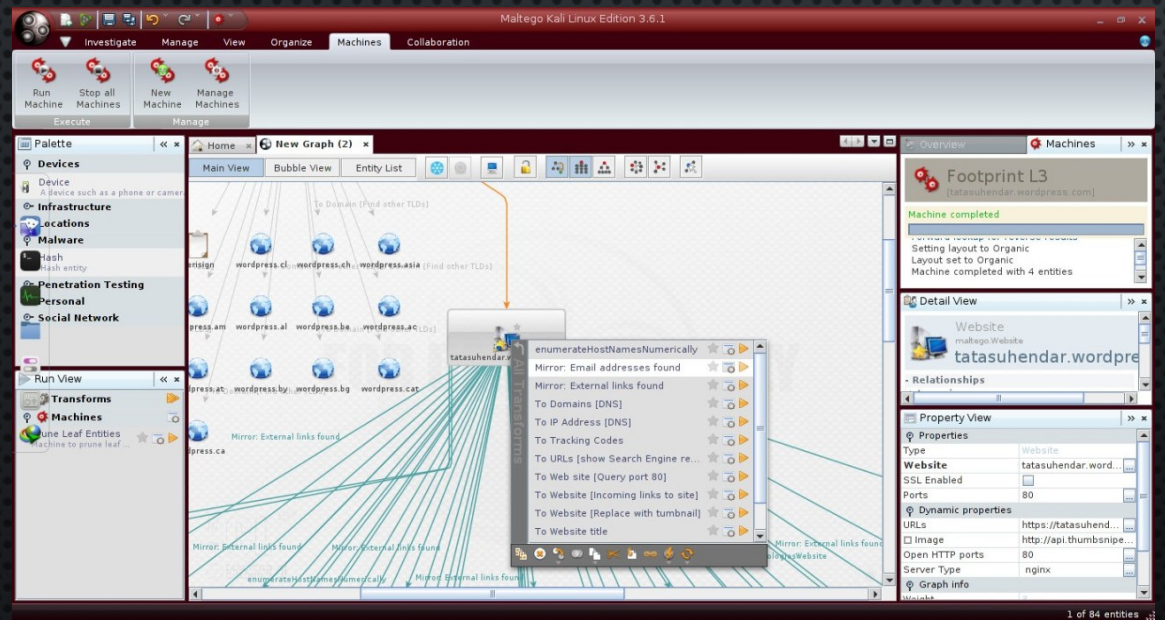
5. BEGINILAH TAMPILAN WEBSITE YANG DITARGETKAN TADI SUDAH DI ALL TRANSFORMS



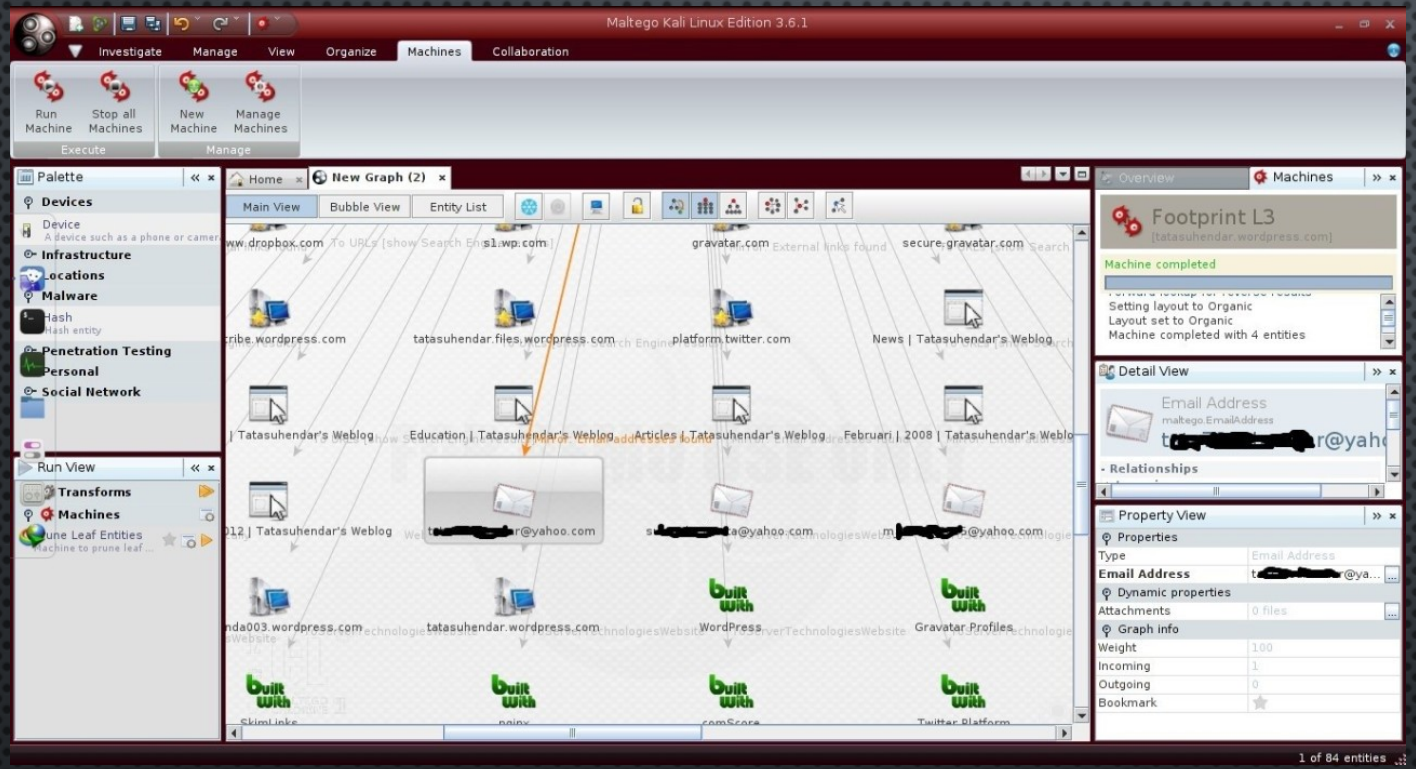
DAN DIBAWAH INI DALAM TAMPILAN ENTRY LIST



6. UNTUK MENCARI INFORMASI TENTANG ALAMAT EMAIL, PILIH IKON WEBNYA LALU KLIK KANAN PILIH“MIRROR: EMAIL ADDRESS FOUND”. INILAH HASILNYA TERDAPAT 3 EMAIL YG TERHUBUNG DENGAN WEB TERSEBUT



7. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA



8. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA

SOURCE

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

https://www.gagaltotal666.site/2016/06/cara-menggunakan-maltego-di-kali-linux.html?m=1

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

TERIMAKASIH

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

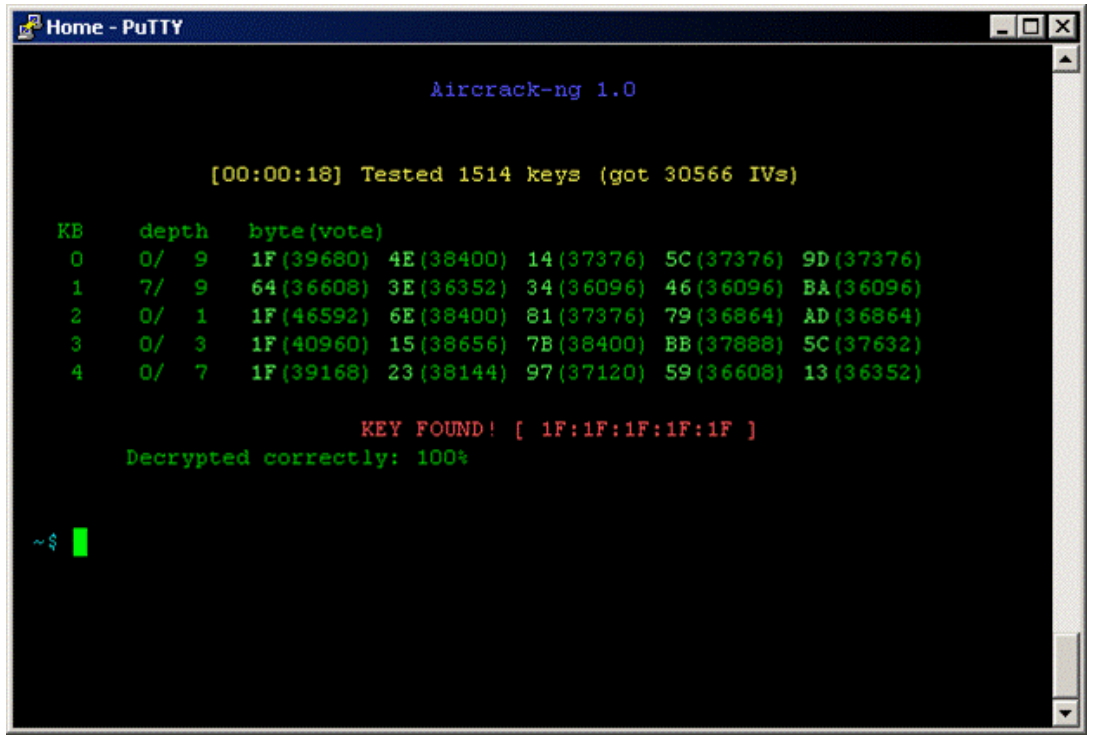
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

Cracking WPA2-PSK Password Wi-FI dengan Aircrack-ng

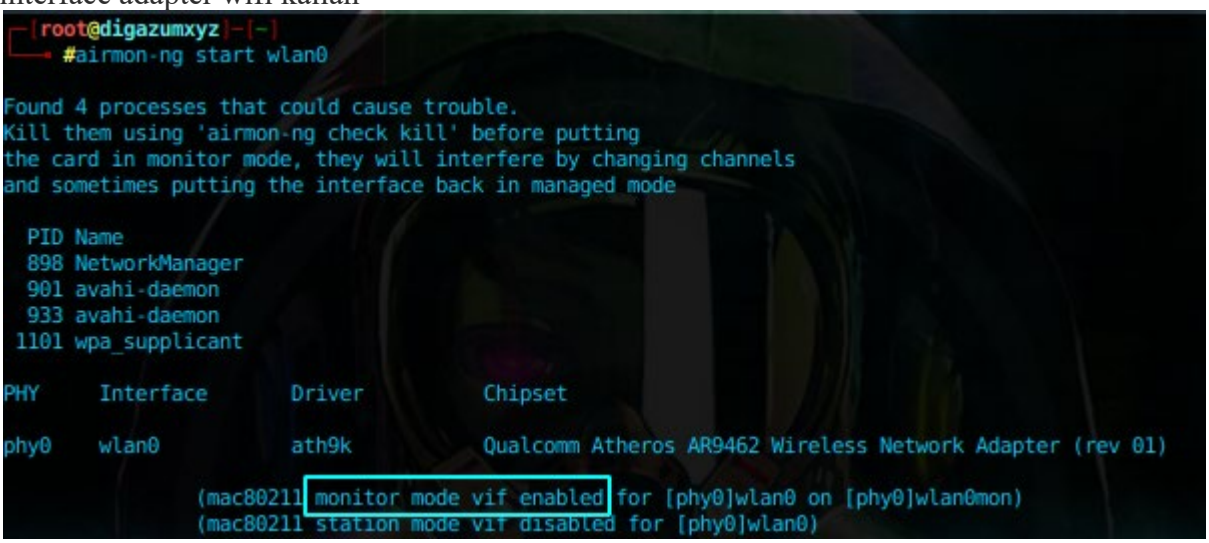
Ketika Wi-Fi pertama kali dikembangkan pada akhir 1990-an, Wired Equivalent Privacy dibuat untuk memberikan kerahasiaan komunikasi nirkabel. WEP, seperti yang diketahui, terbukti sangat rentan dan mudah untuk di bobol.

Sebagai gantinya, sebagian besar titik akses nirkabel sekarang menggunakan Wi-Fi Protected Access II dengan kunci yang dibagikan sebelumnya untuk keamanan nirkabel, yang dikenal sebagai WPA2-PSK. WPA2 menggunakan algoritma enkripsi yang lebih kuat, AES, yang sangat sulit untuk dipecahkan — tetapi bukan tidak mungkin

Kelemahan dalam sistem WPA2-PSK adalah bahwa kata sandi terenkripsi dibagi dalam apa yang dikenal sebagai jabat tangan 4 arah (handshake). Ketika klien mengotentikasi ke titik akses (AP), klien dan AP pergi melalui proses 4 langkah untuk mengotentikasi pengguna ke AP. Jika kami dapat mengambil kata sandi saat itu, kami kemudian dapat mencoba memecahkannya.

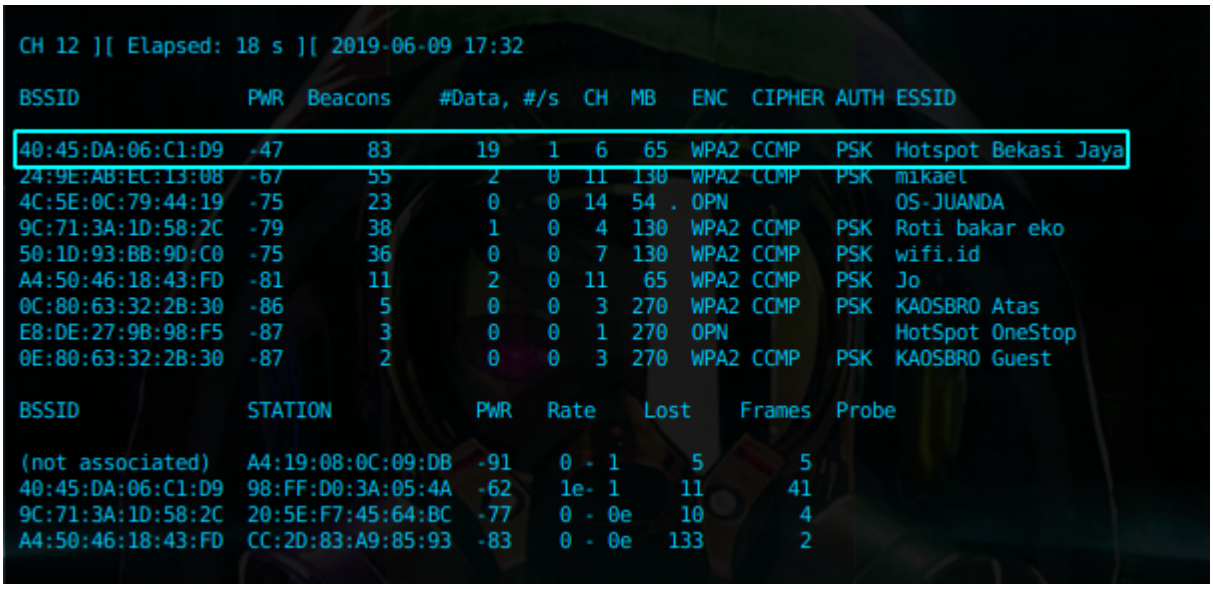
Oke untuk memulai membobol password wifi dengan Keamanan WPA2-PSK lalu pastinya juga dengan algoritma enkripsi yang lebih kuat, disini kita langsung saja mulai ke tutorial cara Crack password Wifi tersebut dengan Keamanan WPA2-PSK, disini kita menggunakan **Aircrack-ng. Aircrack-ng** adalah paket perangkat lunak jaringan yang terdiri dari detektor, packet sniffer, WEP dan WPA / WPA2-PSK cracker dan alat analisis untuk 802.11 LAN nirkabel.

Langkah Pertama Yang kita Mulai ialah memasuki Monitor mode Hal ini memungkinkan kita untuk melihat semua lalu lintas nirkabel (Wifi) yang melewati kita atau disekitar kita, ketikkan saja perintah di terminal **airmon-ng start wlan0** keterangan ***wlan0*** ialah nama interface adapter wifi kalian



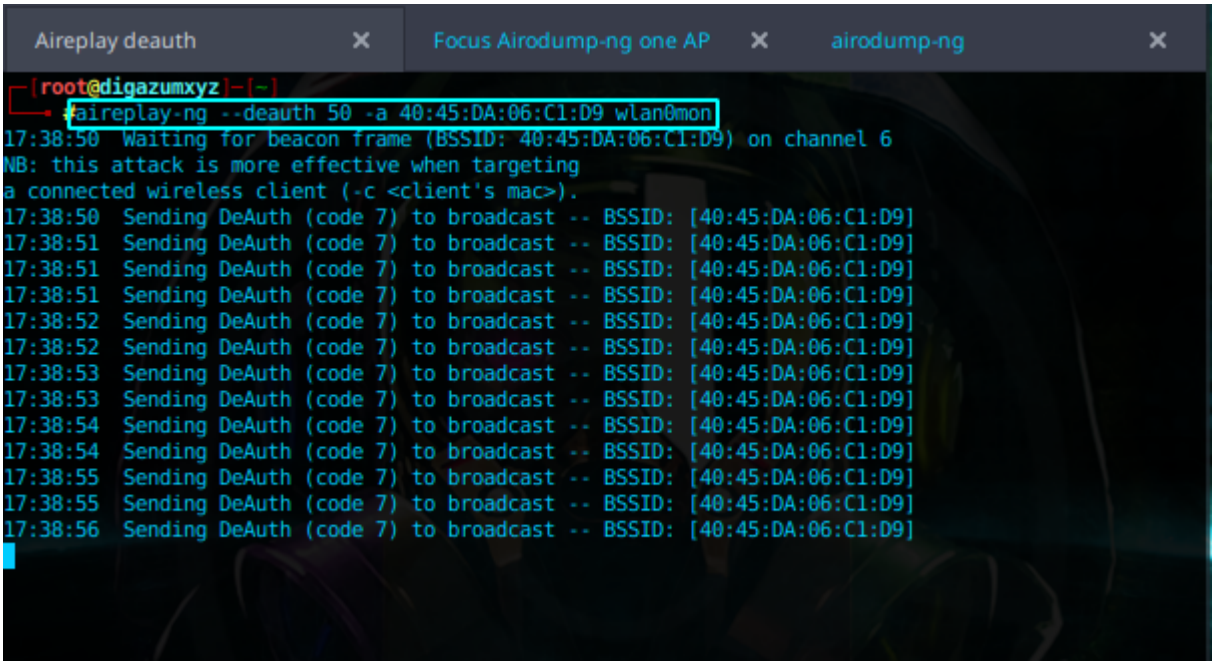
Langkah Kedua ialah Menangkap paket traffic akses point (Wi-FI) sekitar kalian, Perintah ini mengambil semua lalu lintas yang adaptor nirkabel Anda dapat melihat dan menampilkan informasi penting tentang itu, termasuk ***BSSID*** (alamat MAC AP), daya, jumlah bingkai suar, jumlah bingkai data, saluran, kecepatan, enkripsi (jika apa saja), dan akhirnya, ***ESSID*** (yang sebagian besar dari kita sebut sebagai SSID). Mari kita lakukan ini dengan

mengetik **airodump-ng wlan0mon** keterangan ***wlan0mon*** ialah adapter wifi yang sudah mode monitor

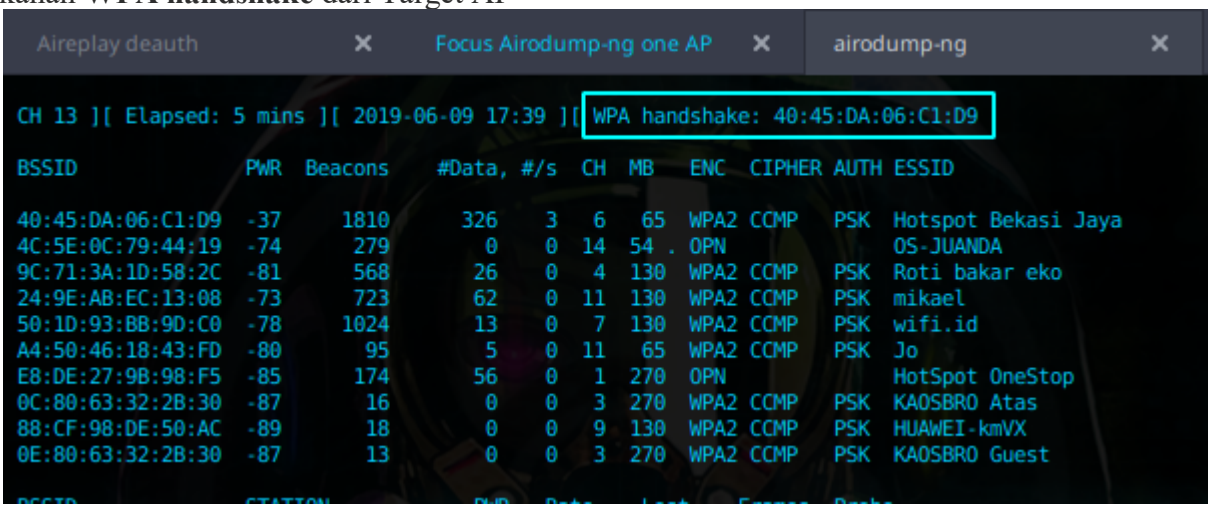


Langkah Ketiga sekarang buka tab baru diterminal, Fokus pada Satu target AP yang kita lakukan nantinya ialah menangkap paket dan traffic dari AP Tersebut, Disini Saya Sudah mendapat Target yaitu AP dengan **ESSID** Hotspot Bekasi Jaya, perintah yang dimasukkan ialah **airodump-ng -c 6 --bssid 40:45:DA:06:C1:D9 --write bekasijaya wlan0mon** keterangan ***40:45:DA:06:C1:D9*** ialah BSSID dari Target AP, ***6*** ialah channel AP, ***bekasijaya*** adalah file yang ingin anda tulis nantinya untuk paket capture file

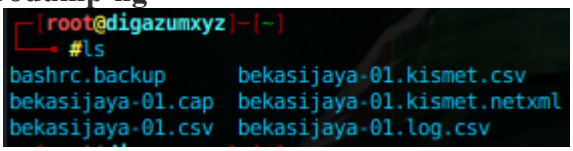
Langkah Keempat buka tab baru terminal, Untuk mendapatkan kata sandi yang dienkripsi, kita harus meminta klien untuk melakukan otentikasi terhadap AP. Jika sudah diautentikasi, kita dapat membatalkan otentikasi (kick off) dan sistem mereka akan secara otomatis mengautentikasi ulang, di mana kita dapat mengambil kata sandi terenkripsi mereka dalam proses. masukkan perintah **aireplay-ng --deauth 50 -a 40:45:DA:06:C1:D9 wlan0mon** keterangan ***50*** ialah jumlah angka de-authenticate frames yang ingin anda kirim, ***40:45:DA:06:C1:D9*** BSSID Target AP



Langkah Kelima, disaat kita sedang melakukan deauthentication frames pada target ap disini kita sekaligus menunggu penangkapan paket handshake (jabat tangan), jadi kita memantulkan pengguna dari AP mereka sendiri, dan sekarang ketika mereka mengautentikasi ulang, airodump-ng akan berusaha mengambil kata sandi mereka dalam jabat tangan 4-arah yang baru. Mari kita kembali ke terminal airodump-ng kami dan memeriksa untuk melihat apakah kita sudah berhasil atau tidak. Jika Sudah Berhasil Maka Akan Ada tulisan di pojok kanan **WPA handshake** dari Target AP

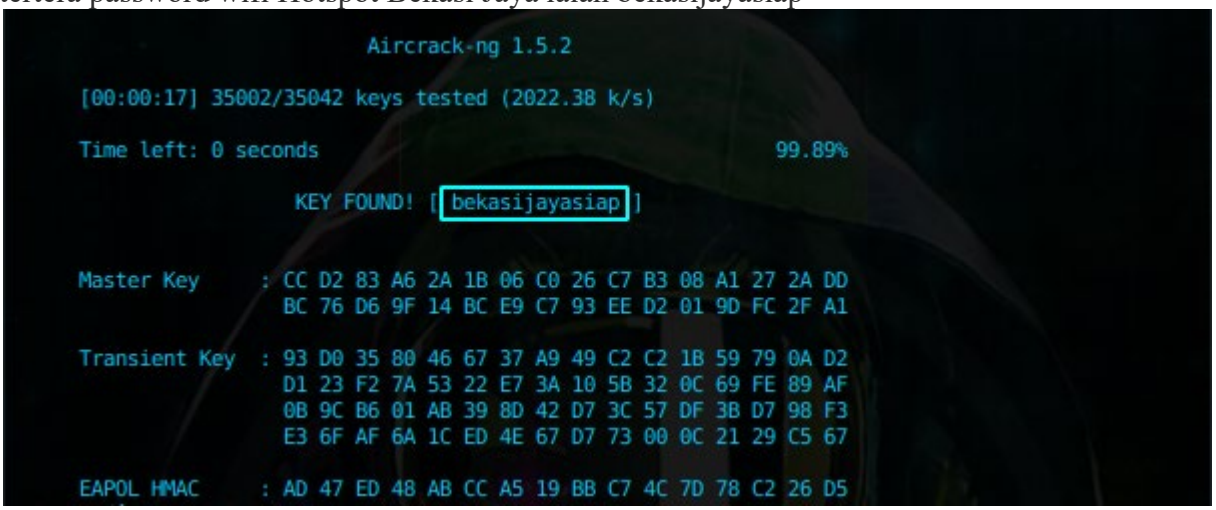


Saatnya Cracking Password Target AP Tersebut, sebelumnya untuk mengcrack password tersebut kita membutuhkan file hasil capture tadi biasanya tersimpan di direktori saat kalian menjalankan perintah **airodump-ng**

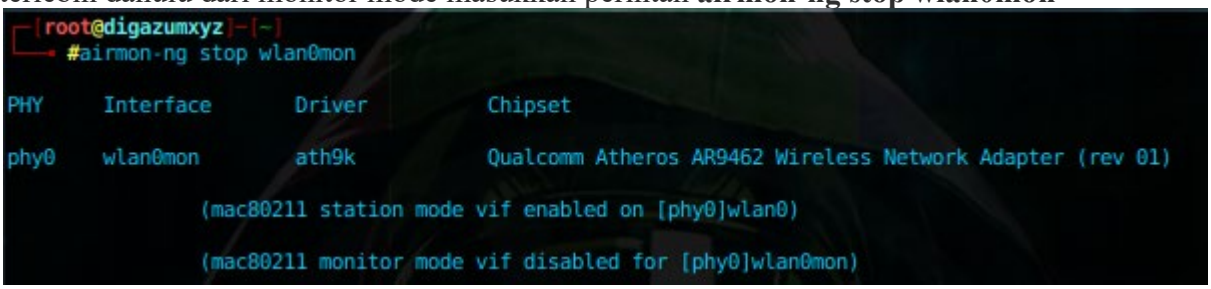


Mulai Crack!! langkah pertama sebelum crack ialah kita membutuhkan wordlist banyak tools pembuat wordlist generator seperti crunch, cewl, cupp dan masih banyak lagi,, oke saatnya crack masukkan perintah **aircrack-ng bekasijaya-01.cap -w /home/galangxyz/wordlistbekasi.txt** keterangan ***bekasijaya-01.cap*** ialah adalah nama file yang kita tulis dalam perintah airodump-ng lau ***/home/galangxyz/wordlistbekasi.txt*** ialah

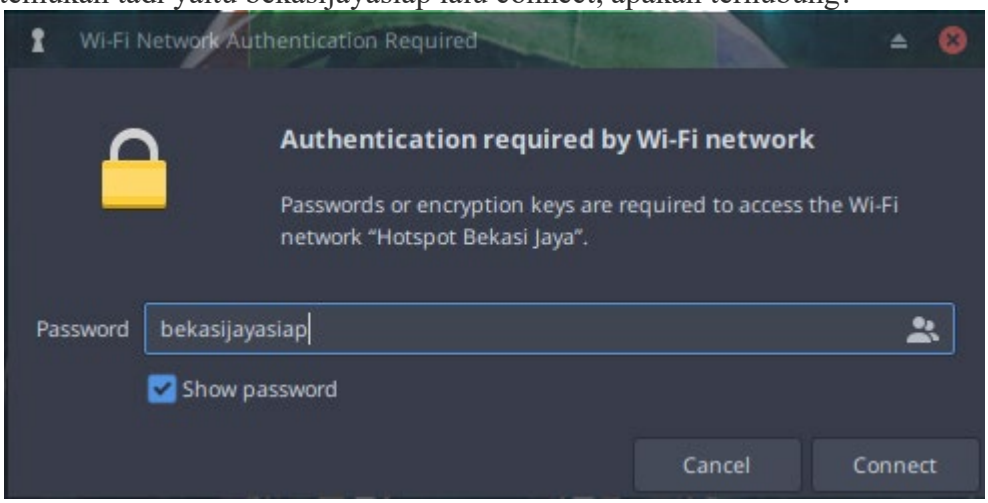
path wordlist yang saya buat, prosesnya bisa relatif lambat dan membosankan. Tergantung pada panjang daftar kata sandi kalian, Anda bisa menunggu beberapa menit hingga beberapa hari, Jika sudah menemukan Kata sandi yang cocok maka akan muncul **KEY FOUND!** disitu tertera password wifi Hotspot Bekasi Jaya ialah bekasijayasiap



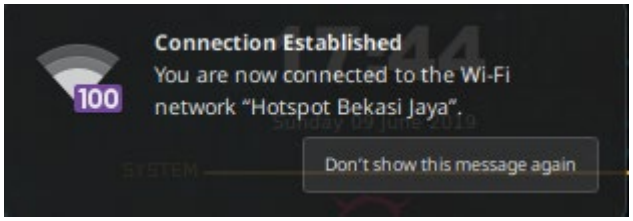
Sebelum kita Menguji Passwordnya apakah benar apa tidak alangkah baiknya kita stop terlebih dahulu dari monitor mode masukkan perintah **airmon-ng stop wlan0mon**



Pengujian Sambungkan saja Ke wifi Hotspot Bekasi Jaya lalu massukan password yang sudah ditemukan tadi yaitu bekasijayasiap lalu connect, apakah terhubung?



Yap benar sekali disini sudah berhasil :D



Oke Mungkin itu saja sekian dari saya semoga bermanfaat.... ini hanya untuk pembelajaran..

Hack Password Windows 7 / Vista With OphCrack

Beberapa alasan mengapa orang-orang harus menggunakan tool yang bisa *cracking password* di sistem operasinya diantaranya adalah karena masalah klise seperti lupa akan passwordnya, kemudian ada juga yang penasaran ingin tau password milik orang lain, tetapi ada lagi yg tidak terpuji yaitu ingin mencuri password dan melakukan tindakan kriminal.
Ibarat sebuah pisau mempunyai fungsi yang berbeda ketika dipegang oleh orang yang berbeda, ibu-ibu mungkin menggunakan pisau untuk mencincang daging, mengupas kentang atau buah-buahan dan memotong sayur, tapi jika ditangan seorang maling, pisau bisa digunakan untuk menodong bahkan membunuh.

Sama halnya dengan OphCrack, software / tool ini bisa digunakan untuk *merecovery password* yang kelupaan di windows 7 / Vista. Tapi tool yang sama juga dapat disalahgunakan oleh orang-orang yang tidak bertanggungjawab untuk mencuri password Windows 7 / Vista.
OphCrack bisa dijalankan di lingkungan Windows ataupun secara live CD. Mekanisme *tool hacking password* di Windows 7 / Vista tidak terlalu saya pahami, tetapi yang jelas adalah mereka menggunakan *teknik hashing* kelas atas. Password yang lupa bisa direcovery dalam jangka waktu yang sangat singkat. Nah, jika lupa password komputer yang menggunakan Windows 7 dan Vista, gunakan software ini untuk mengembalikan password yang lupa tsb. Gunakan dengan bijak, jangan untuk mencuri atau crack yang tidak berguna.

Software / program ini disediakan gratis dan bisa di-download sourceforge
NB: AVG akan mendeteksi program ini sebagai aktivitas yang mencurigakan.

Cara Mengatasi Lupa Password Log In Windows 7. Bagi sobat-sobat yang lupa dengan ***password log in*** pada **windows 7** **sobat**, Disini saya punya tipsnya. dan tips ini bukan hacking lo karena cara ini tanpa melakukan reset password lama. ok langsung aja ya mas

bro…

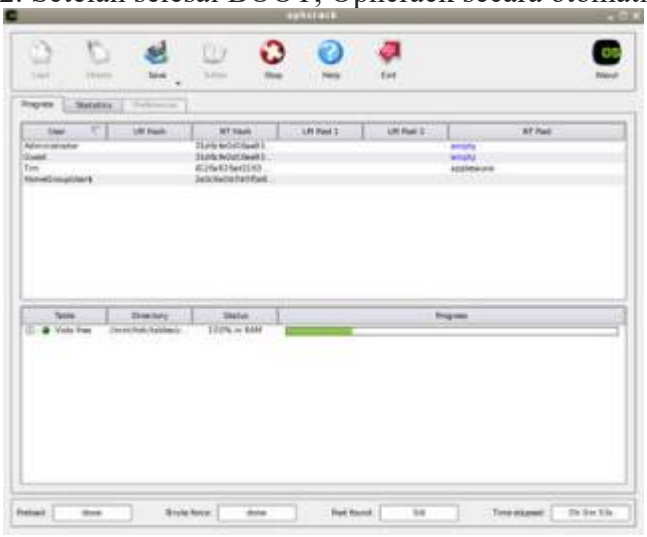
Cara Mengatasi Lupa Password Log In Windows 7
Download:

- Download image CD di situs Ophcrack
- Pastikan sobat mendownload sesuai dengan System Operation yang sobat pakai. Jika sobat menggunakan WINDOWS 7 maka download versi VISTA, karena versi ini dapat berjalan pada Vista maupun Windows 7.
- Setelah mendownload file ISO, burn file ISO tersebut ke CD
- Jika sudah Boot dari CD

Cara penggunaan:

1. Boot komputer dari CD yang telah dibuat tadi.

2. Setelah selesai BOOT, Ophcrack secara otomatis melakukan cracking password.



3. Pada gambar diatas merupakan tampilan ***OPHCRACK*** setelah selesai boot. Selanjutnnya Ophcrack akan mencoba recovery password semua account user.

4. Perhatikan kolom user pada tabel diatas, itu merupakan user account yang dipakai pada WINDOWS 7. Dan pada tabel Nt pwd adalah password log in WINDOWS 7. Jika password pada tabel Nt pwd belum kosong untuk user tertentu berarti password tersebut belum dipulihkan.
5. Jika pada tabel Nt pwd sudah empty, sekarang sobat dapat log in WINDOWS 7 tanpa password. Dengan catatan user account diaktifkan.
6. Setelah Ophrack selesai menghapus akun, keluarkan CD OPHCRACK dari CD Drive sobat, dan restartlah PC sobat. Dengan cara ini seharusnnya sobat sudah bisa Log in ke OS sobat tanpa password.

References :

https://digazumxyz.blogspot.com/2019/06/cracking-wpa2-psk-password-wi-fi-dengan.html

https://alfairuz69.wordpress.com/cara-membobol-pasword-windows-menggunakan-ophcrack/

METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIYANSAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

Program Pascasarjana
Magister Teknik Informatika
MTI – 20A

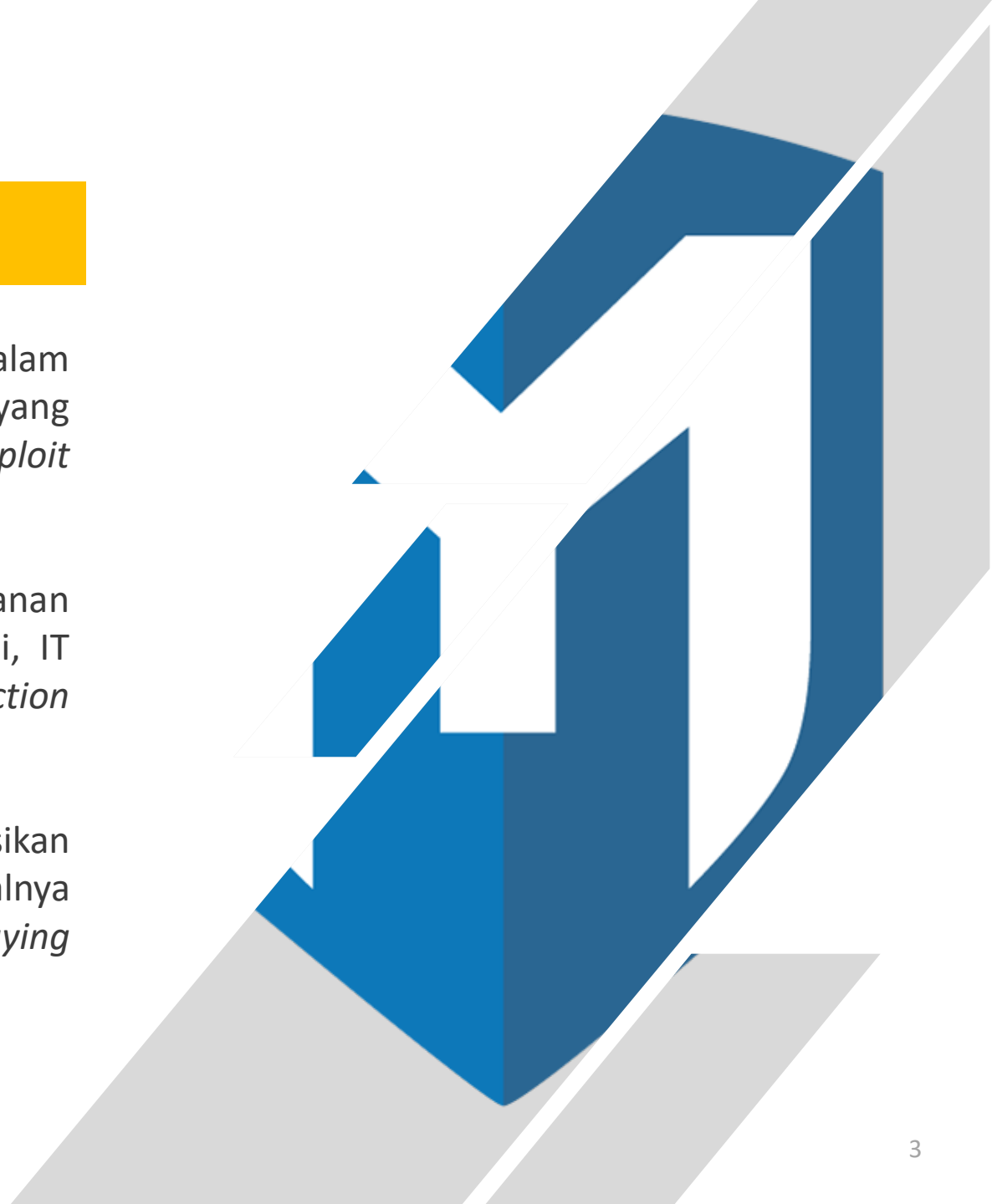
metasploit®

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.



TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

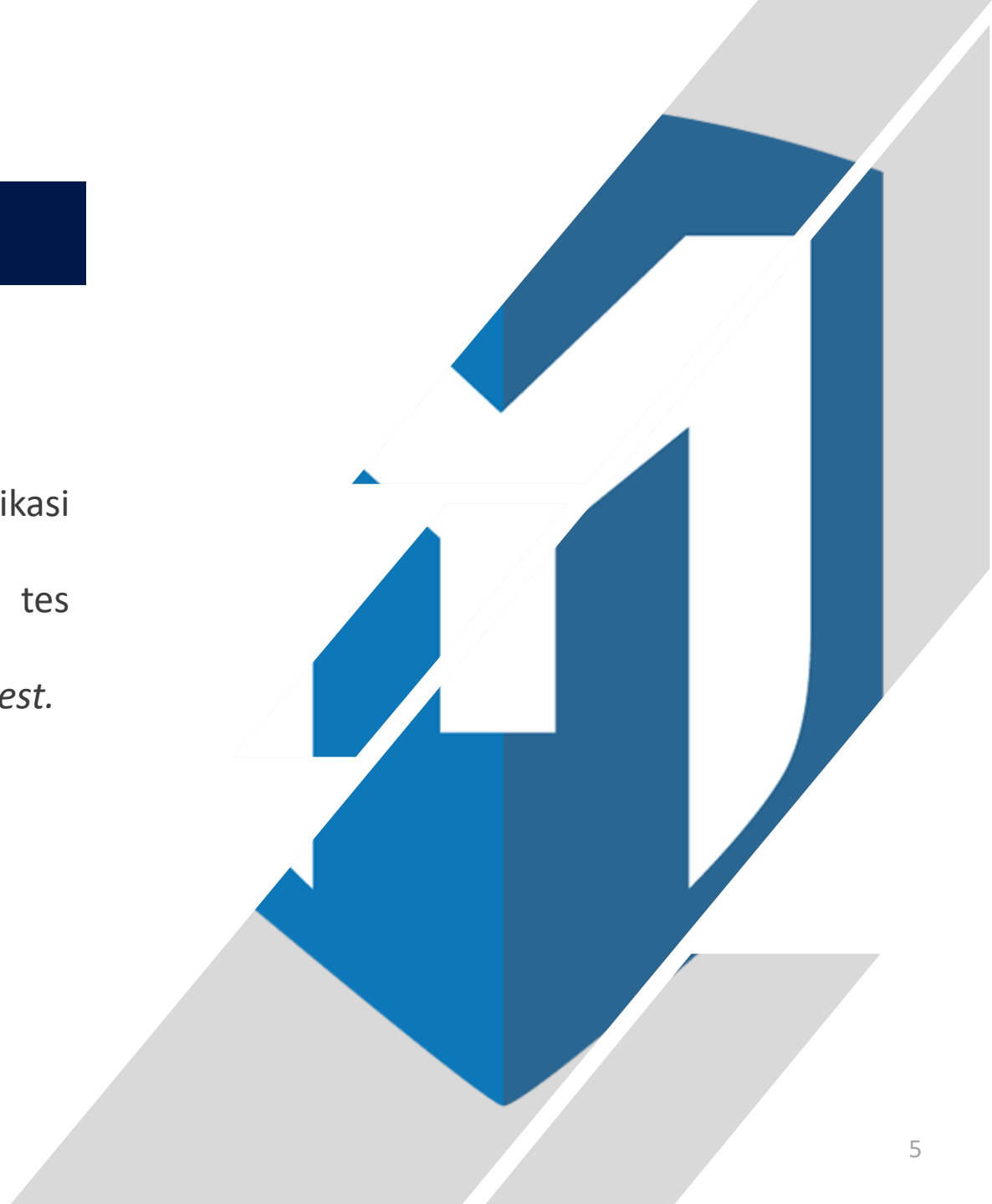
Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.



MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

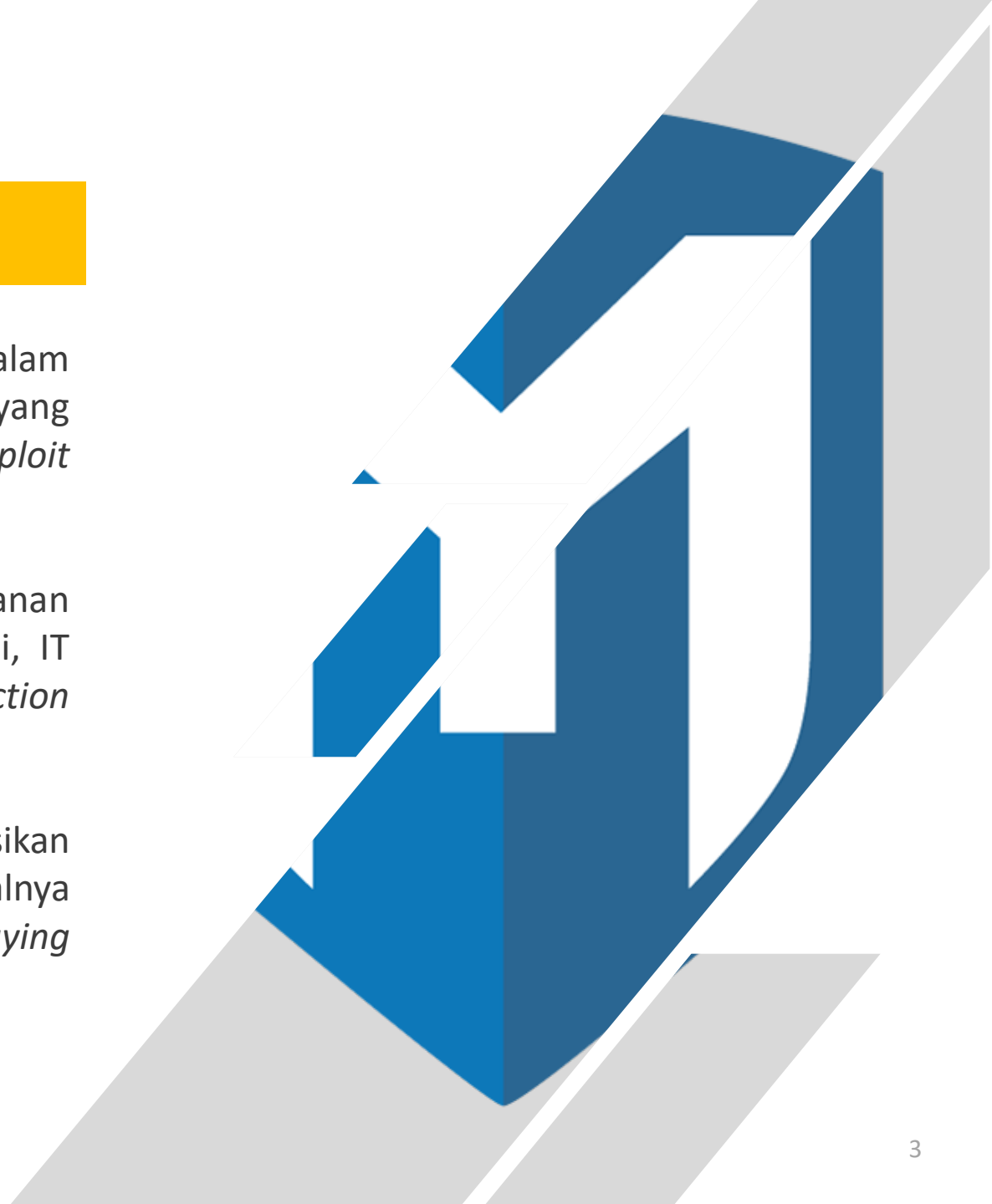
1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIE ANSYAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.



TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

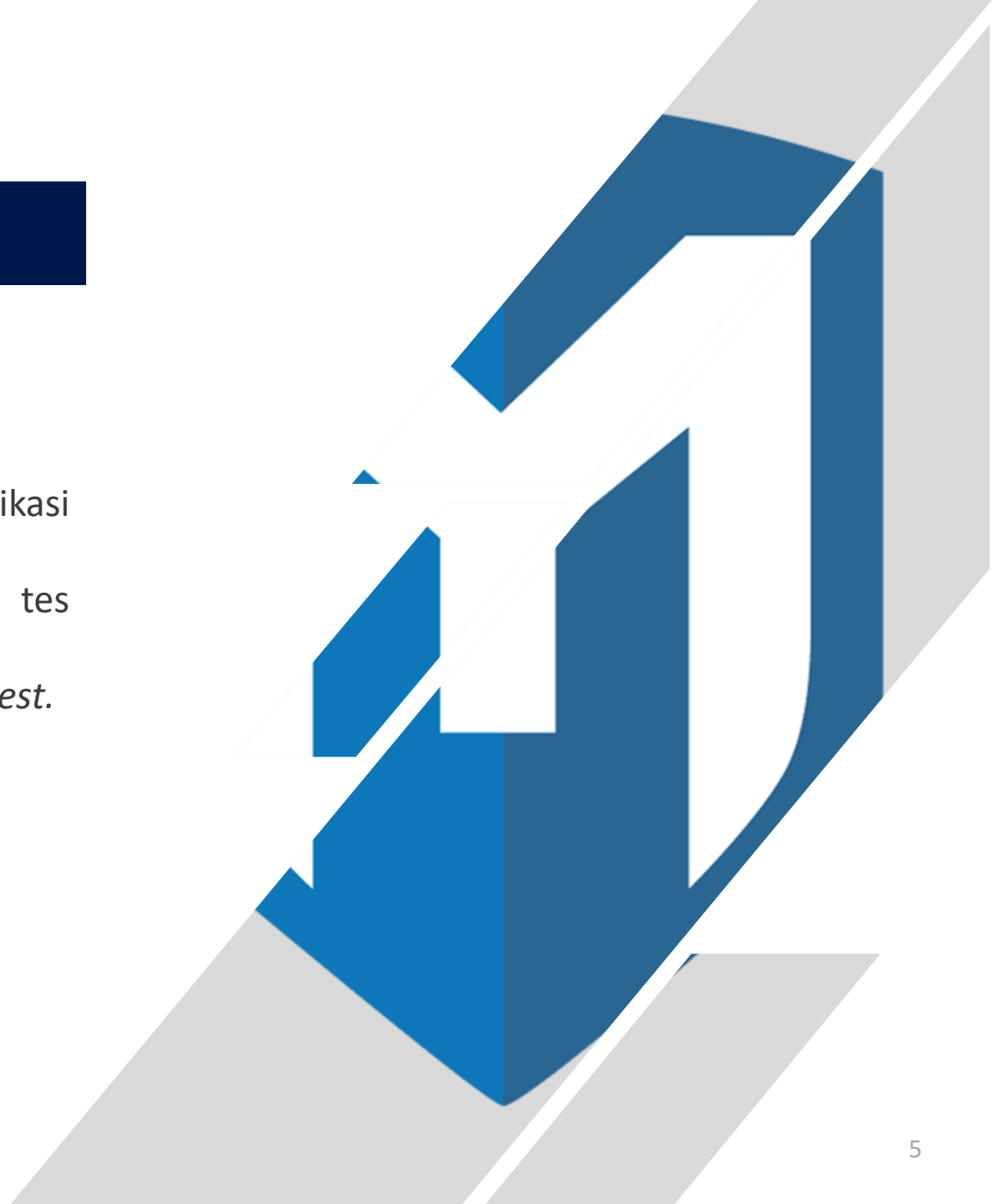
Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.



MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

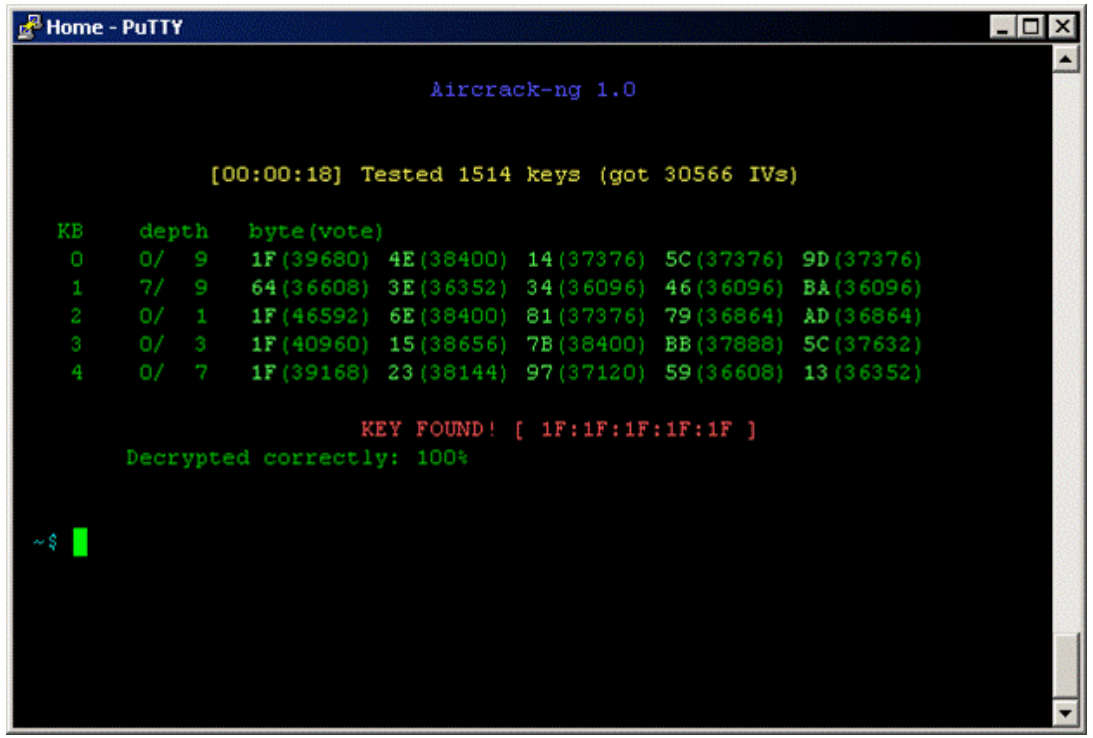
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

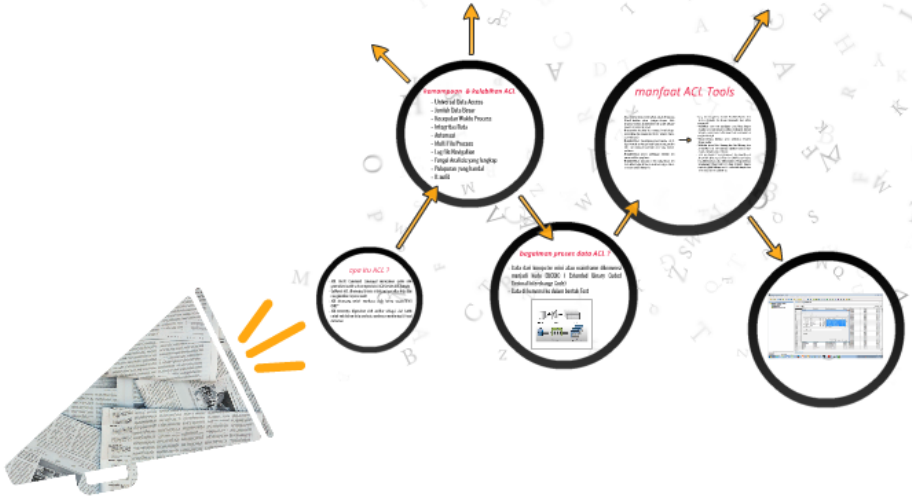
References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

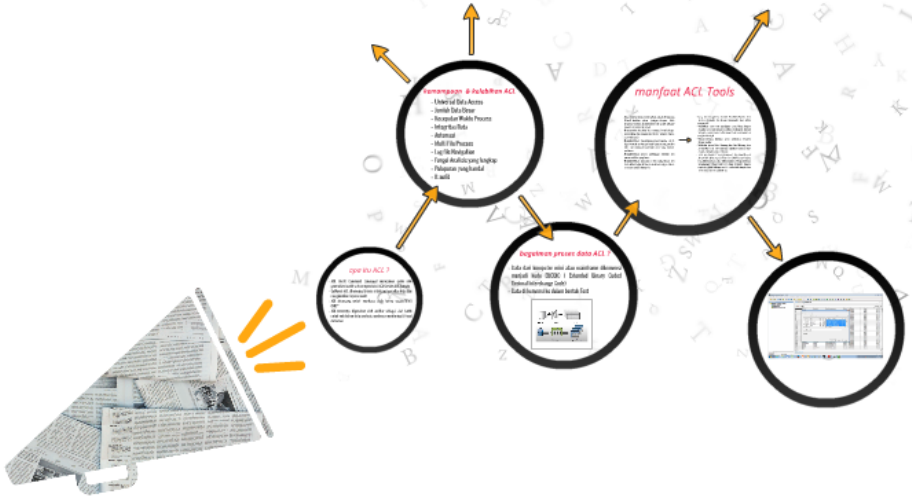
IT AUDIT SOFTWARE ACL

KELOMPOK 3
Caesario Rian Saputra (182420131)
Masroni Dedi Kiswanto (182420139)
Hamzah Ramadhan (182420124)



IT AUDIT SOFTWARE ACL

KELOMPOK 3
Caesario Rian Saputra (182420131)
Masroni Dedi Kiswanto (182420139)
Hamzah Ramadhan (182420124)



apa itu ACL ?

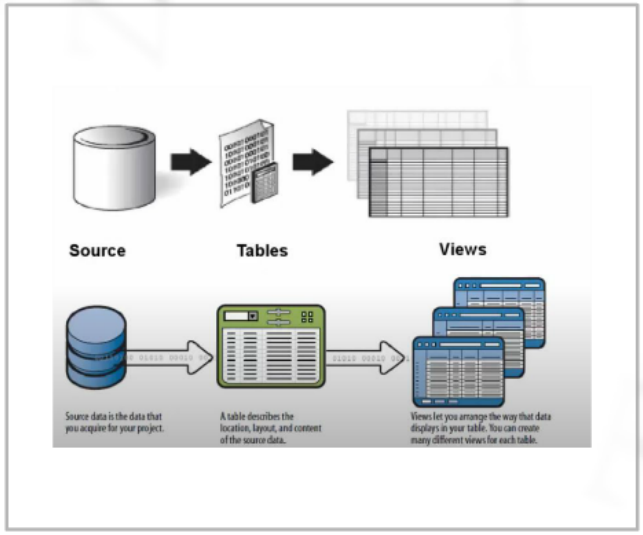
- ACL (Audit Command Language) merupakan salah satu generalized audit software produksi ACL Servies Ltd, Canada
- Software ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit
- ACL dirancang untuk membaca data hanya secara"READ ONLY"
- ACL umumnya digunakan oleh auditor sebagai alat bantu untuk melakukan data analysis, continous monitoring & froud detection

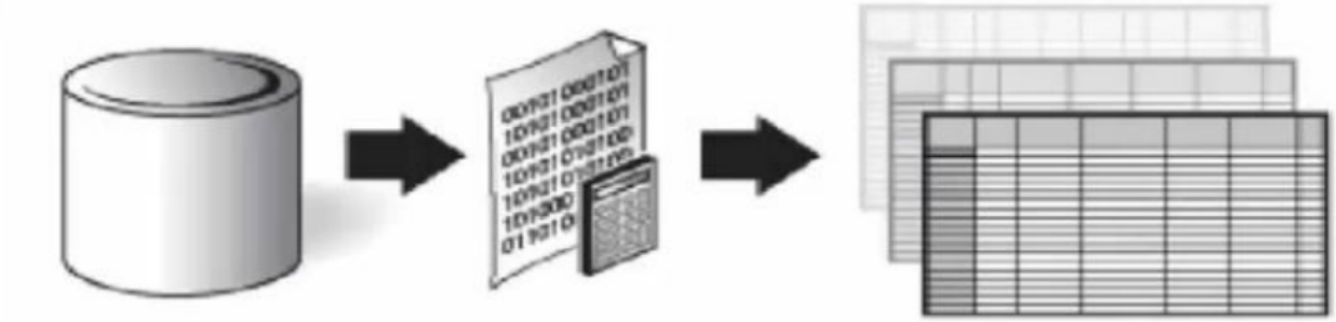
kemampuan & kelebihan ACL

- Universal Data Access
- Jumlah Data Besar
- Kecepatan Waktu Process
- Integritas Data
- Automasi
- Multi File Process
- Log file Navigation
- Fungsi Analisis yang lengkap
- Pelaporan yang handal
- It aufit

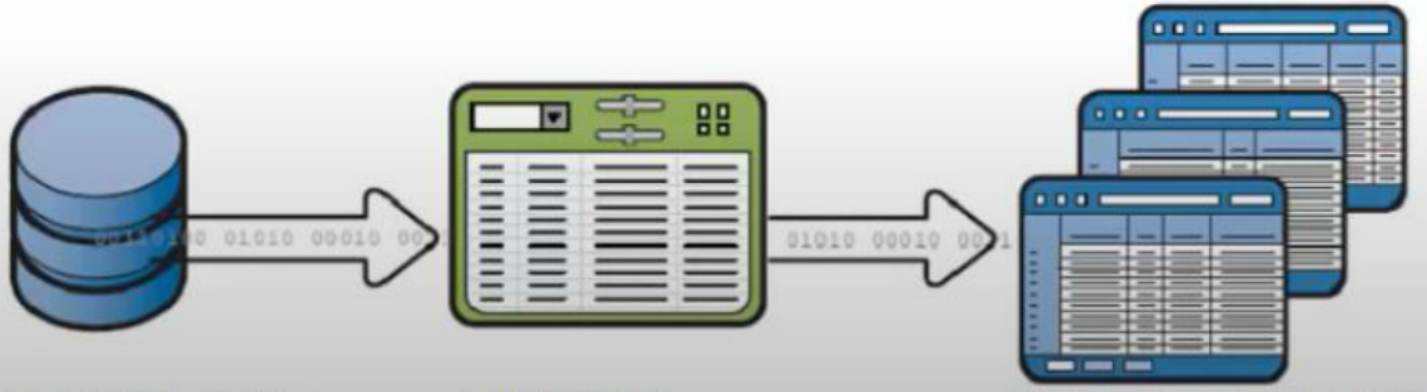
bagaiman proses data ACL ?

- Data dari komputer mini atau mainframe dikonversi menjadi kode EBCDIC (Extended Binary Coded Decimal Interchange Code)
- Data di konversi ke dalam bentuk Text





Source **Tables** **Views**



Source data is the data that you acquire for your project.

A table describes the location, layout, and content of the source data.

Views let you arrange the way that data displays in your table. You can create many different views for each table.

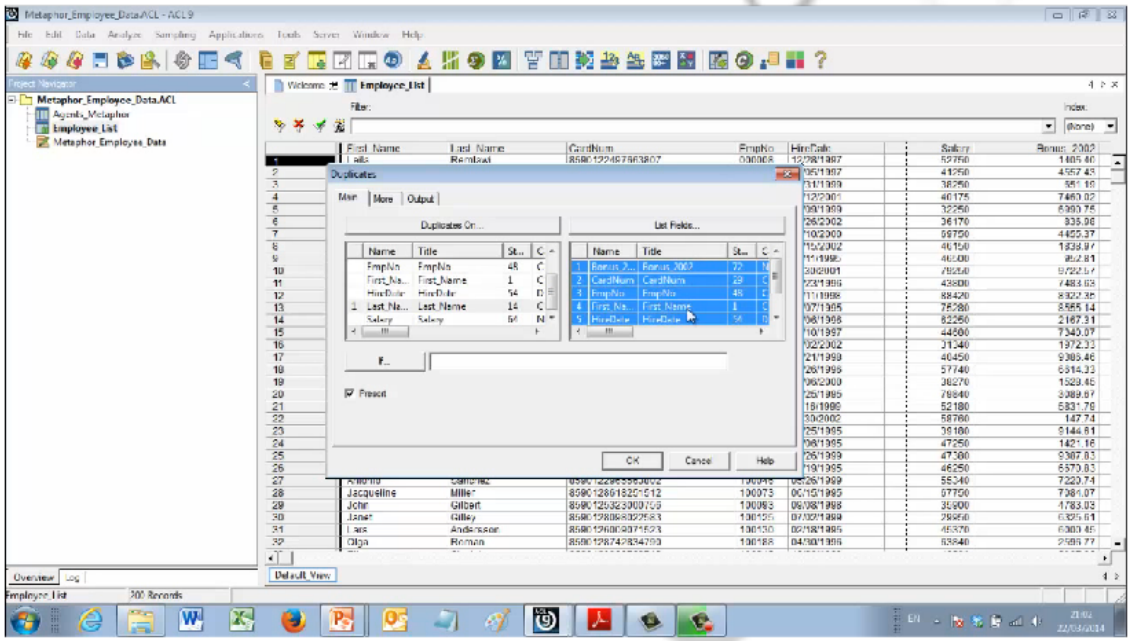
manfaat ACL Tools

- Dapat membantu dalam mengAkses data baik langsung (Direct) kedalam system jaringan ataupun tidak langsung (InDirect) melalui media lain seperti softcopy dalam bentuk teks file/report.
- Menempatkan kesalahan dan potensial fraud sebagai pembanding dan menganalisa file-file menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.

- Aging dan menganalisa Account Receivable/Payable atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor Invoice/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan supplier.
- Melakukan proses Data Cleansing dan Data Matching atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh End-User.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (Fraud Detection) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

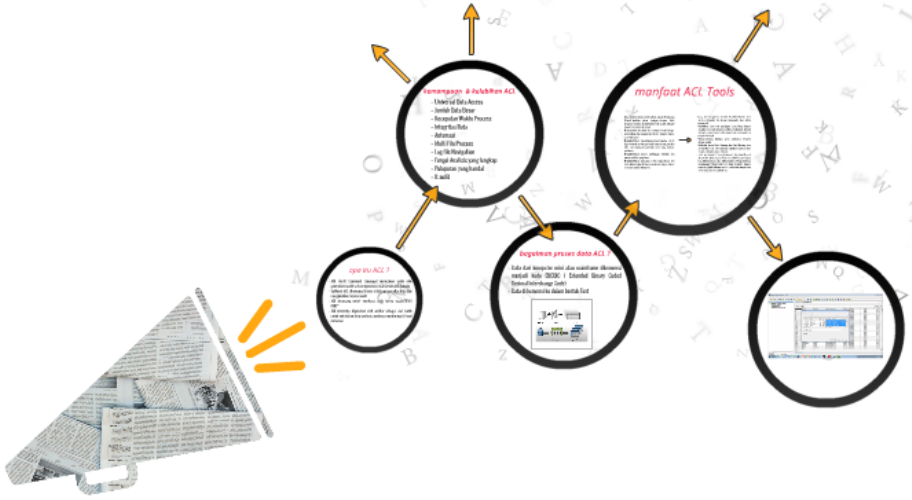
- Dapat membantu dalam mengAkses data baik langsung (Direct) kedalam system jaringan ataupun tidak langsung (InDirect) melalui media lain seperti softcopy dalam bentuk teks file/report.
- Menempatkan kesalahan dan potensial fraud sebagai pembanding dan menganalisa file-file menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.

- Aging dan menganalisa Account Receivable/Payable atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor Invoice/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan supplier.
- Melakukan proses Data Cleansing dan Data Matching atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh End-User.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (Fraud Detection) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.


Metaphor_Employee_Data.ACL
Employee_List
Duplicates
Main
More
Output
Duplicates On...
List Fields...
Preset
OK
Cancel
Help

IT AUDIT SOFTWARE ACL

KELOMPOK 3
Caesario Rian Saputra (182420131)
Masroni Dedi Kiswanto (182420139)
Hamzah Ramadhan (182420124)



METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

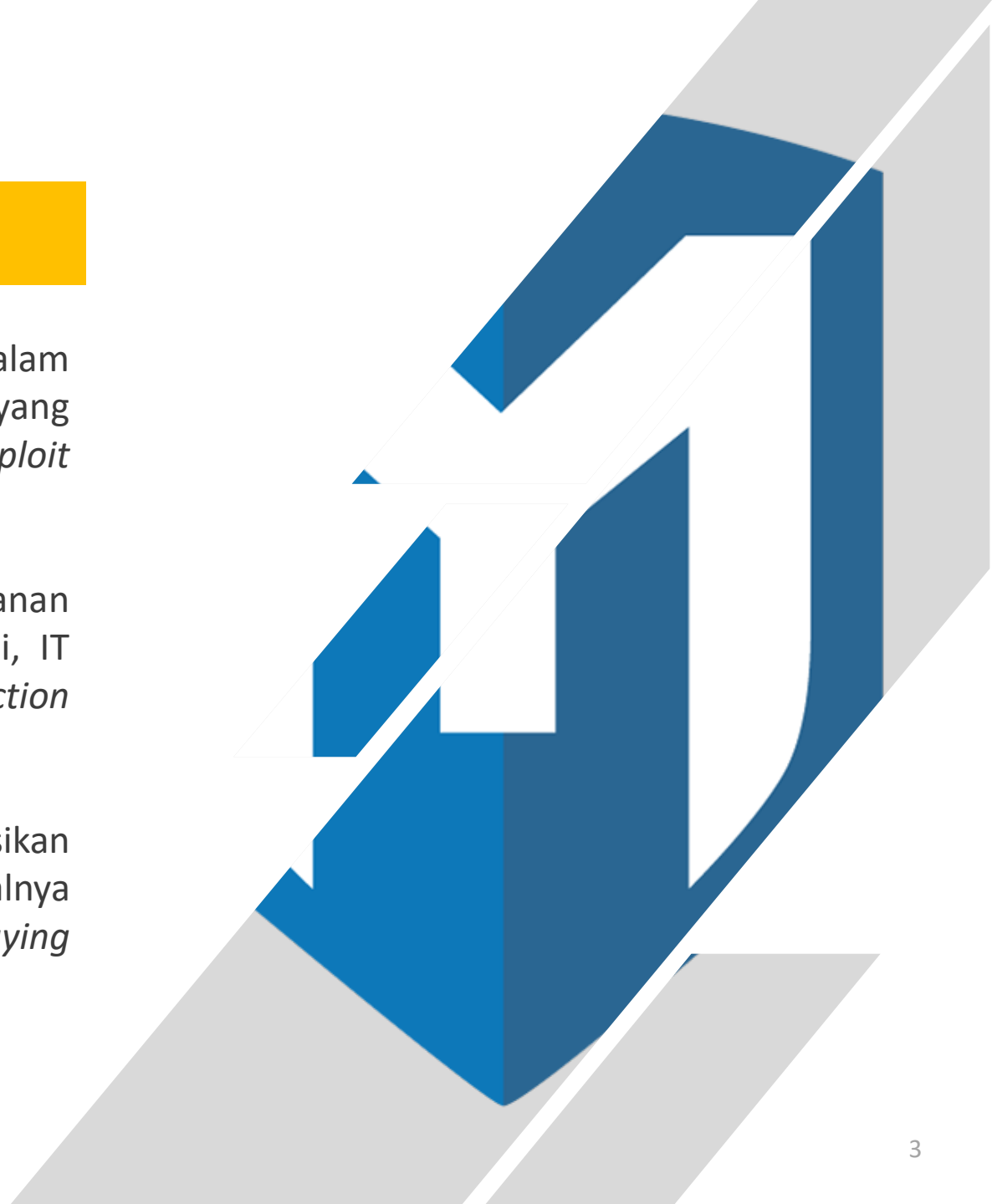
1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIE ANSYAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.



TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

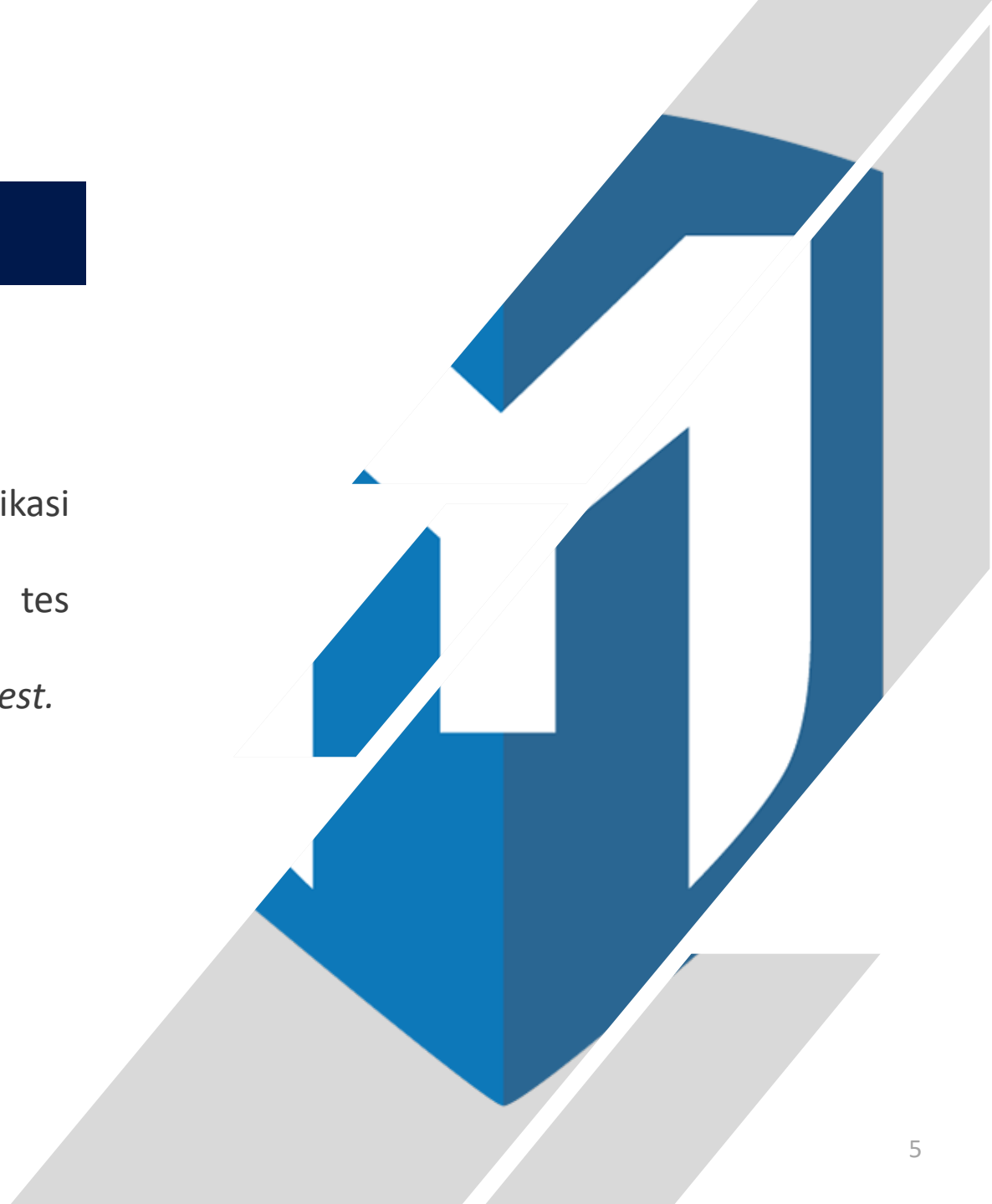
Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.



MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

Nama : Mefta Eko Saputra
NIP : 182420113
Kelas : MTI20A
Study : IT Audit

Rangkuman Persentasi IT Audit Tools

1. Password cracking tools / Alat pemecahan kata password

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data. Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.** Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

a. Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. Fitur dari AirCrack adalah mendukung Brute Force, tersedia untuk berbagai OS tersedia dalam live CD dan banyak ditemukan di internet. AirCrack paling sesuai dengan standar 802.11a/b/g.

Standardisasi IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

Standardisasi IEEE 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

Standardisasi IEEE 802.11g Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

b. OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force. Fitur OphCrack dapat digunakan di berbagai OS menggunakan LM Hash dan NTLM hash, pelangi table yyang tersedia secara gratis dan banyak di temukan di internet.

2. METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan. Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.

Perjalanan METASPLOIT dari waktu kewaku bermula pada tahun 2003 H. More Menulis METASPLOIT dalam basaha PERL, tahun 2007 Tim menuliskannya kembali dengan bahasa RUBY, tahun 2009 Diakuisi oelh perusahaan RAPID& dan dari tahun 2009 sampai sekarang telah tersedia varian METASPLOUIT Freemwork & METASPLOIT Community yang di berikan secaa gratis seangkan untuk versi METASPLOIT Express & METASPLOIT Profesional merukan produk KOMERSIAL.

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.

MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

3. MALTEGO

Maltego ini disebut OSINT (Open Source Intelligence Gathering) sebuah alat untuk melakukan *footprinting*, digunakan untuk mengumpulkan informasi sebanyak mungkin dengan tujuan forensik, *pen testing*, atau *ethical hacking*. Aplikasi yang digunakan untuk memetakan jaringan komunikasi Yang berada di internet tujuannya adalah mengumpulkan informasi tentang target dan menampilkan informasi tersebut dalam format yang mudah dimengerti, memvisualisasikan informasi tersebut ke dalam sebuah format graph, sangat cocok untuk *link analysis* dan *data mining*. Maltego dibedakan menjadi versi komersial (commercial edition) dan versi gratis (community edition). Versi gratis yang tersedia di Kali Linux hanya dapat menampilkan maksimal 12 hasil transformasi, Sebagai sebuah front-end untuk server OSINT, Maltego versi gratis hanya dapat memakai layanan server milik Paterva. Karena versi yang disediakan oleh Kali Linux adalah versi gratis dari Maltego.

Fungsi MALTEGO adalah memudahkan seseoorang yang mencari informasi tentang apa yang mereka selidiki atau mereka incar sebagai target, contoh ketika seorang mencari informasi dari sebuah domain menggunakan maltego, maka maltego akan menampikan bebrap informasi seperti Block IP Hosting, Domain Rigister, Email USER Dan Admin, Phone Number, serta Peta Jarinagan .

4. W3AF

W3AF (*Web Application Attack And Audit Framework*) merupakan sebuah aplikasi yang bisa dijalankan di LINUX OS dan WINDOWS OS. Aplikasi ini sangat banyak di gemari oleh para heker W3AF adalah sebuah kerangka untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk meng-scan suatu website sehingga data mengetahui celah suatu kelemahan website. Aplikasi ini dibuat menggunakan bahasa pemrograman PHYTON.

Fungsi TOOL W3AF dalam IT Audit adalah

Membuat Perencanaan Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell

Mengolah ancaman Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman

Kesimpulan Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

IT AUDIT SOFTWARE

Nama Kelompok :
1.Dhea Noranita Putri (182420112)
2.Reynaldi (182420111)
3.Dini Rahmadia (182420134)
4.Mezi Puspayani (182420120)

MTI REG B 2019
Magister Tehnik Informatika
Universitas Bina Darma
Palembang

Apa itu Nessus ?

- **Nessus** *dibuat oleh Renaud Deraison pada tahun 1998. Nessus adalah* salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan.

Nessus Terbagi Menjadi 3 Tipe, Yaitu :

- **Nessus Home** : digunakan untuk personal
- **Nessus Profesional** : Digunakan untuk penggunaan komersial.
- **Nessus Manager / Nessus Cloud** : Fungsinya Vulnerability Manajemen untuk expert Security teams.

Fungsi nessus?

fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem

Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem. Sebelum Nessus versi 3, aplikasi ini bersifat open source dan menjadi salah satu primadona di dunia open source. Namun sekarang mulai Nessus versi 3 oleh Teenable Security dijadikan sebagai aplikasi propietary dan closed source

Fitur – fitur yang dimiliki Nessus :

1. **Plug-in architecture**
   Setiap security test ditulis sebagai external plugin. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca
   kode dari nessusd engine.
2. **NASL (Nessus Attack Scrpiting Language)**
   NASL adalah sebuah bahasa yang didesain untuk menulis program security test
   dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulils program security test.
3. **Up-to-date security vulnerability database**.

Fitur – fitur yang dimiliki Nessus :

4. Client-sever architecture

Nessus security scanner terdiri dari dua bagian yaitu: sebuah server yang berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagaifrontend. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC,dengan server yang melakukan serangan ke jaringan yang dituju.

Fitur – fitur yang dimiliki Nessus :

5. **host yang banyak dalam waktu yang sama.**

6. Smart service recognation.
Nessus tidak mempercayai host yang dituju menggunakan port standar yang
ditentukan oleh IANA. Ini berarti Nessus dapat mengenali sebuah Web server
yang berjalan pada port yang bukan merupakan port standar (contohnya pada port8080), atau sebuah FTP server yang berjalan pada port 31337.

Fitur – fitur yang dimiliki Nessus :

7. **Multiple Services**
   Apabila ada dua buah Web server pada host yang dituju maka Nessus akan mengetes kedua Web server tersebut.
8. **Complete reports.**
   Nessus tidak hanya memberi tahu kelemahan dari jaringan yang dituju tetapi juga memberikan cara yang dapat digunakan untuk mencegah the bad guy utnuk
   mengeksploitasi kelemahan dari jaringan dan juga memberikan level resiko dari setiap masalah yang ditemukan.

Fitur – fitur yang dimiliki Nessus :

9. **Unix client** dapat mengekspor laporan sebagai Ascii text, HTML, LaTeX, dll.

Cara Kerja/pengoperasian Nessus :

- 1. memulai scanning
- 2. sebelum memulai scanning harus membuat template /policy untuk mendefinisikan scanning
- 3. jika sudah terbuat, maka akan muncul all policies
- 4. kemudian pilih menu scans>new scans
- 5. pada sub general isi nama sesuai keinginan

Cara Kerja/pengoperasian Nessus :

- 6. pada contoh ini akan melakukan scanning pada mesin so 7 dengan alamat IP 192.168.1.2 kemudian save
- Selesai
- Hasil yang di dapat adalah menampilkan semua informasi kerentanan atau celah yang dapat dimanfaatkan oleh seseorang hacker . Kita bias melihat apakah tingkat dari celah itu sedang, kritis atau hanya sekedar informasi saja

Nessus dapat digunakan untuk melakukan audit sebagai berikut:

- Credentialed and un-credentialed port scanning.
- Network based vulnerability scanning.
- Credentialed based patch audits for Windows and most UNIX platforms.
- Redentialed configuration auditing of most Windows and UNIX platforms.
- Robust and comprehensive credentialed security testing of 3rd party applications.
- Custom and embedded web application vulnerability testing.
- SQL database configuration auditing.
- Software enumeration on Unix and Windows.
- Testing anti-virus installs for out-of date signatures and configuration errors.

Download Nessus :

- Kita bisa mendapatkan software nessus pada laman https://www.tenable.com/downloads/nessus?loginAttempted=true
- Website Resmi

http://www.tenable.com/products/nessus-vulnerability-scanner.

Kelebihan Nessus :

- Advanced vulnerability scanning dan configuration audit.
- Mampu mendeteksi process/program mencurigakan dan juga worms.
- Mampu melakukan multiple network scanning (IP, IPv6, Hybrid).
- Automatic scanning scheduler.
- Custom report & Notification.

Kekurangan Nessus :

- Sulit menemukan issue tertentu karna biasanya hasil scanningnya merupakan general case. Biasanya butuh versi profesional untuk fitur yang lebih baik.

Kesimpulan :

- Nessus merupakan sebuah program yang dapat digunakan untuk mencari kelemahan pada sebuah sistem komputer. Nessus juga dapat melakukan pengecekan terhadap kerentanan system komputer, dan meningkatkan keamanan sistem yang kita miliki.
- Nessus juga memberikan Informasi dalam menampilkan secara detail apa yang menjadi penyebab kelemahan sistem serta saran untuk mengatasi kelemahan tersebut. Informasi yang ditampilkan sudah dikelompokkan berdasarkan penyebab terjadinya kelemahan.
- Semua kategori kelemahan hasil dari scan menggunakan Nessus ditampikan penjelesan tentang kelemahan yang ada. Penjelasan mengenai kelemahan sistem tersebut bisa dijadikan acuan untuk administrator untuk memperbaiki kelemahan sistem yang muncul sebelum di unggah di web server.

Kesimpulan :

- **Saran**
- Semakin banyak vulnerabilitas dan ancaman yang dapat terjadi di dalam suatu sistem, sudah seharusnya semakin tinggi pula kesadaran kita untuk dapat memproteksi sistem dan informasi yang berada di dalamnya. Sebuah teknik untuk melindungi suatu sistem dinamakan dengan tindakan pencegahan sehingga kita perlu melakukan tindakan pencegahan salah satunya menggunakan tools keamanan seperti nessus

Tutorial menginstal dan mengunakan Nessus :

- Anda dapat dapat mempelajari lewat video dari laman ini :

https://www.youtube.com/watch?v=35a0VhzIO2Y

- Anda juga dapat mempelajari langkah-langkanya dengan mendowload dari pdf berikut ini :

https://www.academia.edu/37659321/PROSES_AUDIT_SERVER_DENGAN_NESSUS

TERIMA KASIH

Nama : **Miftahul Fallah**
Nim : **182420132**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

RINGKASAN HASIL PRESENTASI KELOMPOK 1-4

Kelompok 1

Ringkasan Materi Password cracking tools /Alat pemecahan kata password

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.

Aircrack: Alat Cracking Cepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Kelompok 2

Ringkasan Materi Metasploit

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).
Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

Kelompok 3

Ringkasan Materi Maltego

Maltego ini disebut OSINT (Open Source Intelligence Gathering) sebuah alat untuk melakukan *footprinting*, digunakan untuk mengumpulkan informasi sebanyak mungkin dengan tujuan forensik, *pen testing*, atau *ethical hacking*. Aplikasi yang digunakan untuk memetakan jaringan komunikasi Yang berada di internet tujuannya adalah mengumpulkan informasi tentang target dan menampilkan informasi tersebut dalam format yang mudah dimengerti, memvisualisasikan informasi tersebut ke dalam sebuah format graph, sangat cocok untuk *link analysis* dan *data mining*.

Fungsi dari maltego adalah memudahkan seseoorang yang mencari informasi tentang apa yang mereka selidiki atau mereka incar sebagai target, contoh ketika seorang mencari informasi dari sebuah domain menggunakan maltego, maka maltego akan menampikan bebrap informasi seperti berikut:

- Block IP hosting
- Domain registe
- Email user & admin
- Phone number
- Peta jaringan

Maltego dibedakan menjadi versi komersial (commercial edition) dan versi gratis (community edition). Versi gratis yang tersedia di Kali Linux hanya dapat menampilkan maksimal 12 hasil transformasi, Sebagai sebuah front-end untuk server OSINT, Maltego versi gratis hanya dapat memakai layanan server milik Paterva. Karena versi yang disediakan oleh Kali Linux adalah versi gratis dari Maltego.

Kelompok 4

Ringkasan Materi W3af

W3af adalah Web Aplication Attack And Audit Framework. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengekploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu kelemahan website.

w3af (Web Application Attack and Audit Framework) hampir mirip dengan metasploit, bedanya hanya pada objek yang dikerjakan. w3af fokus pada bagian aplikasi web, sedangkan metasploit lebih ke sistem operasi secara keseluruhan. w3af gratis dan opensource, terdiri dari beberapa bagian plugin untuk serangan yaitu mangle, grep, discovery, audit, evasion, dan bruteforce.

Aplikasi ini dibuat menggunakan bahasa pemrograman python. Untuk persiapan menggunakan w3af, banyak program berbasis python yang harus diinstal seperti python-soappy, python-pyopenssl, dll.

FUNGSI TOOL W3AF DALAM IT AUDIT

IT Audit membuat kerangka Konseptual, sehingga audit dapat berjalan sesuai dengan yang diharapkan, Kerangka konseptual dijelaskan sebagai berikut :

- **Membuat Perencanaan**
  Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell
- **Mengolah ancaman**
  Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman
- **Kesimpulan**
  Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

W3AF

Universitas Bina Darma

KELOMPOK 4

MTI.20A

1. Ekariva Annas Asmara (182420133)
2. Hari Febriadi (182420127)
3. Mifathul Fallah (182420132)
4. Fajar Prayoga (182420136)

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Aplikasi yang akan saya bahas adalah **W3AF**, aplikasi yang bisa di jalankan di linux dan di windows ini sangat banyak di gemari oleh sang **H4Ck3R**, walau lebih banyak yang menggunakannya di linux namun tidak sedikit pula yang menggunakannya di windows. Tetapi

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

W3af adalah ***Web Aplication Attack And Audit Framework***. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu **Kelemahan** website.

Aplikasi ini di buat menggunakan bahasa pemprograman **python**. Sebenarnya pengetahuan saya tentang aplikasi ini sangatlah minim, jadi buat kalian yang ingin menggunakannya dan menguasainya kunjungi situs resminya di : **w3af.org**.

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Berikut tampilan GUI untuk w3af yang saya install pada windows XP :

Universitas Bina Darma

KOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Universitas Bina Darma

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Sumber : https://infobacktrack.wordpress.com/category/deface/

Dalam uji coba ini saya menggunakan backtrack 5, dan secara default sudah terinstall. Untuk bagian menunya bisa dilihat seperti banner diatas. Jika anda menggunakan ubuntu, bisa langsung di ketik

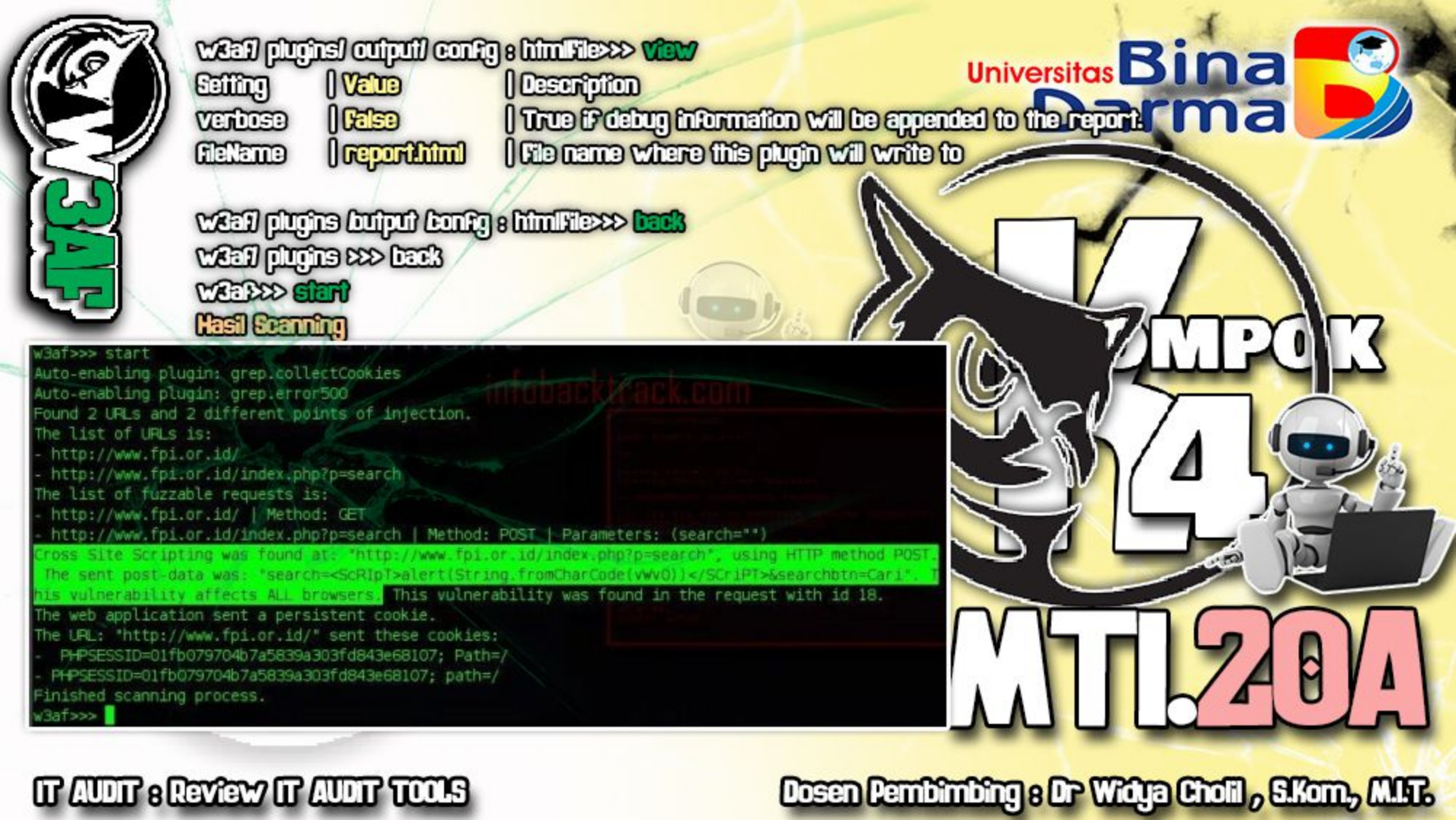
sudo apt-get install w3af

Oke, saya anggap smua sudah memulai tampilan awalnya yah. disini saya mengetik help.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.


w3af/plugins/output/config : htmlFile>>> view
Setting | Value | Description
verbose | False | True if debug information will be appended to the report.
fileName | report.html | File name where this plugin will write to
w3af/plugins/output/config : htmlFile>>> back
w3af/plugins >>> back
w3af>>> start
Hasil Scanning
w3af>>> start
Auto-enabling plugin: grep.collectCookies
Auto-enabling plugin: grep.error500
Found 2 URLs and 2 different points of injection.
The list of URLs is:
- http://www.fpi.or.id/
- http://www.fpi.or.id/index.php?p=search
The list of fuzzable requests is:
- http://www.fpi.or.id/ | Method: GET
- http://www.fpi.or.id/index.php?p=search | Method: POST | Parameters: (search="")
Cross Site Scripting was found at: "http://www.fpi.or.id/index.php?p=search", using HTTP method POST. The sent post-data was: "search=<ScRIpT>alert(String.fromCharCode(vWv0))</SCriPT>&searchbtn=Cari". This vulnerability affects ALL browsers. This vulnerability was found in the request with id 18.
The web application sent a persistent cookie.
The URL: "http://www.fpi.or.id/" sent these cookies:
- PHPSESSID=01fb079704b7a5839a303fd843e68107; Path=/
- PHPSESSID=01fb079704b7a5839a303fd843e68107; path=/
Finished scanning process.
w3af>>>
Universitas Bina Darma
KELOMPOK 4
MTI.20A
IT AUDIT : Review IT AUDIT TOOLS
Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

SIMPULAN

- Dari hasil scanning diatas, dapat di Simpulkan bahwa web tersebut memiliki kelemahan pada XSS.
- Potensi serangan yang dapat dilakukan attacker adalah melakukan pemanggilan Get Web Shell, setelah pemanggilan web shell, maka web tersebut dapat diambil alih.

w3af

Web Application Attack and Audit Framework

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

FUNGSI TOOL W3AF DALAM IT AUDIT

- IT Audit membuat kerangka Konseptual, sehingga audit dapat berjalan sesuai dengan yang diharapkan, Kerangka konseptual dijelaskan sebagai berikut :
  - ✓ **Membuat Perencanaan**
    - Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell
  - ✓ **Mengolah ancaman**
    - Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman
  - ✓ **Kesimpulan**
    - Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

Universitas Bina Darma

Terima Kasih

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

w3af

Web Application Attack and Audit Framework

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

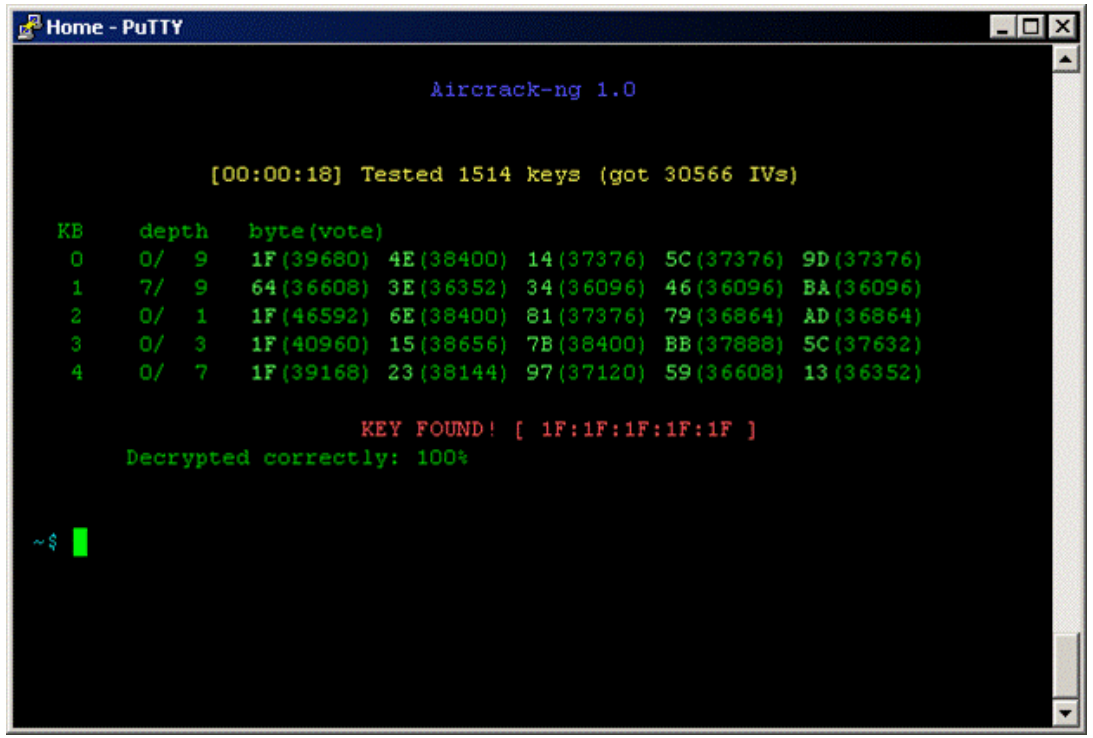
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

Cracking WPA2-PSK Password Wi-FI dengan Aircrack-ng

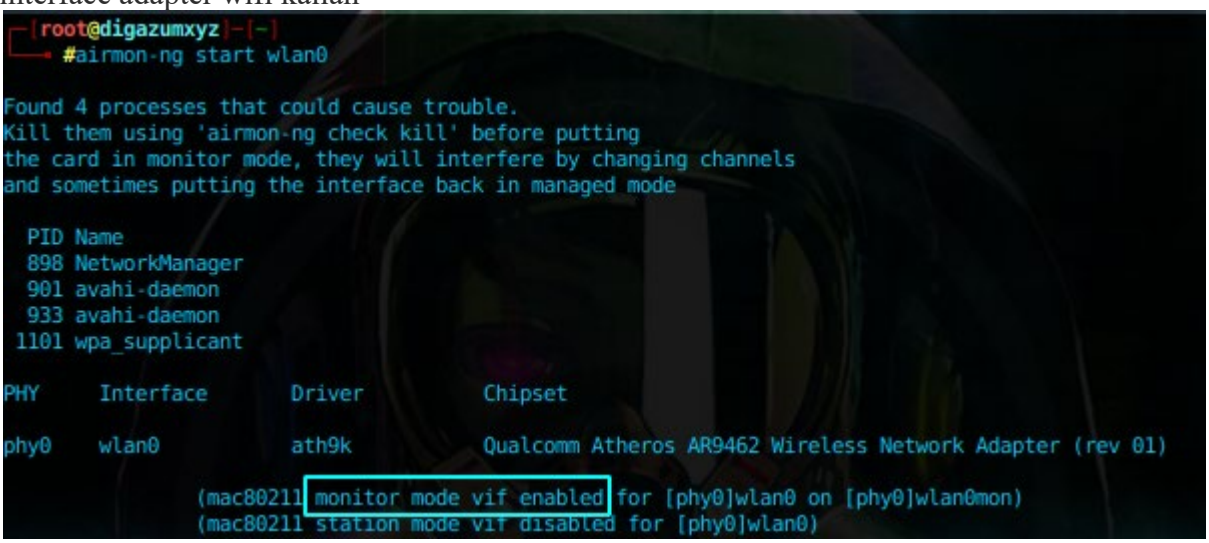
Ketika Wi-Fi pertama kali dikembangkan pada akhir 1990-an, Wired Equivalent Privacy dibuat untuk memberikan kerahasiaan komunikasi nirkabel. WEP, seperti yang diketahui, terbukti sangat rentan dan mudah untuk di bobol.

Sebagai gantinya, sebagian besar titik akses nirkabel sekarang menggunakan Wi-Fi Protected Access II dengan kunci yang dibagikan sebelumnya untuk keamanan nirkabel, yang dikenal sebagai WPA2-PSK. WPA2 menggunakan algoritma enkripsi yang lebih kuat, AES, yang sangat sulit untuk dipecahkan — tetapi bukan tidak mungkin

Kelemahan dalam sistem WPA2-PSK adalah bahwa kata sandi terenkripsi dibagi dalam apa yang dikenal sebagai jabat tangan 4 arah (handshake). Ketika klien mengotentikasi ke titik akses (AP), klien dan AP pergi melalui proses 4 langkah untuk mengotentikasi pengguna ke AP. Jika kami dapat mengambil kata sandi saat itu, kami kemudian dapat mencoba memecahkannya.

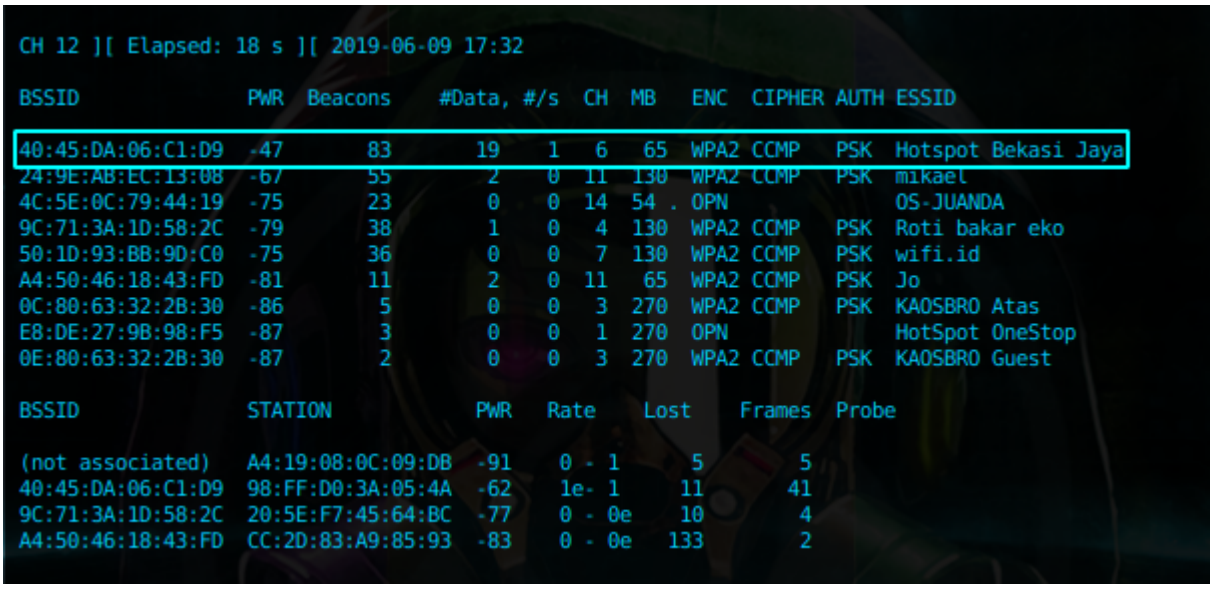
Oke untuk memulai membobol password wifi dengan Keamanan WPA2-PSK lalu pastinya juga dengan algoritma enkripsi yang lebih kuat, disini kita langsung saja mulai ke tutorial cara Crack password Wifi tersebut dengan Keamanan WPA2-PSK, disini kita menggunakan **Aircrack-ng? Aircrack-ng** adalah paket perangkat lunak jaringan yang terdiri dari detektor, packet sniffer, WEP dan WPA / WPA2-PSK cracker dan alat analisis untuk 802.11 LAN nirkabel.

Langkah Pertama Yang kita Mulai ialah memasuki Monitor mode Hal ini memungkinkan kita untuk melihat semua lalu lintas nirkabel (Wifi) yang melewati kita atau disekitar kita, ketikkan saja perintah di terminal **airmon-ng start wlan0** keterangan ***wlan0*** ialah nama interface adapter wifi kalian



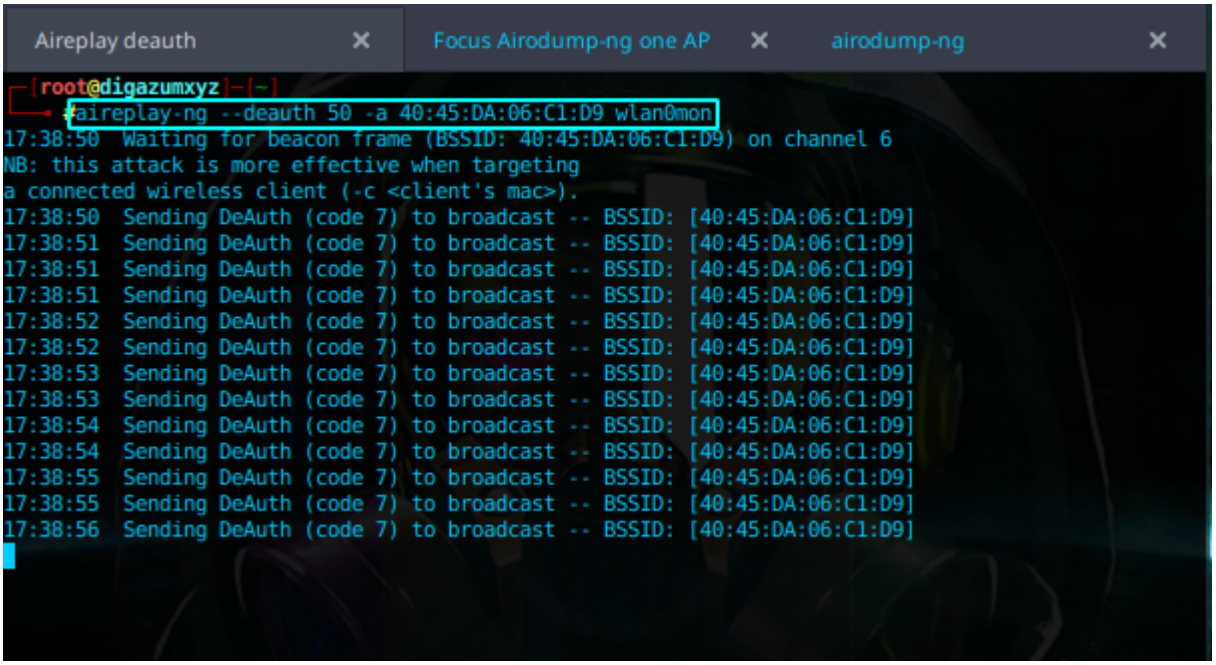
Langkah Kedua ialah Menangkap paket traffic akses point (Wi-FI) sekitar kalian, Perintah ini mengambil semua lalu lintas yang adaptor nirkabel Anda dapat melihat dan menampilkan informasi penting tentang itu, termasuk ***BSSID*** (alamat MAC AP), daya, jumlah bingkai suar, jumlah bingkai data, saluran, kecepatan, enkripsi (jika apa saja), dan akhirnya, ***ESSID*** (yang sebagian besar dari kita sebut sebagai SSID). Mari kita lakukan ini dengan

mengetik **airodump-ng wlan0mon** keterangan ***wlan0mon*** ialah adapter wifi yang sudah mode monitor

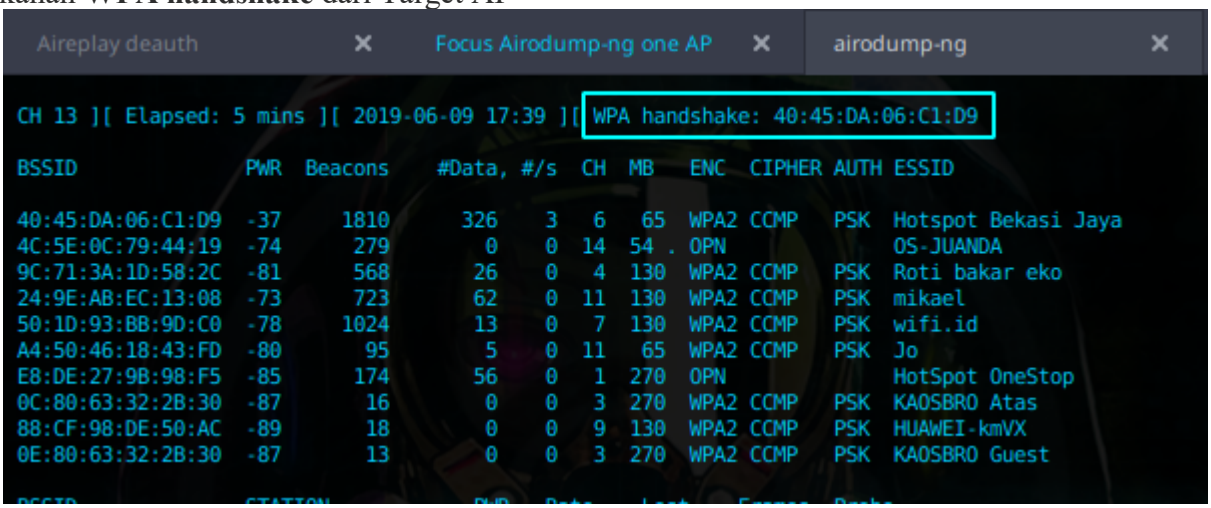


Langkah Ketiga sekarang buka tab baru diterminal, Fokus pada Satu target AP yang kita lakukan nantinya ialah menangkap paket dan traffic dari AP Tersebut, Disini Saya Sudah mendapat Target yaitu AP dengan **ESSID** Hotspot Bekasi Jaya, perintah yang dimasukkan ialah **airodump-ng -c 6 --bssid 40:45:DA:06:C1:D9 --write bekasijaya wlan0mon** keterangan ***40:45:DA:06:C1:D9*** ialah BSSID dari Target AP, ***6*** ialah channel AP, ***bekasijaya*** adalah file yang ingin anda tulis nantinya untuk paket capture file

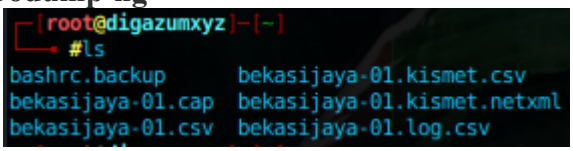
Langkah Keempat buka tab baru terminal, Untuk mendapatkan kata sandi yang dienkripsi, kita harus meminta klien untuk melakukan otentikasi terhadap AP. Jika sudah diautentikasi, kita dapat membatalkan otentikasi (kick off) dan sistem mereka akan secara otomatis mengautentikasi ulang, di mana kita dapat mengambil kata sandi terenkripsi mereka dalam proses. masukkan perintah **aireplay-ng --deauth 50 -a 40:45:DA:06:C1:D9 wlan0mon** keterangan ***50*** ialah jumlah angka de-authenticate frames yang ingin anda kirim, ***40:45:DA:06:C1:D9*** BSSID Target AP



Langkah Kelima, disaat kita sedang melakukan deauthentication frames pada target ap disini kita sekaligus menunggu penangkapan paket handshake (jabat tangan), jadi kita memantulkan pengguna dari AP mereka sendiri, dan sekarang ketika mereka mengautentikasi ulang, airodump-ng akan berusaha mengambil kata sandi mereka dalam jabat tangan 4-arah yang baru. Mari kita kembali ke terminal airodump-ng kami dan memeriksa untuk melihat apakah kita sudah berhasil atau tidak. Jika Sudah Berhasil Maka Akan Ada tulisan di pojok kanan **WPA handshake** dari Target AP

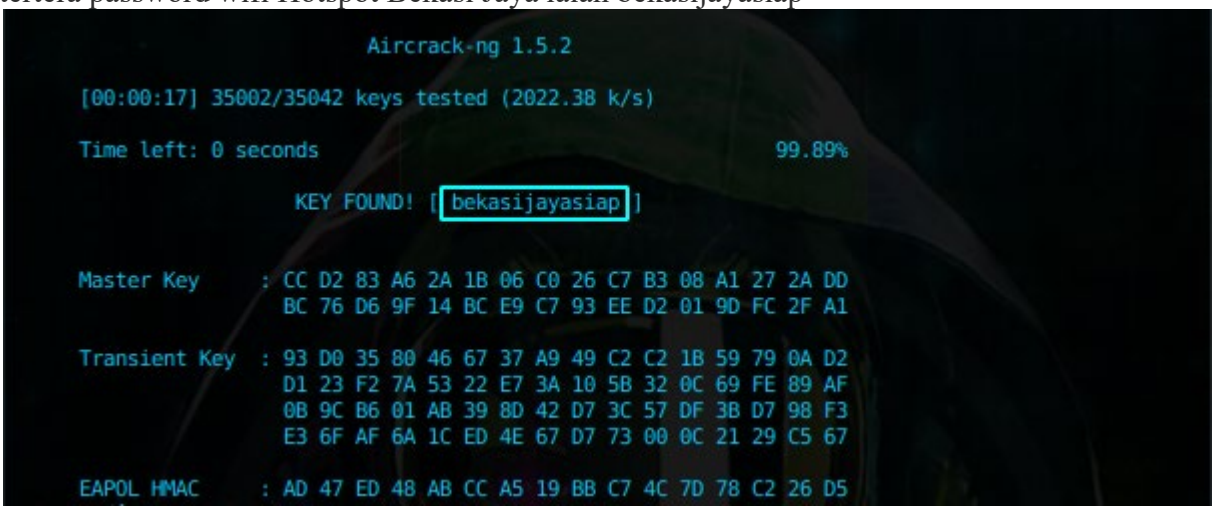


Saatnya Cracking Password Target AP Tersebut, sebelumnya untuk mengcrack password tersebut kita membutuhkan file hasil capture tadi biasanya tersimpan di direktori saat kalian menjalankan perintah **airodump-ng**

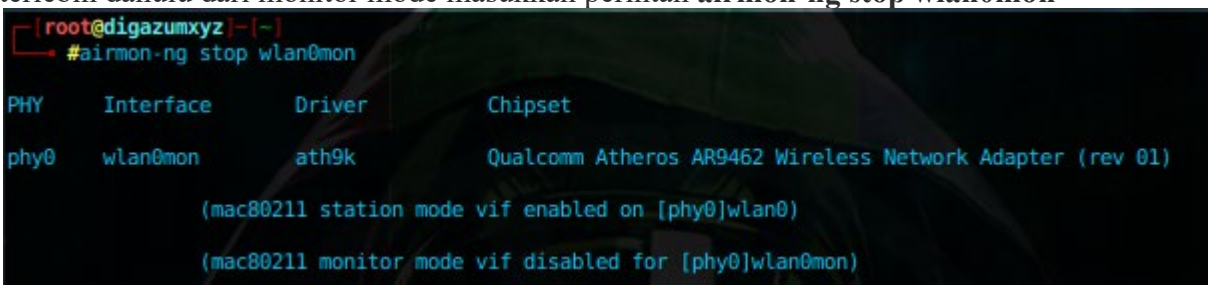


Mulai Crack!! langkah pertama sebelum crack ialah kita membutuhkan wordlist banyak tools pembuat wordlist generator seperti crunch, cewl, cupp dan masih banyak lagi,, oke saatnya crack masukkan perintah **aircrack-ng bekasijaya-01.cap -w /home/galangxyz/wordlistbekasi.txt** keterangan ***bekasijaya-01.cap*** ialah adalah nama file yang kita tulis dalam perintah airodump-ng lau ***/home/galangxyz/wordlistbekasi.txt*** ialah

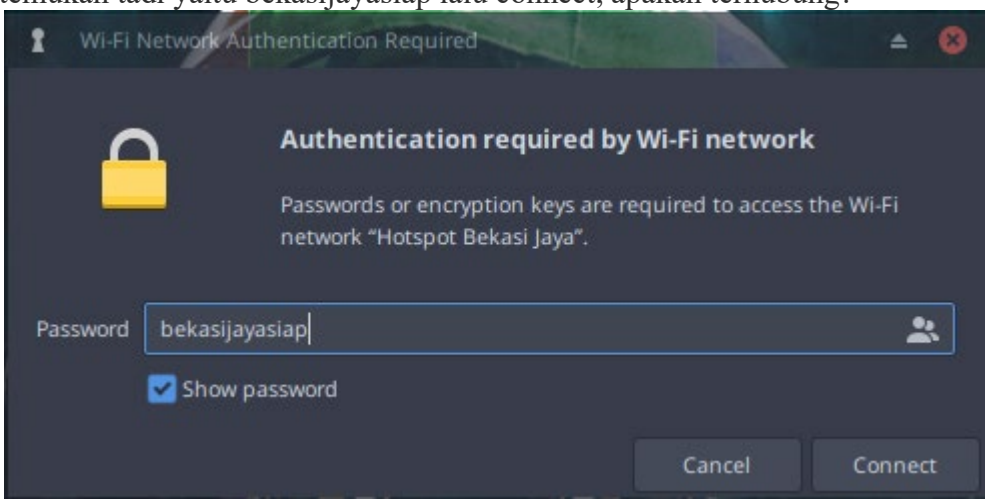
path wordlist yang saya buat, prosesnya bisa relatif lambat dan membosankan. Tergantung pada panjang daftar kata sandi kalian, Anda bisa menunggu beberapa menit hingga beberapa hari, Jika sudah menemukan Kata sandi yang cocok maka akan muncul **KEY FOUND!** disitu tertera password wifi Hotspot Bekasi Jaya ialah bekasijayasiap



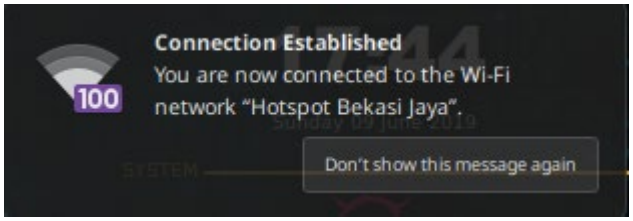
Sebelum kita Menguji Passwordnya apakah benar apa tidak alangkah baiknya kita stop terlebih dahulu dari monitor mode masukkan perintah **airmon-ng stop wlan0mon**



Pengujian Sambungkan saja Ke wifi Hotspot Bekasi Jaya lalu massukan password yang sudah ditemukan tadi yaitu bekasijayasiap lalu connect, apakah terhubung?



Yap benar sekali disini sudah berhasil :D



Oke Mungkin itu saja sekian dari saya semoga bermanfaat.... ini hanya untuk pembelajaran..

Hack Password Windows 7 / Vista With OphCrack

Beberapa alasan mengapa orang-orang harus menggunakan tool yang bisa *cracking password* di sistem operasinya diantaranya adalah karena masalah klise seperti lupa akan passwordnya, kemudian ada juga yang penasaran ingin tau password milik orang lain, tetapi ada lagi yg tidak terpuji yaitu ingin mencuri password dan melakukan tindakan kriminal.
Ibarat sebuah pisau mempunyai fungsi yang berbeda ketika dipegang oleh orang yang berbeda, ibu-ibu mungkin menggunakan pisau untuk mencincang daging, mengupas kentang atau buah-buahan dan memotong sayur, tapi jika ditangan seorang maling, pisau bisa digunakan untuk menodong bahkan membunuh.

Sama halnya dengan OphCrack, software / tool ini bisa digunakan untuk *merecovery password* yang kelupaan di windows 7 / Vista. Tapi tool yang sama juga dapat disalahgunakan oleh orang-orang yang tidak bertanggungjawab untuk mencuri password Windows 7 / Vista.
OphCrack bisa dijalankan di lingkungan Windows ataupun secara live CD. Mekanisme *tool hacking password* di Windows 7 / Vista tidak terlalu saya pahami, tetapi yang jelas adalah mereka menggunakan *teknik hashing* kelas atas. Password yang lupa bisa direcovery dalam jangka waktu yang sangat singkat. Nah, jika lupa password komputer yang menggunakan Windows 7 dan Vista, gunakan software ini untuk mengembalikan password yang lupa tsb. Gunakan dengan bijak, jangan untuk mencuri atau crack yang tidak berguna.

Software / program ini disediakan gratis dan bisa di-download sourceforge
NB: AVG akan mendeteksi program ini sebagai aktivitas yang mencurigakan.

Cara Mengatasi Lupa Password Log In Windows 7. Bagi sobat-sobat yang lupa dengan ***password log in*** pada **windows 7** **sobat**, Disini saya punya tipsnya. dan tips ini bukan hacking lo karena cara ini tanpa melakukan reset password lama. ok langsung aja ya mas

bro…

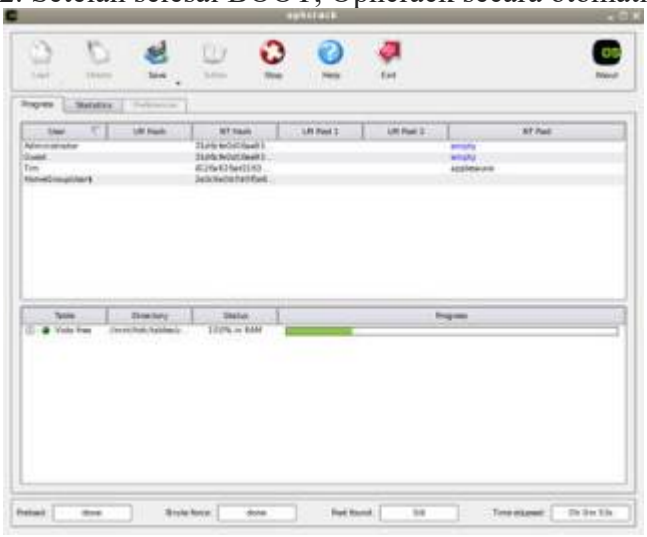
Cara Mengatasi Lupa Password Log In Windows 7
Download:

- Download image CD di situs Ophcrack
- Pastikan sobat mendownload sesuai dengan System Operation yang sobat pakai. Jika sobat menggunakan WINDOWS 7 maka download versi VISTA, karena versi ini dapat berjalan pada Vista maupun Windows 7.
- Setelah mendownload file ISO, burn file ISO tersebut ke CD
- Jika sudah Boot dari CD

Cara penggunaan:

1. Boot komputer dari CD yang telah dibuat tadi.

2. Setelah selesai BOOT, Ophcrack secara otomatis melakukan cracking password.



3. Pada gambar diatas merupakan tampilan ***OPHCRACK*** setelah selesai boot. Selanjutnnya Ophcrack akan mencoba recovery password semua account user.

4. Perhatikan kolom user pada tabel diatas, itu merupakan user account yang dipakai pada WINDOWS 7. Dan pada tabel Nt pwd adalah password log in WINDOWS 7. Jika password pada tabel Nt pwd belum kosong untuk user tertentu berarti password tersebut belum dipulihkan.
5. Jika pada tabel Nt pwd sudah empty, sekarang sobat dapat log in WINDOWS 7 tanpa password. Dengan catatan user account diaktifkan.
6. Setelah Ophrack selesai menghapus akun, keluarkan CD OPHCRACK dari CD Drive sobat, dan restartlah PC sobat. Dengan cara ini seharusnnya sobat sudah bisa Log in ke OS sobat tanpa password.

References :

https://digazumxyz.blogspot.com/2019/06/cracking-wpa2-psk-password-wi-fi-dengan.html

https://alfairuz69.wordpress.com/cara-membobol-pasword-windows-menggunakan-ophcrack/

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

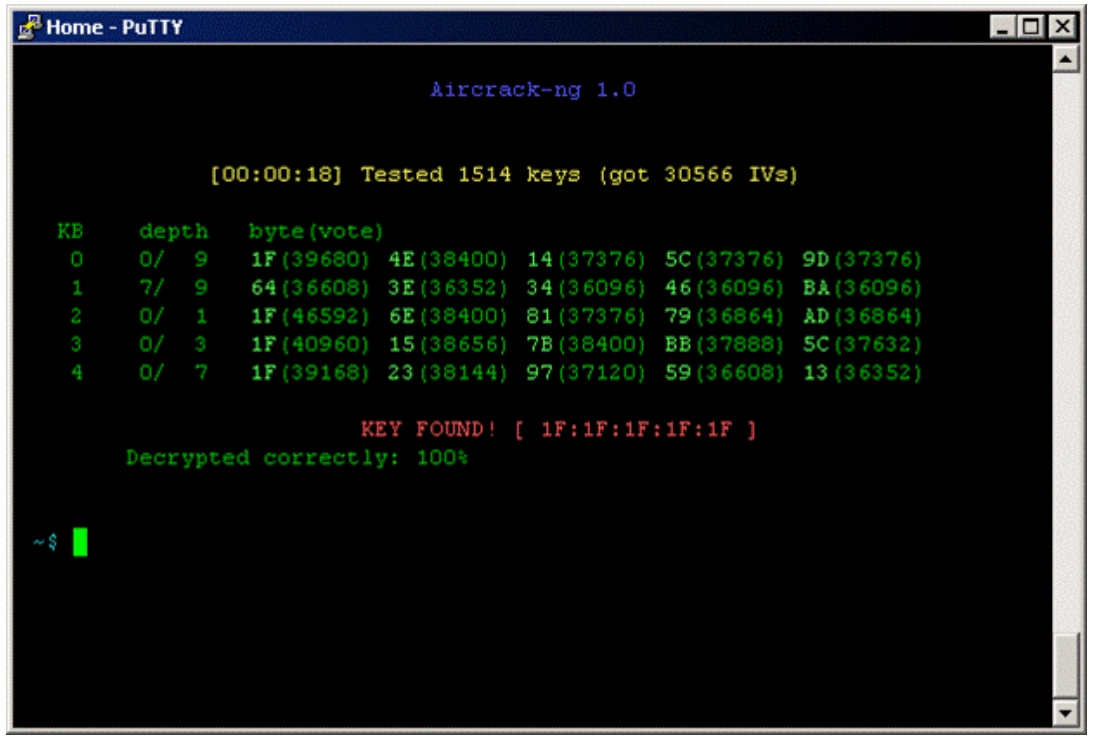
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

MALTEGO

HARLI SEPTIA FANI (182420122)
PUTRI ARMILIA PRAYESY (182420125)
DEVIAN SAPUTRA (182420128)
I MADE HARYA WIJAYA OKA RAFFLESIA (182420129)
PUTRI ELEINA NURRAHMA (182420138)

MALTEGO

MALTEGO INI DISEBUT **OSINT** (**O**PEN **S**OURCE **I**NTELLIGENCE **G**ATHERING) SEBUAH ALAT UNTUK MELAKUKAN *FOOTPRINTING*, DIGUNAKAN UNTUK MENGUMPULKAN INFORMASI SEBANYAK MUNGKIN DENGAN TUJUAN FORENSIK, *PEN TESTING*, ATAU *ETHICAL HACKING*. APLIKASI YANG DIGUNAKAN UNTUK MEMETAKAN JARINGAN KOMUNIKASI YANG BERADA DI INTERNET TUJUANNYA ADALAH MENGUMPULKAN INFORMASI TENTANG TARGET DAN MENAMPILKAN INFORMASI TERSEBUT DALAM FORMAT YANG MUDAH DIMENGERTI, MEMVISUALISASIKAN INFORMASI TERSEBUT KE DALAM SEBUAH FORMAT GRAPH, SANGAT COCOK UNTUK *LINK ANALYSIS* DAN *DATA MINING*.

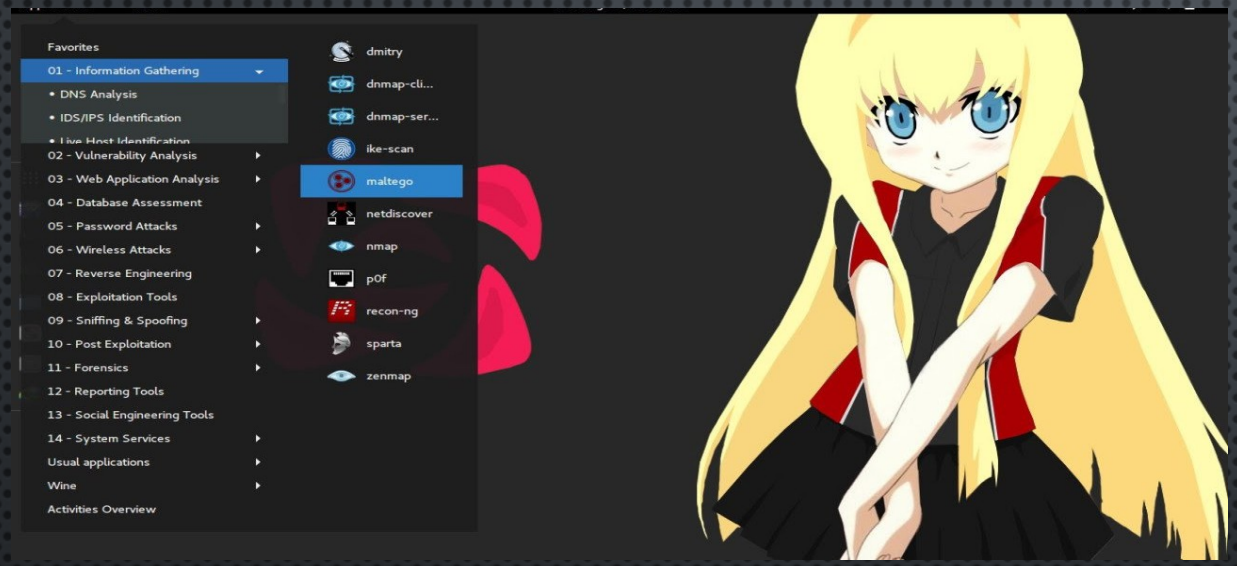
FUNGSI DARI MALTEGO ADALAH MEMUDAHKAN SESEOORANG YANG MENCARI INFORMASI TENTANG APA YANG MEREKA SELIDIKI ATAU MEREKA INCAR SEBAGAI TARGET, CONTOH KETIKA SEORANG MENCARI INFORMASI DARI SEBUAH DOMAIN MENGGUNAKAN MALTEGO, MAKA MALTEGO AKAN MENAMPIKAN BEBRAP INFORMASI SEPERTI BERIKUT:

- BLOCK IP HOSTING
- DOMAIN REGISTE
- EMAIL USER & ADMIN
- PHONE NUMBER
- PETA JARINGAN

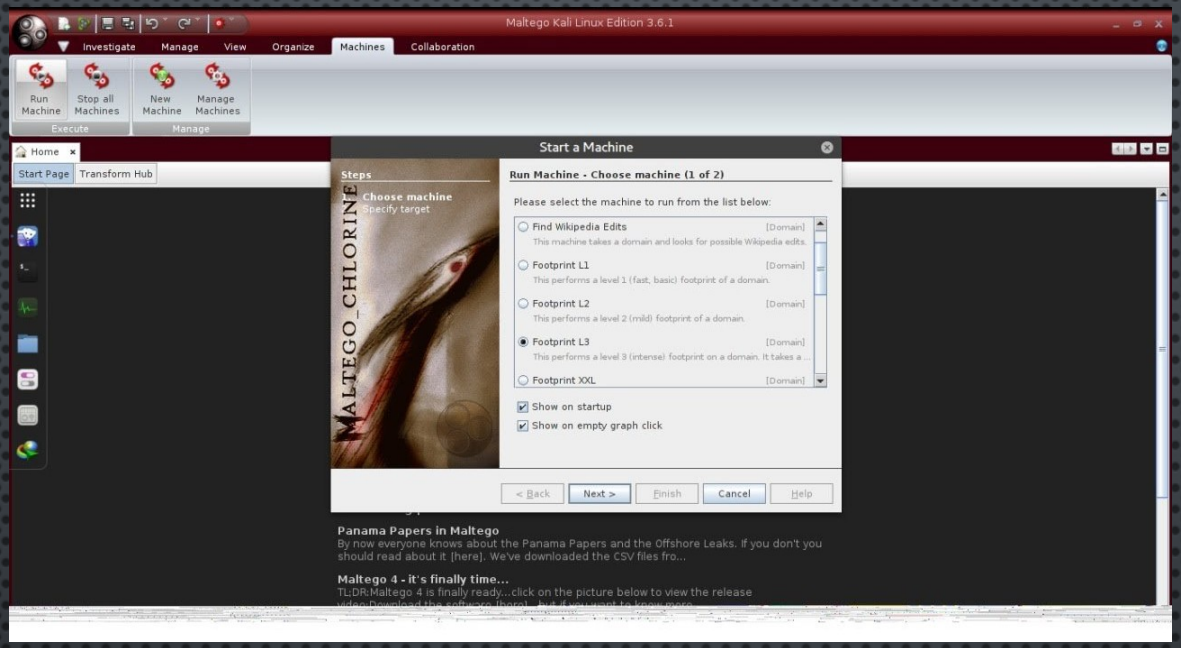
MALTEGO DIBEDAKAN MENJADI VERSI KOMERSIAL (COMMERCIAL EDITION) DAN VERSI GRATIS (COMMUNITY EDITION). VERSI GRATIS YANG TERSEDIA DI KALI LINUX HANYA DAPAT MENAMPILKAN MAKSIMAL 12 HASIL TRANSFORMASI, SEBAGAI SEBUAH FRONT-END UNTUK SERVER OSINT, MALTEGO VERSI GRATIS HANYA DAPAT MEMAKAI LAYANAN SERVER MILIK PATERVA. KARENA VERSI YANG DISEDIAKAN OLEH KALI LINUX ADALAH VERSI GRATIS DARI MALTEGO

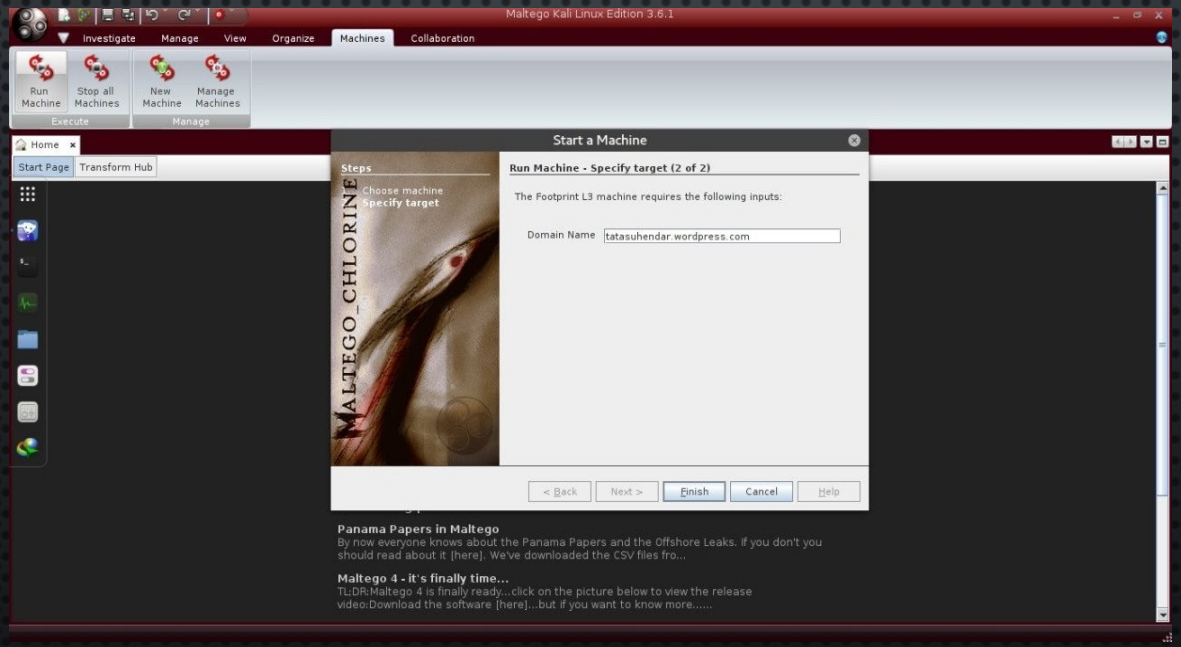
TAHAPAN DALAM PENGGUNAAN MALTEGO

1. BUKA MALTEGO PADA KALI LINUK ANDA, ADA DI MENU INFORMATION GATHERING > MALTEGO

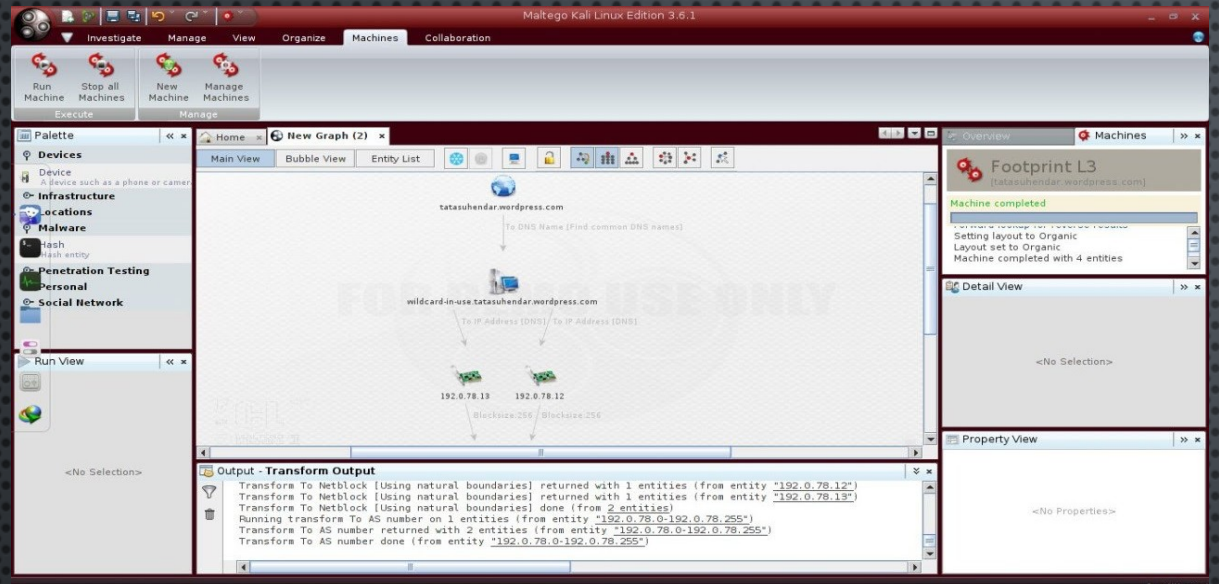


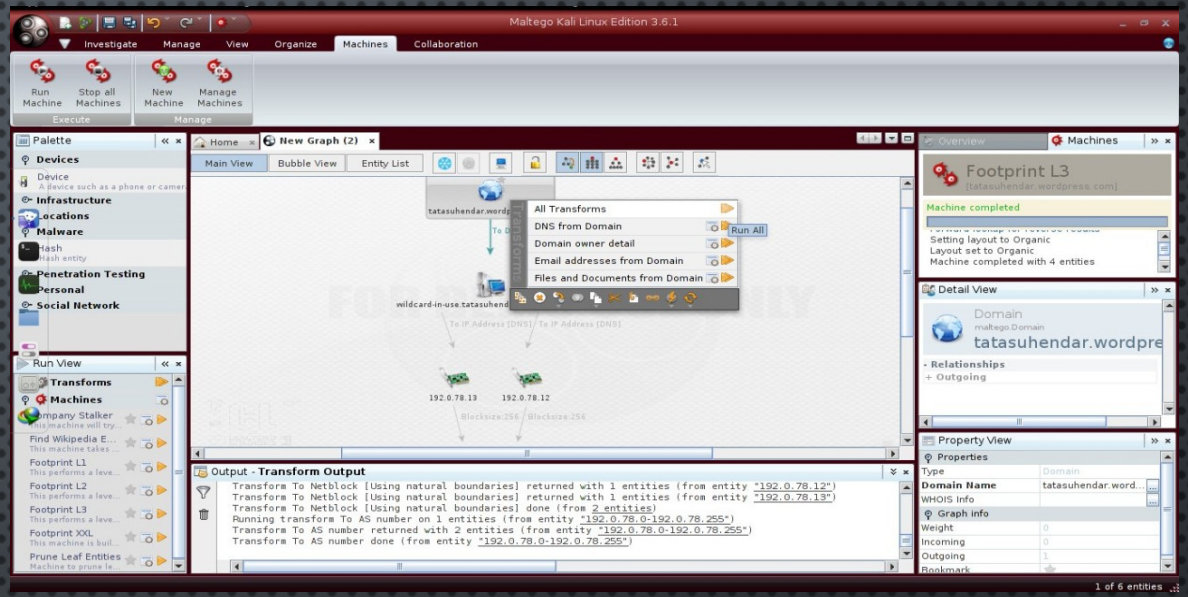
2. LOGIN DENGAN EMAIL DAN PASSWORD YANG TELAH TERDAFTAR
3. SETELAH SELESAI LOGIN MAKA AKAN MUNCUL DIALOG START A MACHINE, PILIH FOOTPRINTING L3 LALU DI STEP KEDUA KITA HARUS MAMASUKAN DOMAIN ATAU LINK WEBSITE TAGE


Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a ...
Footprint XXL [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release

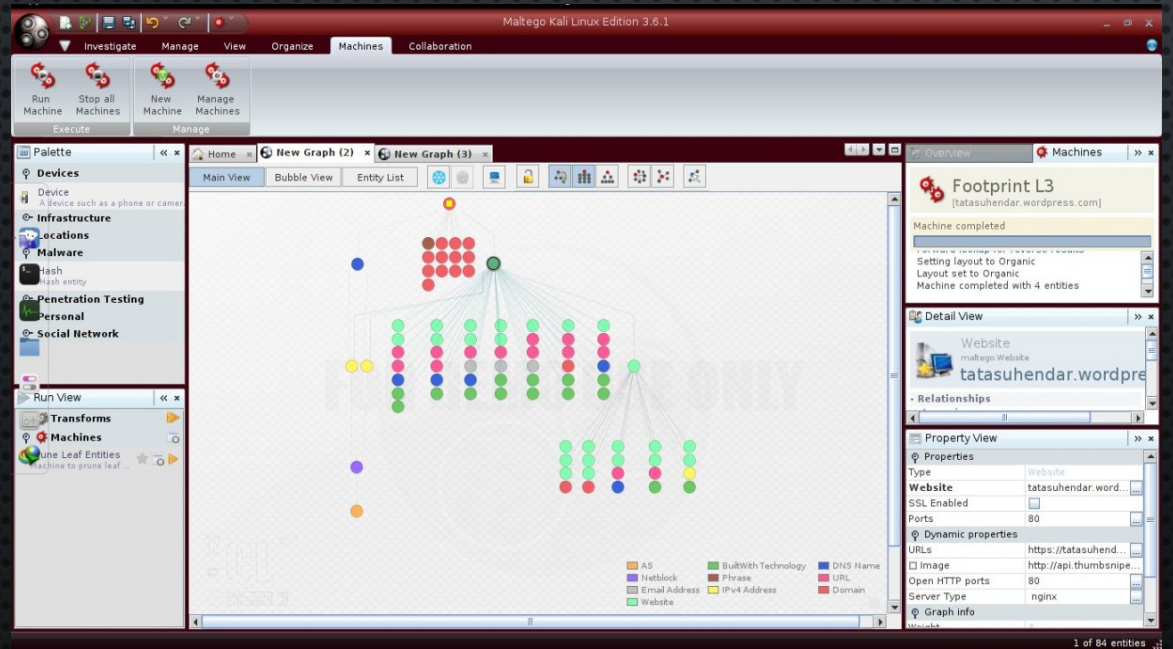

Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Specify target (2 of 2)
The Footprint L3 machine requires the following inputs:
Domain Name
tatasuhendar.wordpress.com
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more.....

4. TAMPILAN AWALNYA KURANG LEBIH SEPERTI INI, DAN DISINI KITA BISA MENGGALI INFORMASI DARI TARGET DENGAN KLIK KANAN PADA WEB TARGET DAN RUN ALL TRANSFORMS

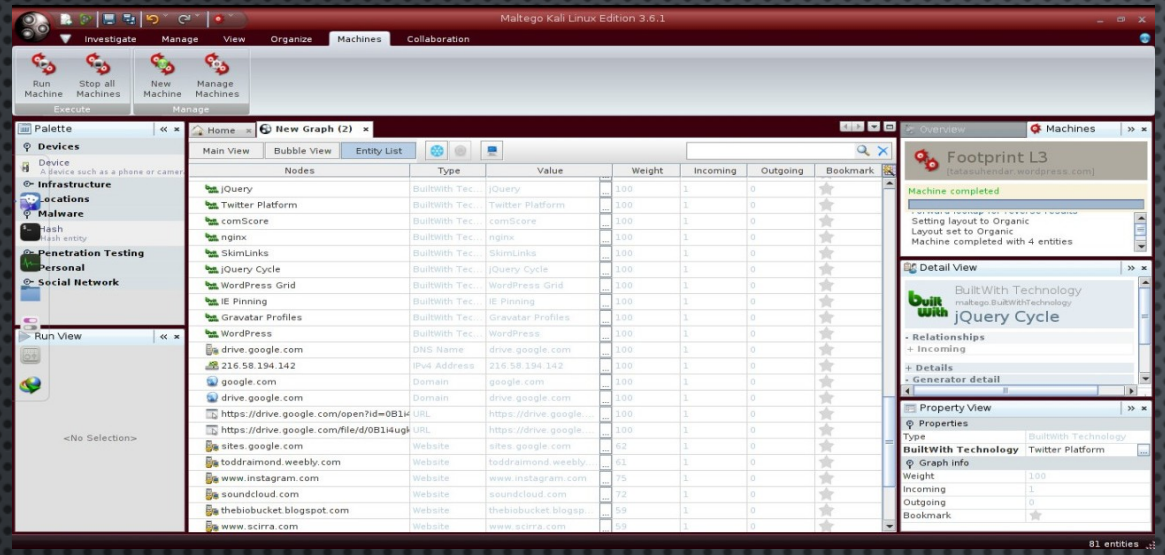




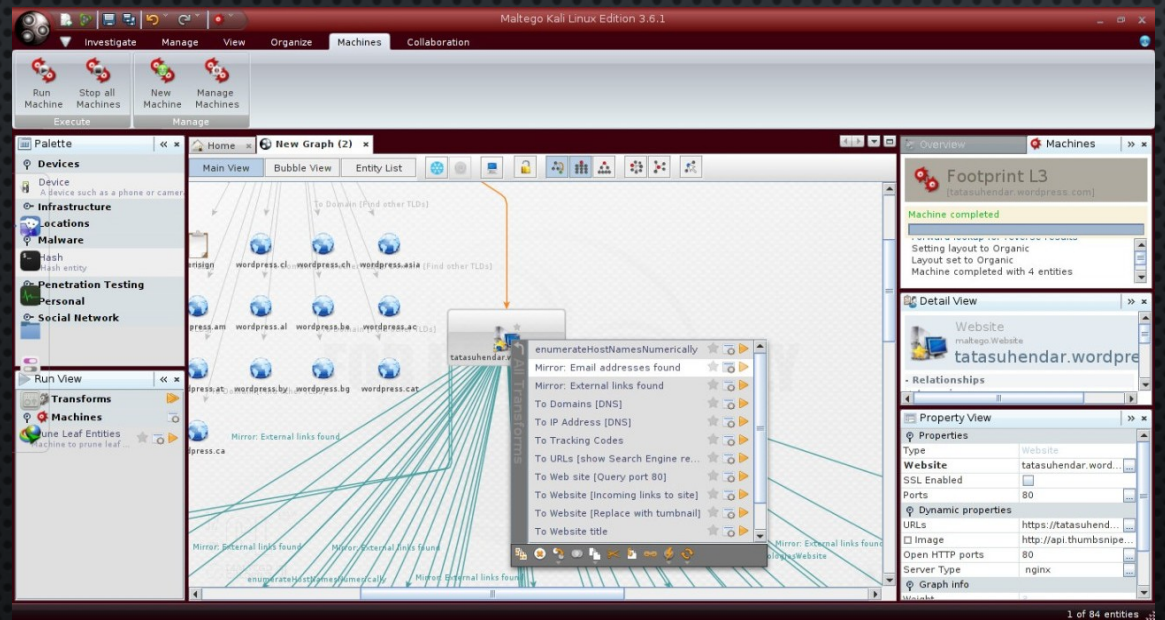
5. BEGINILAH TAMPILAN WEBSITE YANG DITARGETKAN TADI SUDAH DI ALL TRANSFORMS



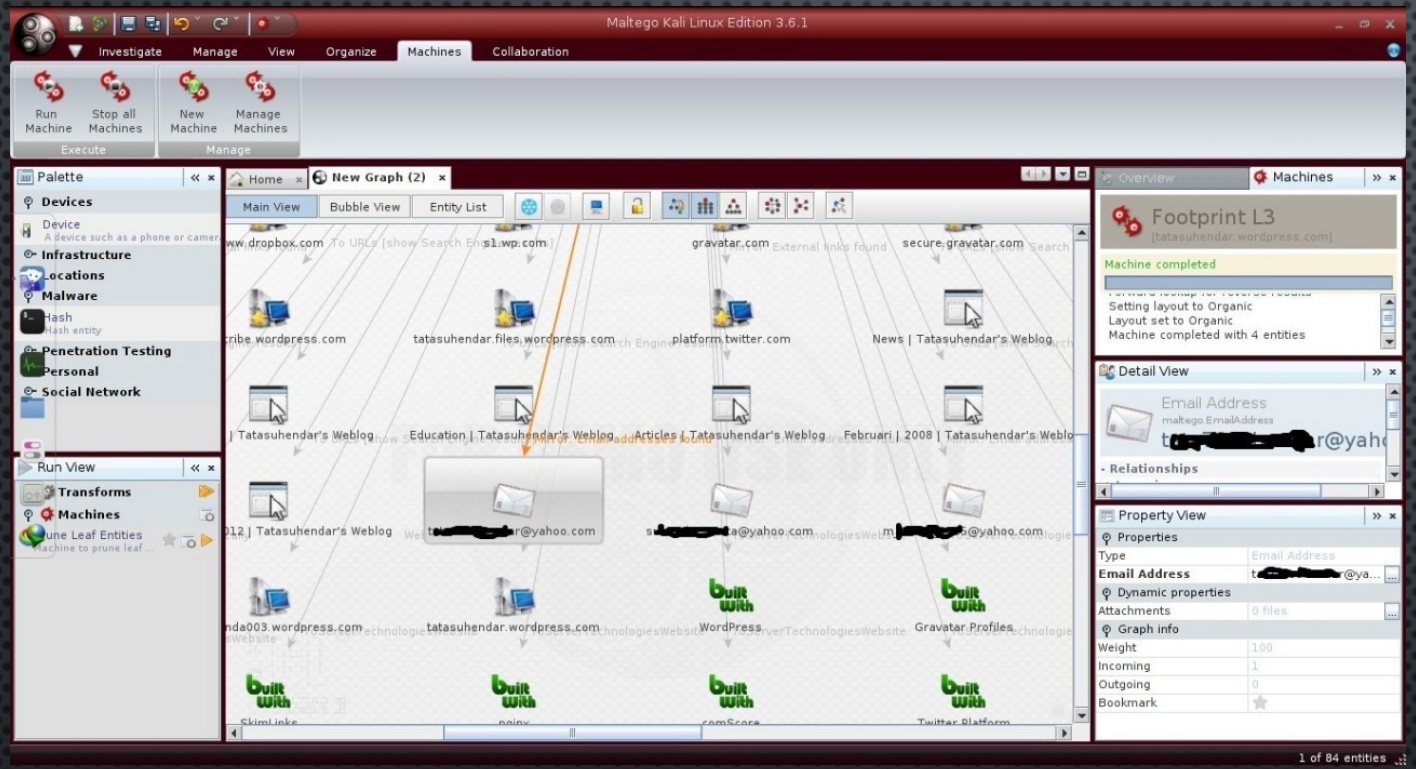
DAN DIBAWAH INI DALAM TAMPILAN ENTRY LIST



6. UNTUK MENCARI INFORMASI TENTANG ALAMAT EMAIL, PILIH IKON WEBNYA LALU KLIK KANAN PILIH“MIRROR: EMAIL ADDRESS FOUND”. INILAH HASILNYA TERDAPAT 3 EMAIL YG TERHUBUNG DENGAN WEB TERSEBUT



7. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA



8. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA

SOURCE

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

https://www.gagaltotal666.site/2016/06/cara-menggunakan-maltego-di-kali-linux.html?m=1

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

TERIMAKASIH

NMAP

KELOMPOK 2

- Nama Kelompok……..
  1. Rahmad Kartolo
- 2. Rio Permata
- 3.Muhammad Syahril
- 4.Yeni

- NMAP adalah singkatan dari *Network Mapper* yang merupakan sebuah *tool* atau alat yang bersifat *open source*. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan. Seseorang yang berjasa mengukirkan namanya sebagai penemu atau pencipta dari NMAP adalah Gordon Lyon

- FUNGSI NMAP?

- **1. Digunakan untuk memeriksa jaringan**
- Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada host tunggal. Cara kerjanya adalah dengan menggunakan IP raw yang berfungsi untuk menentukan mana host yang tersedia di dalam jaringan

- **2. Melakukan scanning pada port jaringan**
- Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer

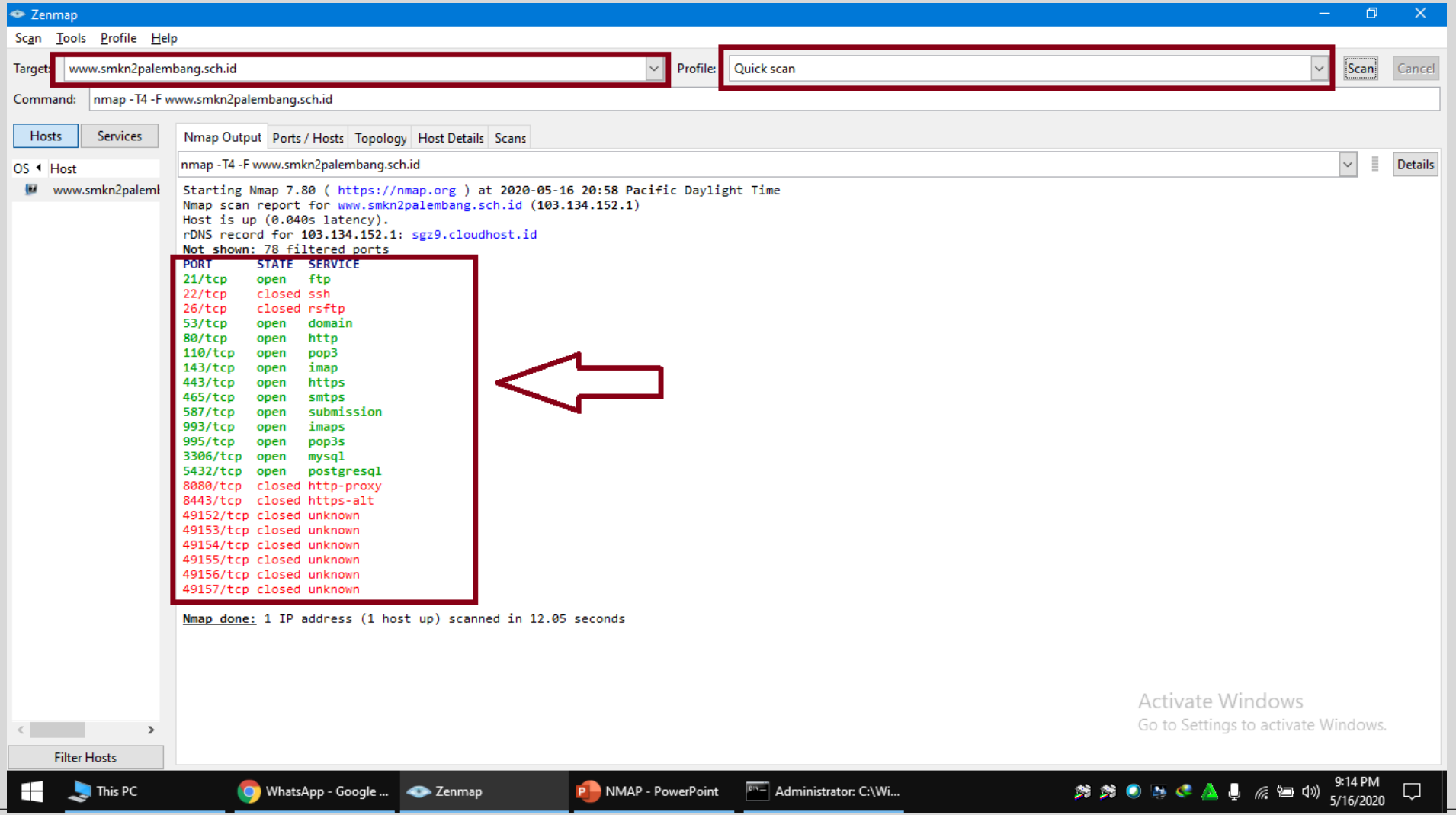
- Studi Kasus

  pada web SMK NEGERI 2 Palembang

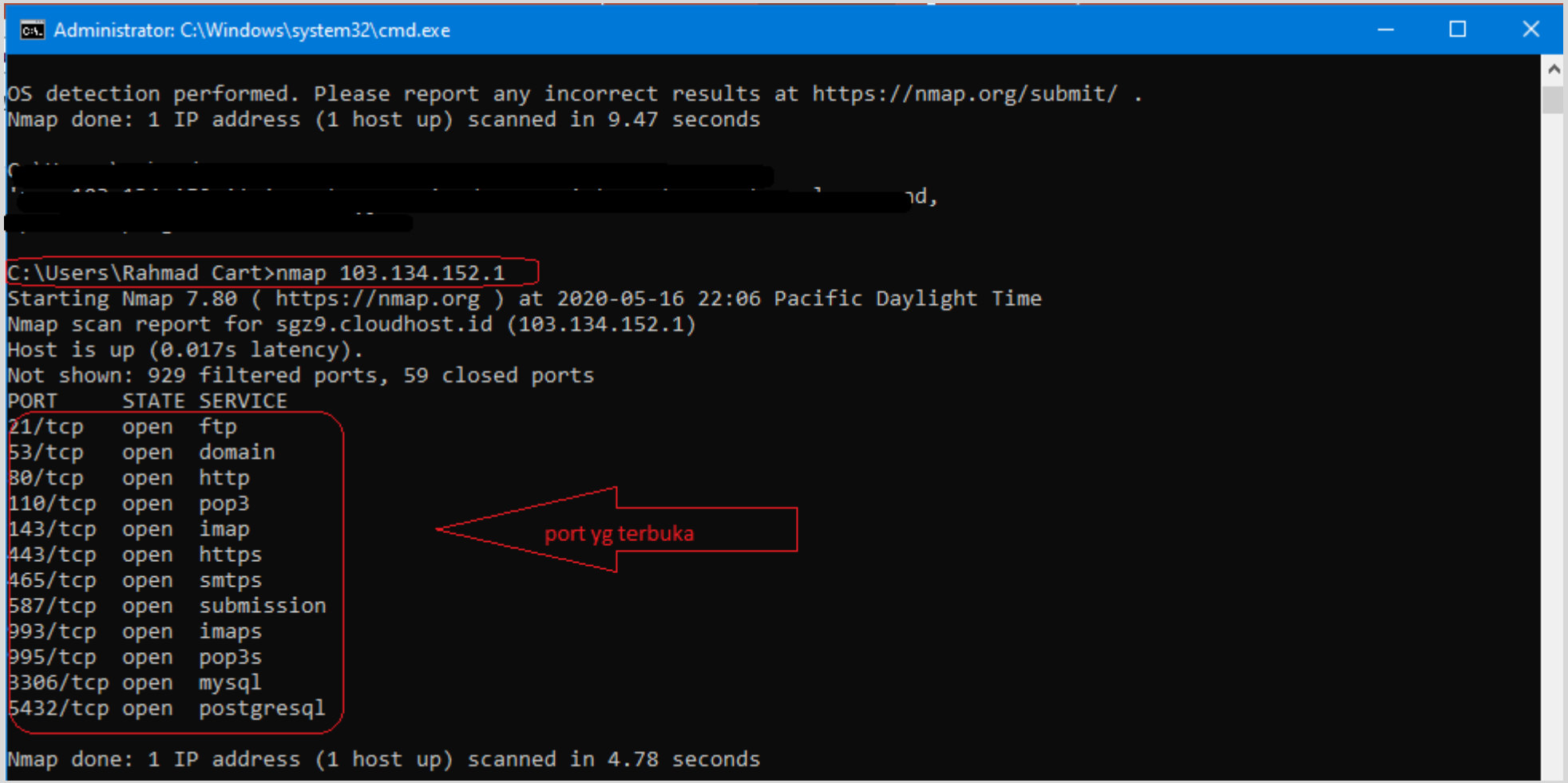
  www.smkn2palembang.sch.id

- Atau ip addres 103.134.152.1

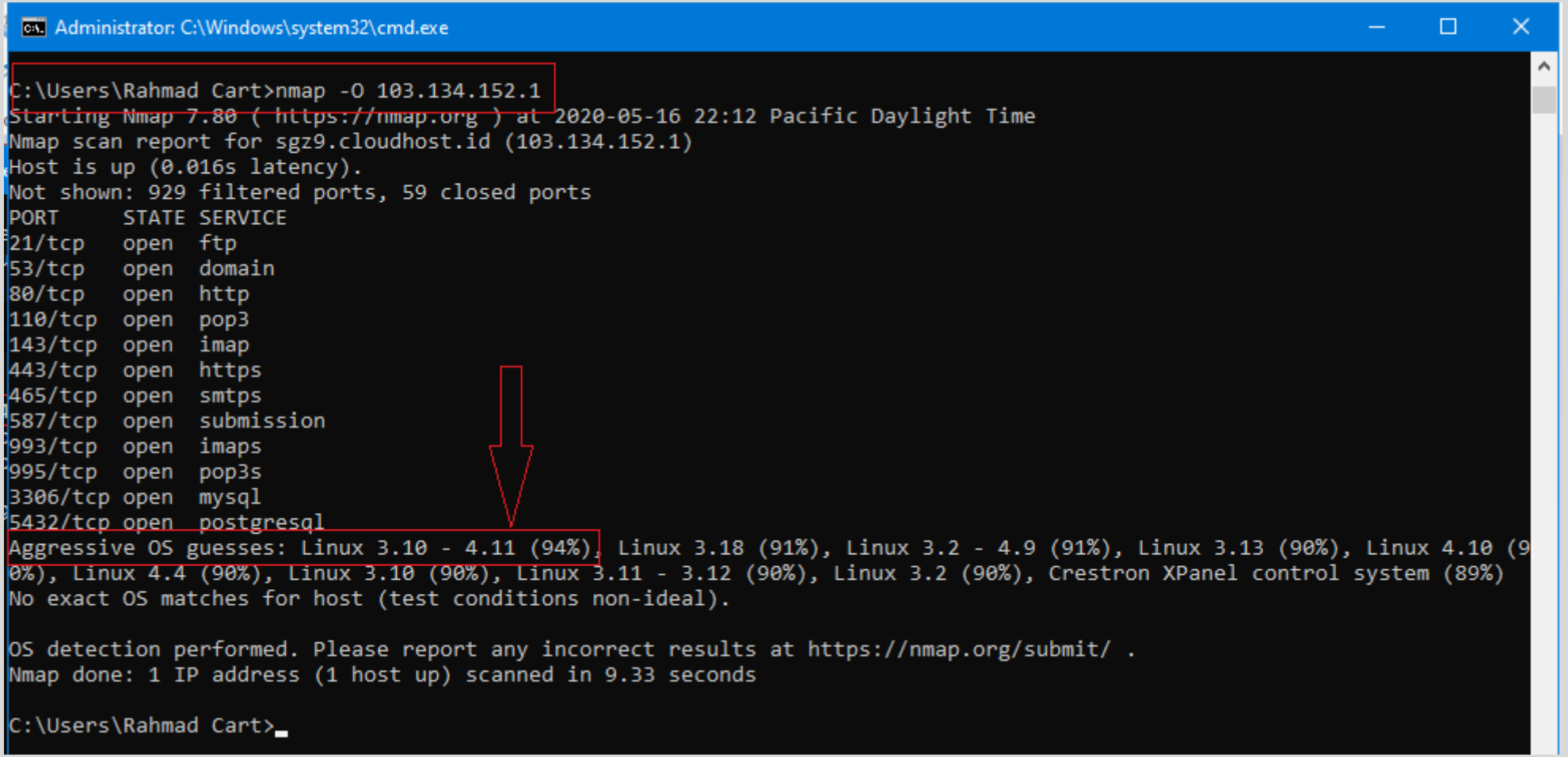
Pertama kita scan pada web smkn2palembang.sch.id
seperi gambar di bwah ini



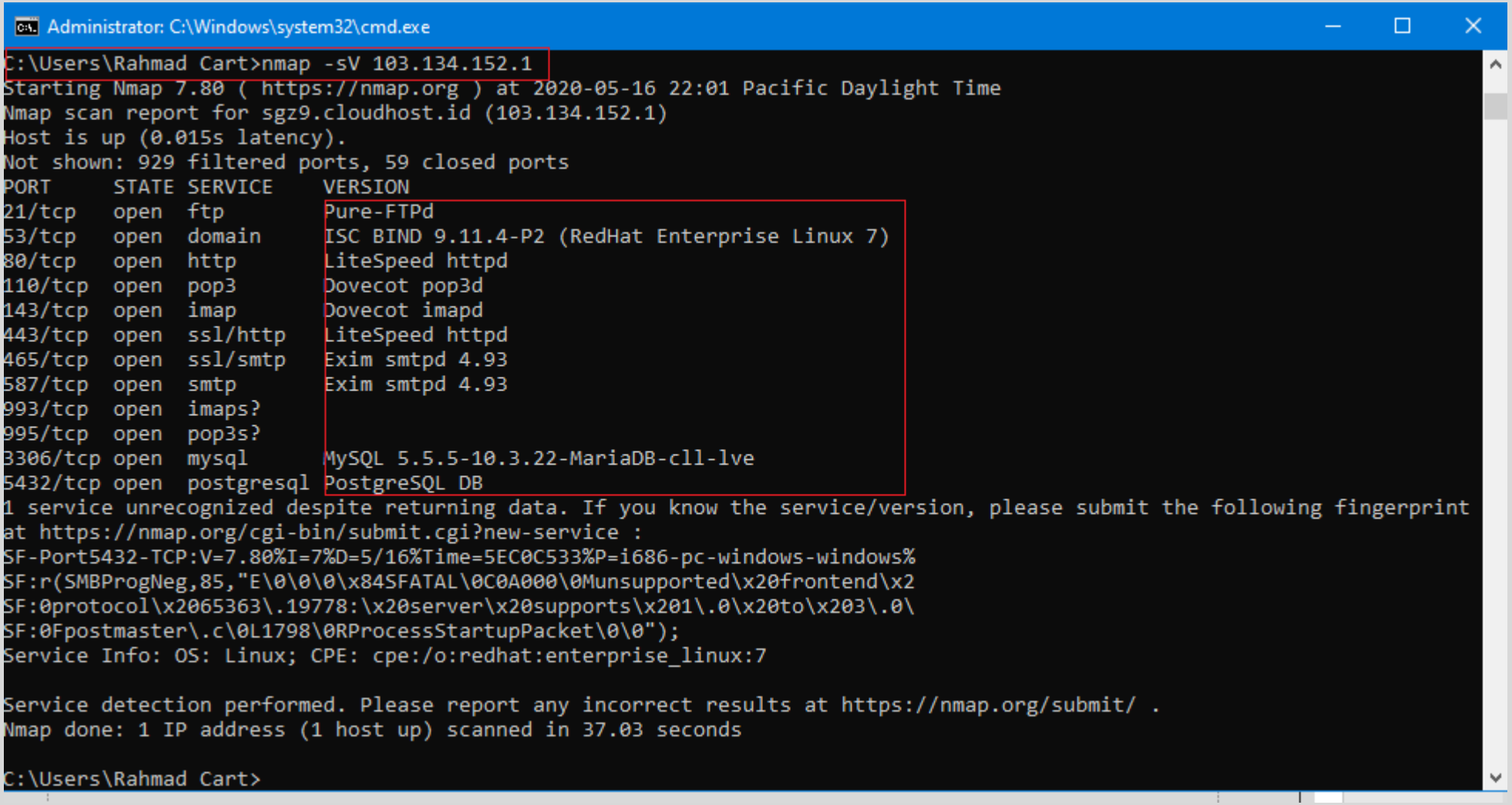
- Langkah selanjutnya Kita scaning mengunakan ip address 103.134.152.1
-



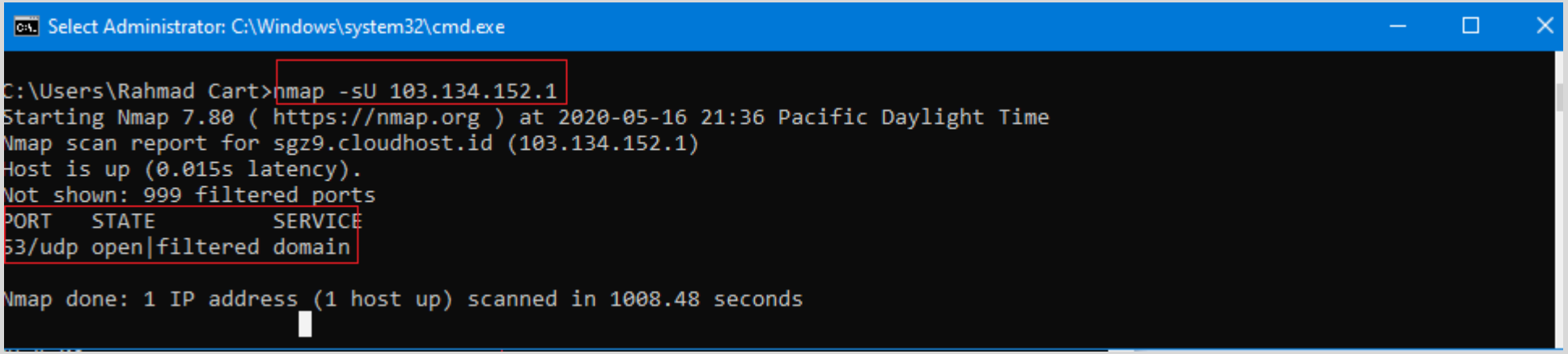
- Langkah selanjutnya kita akan melihat operstion system yg berjalan pada web tersebut mengguanakan perintah “nmap –O 103.134.152.1



- Langkah selanjutnya kita akan versi packet yg berjalan pada packet atau web tersebut mengguanakan perintah “nmap –sV 103.134.152.1

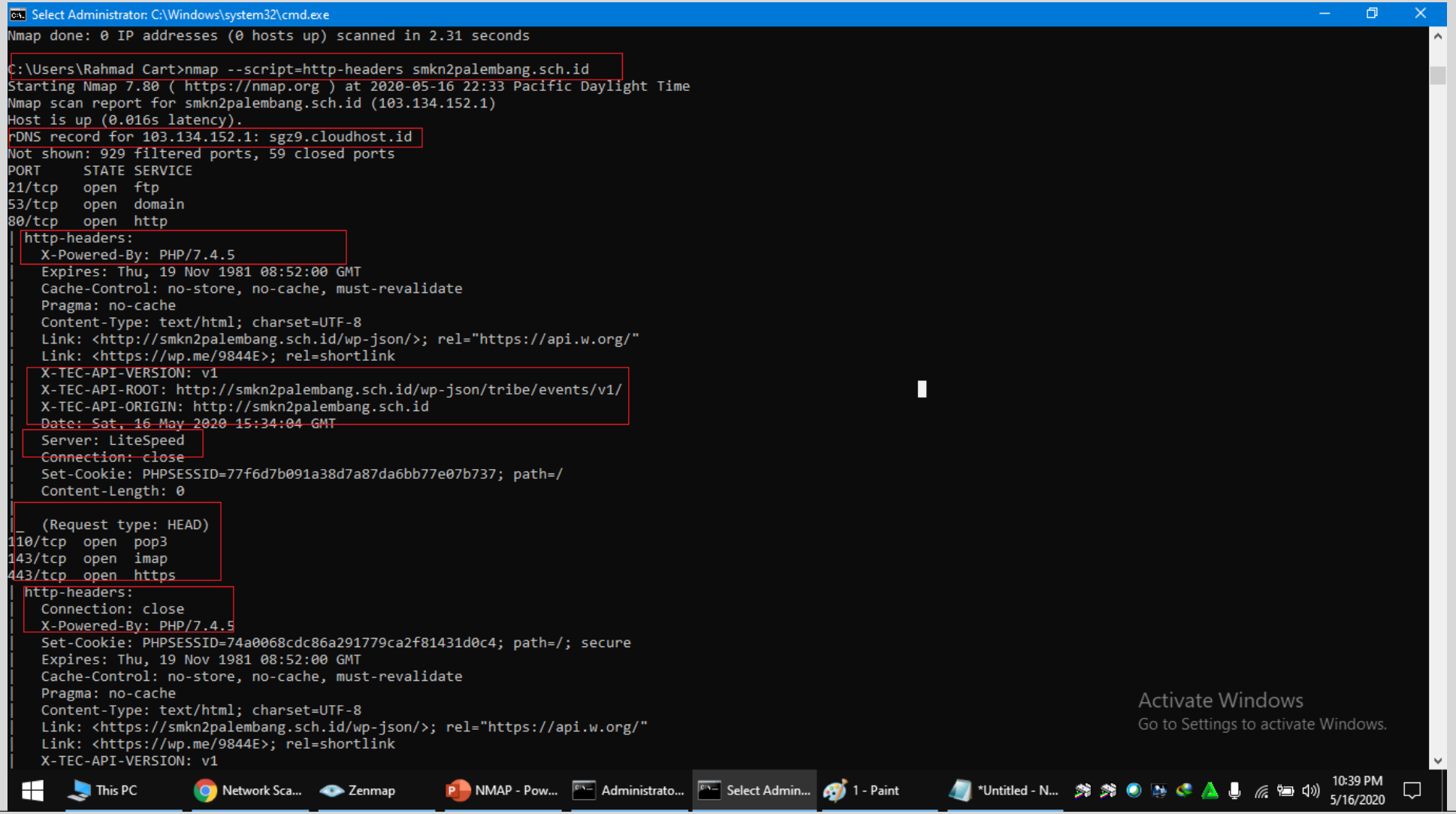


- Langkah selanjutnya kita akan mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP pada web mengguanakan perintah “nmap –sU 103.134.152.1



- Didapat openlfiltered yang berarti
- Nmap menganggap port dalam status ini bila ia tidak dapat menentukan apakah port open atau filtered. Hal ini terjadi untuk jenis pemeriksaan ketika port terbuka tidak memberi respon. Tidak adanya tanggapan dapat pula berarti bahwa packet filter men-drop probe atau respon yang diberikan. Sehingga Nmap tidak dapat mengetahui dengan tepat apakah port terbuka atau difilter. Scan UDP, IP protocol, FIN, NULL, dan Xmas mengklasifikasikan port dengan cara ini.

- Langkah selanjutnya kita akan mengidentifikasi header http pada web menggunakan perintah “nmap --script=http-headers smkn2palembang.sch.id”



- TERIMAH KASIH

MALTEGO

HARLI SEPTIA FANI (182420122)
PUTRI ARMILIA PRAYESY (182420125)
DEVIAN SAPUTRA (182420128)
I MADE HARYA WIJAYA OKA RAFFLESIA (182420129)
PUTRI ELEINA NURRAHMA (182420138)

MALTEGO

MALTEGO INI DISEBUT **OSINT** (**O**PEN **S**OURCE **I**NTELLIGENCE **G**ATHERING) SEBUAH ALAT UNTUK MELAKUKAN *FOOTPRINTING*, DIGUNAKAN UNTUK MENGUMPULKAN INFORMASI SEBANYAK MUNGKIN DENGAN TUJUAN FORENSIK, *PEN TESTING*, ATAU *ETHICAL HACKING*. APLIKASI YANG DIGUNAKAN UNTUK MEMETAKAN JARINGAN KOMUNIKASI YANG BERADA DI INTERNET TUJUANNYA ADALAH MENGUMPULKAN INFORMASI TENTANG TARGET DAN MENAMPILKAN INFORMASI TERSEBUT DALAM FORMAT YANG MUDAH DIMENGERTI, MEMVISUALISASIKAN INFORMASI TERSEBUT KE DALAM SEBUAH FORMAT GRAPH, SANGAT COCOK UNTUK *LINK ANALYSIS* DAN *DATA MINING*.

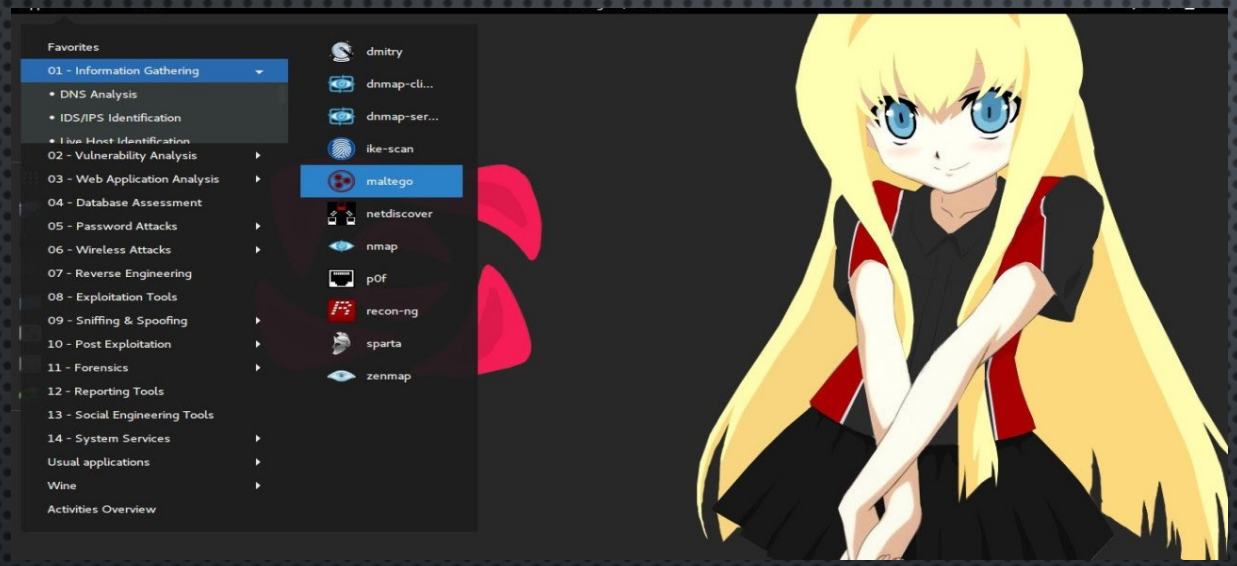
FUNGSI DARI MALTEGO ADALAH MEMUDAHKAN SESEOORANG YANG MENCARI INFORMASI TENTANG APA YANG MEREKA SELIDIKI ATAU MEREKA INCAR SEBAGAI TARGET, CONTOH KETIKA SEORANG MENCARI INFORMASI DARI SEBUAH DOMAIN MENGGUNAKAN MALTEGO, MAKA MALTEGO AKAN MENAMPIKAN BEBRAP INFORMASI SEPERTI BERIKUT:

- BLOCK IP HOSTING
- DOMAIN REGISTE
- EMAIL USER & ADMIN
- PHONE NUMBER
- PETA JARINGAN

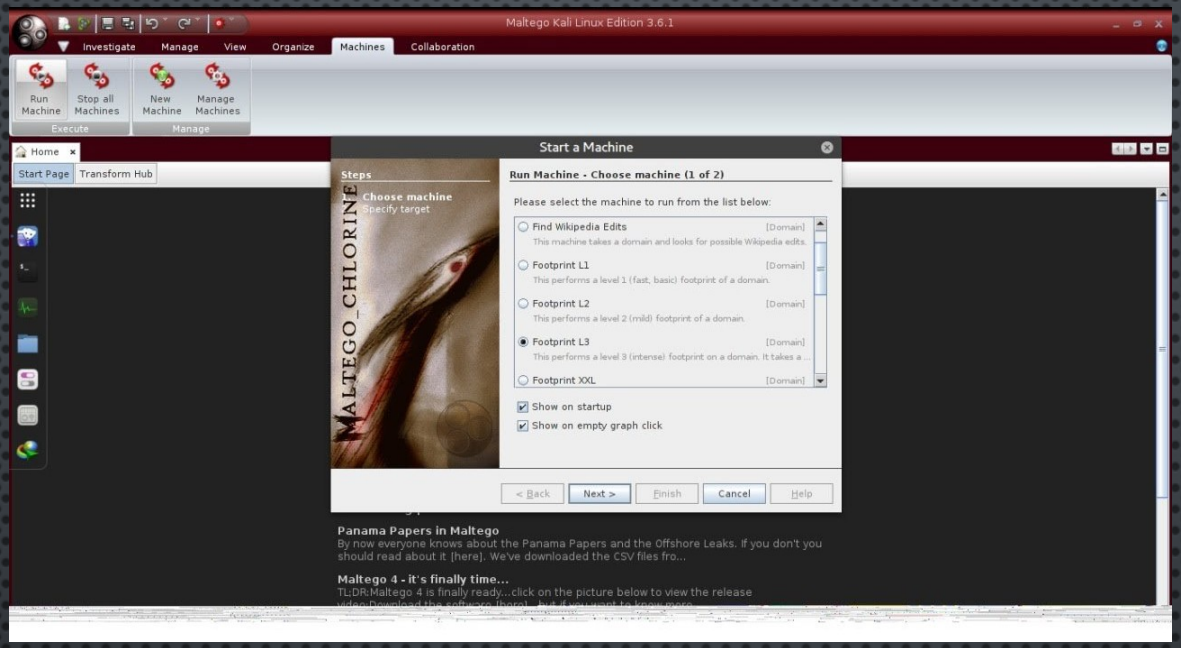
MALTEGO DIBEDAKAN MENJADI VERSI KOMERSIAL (COMMERCIAL EDITION) DAN VERSI GRATIS (COMMUNITY EDITION). VERSI GRATIS YANG TERSEDIA DI KALI LINUX HANYA DAPAT MENAMPILKAN MAKSIMAL 12 HASIL TRANSFORMASI, SEBAGAI SEBUAH FRONT-END UNTUK SERVER OSINT, MALTEGO VERSI GRATIS HANYA DAPAT MEMAKAI LAYANAN SERVER MILIK PATERVA. KARENA VERSI YANG DISEDIAKAN OLEH KALI LINUX ADALAH VERSI GRATIS DARI MALTEGO

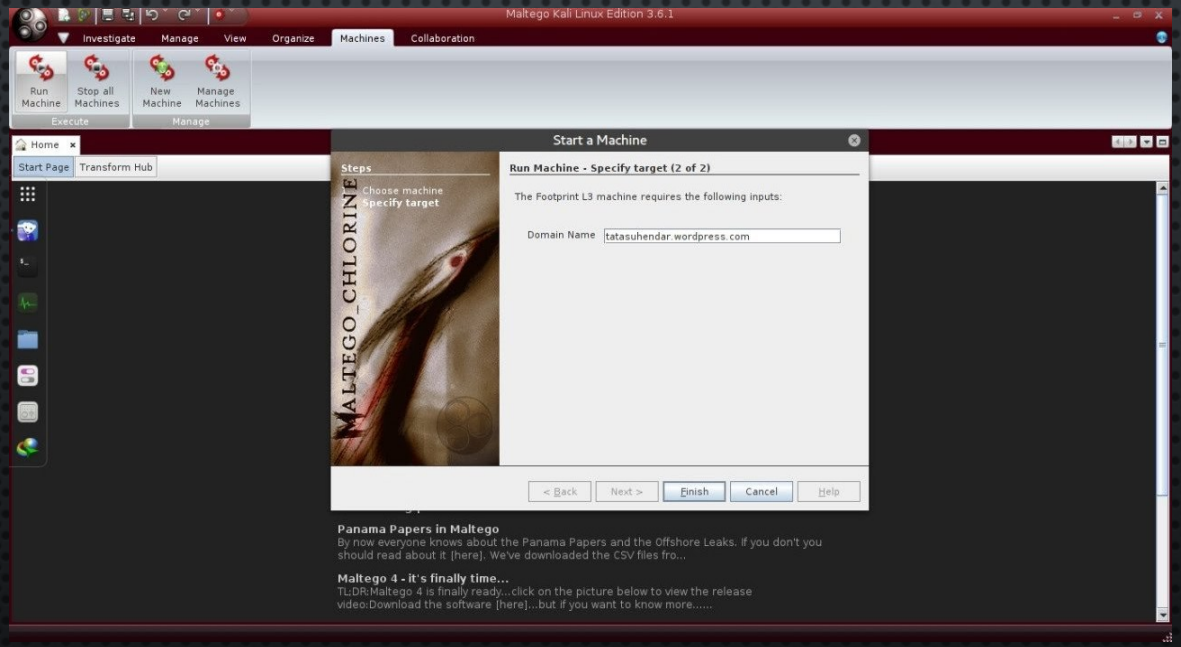
TAHAPAN DALAM PENGGUNAAN MALTEGO

1. BUKA MALTEGO PADA KALI LINUK ANDA, ADA DI MENU INFORMATION GATHERING > MALTEGO

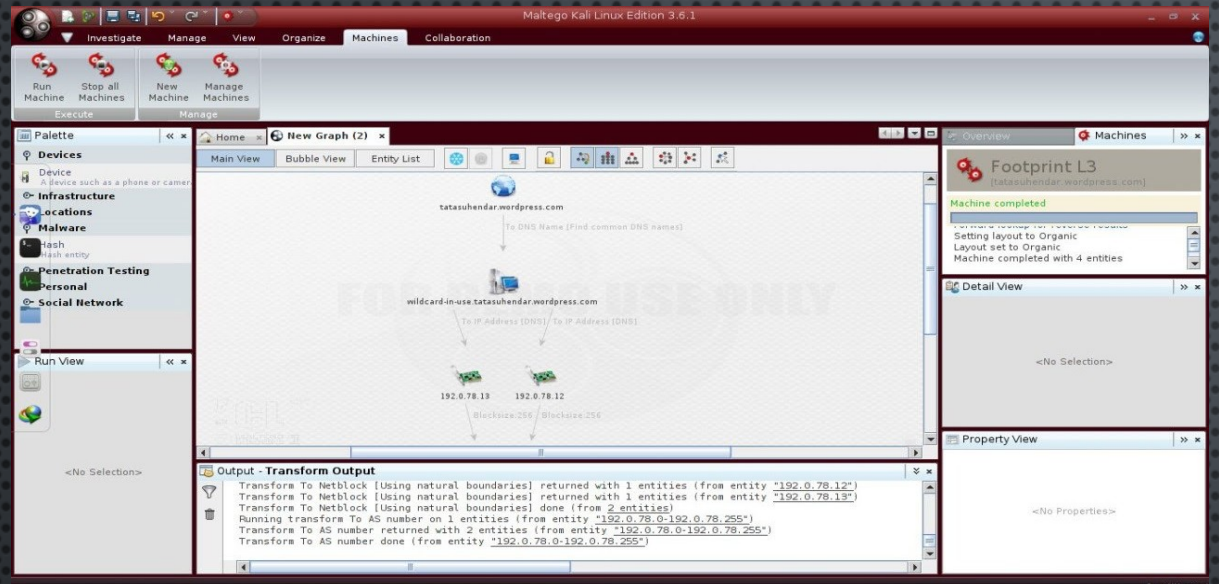


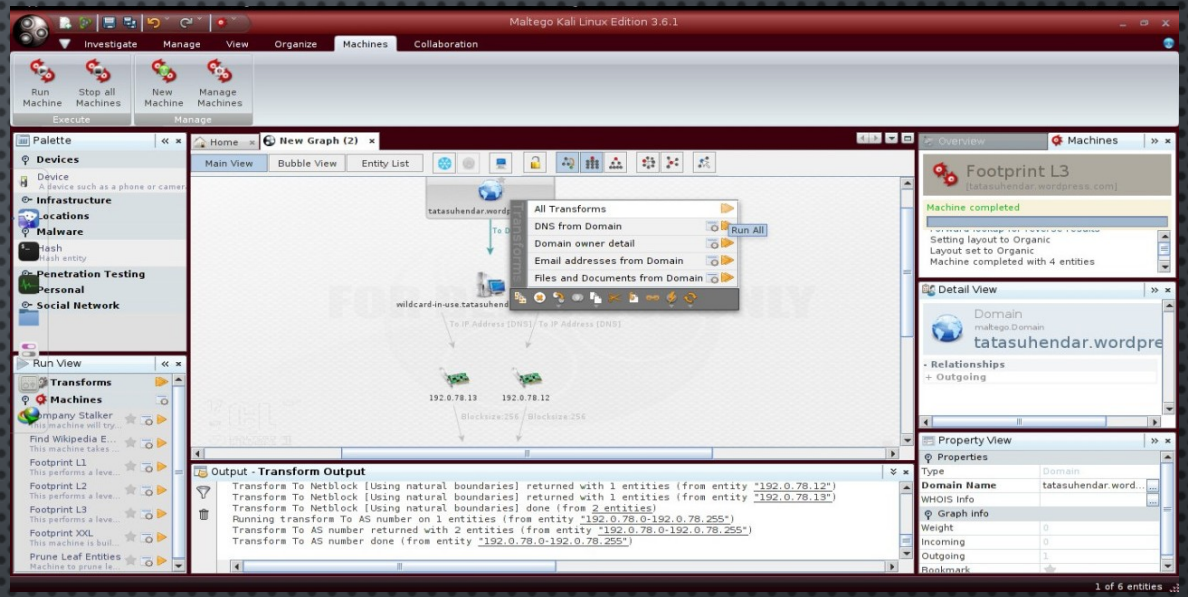
2. LOGIN DENGAN EMAIL DAN PASSWORD YANG TELAH TERDAFTAR
3. SETELAH SELESAI LOGIN MAKA AKAN MUNCUL DIALOG START A MACHINE, PILIH FOOTPRINTING L3 LALU DI STEP KEDUA KITA HARUS MAMASUKAN DOMAIN ATAU LINK WEBSITE TAGE


Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a ...
Footprint XXL [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release

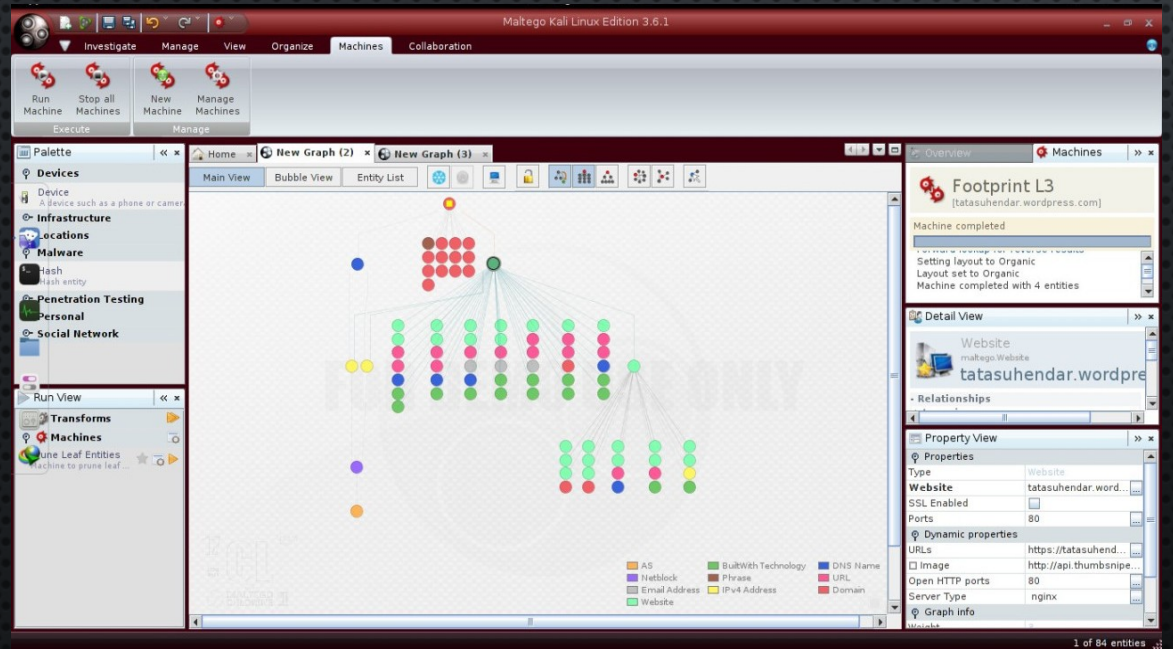

Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Specify target (2 of 2)
The Footprint L3 machine requires the following inputs:
Domain Name
tatasuhendar.wordpress.com
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more.....

4. TAMPILAN AWALNYA KURANG LEBIH SEPERTI INI, DAN DISINI KITA BISA MENGGALI INFORMASI DARI TARGET DENGAN KLIK KANAN PADA WEB TARGET DAN RUN ALL TRANSFORMS

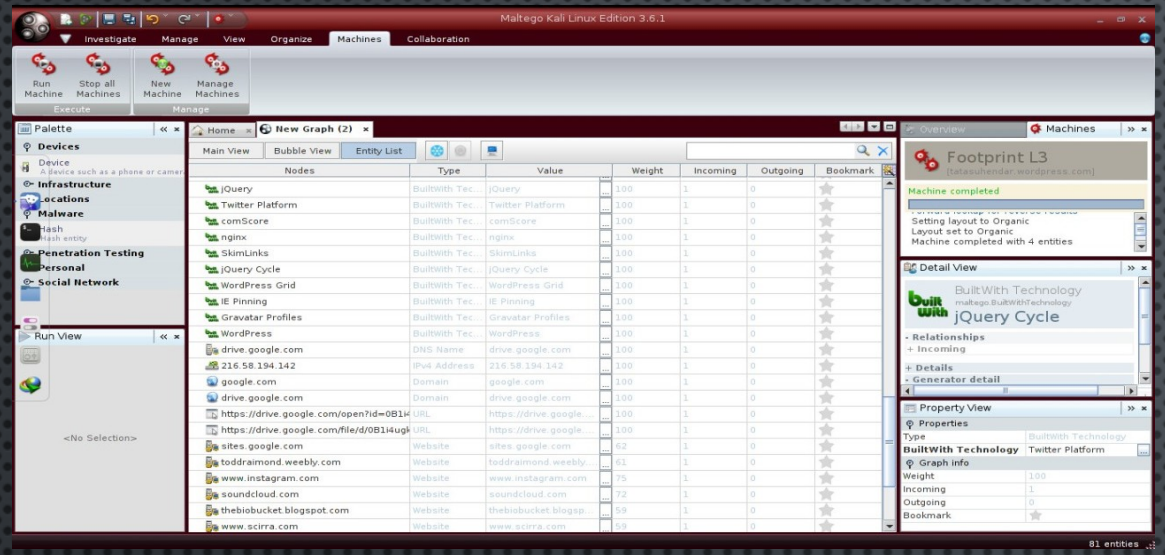




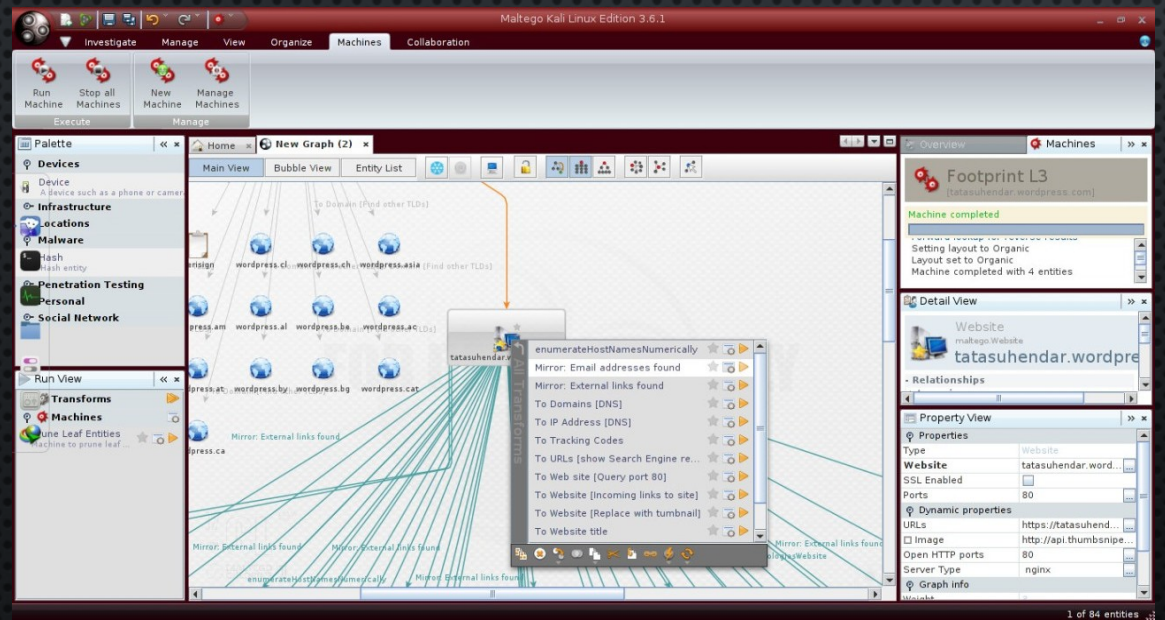
5. BEGINILAH TAMPILAN WEBSITE YANG DITARGETKAN TADI SUDAH DI ALL TRANSFORMS



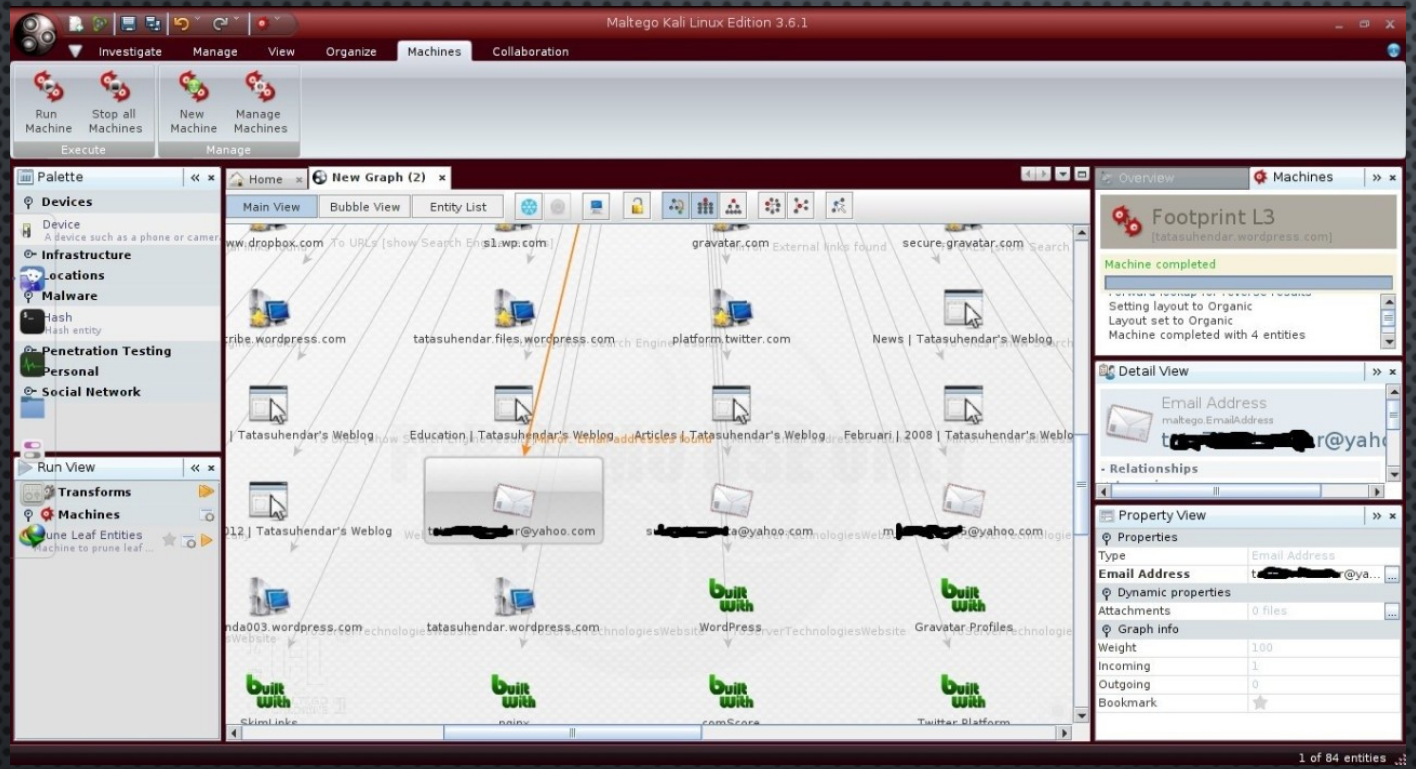
DAN DIBAWAH INI DALAM TAMPILAN ENTRY LIST



6. UNTUK MENCARI INFORMASI TENTANG ALAMAT EMAIL, PILIH IKON WEBNYA LALU KLIK KANAN PILIH“MIRROR: EMAIL ADDRESS FOUND”. INILAH HASILNYA TERDAPAT 3 EMAIL YG TERHUBUNG DENGAN WEB TERSEBUT



7. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA



8. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA

SOURCE

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

https://www.gagaltotal666.site/2016/06/cara-menggunakan-maltego-di-kali-linux.html?m=1

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

TERIMAKASIH

MALTEGO

HARLI SEPTIA FANI (182420122)
PUTRI ARMILIA PRAYESY (182420125)
DEVIAN SAPUTRA (182420128)
I MADE HARYA WIJAYA OKA RAFFLESIA (182420129)
PUTRI ELEINA NURRAHMA (182420138)

MALTEGO

MALTEGO INI DISEBUT **OSINT** (**O**PEN **S**OURCE **I**NTELLIGENCE **G**ATHERING) SEBUAH ALAT UNTUK MELAKUKAN *FOOTPRINTING*, DIGUNAKAN UNTUK MENGUMPULKAN INFORMASI SEBANYAK MUNGKIN DENGAN TUJUAN FORENSIK, *PEN TESTING*, ATAU *ETHICAL HACKING*. APLIKASI YANG DIGUNAKAN UNTUK MEMETAKAN JARINGAN KOMUNIKASI YANG BERADA DI INTERNET TUJUANNYA ADALAH MENGUMPULKAN INFORMASI TENTANG TARGET DAN MENAMPILKAN INFORMASI TERSEBUT DALAM FORMAT YANG MUDAH DIMENGERTI, MEMVISUALISASIKAN INFORMASI TERSEBUT KE DALAM SEBUAH FORMAT GRAPH, SANGAT COCOK UNTUK *LINK ANALYSIS* DAN *DATA MINING*.

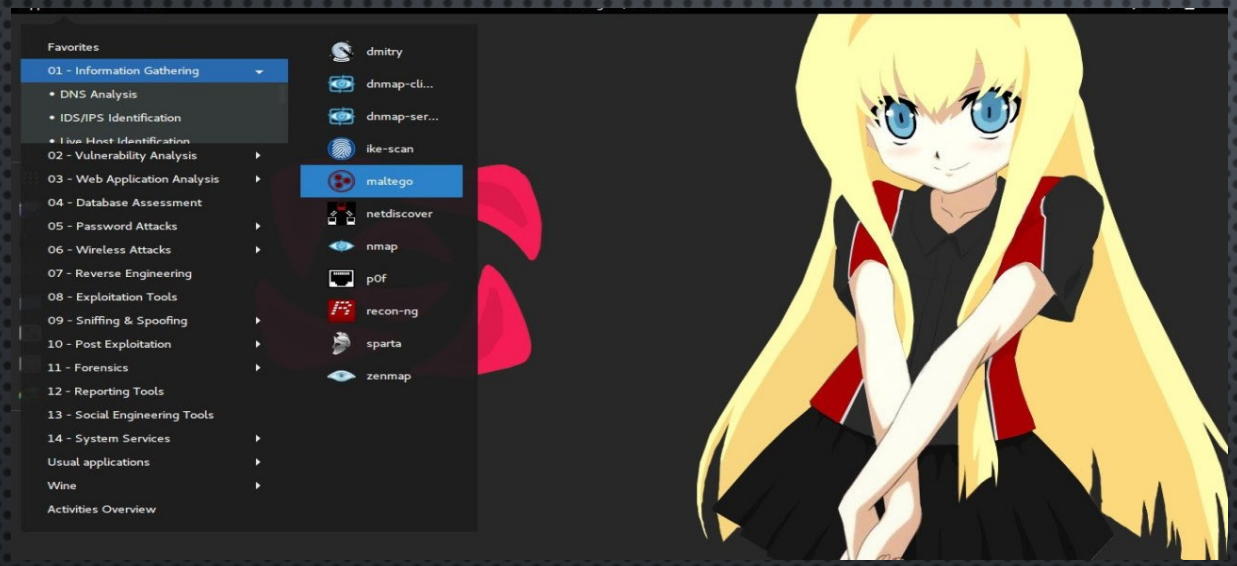
FUNGSI DARI MALTEGO ADALAH MEMUDAHKAN SESEOORANG YANG MENCARI INFORMASI TENTANG APA YANG MEREKA SELIDIKI ATAU MEREKA INCAR SEBAGAI TARGET, CONTOH KETIKA SEORANG MENCARI INFORMASI DARI SEBUAH DOMAIN MENGGUNAKAN MALTEGO, MAKA MALTEGO AKAN MENAMPIKAN BEBRAP INFORMASI SEPERTI BERIKUT:

- BLOCK IP HOSTING
- DOMAIN REGISTE
- EMAIL USER & ADMIN
- PHONE NUMBER
- PETA JARINGAN

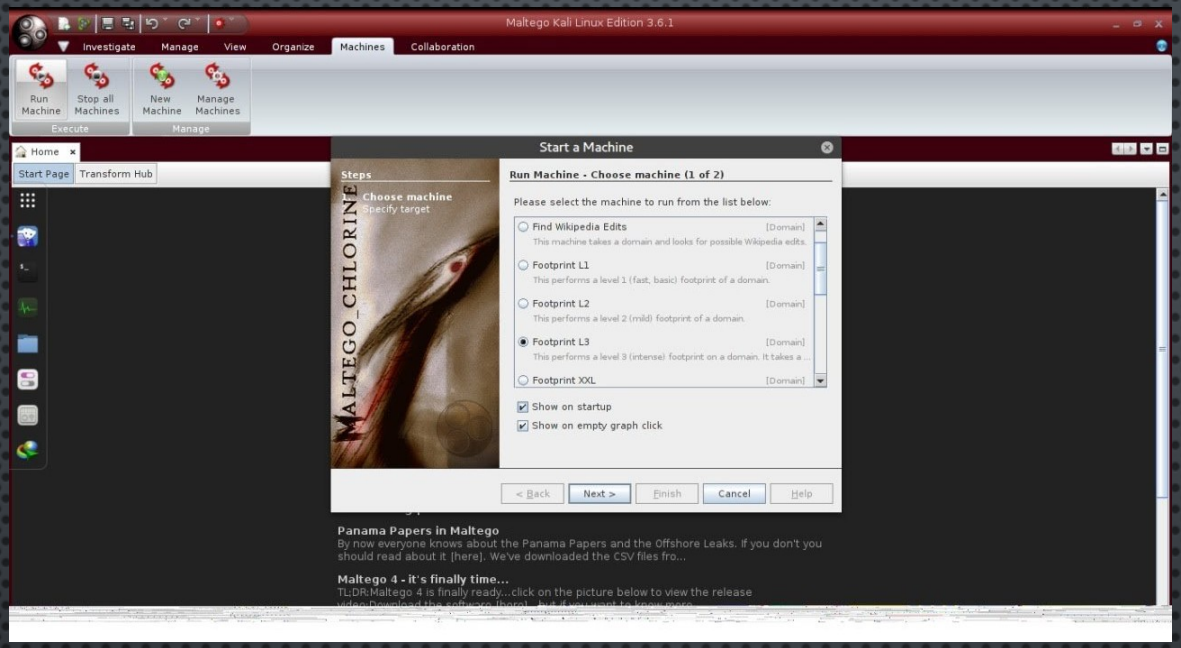
MALTEGO DIBEDAKAN MENJADI VERSI KOMERSIAL (COMMERCIAL EDITION) DAN VERSI GRATIS (COMMUNITY EDITION). VERSI GRATIS YANG TERSEDIA DI KALI LINUX HANYA DAPAT MENAMPILKAN MAKSIMAL 12 HASIL TRANSFORMASI, SEBAGAI SEBUAH FRONT-END UNTUK SERVER OSINT, MALTEGO VERSI GRATIS HANYA DAPAT MEMAKAI LAYANAN SERVER MILIK PATERVA. KARENA VERSI YANG DISEDIAKAN OLEH KALI LINUX ADALAH VERSI GRATIS DARI MALTEGO

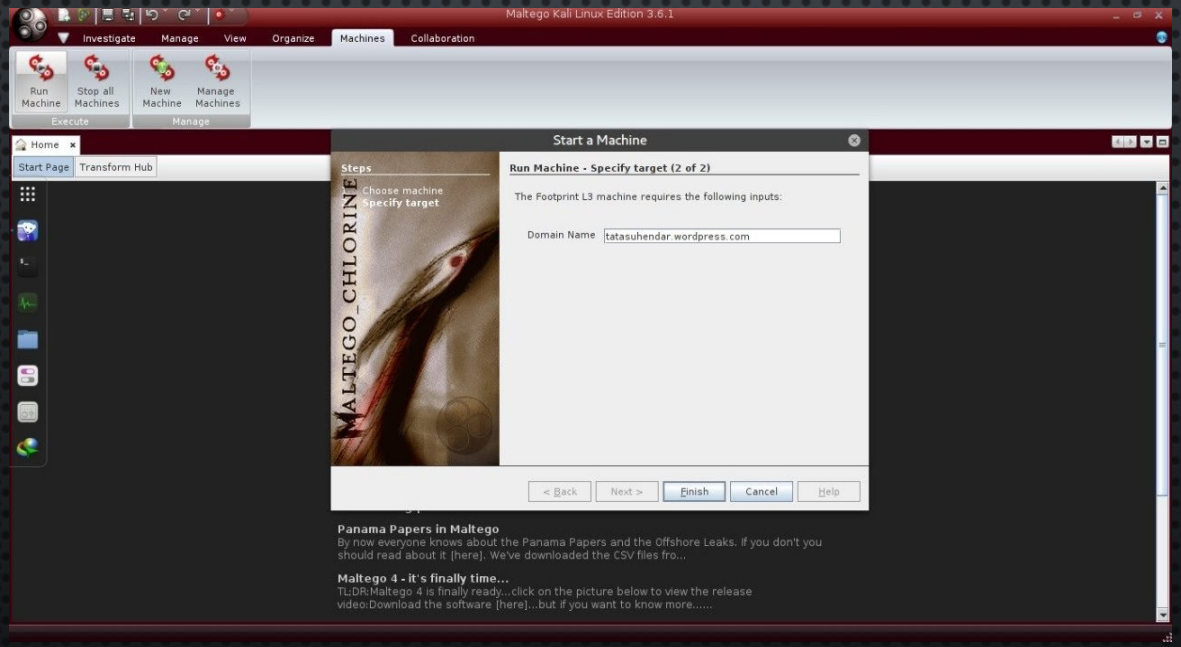
TAHAPAN DALAM PENGGUNAAN MALTEGO

1. BUKA MALTEGO PADA KALI LINUK ANDA, ADA DI MENU INFORMATION GATHERING > MALTEGO

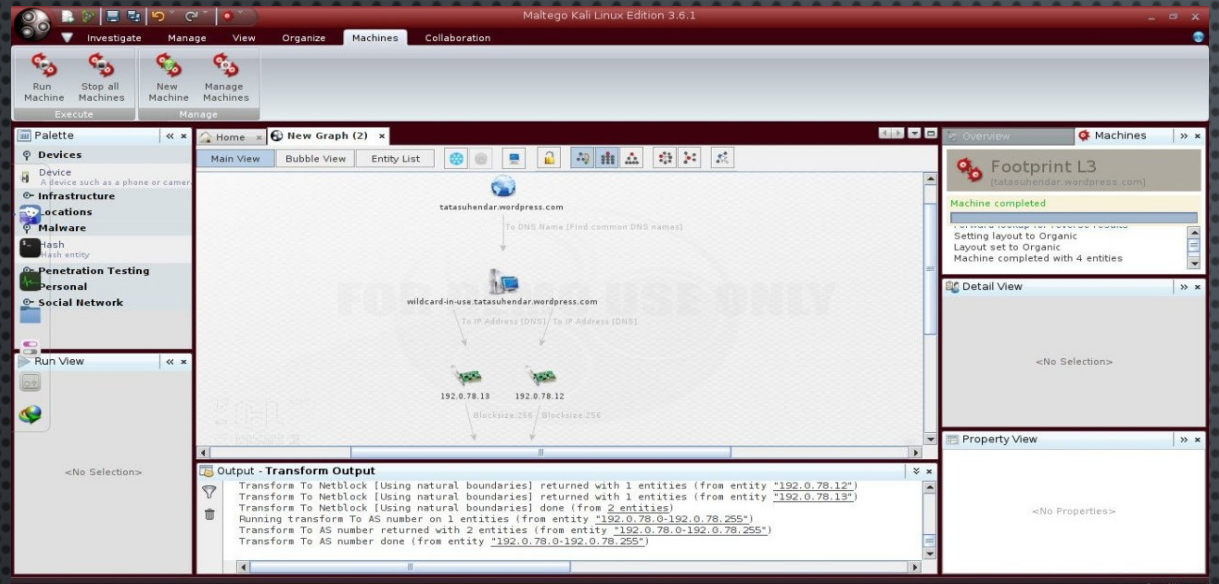


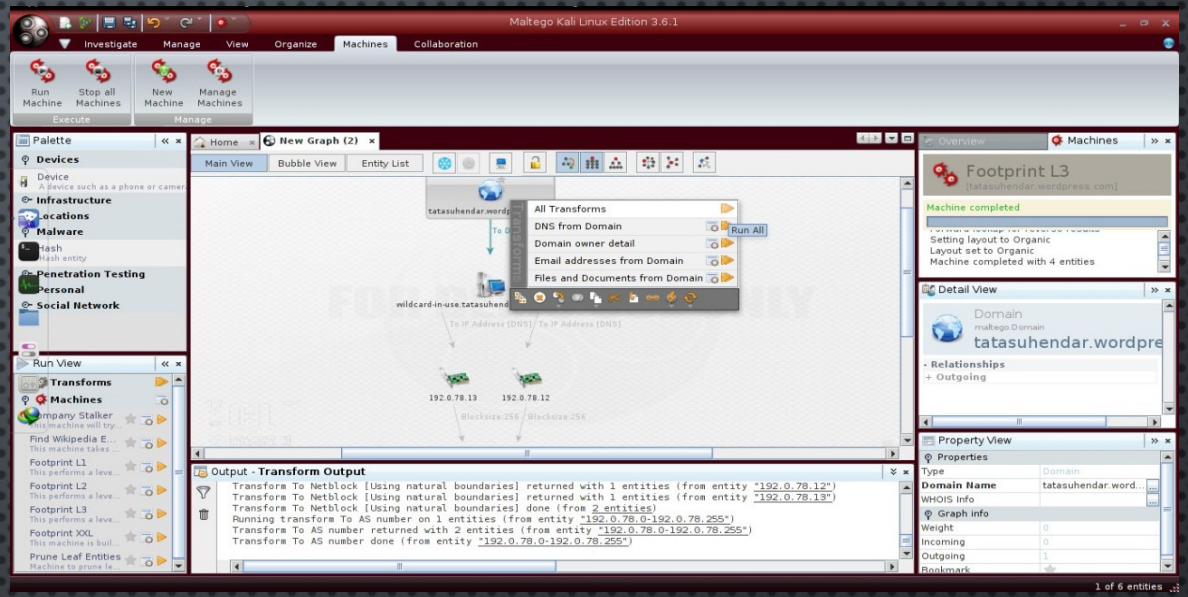
2. LOGIN DENGAN EMAIL DAN PASSWORD YANG TELAH TERDAFTAR
3. SETELAH SELESAI LOGIN MAKA AKAN MUNCUL DIALOG START A MACHINE, PILIH FOOTPRINTING L3 LALU DI STEP KEDUA KITA HARUS MAMASUKAN DOMAIN ATAU LINK WEBSITE TAGE


Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a ...
Footprint XXL [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release

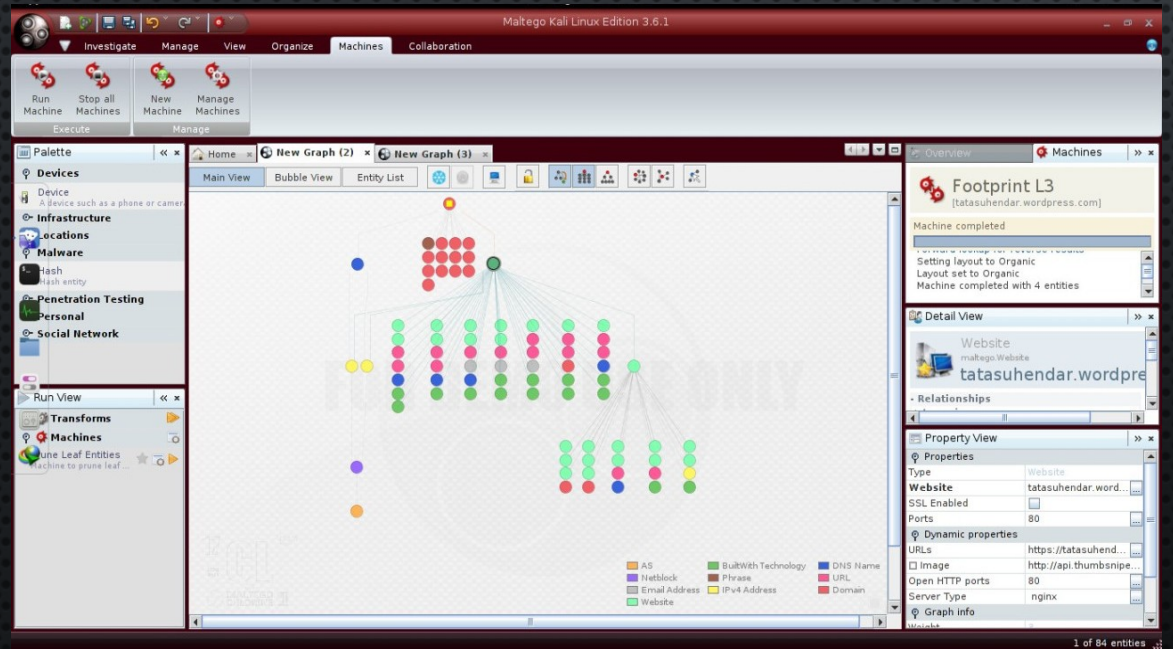

Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Specify target (2 of 2)
The Footprint L3 machine requires the following inputs:
Domain Name
tatasuhendar.wordpress.com
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more.....

4. TAMPILAN AWALNYA KURANG LEBIH SEPERTI INI, DAN DISINI KITA BISA MENGGALI INFORMASI DARI TARGET DENGAN KLIK KANAN PADA WEB TARGET DAN RUN ALL TRANSFORMS

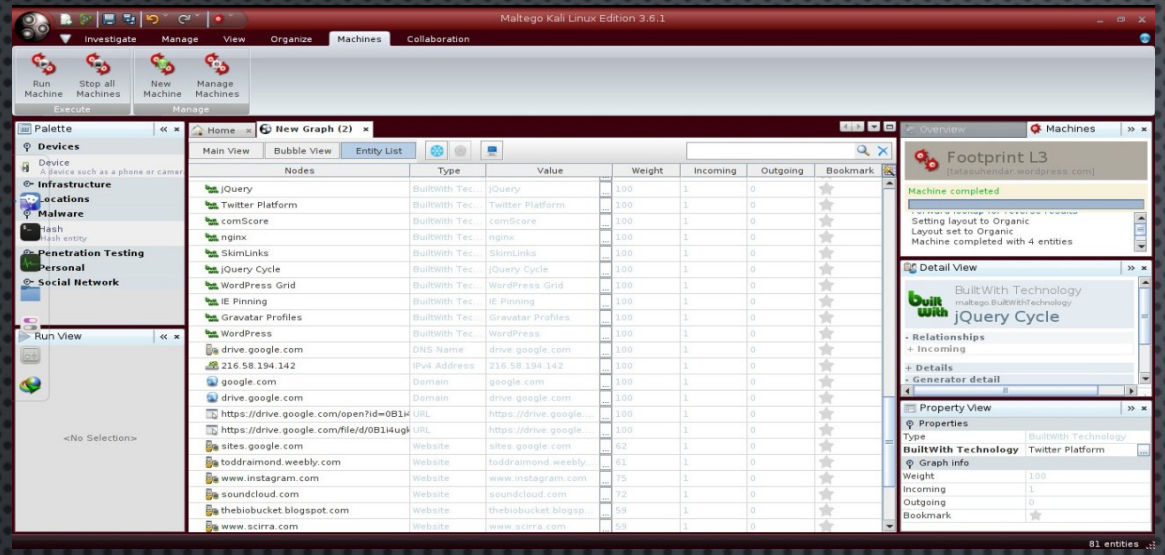




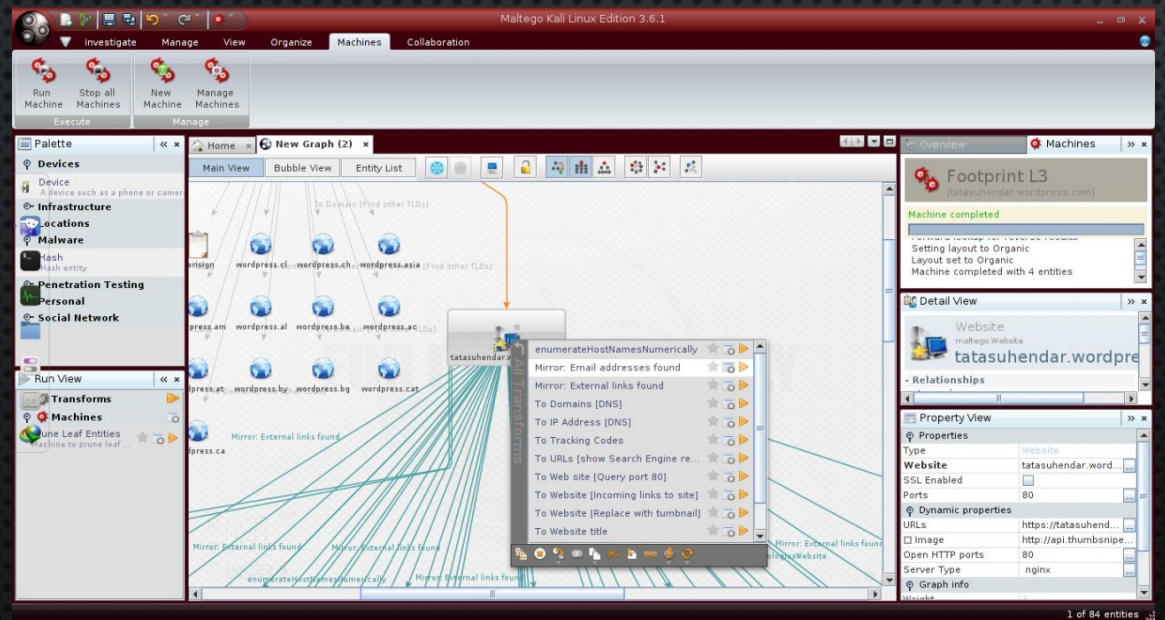
5. BEGINILAH TAMPILAN WEBSITE YANG DITARGETKAN TADI SUDAH DI ALL TRANSFORMS



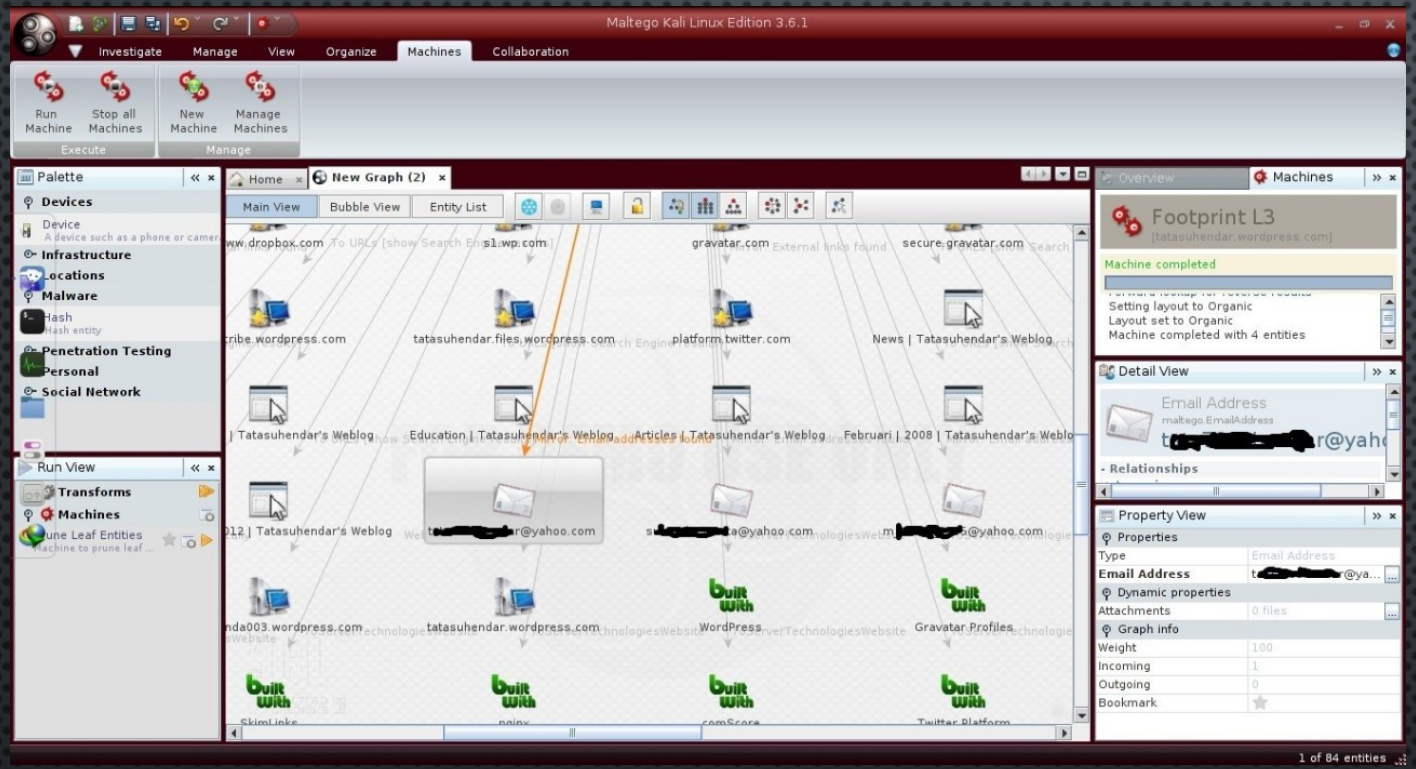
DAN DIBAWAH INI DALAM TAMPILAN ENTRY LIST



6. UNTUK MENCARI INFORMASI TENTANG ALAMAT EMAIL, PILIH IKON WEBNYA LALU KLIK KANAN PILIH“MIRROR: EMAIL ADDRESS FOUND”. INILAH HASILNYA TERDAPAT 3 EMAIL YG TERHUBUNG DENGAN WEB TERSEBUT



7. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA



8. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA

SOURCE

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

https://www.gagaltotal666.site/2016/06/cara-menggunakan-maltego-di-kali-linux.html?m=1

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

TERIMAKASIH

NMAP

KELOMPOK 2

- Nama Kelompok……..
  1. Rahmad Kartolo
- 2. Rio Permata
- 3.Muhammad Syahril
- 4.Yeni

- NMAP adalah singkatan dari *Network Mapper* yang merupakan sebuah *tool* atau alat yang bersifat *open source*. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan. Seseorang yang berjasa mengukirkan namanya sebagai penemu atau pencipta dari NMAP adalah Gordon Lyon

- FUNGSI NMAP?

- **1. Digunakan untuk memeriksa jaringan**
- Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada host tunggal. Cara kerjanya adalah dengan menggunakan IP raw yang berfungsi untuk menentukan mana host yang tersedia di dalam jaringan

- **2. Melakukan scanning pada port jaringan**
- Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer

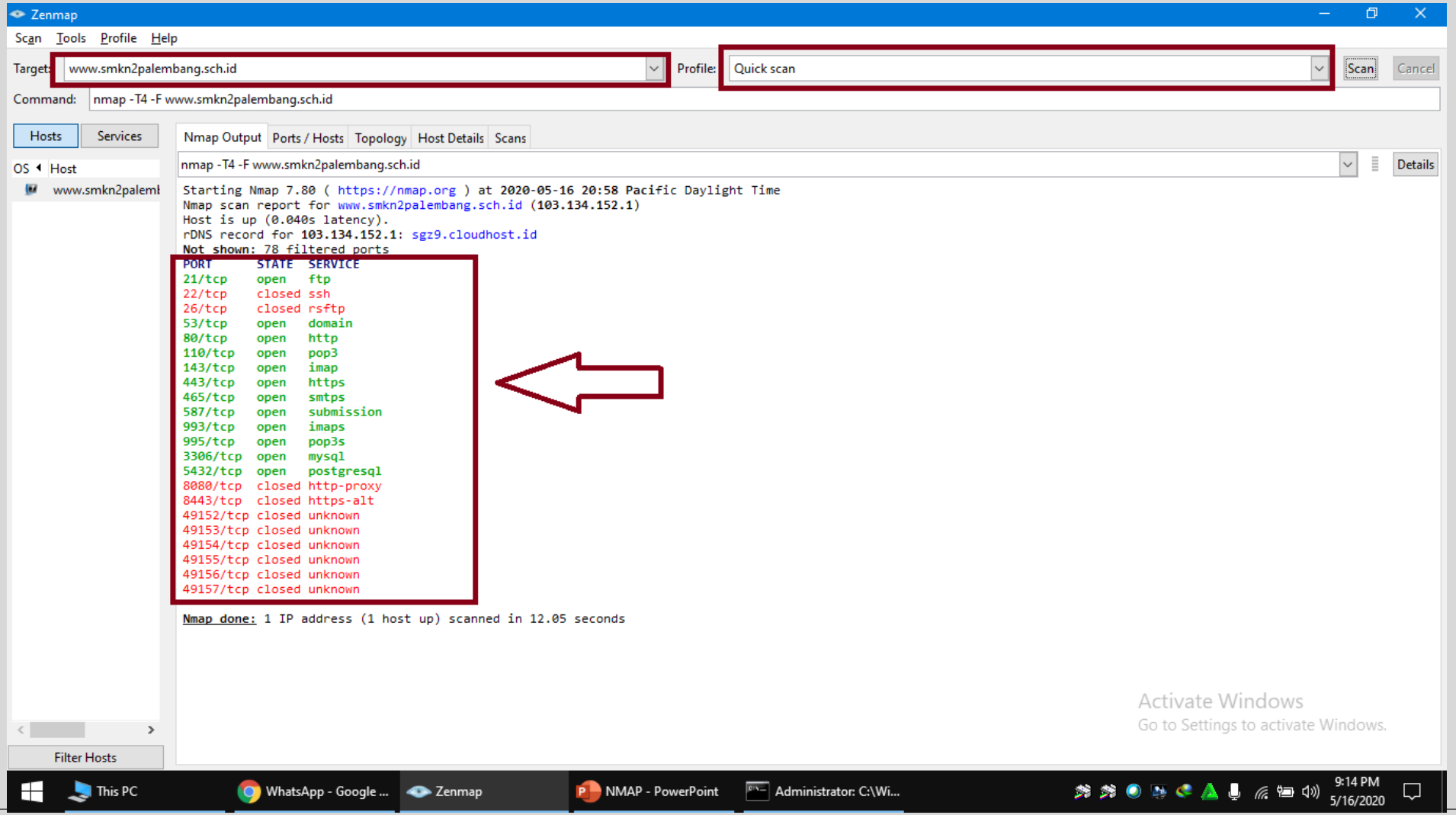
- Studi Kasus

  pada web SMK NEGERI 2 Palembang

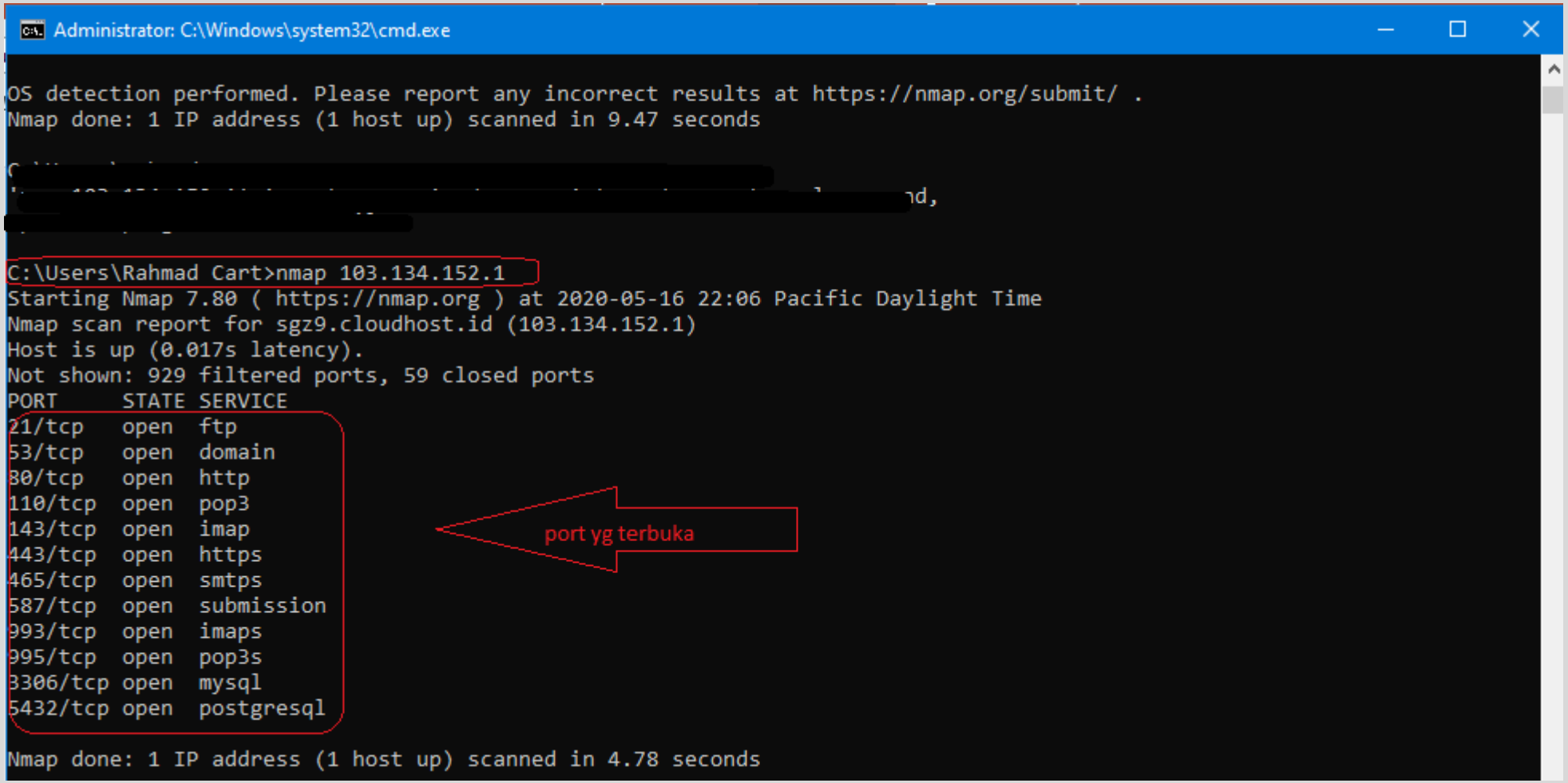
  www.smkn2palembang.sch.id

- Atau ip addres 103.134.152.1

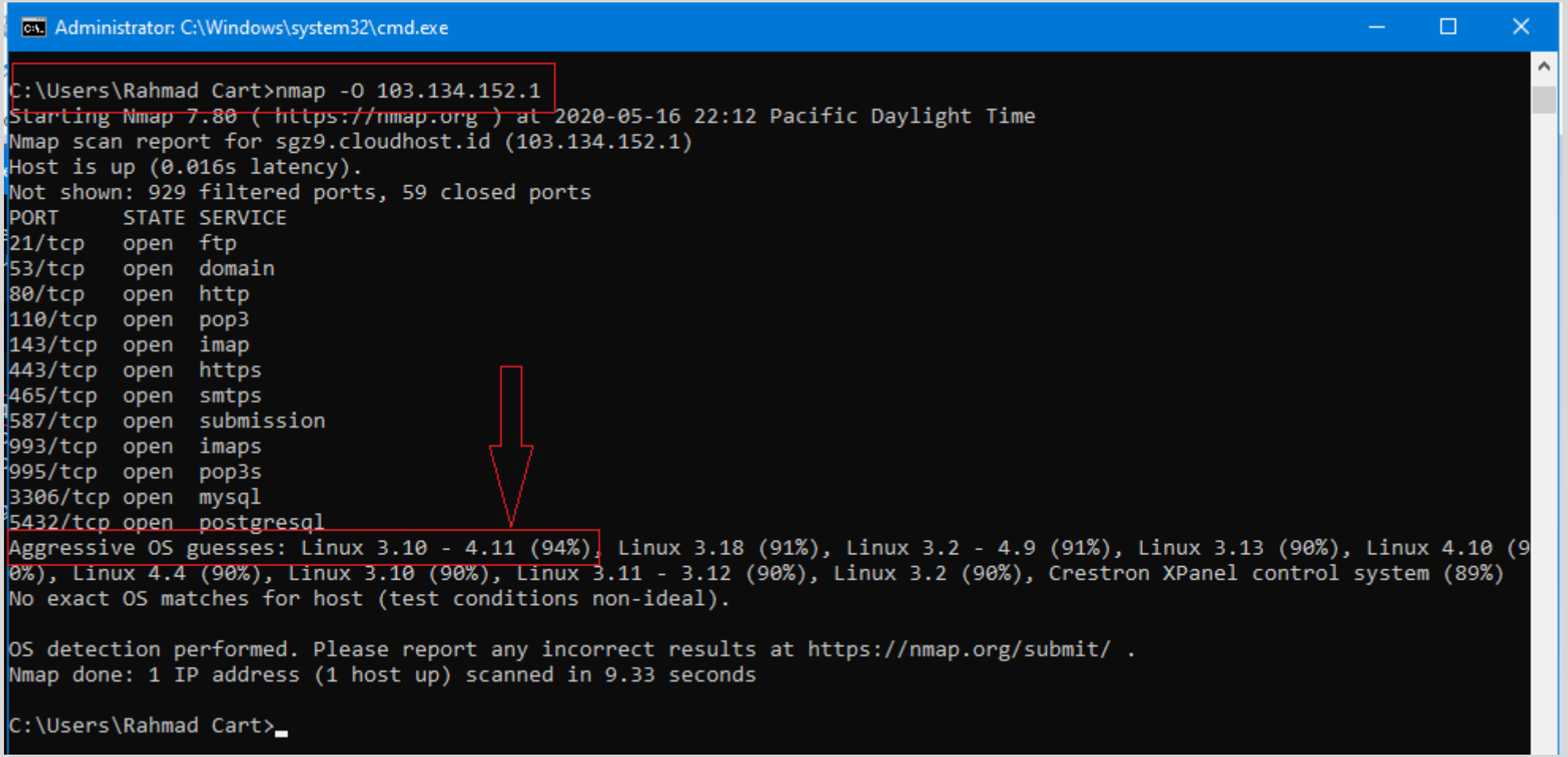
Pertama kita scan pada web smkn2palembang.sch.id
seperi gambar di bwah ini



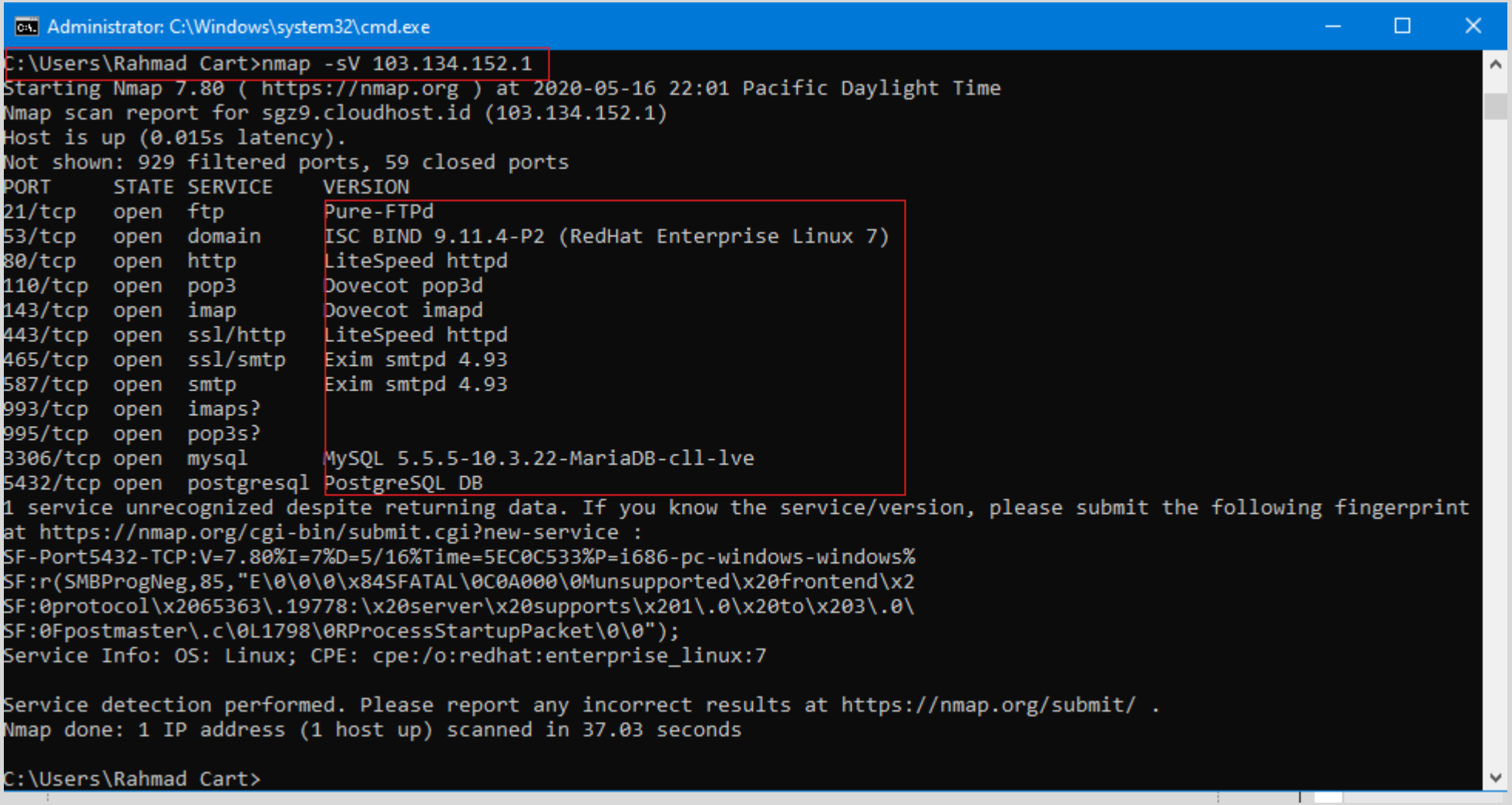
- Langkah selanjutnya Kita scaning mengunakan ip address 103.134.152.1
-



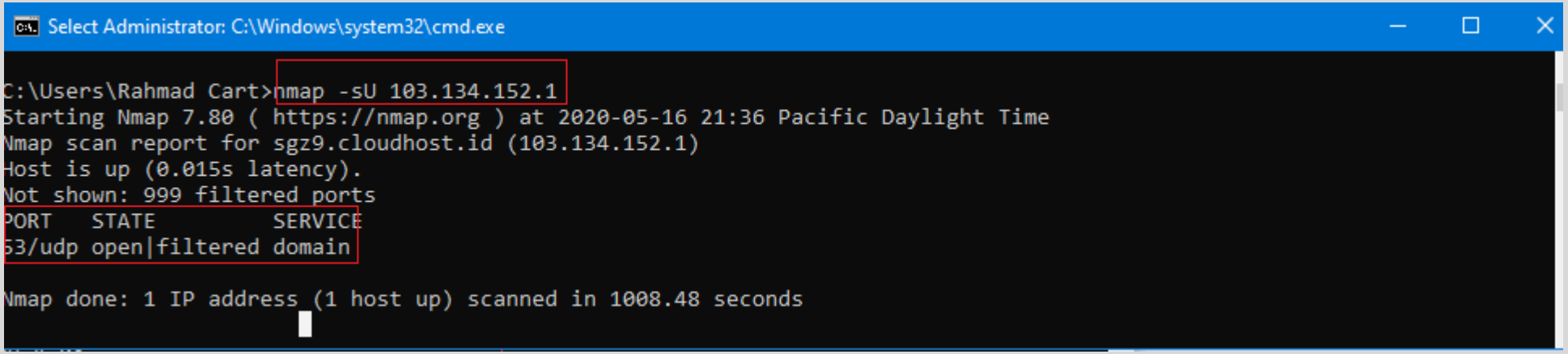
- Langkah selanjutnya kita akan melihat operstion system yg berjalan pada web tersebut mengguanakan perintah “nmap –O 103.134.152.1



- Langkah selanjutnya kita akan versi packet yg berjalan pada packet atau web tersebut mengguanakan perintah “nmap –sV 103.134.152.1

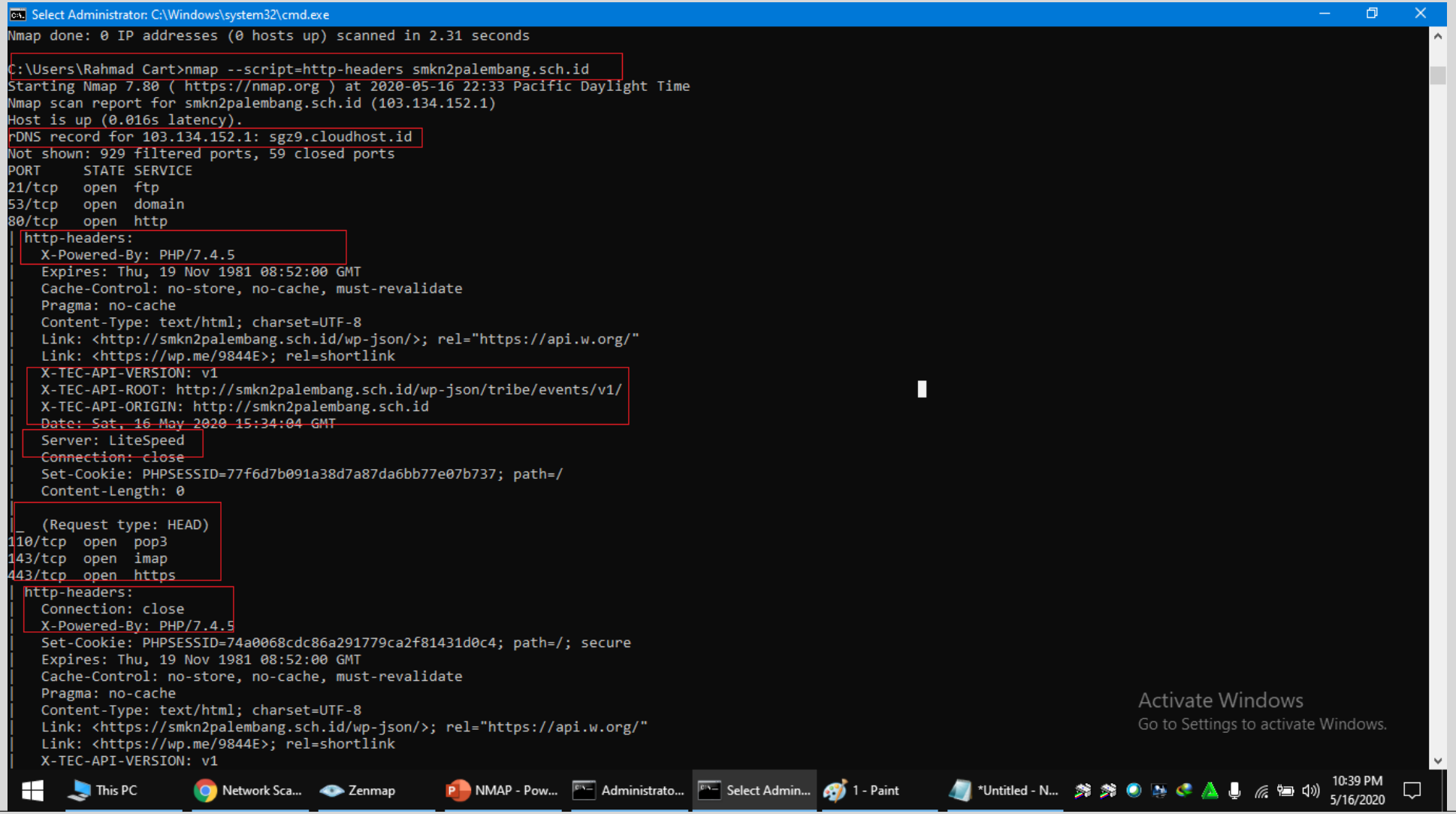


- Langkah selanjutnya kita akan mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP pada web mengguanakan perintah “nmap –sU 103.134.152.1



- Didapat openlfiltered yang berarti
- Nmap menganggap port dalam status ini bila ia tidak dapat menentukan apakah port open atau filtered. Hal ini terjadi untuk jenis pemeriksaan ketika port terbuka tidak memberi respon. Tidak adanya tanggapan dapat pula berarti bahwa packet filter men-drop probe atau respon yang diberikan. Sehingga Nmap tidak dapat mengetahui dengan tepat apakah port terbuka atau difilter. Scan UDP, IP protocol, FIN, NULL, dan Xmas mengklasifikasikan port dengan cara ini.

- Langkah selanjutnya kita akan mengidentifikasi header http pada web menggunakan perintah “nmap --script=http-headers smkn2palembang.sch.id”



- TERIMAH KASIH

IT AUDIT SOFTWARE

Nama Kelompok :

1.Dhea Noranita Putri (182420112)
2.Reynaldi (182420111)
3.Dini Rahmadia (182420134)
4.Mezi Puspayani (182420120)

MTI REG B 2019
Magister Tehnik Informatika
Universitas Bina Darma
Palembang

Apa itu Nessus ?

- **Nessus** *dibuat oleh Renaud Deraison pada tahun 1998. Nessus adalah* salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan.
- Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem. Sebelum Nessus versi 3, aplikasi ini bersifat open source dan menjadi salah satu primadona di dunia open source. Namun sekarang mulai Nessus versi 3 oleh Teenable Security dijadikan sebagai aplikasi propietary dan closed source

Fitur – fitur yang dimiliki Nessus :

1. Plug-in architecture
   Setiap security test ditulis sebagai external plugin. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca kode dari nessusd engine.
2. NASL (Nessus Attack Scrpiting Language)
   NASL adalah sebuah bahasa yang didesain untuk menulis program security test dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulils program security test.
3. Up-to-date security vulnerability database.

Fitur – fitur yang dimiliki Nessus :

4. Client-sever architecture
   Nessus security scanner terdiri dari dua bagian yaitu: sebuah server yang
   berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagai
   frontend. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari
   fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC,
   dengan server yang melakukan serangan ke jaringan yang dituju.
5. Dapat mengetes jumlah host yang banyak dalam waktu yang sama.
6. Smart service recognation.
   Nessus tidak mempercayai host yang dituju menggunakan port standar yang
   ditentukan oleh IANA. Ini berarti Nessus dapat mengenali sebuah Web server
   yang berjalan pada port yang bukan merupakan port standar (contohnya pada port8080), atau sebuah FTP server yang berjalan pada port 31337.

Fitur – fitur yang dimiliki Nessus :

7. Multiple Services
   Apabila ada dua buah Web server pada host yang dituju maka Nessus akan mengetes kedua Web server tersebut.
8. Complete reports.
   Nessus tidak hanya memberi tahu kelemahan dari jaringan yang dituju tetapi juga memberikan cara yang dapat digunakan untuk mencegah the bad guy utnuk mengeksploitasi kelemahan dari jaringan dan juga memberikan level resiko dari setiap masalah yang ditemukan.
9. Exportable reports.
   Unix client dapat mengekspor laporan sebagai Ascii text, HTML, LaTeX, dll.

Nessus dapat digunakan untuk melakukan audit sebagai berikut:

- Credentialed and un-credentialed port scanning.
- Network based vulnerability scanning.
- Credentialed based patch audits for Windows and most UNIX platforms.
- Redentialed configuration auditing of most Windows and UNIX platforms.
- Robust and comprehensive credentialed security testing of 3rd party applications.
- Custom and embedded web application vulnerability testing.
- SQL database configuration auditing.
- Software enumeration on Unix and Windows.
- Testing anti-virus installs for out-of date signatures and configuration errors.

Download Nessus :

- Kita bisa mendapatkan software nessus pada laman https://www.tenable.com/downloads/nessus?loginAttempted=true
- Website Resmi

http://www.tenable.com/products/nessus-vulnerability-scanner.

Kelebihan Nessus :

- Advanced vulnerability scanning dan configuration audit.
- Mampu mendeteksi process/program mencurigakan dan juga worms.
- Mampu melakukan multiple network scanning (IP, IPv6, Hybrid).
- Automatic scanning scheduler.
- Custom report & Notification.

Kekurangan Nessus :

- Sulit menemukan issue tertentu karna biasanya hasil scanningnya merupakan general case. Biasanya butuh versi profesional untuk fitur yang lebih baik.

Tutorial menginstal dan mengunakan Nessus :

- Anda dapat dapat mempelajari lewat video dari laman ini :

https://www.youtube.com/watch?v=35a0VhzIO2Y

- Anda juga dapat mempelajari langkah-langkanya dengan mendowload dari pdf berikut ini :

https://www.academia.edu/37659321/PROSES_AUDIT_SERVER_DENGAN_NESSUS

TERIMA KASIH

NMAP

KELOMPOK 2

- Nama Kelompok……..
  1. Rahmad Kartolo
- 2. Rio Permata
- 3.Muhammad Syahril
- 4.Yeni Gustini

- NMAP adalah singkatan dari *Network Mapper* yang merupakan sebuah *tool* atau alat yang bersifat *open source*. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan. Seseorang yang berjasa mengukirkan namanya sebagai penemu atau pencipta dari NMAP adalah Gordon Lyon

- FUNGSI NMAP?

- **1. Digunakan untuk memeriksa jaringan**
- Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada host tunggal. Cara kerjanya adalah dengan menggunakan IP raw yang berfungsi untuk menentukan mana host yang tersedia di dalam jaringan

- **2. Melakukan scanning pada port jaringan**
- Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer

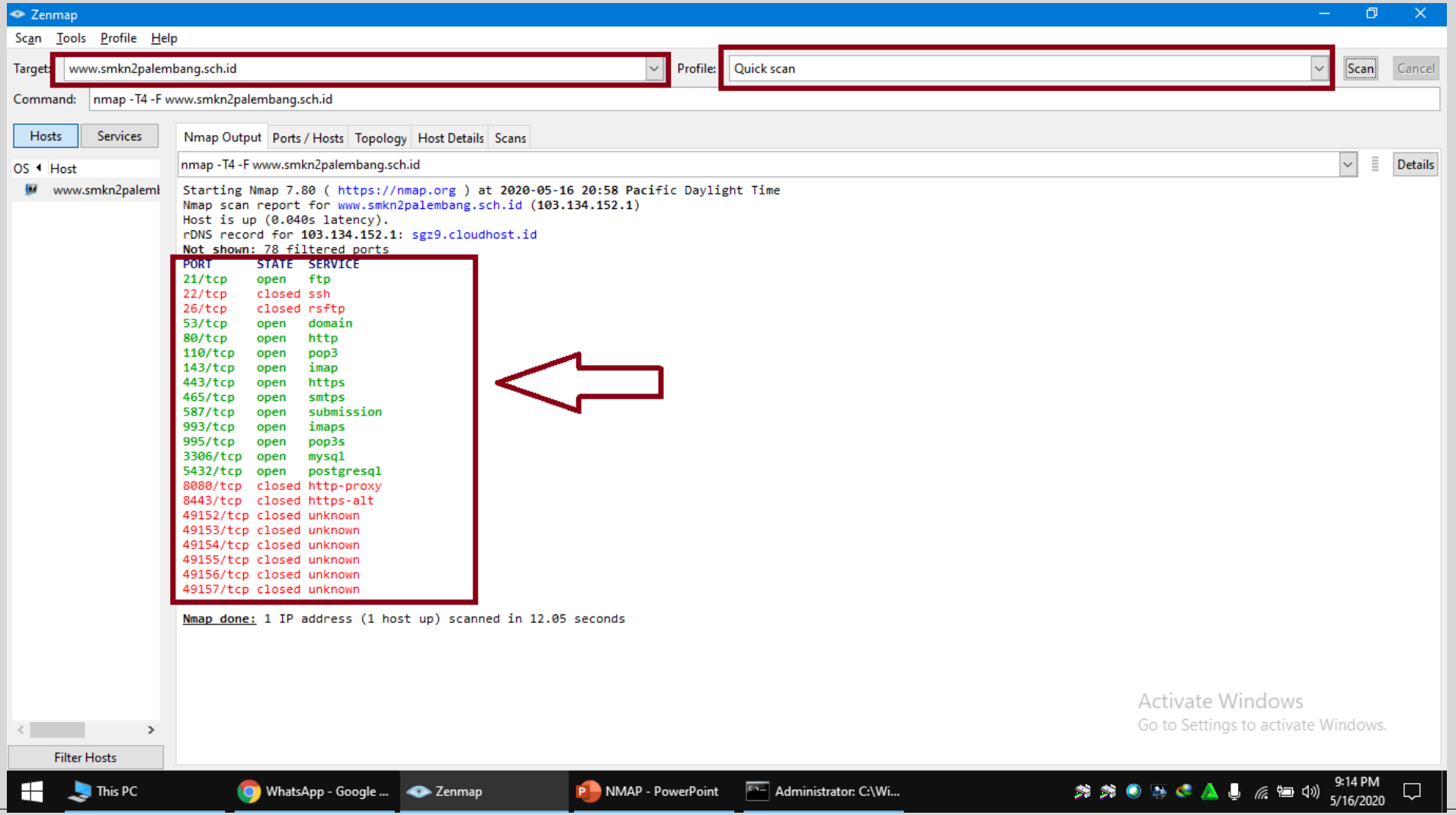
- Studi Kasus

  pada web SMK NEGERI 2 Palembang

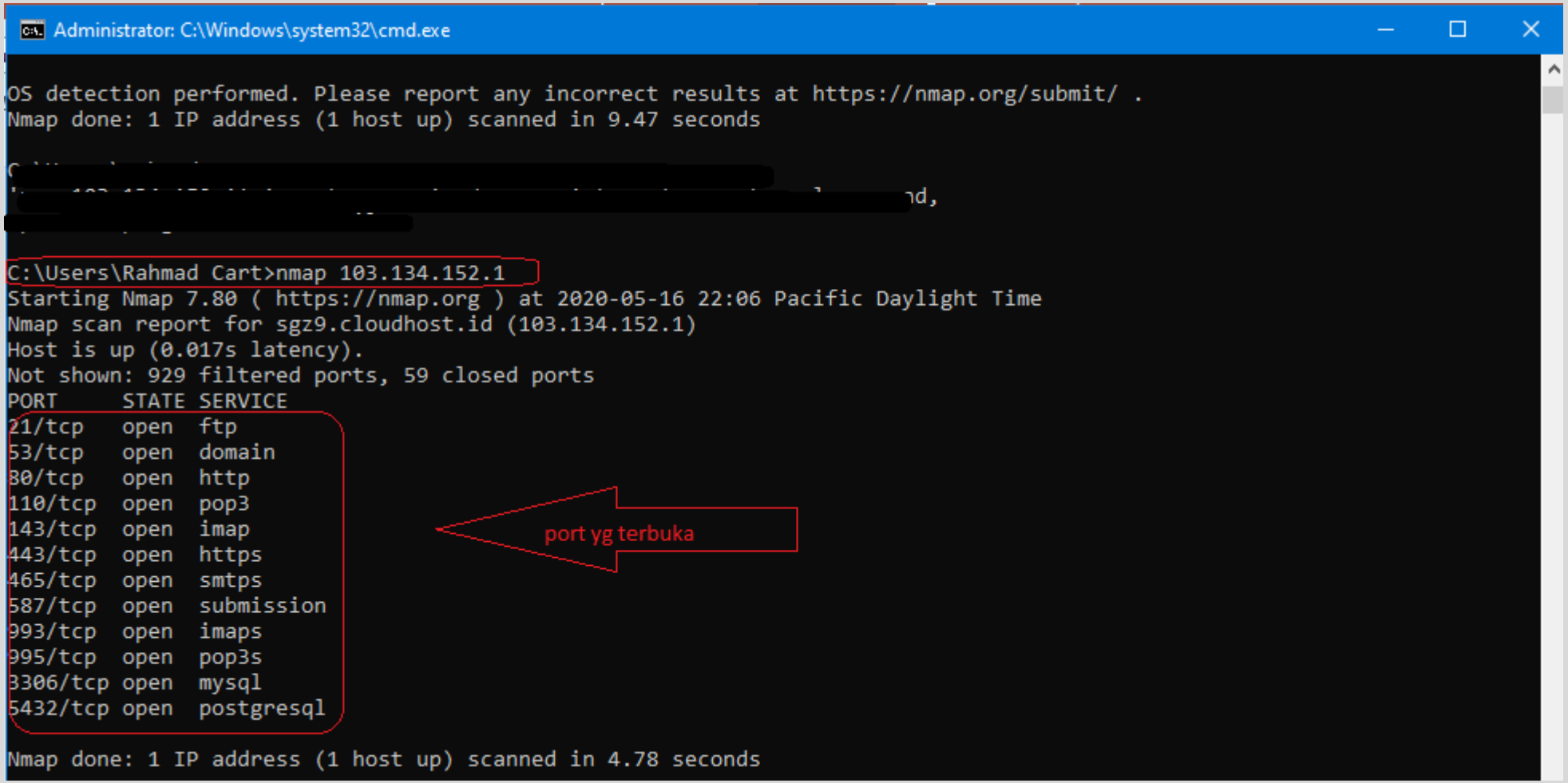
  www.smkn2palembang.sch.id

- Atau ip addres 103.134.152.1

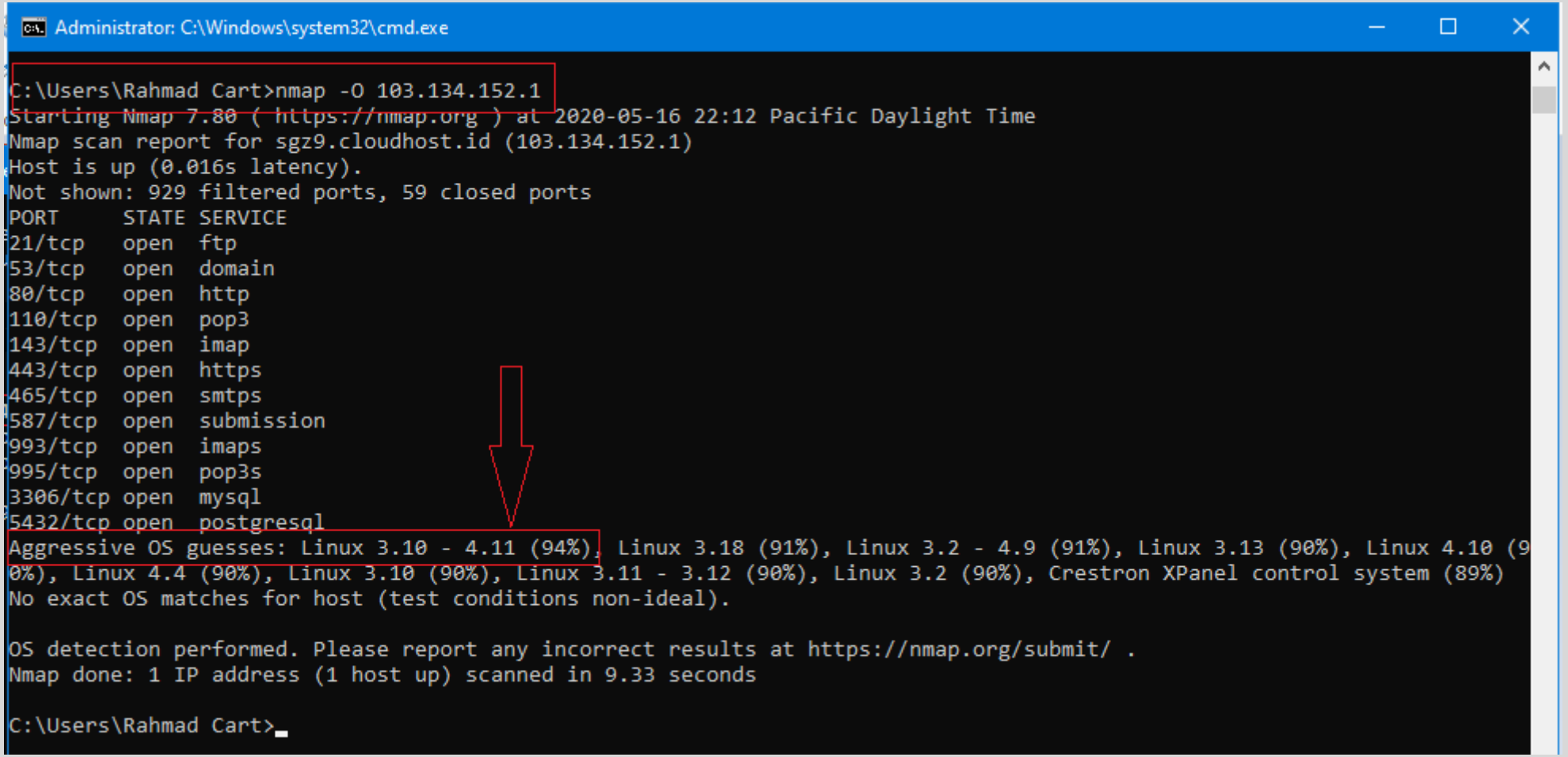
Pertama kita scan pada web smkn2palembang.sch.id
seperi gambar di bwah ini



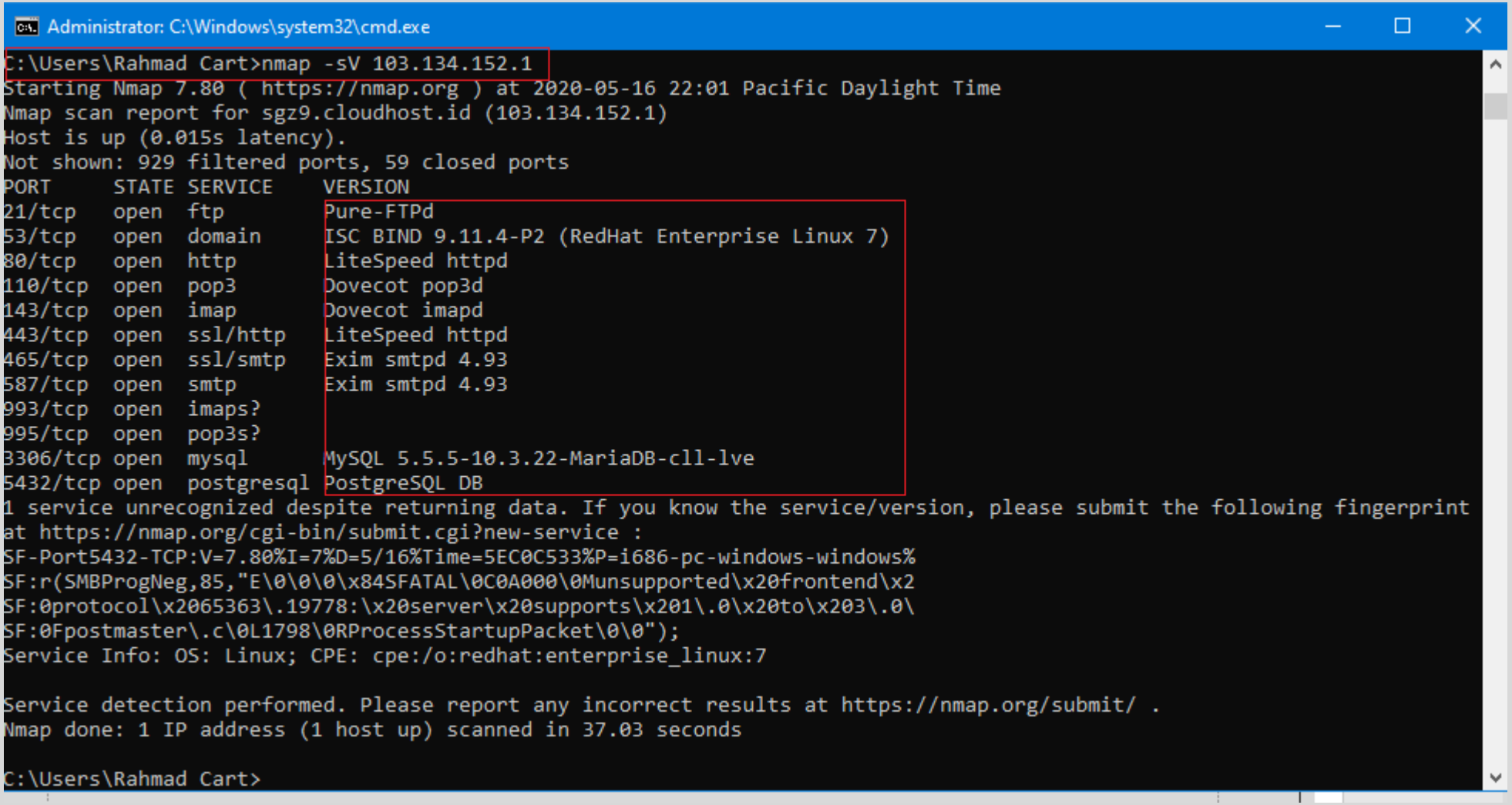
- Langkah selanjutnya Kita scaning mengunakan ip address 103.134.152.1
-



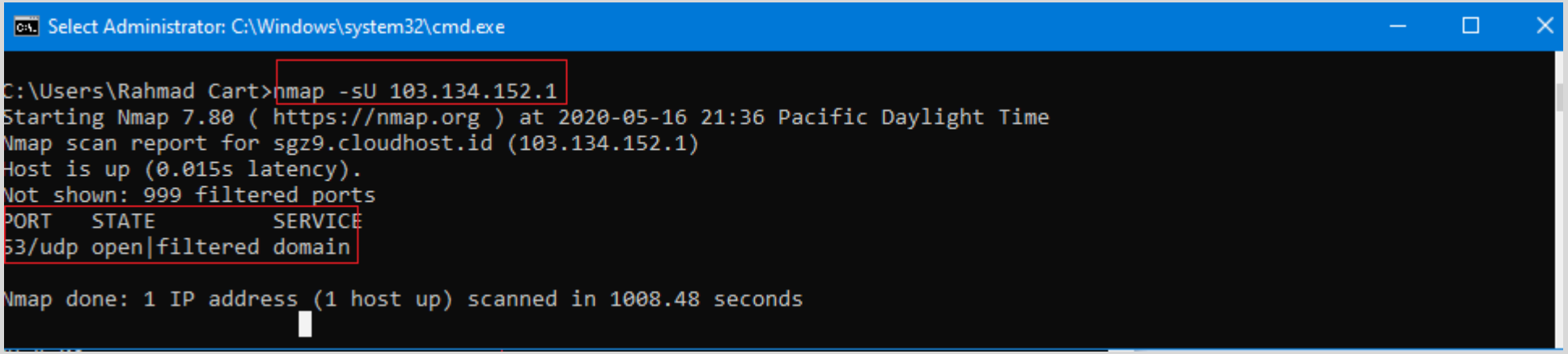
- Langkah selanjutnya kita akan melihat operstion system yg berjalan pada web tersebut mengguanakan perintah “nmap –O 103.134.152.1



- Langkah selanjutnya kita akan versi packet yg berjalan pada packet atau web tersebut mengguanakan perintah “nmap –sV 103.134.152.1

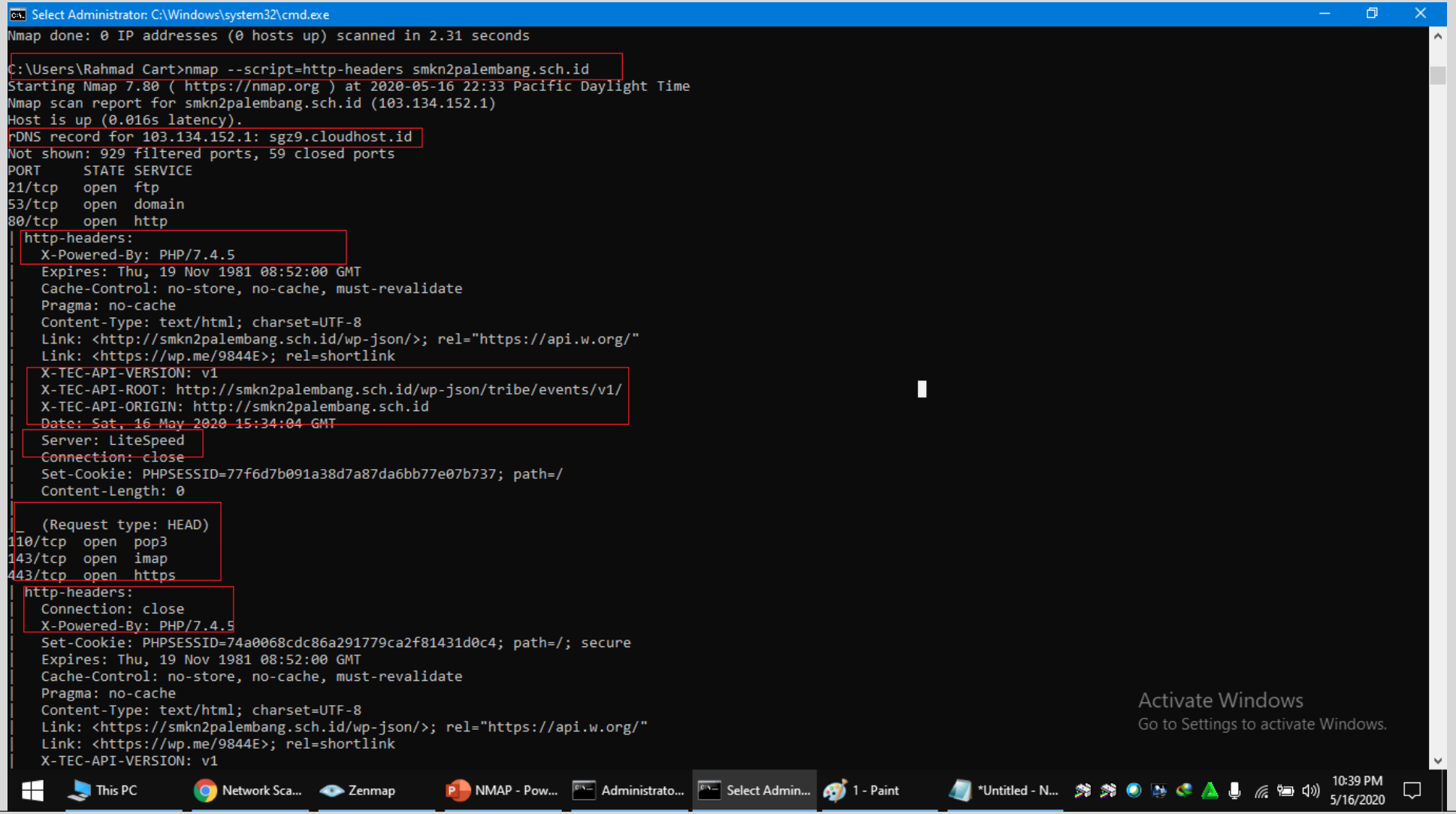


- Langkah selanjutnya kita akan mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP pada web mengguanakan perintah “nmap –sU 103.134.152.1



- Didapat openlfiltered yang berarti
- Nmap menganggap port dalam status ini bila ia tidak dapat menentukan apakah port open atau filtered. Hal ini terjadi untuk jenis pemeriksaan ketika port terbuka tidak memberi respon. Tidak adanya tanggapan dapat pula berarti bahwa packet filter men-drop probe atau respon yang diberikan. Sehingga Nmap tidak dapat mengetahui dengan tepat apakah port terbuka atau difilter. Scan UDP, IP protocol, FIN, NULL, dan Xmas mengklasifikasikan port dengan cara ini.

- Langkah selanjutnya kita akan mengidentifikasi header http pada web menggunakan perintah “nmap --script=http-headers smkn2palembang.sch.id”



- TERIMAH KASIH

NMAP

KELOMPOK 2

- Nama Kelompok……..
  1. Rahmad Kartolo
- 2. Rio Permata
- 3.Muhammad Syahril
- 4.Yeni

- NMAP adalah singkatan dari *Network Mapper* yang merupakan sebuah *tool* atau alat yang bersifat *open source*. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan. Seseorang yang berjasa mengukirkan namanya sebagai penemu atau pencipta dari NMAP adalah Gordon Lyon

- FUNGSI NMAP?

- **1. Digunakan untuk memeriksa jaringan**
- Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada host tunggal. Cara kerjanya adalah dengan menggunakan IP raw yang berfungsi untuk menentukan mana host yang tersedia di dalam jaringan

- **2. Melakukan scanning pada port jaringan**
- Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer

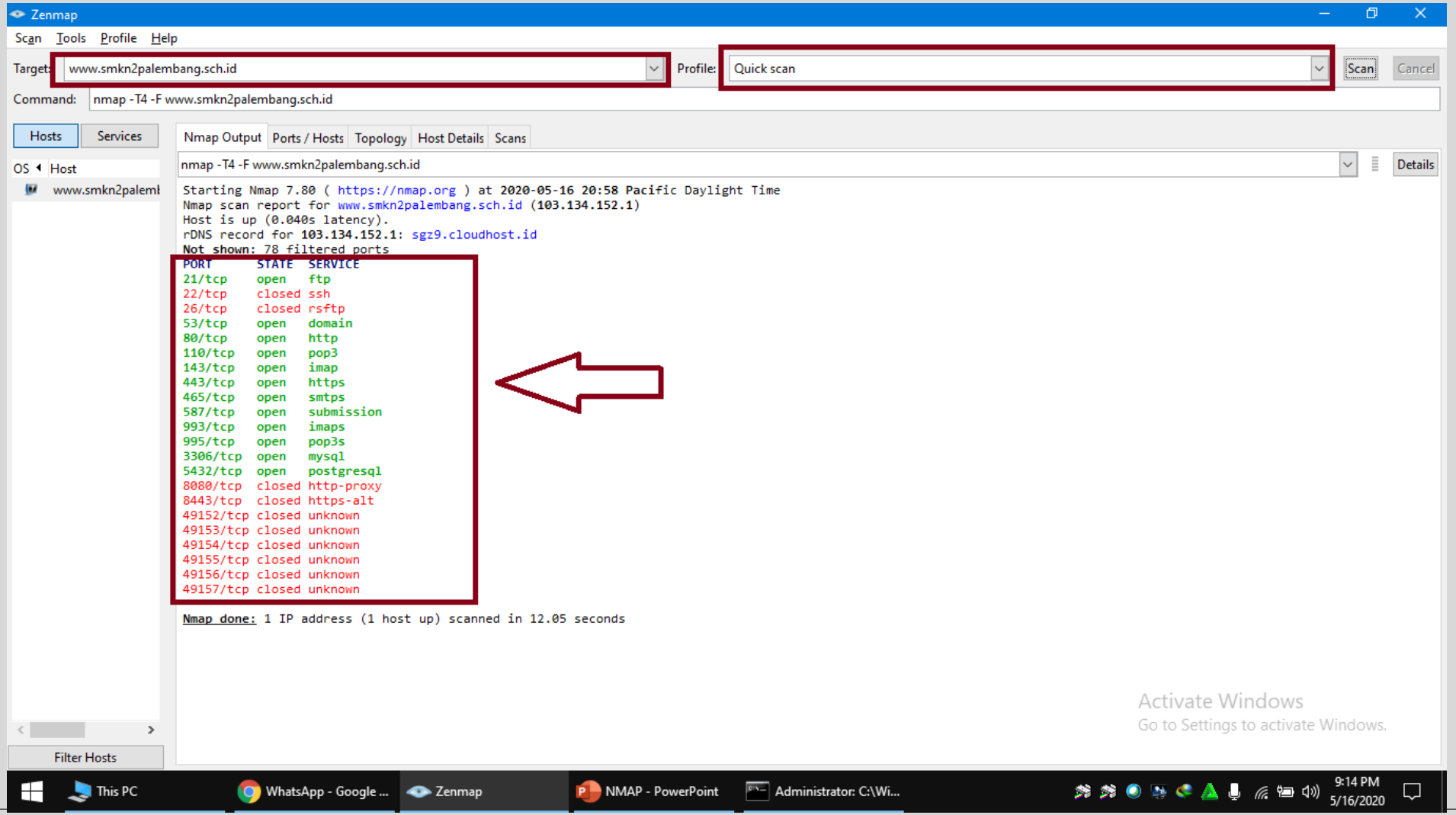
- Studi Kasus

  pada web SMK NEGERI 2 Palembang

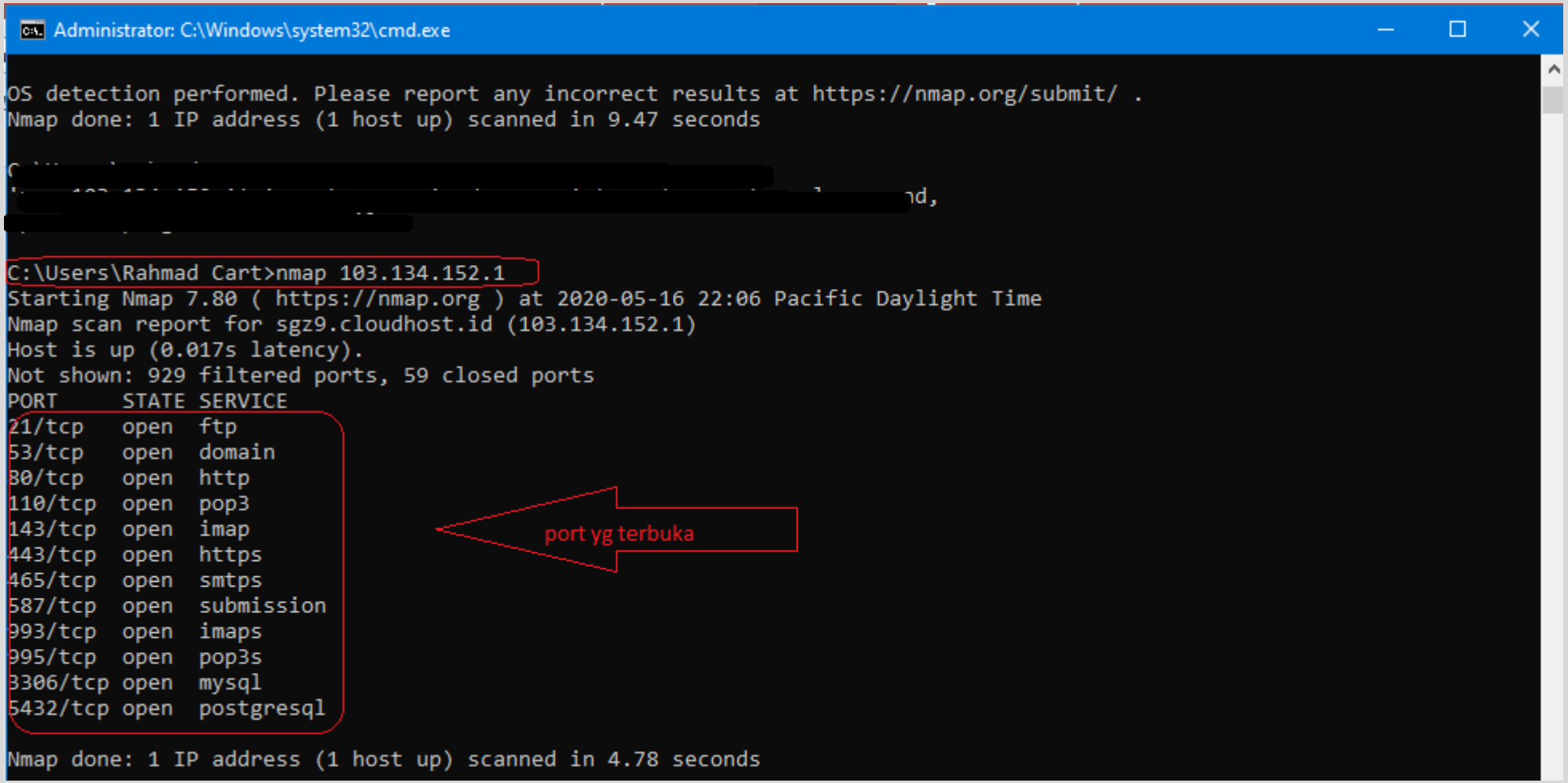
  www.smkn2palembang.sch.id

- Atau ip addres 103.134.152.1

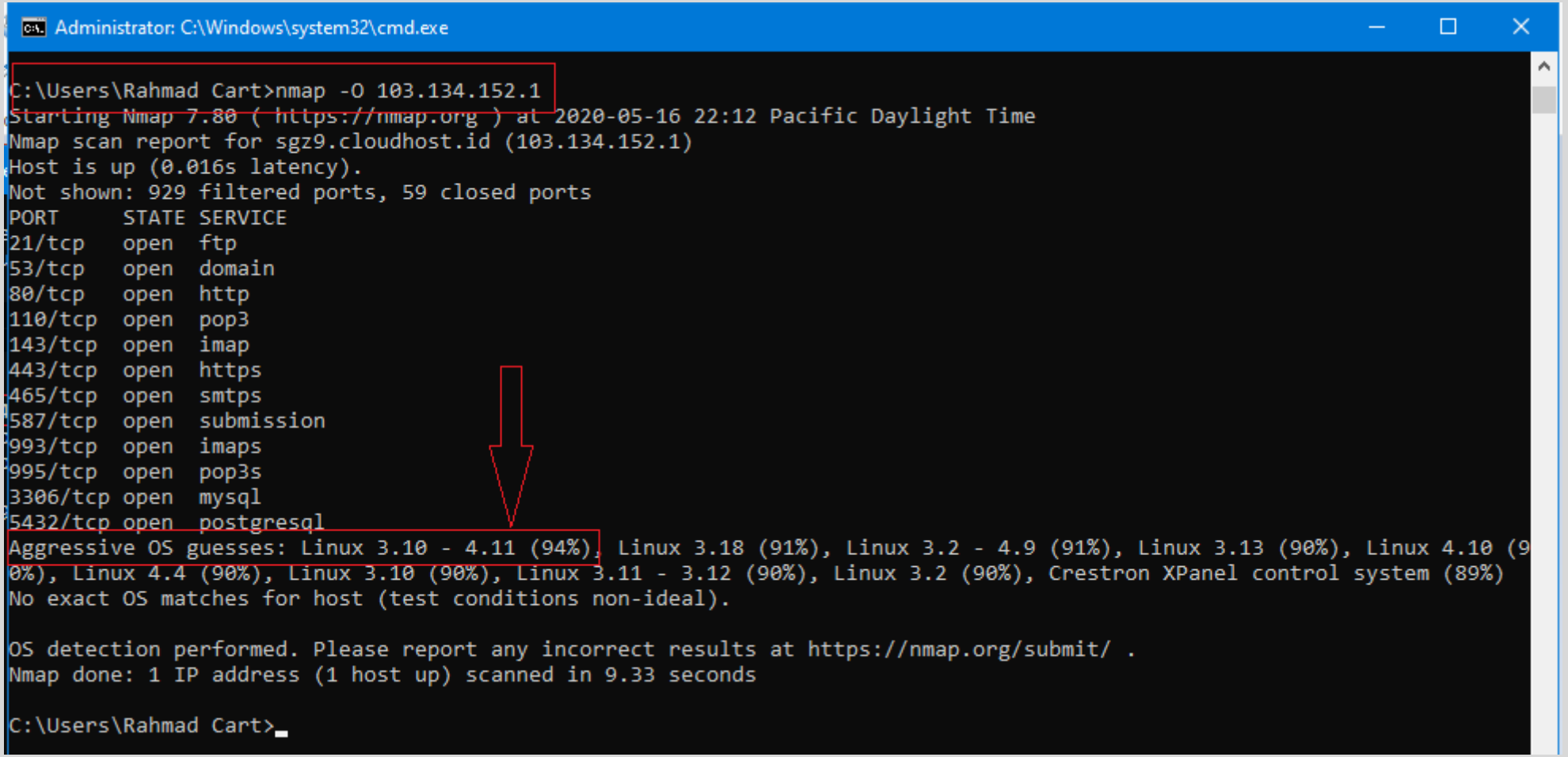
Pertama kita scan pada web smkn2palembang.sch.id
seperi gambar di bwah ini



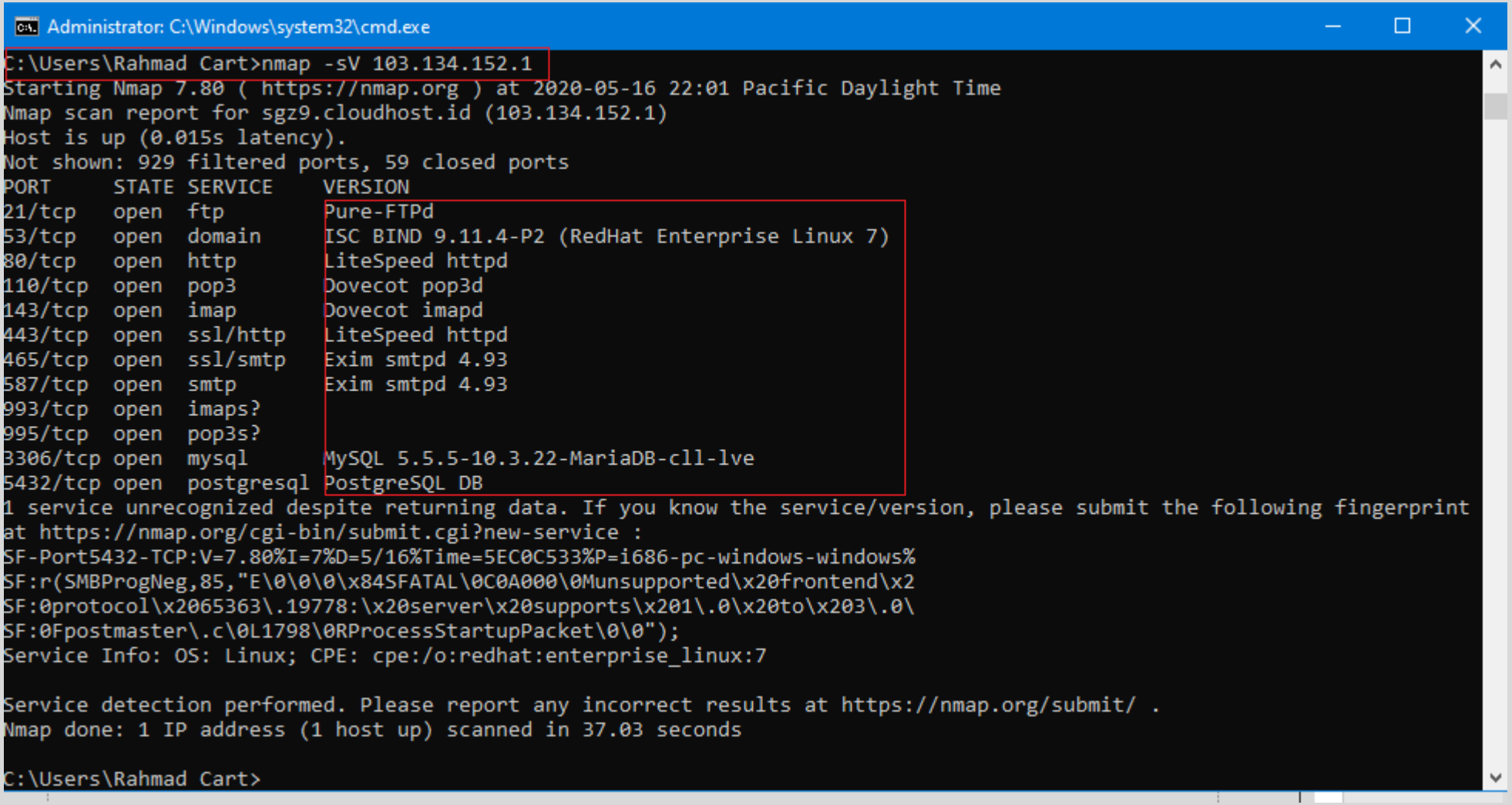
- Langkah selanjutnya Kita scaning mengunakan ip address 103.134.152.1
-



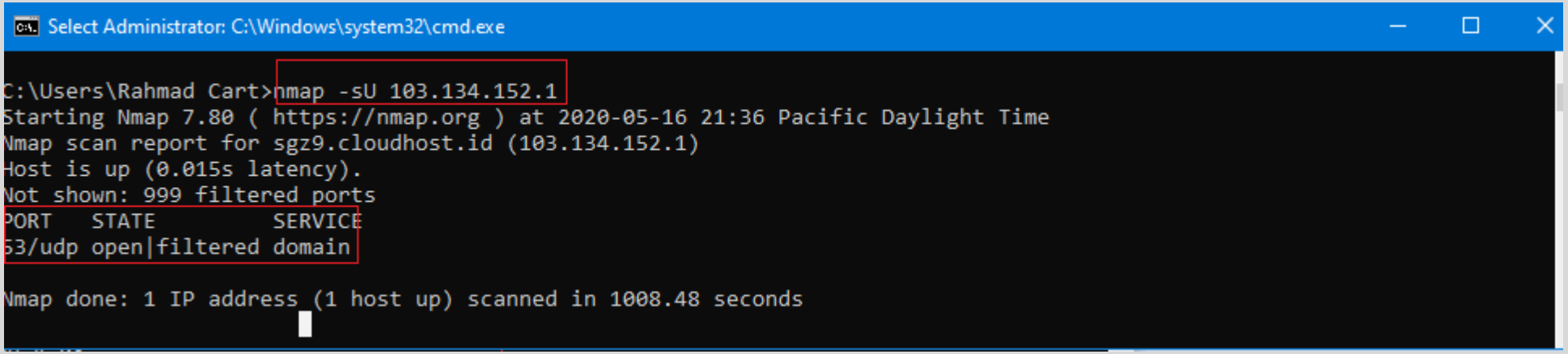
- Langkah selanjutnya kita akan melihat operstion system yg berjalan pada web tersebut mengguanakan perintah “nmap –O 103.134.152.1



- Langkah selanjutnya kita akan versi packet yg berjalan pada packet atau web tersebut mengguanakan perintah “nmap –sV 103.134.152.1

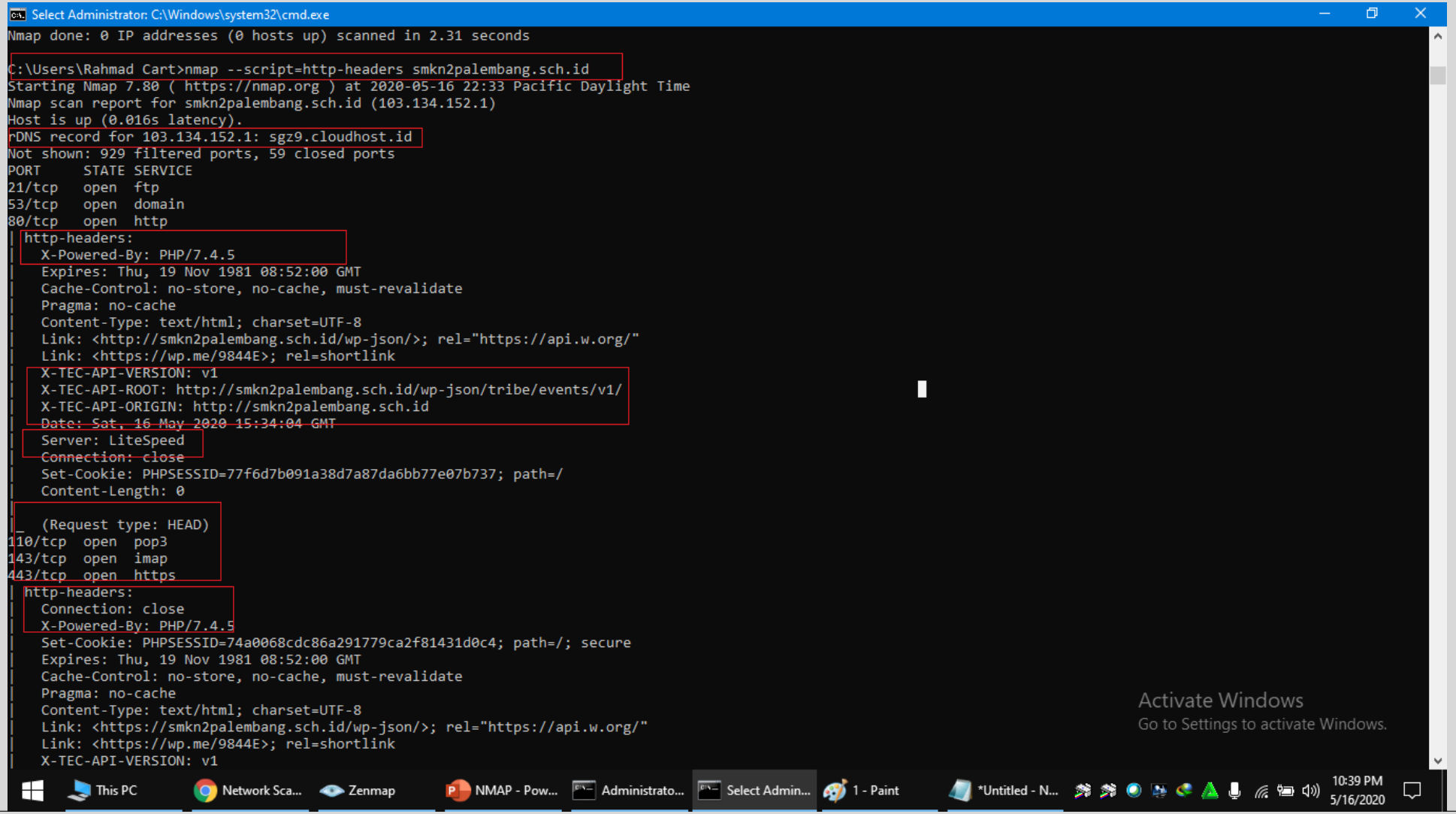


- Langkah selanjutnya kita akan mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP pada web mengguanakan perintah “nmap –sU 103.134.152.1



- Didapat openlfiltered yang berarti
- Nmap menganggap port dalam status ini bila ia tidak dapat menentukan apakah port open atau filtered. Hal ini terjadi untuk jenis pemeriksaan ketika port terbuka tidak memberi respon. Tidak adanya tanggapan dapat pula berarti bahwa packet filter men-drop probe atau respon yang diberikan. Sehingga Nmap tidak dapat mengetahui dengan tepat apakah port terbuka atau difilter. Scan UDP, IP protocol, FIN, NULL, dan Xmas mengklasifikasikan port dengan cara ini.

- Langkah selanjutnya kita akan mengidentifikasi header http pada web menggunakan perintah “nmap --script=http-headers smkn2palembang.sch.id”



- TERIMAH KASIH

KELAS MTI.A 20 IT AUDIT

Nagios®

Kelompok :

1. Agus Wiranto 182420102
2. Yudustira Sira Permana 182420104

Universitas Bina Darma

Apa itu Nagios?

Nagios merupakan sebuah system dan aplikasi pemantauan jaringan yang diciptakan oleh Ethan Galstad (http://nagios.org) dan pertama diluncurkan tahun 1999. Nagios mengawasi host-host dan servis yang telah ditetapkan, memberi peringatan jika keadaan memburuk, dan memberi tahu kapan keadaan tersebut membaik. Nagios dijalankan dalam Linux.

Kebutuhan awal sebelum instalasi Nagios yaitu Web Server (apache), PHP (php 5), Net-SNMP.

Nagios merupakan salah satu Network Monitoring System yang bekerja berdasarkan konsep SNMP (Simple Network Management Protocol) pada pengumpulan informasi statistik jaringan. Proses pengambilan data (lewat SNM Patau skrip) sampai kepada pembuatan grafik dilakukan menggunakan Bahasa pemrograman PHP.

Tampilan Menu Utama Nagios

Tampilan setelah user name dan password dimasukkan adalah menu utama Nagios.

Nagios bisa memberitahukan sebuah peringatan awal tentang suatu masalah jaringan, seringkali memperbolehkan anda untuk merespon kepada masalah sebelum user punya kesempatan untuk mengadu.

Kelebihan Nagios

1. Pemantauan servis jaringan (SMTP, POP3, HTTP, NNTP, PING, dsb)
2. Pemantauan sumber host(load prosesor, penggunaan disk, dsb)
3. Desain plugin yang sederhana, yang mengijinkan pengguna untuk lebih mudah menggunakan pemeriksaan terhadap services.
4. Service cek yang parallel
5. Pemberitahuan ketika terjadi masalah pada servis atau host dan
6. Kemampuan untuk mendefinisikan kejadian yang ditangani selama servis/host berlangsung untuk mempermudah pemecahan masalah
7. Perputaran file log yang otomatis
8. Mendukung implementasi pemantauan dengan host yang berlebih
9. Web interface yangdinamis untukmelihat status network, urutanmasalah dan pemberitahuan, log dan file.

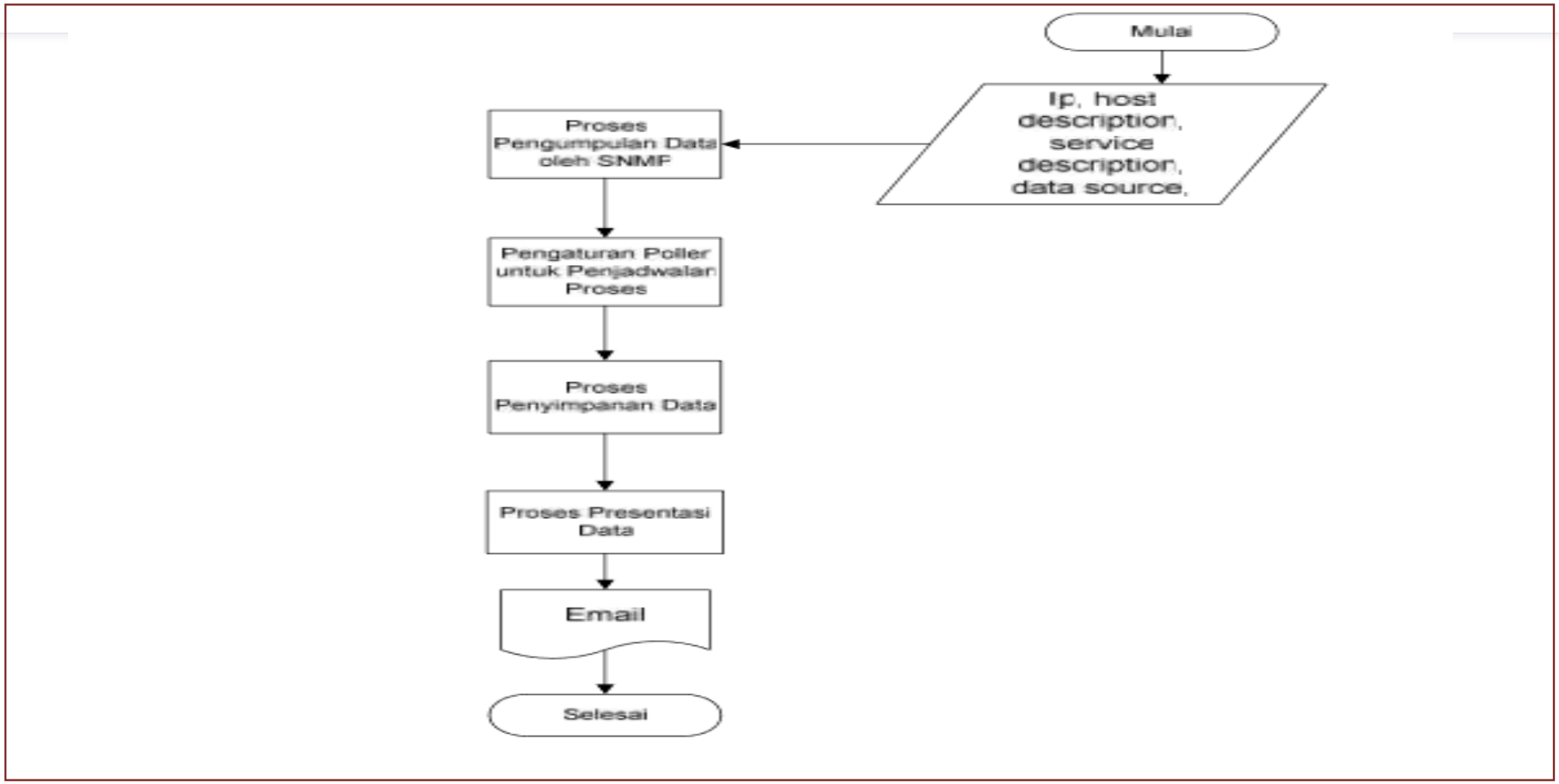
Notifikasi Nagios

Dalam perkembangannya, Nagios mampu memberikan keluaran dalam bentuk email. Email yang dihasilkan merupakan sebuah pesan peringatan akan adanya suatu kerusakan ataupun masalah dalam jaringan.

Nagios sebagai salah satun etwork monitroring system (NMS) memiliki kemampuan untuk mengumpulkan statistic jaringan secara akurat dalam suatu waktu. Nagios juga memiliki kemampuan untuk memberikan pesan peringatan disaat kondisi jaringan sedang bermasalah. Pesan peringatan tersebut dikirimkan dalam bentuk surat elektronik (electronic mail). Email yang dikirimkan kepada administrator berisi pesan peringatan akan adanya kesalahan pada jaringan, yang dalam hal ini terjadi apabila kondisi statistik jaringan pada suatu waktu melebihi nilai ambang batas yang telah ditetapkan.

Secara umum proses pemantauan oleh Nagios dapat dilihat pada gambar berikut.

Flowchart Proses Pengumpulan Statistik Jaringan Oleh Nagios



Perbandingannya bila Nagios menggunakan media SMS sebagai penyampai pesan notifikasi masalah jaringan adalah:

1. Fitur SMS sudah sangat familiar, penggunaannya pun mudah.
2. Reliabilitas dengan semua jenis HP tanpa terkecuali dan penggunaan pulsanya jauh lebih murah dibandingkan fitur lainnya seperti MMS (Multimedia Message Service).
3. Pengoperasian SMS relatif lebih mudah dan lebih cepat dibandingkan email

Kesimpulan

- Secara umum yang dilakukan oleh Nagios adalah mengumpulkan data. Data dikumpulkan dengan Poller yang dieksekusi oleh sistem operasi. Interval pengumpulan data atau dengan kata lain eksekusi Poller dapat diatur melalui fasilitas penjadwalan yang tersedia di sistem operasi. Data yang telah tersedia dihost atau remote target didapatkan dengan SNMP. Sehingga tiap perangkat yang dapat menjalankan fungsi SNMP (managed agents/nodes) dapat dipantau secara bersamaan oleh Nagios

References :

- https://docplayer.info/63016604-Nagios-sebagai-network-monitoring-software.html
- https://q2a-files.com/?q=materi+himpunan+kelas+7+smp+pdf+download

SEKIAN & TERIMA KASIH
KELOMPOK I

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

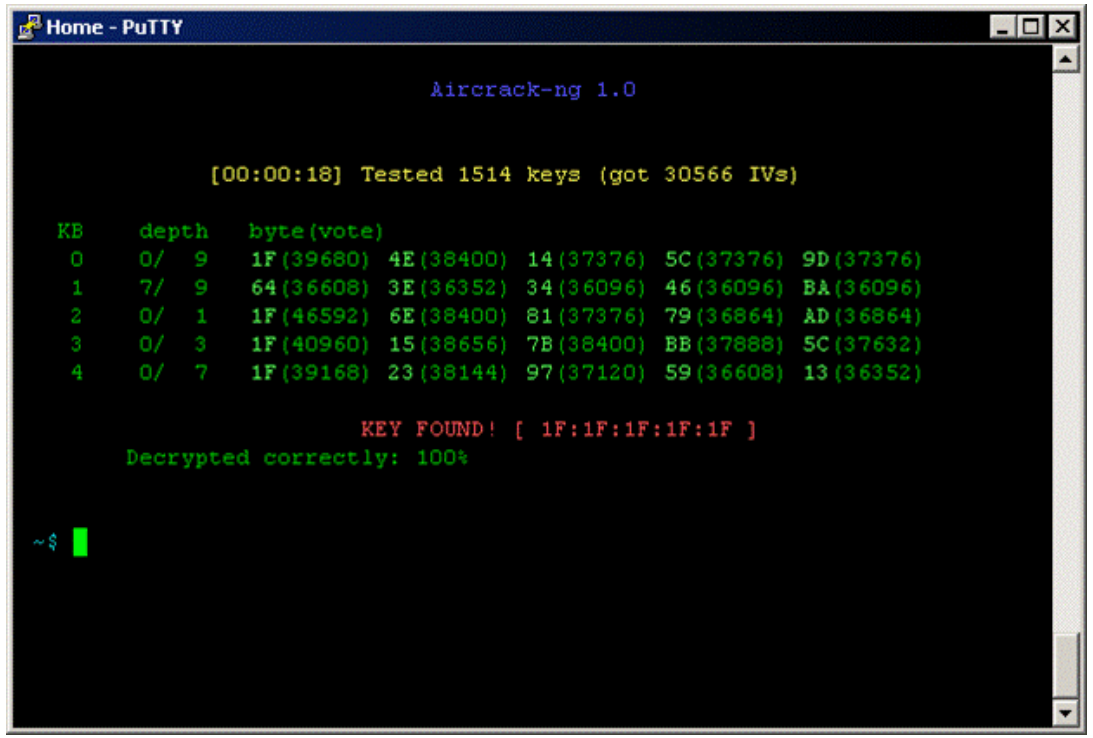
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIYANSAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

Program Pascasarjana
Magister Teknik Informatika
MTI – 20A

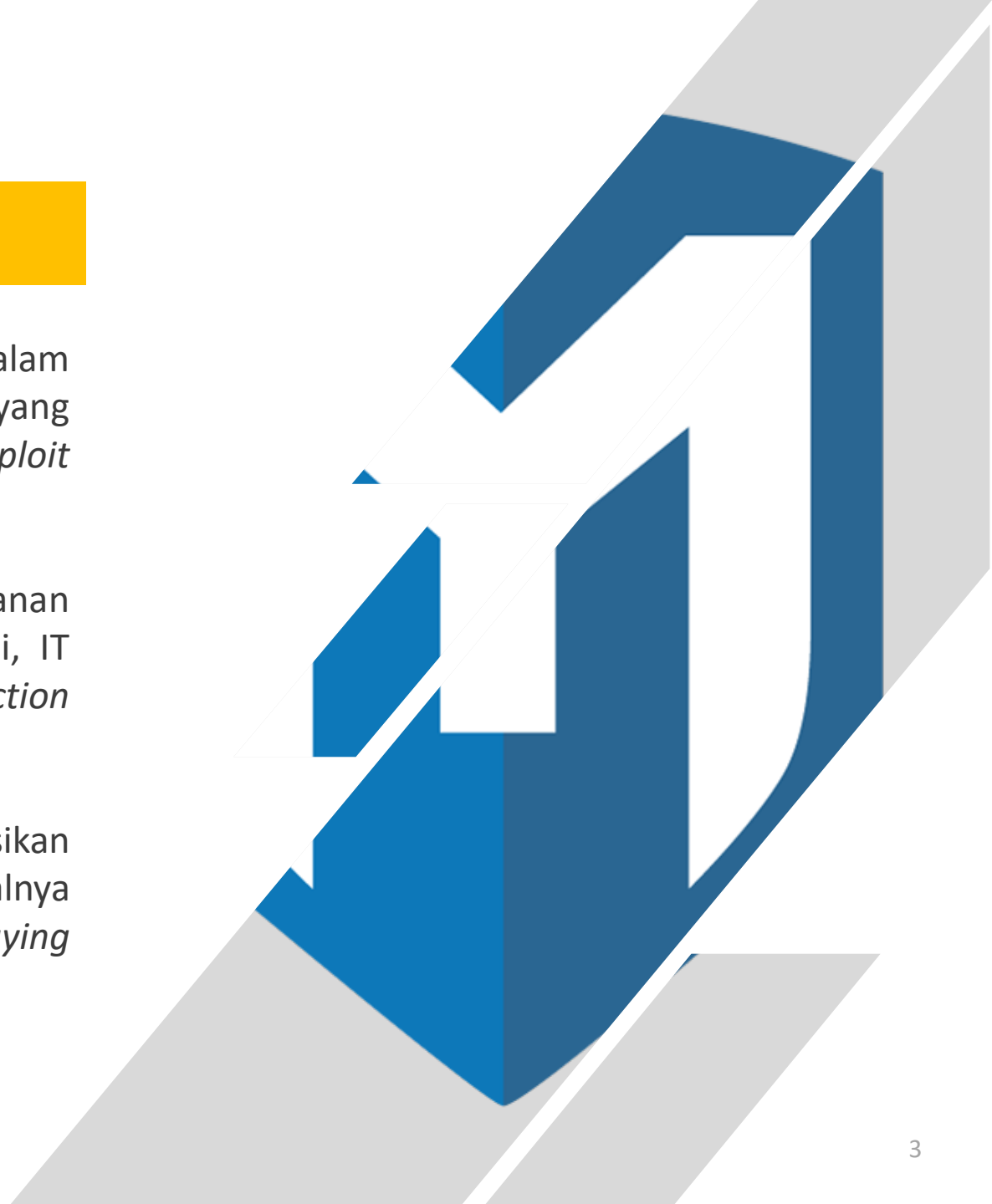
metasploit®

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.



TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

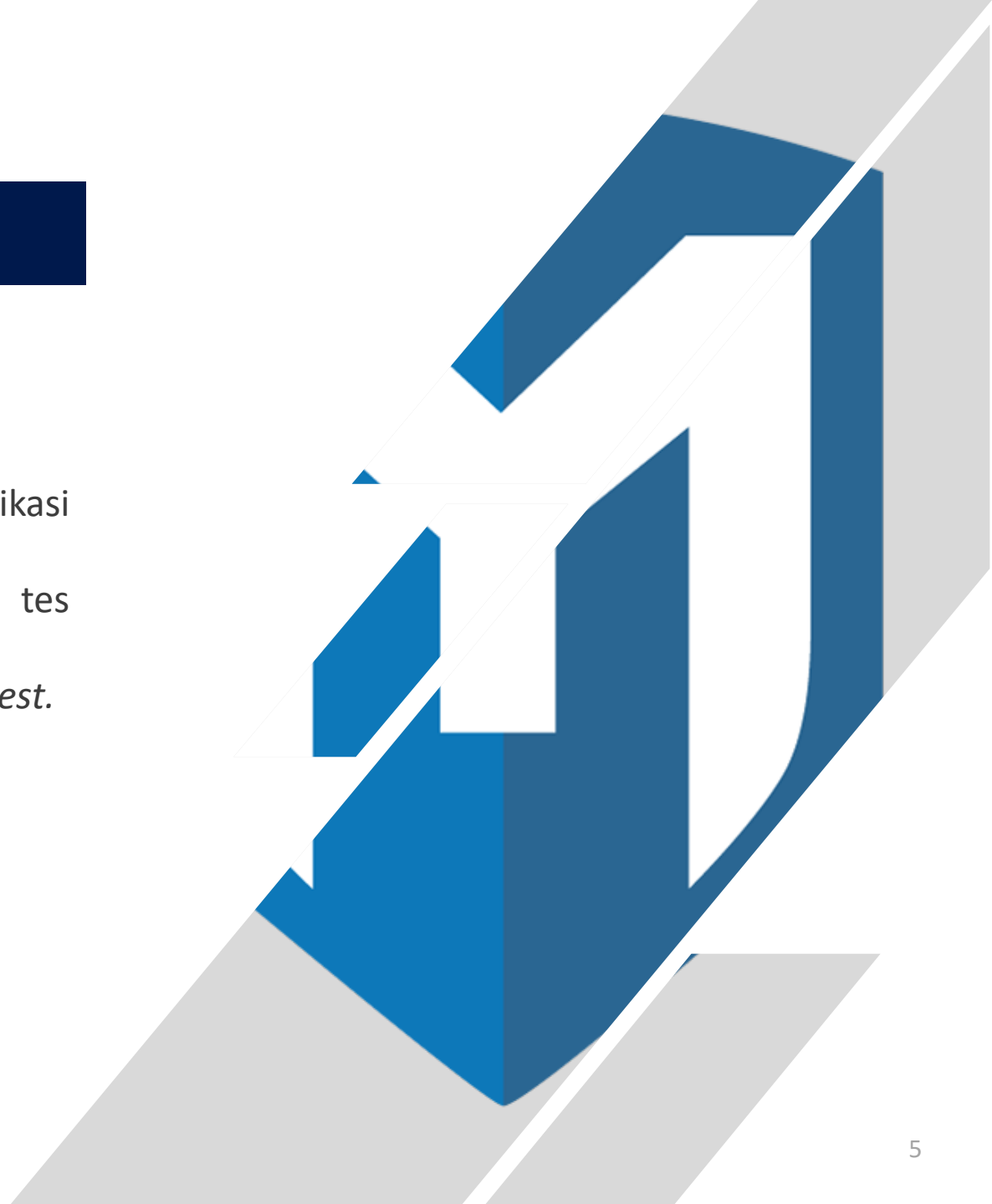
Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.



MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

KELAS MTI.A 20 IT AUDIT

Nagios®

Kelompok :

1. Agus Wiranto 182420102
2. Yudustira Sira Permana 182420104

Universitas Bina Darma

Apa itu Nagios?

Nagios merupakan sebuah system dan aplikasi pemantauan jaringan yang diciptakan oleh Ethan Galstad (http://nagios.org) dan pertama diluncurkan tahun 1999. Nagios mengawasi host-host dan servis yang telah ditetapkan, memberi peringatan jika keadaan memburuk, dan memberi tahu kapan keadaan tersebut membaik. Nagios dijalankan dalam Linux.

Kebutuhan awal sebelum instalasi Nagios yaitu Web Server (apache), PHP (php 5), Net-SNMP.

Nagios merupakan salah satu Network Monitoring System yang bekerja berdasarkan konsep SNMP (Simple Network Management Protocol) pada pengumpulan informasi statistik jaringan. Proses pengambilan data (lewat SNM Patau skrip) sampai kepada pembuatan grafik dilakukan menggunakan Bahasa pemrograman PHP.

Tampilan Menu Utama Nagios

Tampilan setelah user name dan password dimasukkan adalah menu utama Nagios.

Nagios bisa memberitahukan sebuah peringatan awal tentang suatu masalah jaringan, seringkali memperbolehkan anda untuk merespon kepada masalah sebelum user punya kesempatan untuk mengadu.

Kelebihan Nagios

1. Pemantauan servis jaringan (SMTP, POP3, HTTP, NNTP, PING, dsb)
2. Pemantauan sumber host(load prosesor, penggunaan disk, dsb)
3. Desain plugin yang sederhana, yang mengijinkan pengguna untuk lebih mudah menggunakan pemeriksaan terhadap services.
4. Service cek yang parallel
5. Pemberitahuan ketika terjadi masalah pada servis atau host dan
6. Kemampuan untuk mendefinisikan kejadian yang ditangani selama servis/host berlangsung untuk mempermudah pemecahan masalah
7. Perputaran file log yang otomatis
8. Mendukung implementasi pemantauan dengan host yang berlebih
9. Web interface yangdinamis untukmelihat status network, urutanmasalah dan pemberitahuan, log dan file.

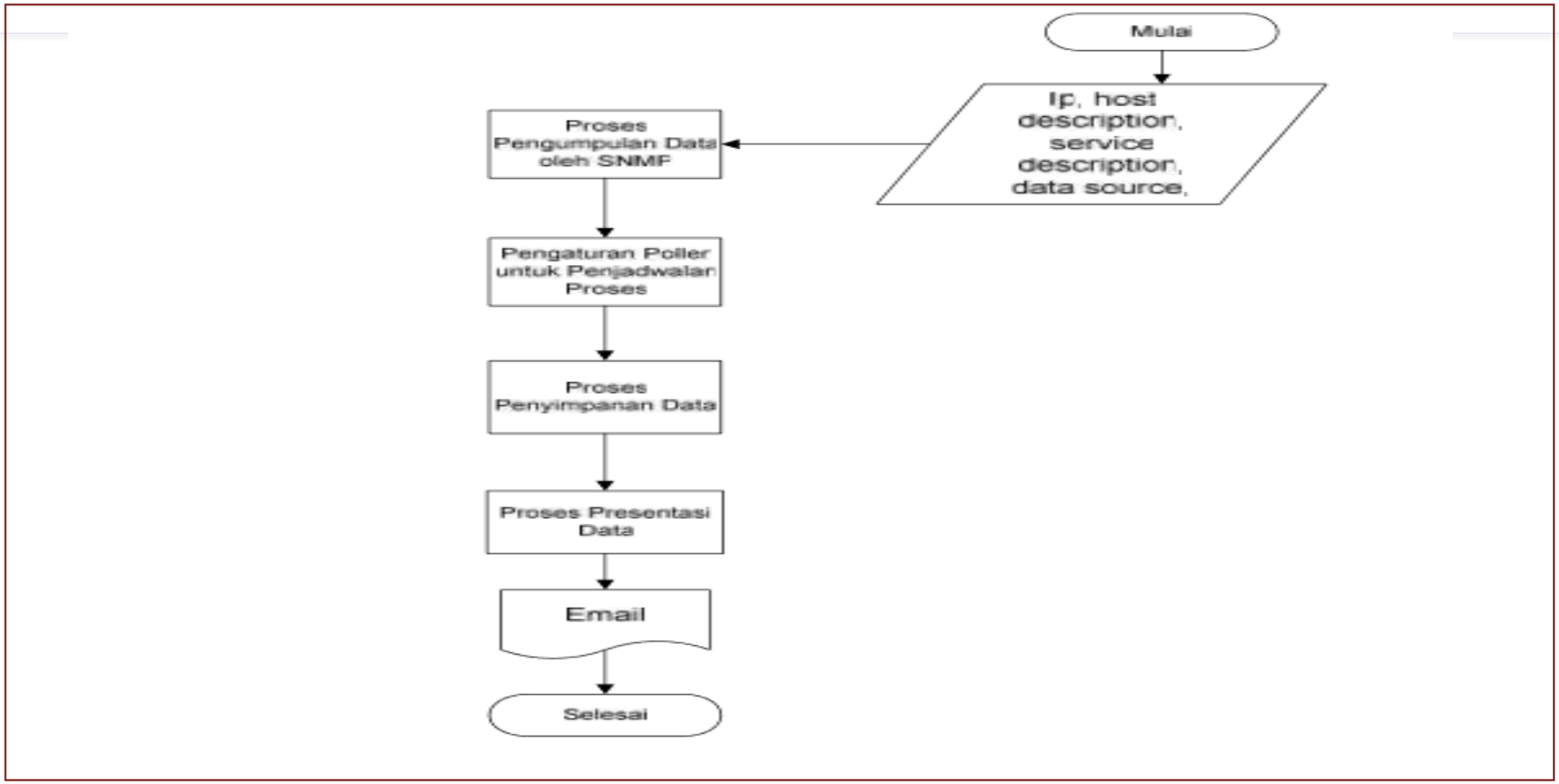
Notifikasi Nagios

Dalam perkembangannya, Nagios mampu memberikan keluaran dalam bentuk email. Email yang dihasilkan merupakan sebuah pesan peringatan akan adanya suatu kerusakan ataupun masalah dalam jaringan.

Nagios sebagai salah satun etwork monitroring system (NMS) memiliki kemampuan untuk mengumpulkan statistic jaringan secara akurat dalam suatu waktu. Nagios juga memiliki kemampuan untuk memberikan pesan peringatan disaat kondisi jaringan sedang bermasalah. Pesan peringatan tersebut dikirimkan dalam bentuk surat elektronik (electronic mail). Email yang dikirimkan kepada administrator berisi pesan peringatan akan adanya kesalahan pada jaringan, yang dalam hal ini terjadi apabila kondisi statistik jaringan pada suatu waktu melebihi nilai ambang batas yang telah ditetapkan.

Secara umum proses pemantauan oleh Nagios dapat dilihat pada gambar berikut.

Flowchart Proses Pengumpulan Statistik Jaringan Oleh Nagios



Perbandingannya bila Nagios menggunakan media SMS sebagai penyampai pesan notifikasi masalah jaringan adalah:

1. Fitur SMS sudah sangat familiar, penggunaannya pun mudah.
2. Reliabilitas dengan semua jenis HP tanpa terkecuali dan penggunaan pulsanya jauh lebih murah dibandingkan fitur lainnya seperti MMS (Multimedia Message Service).
3. Pengoperasian SMS relatif lebih mudah dan lebih cepat dibandingkan email

Kesimpulan

- Secara umum yang dilakukan oleh Nagios adalah mengumpulkan data. Data dikumpulkan dengan Poller yang dieksekusi oleh sistem operasi. Interval pengumpulan data atau dengan kata lain eksekusi Poller dapat diatur melalui fasilitas penjadwalan yang tersedia di sistem operasi. Data yang telah tersedia dihost atau remote target didapatkan dengan SNMP. Sehingga tiap perangkat yang dapat menjalankan fungsi SNMP (managed agents/nodes) dapat dipantau secara bersamaan oleh Nagios

References :

- https://docplayer.info/63016604-Nagios-sebagai-network-monitoring-software.html
- https://q2a-files.com/?q=materi+himpunan+kelas+7+smp+pdf+download

SEKIAN & TERIMA KASIH
KELOMPOK I

METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIE ANSYAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

Program Pascasarjana
Magister Teknik Informatika
MTI – 20A

metasploit®

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.

TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.

MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

KELAS MTI.A 20

Password cracking tools / Alat pemecahan kata password

Kelompok I :

1.	Moh. Rendy Septiyan	182420103
2.	Muhammad Angga Ok	182420123
3.	Erwin Satriyansah	182420110
4.	Agus Wiranto	182420102
5.	Moh Fajar Al Amin	182420121
6.	Adiktia	182420101
7.	Armansyah	182420105
8.	Ibnu Fajariadi	182420109
9.	Ydustira Sira Permana	182420104

Universitas Bina Darma

Apa password cracking?

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. **Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.**

Konsep Password cracking biasanya melakukan proses berulang-ulang di komputer dengan berbagai kombinasi password sampai pencocokan sama persis.

Password cracking tools/Alat peretas kata password merupakan bagian yang tidak dapat dipisahkan dari setiap rangkaian alat audit keamanan TI. Kami merekomendasikan AirCrack (nirkabel) dan Ophcrack (sistem).

Aircrack: Alat CrackingCepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

1. **Standardisasi IEEE 802.11a**

   Standard IEEE 802.11a bekerja pada frekuensi 5 GHz mengikuti standard dari UNII (Unlicensed National Information Infrastructure). Teknologi IEEE 802.11a tidak menggunakan teknologi spread-spectrum melainkan menggunakan standar frequency division multiplexing (FDM). Mampu mentransfer data hingga 54 Mbps

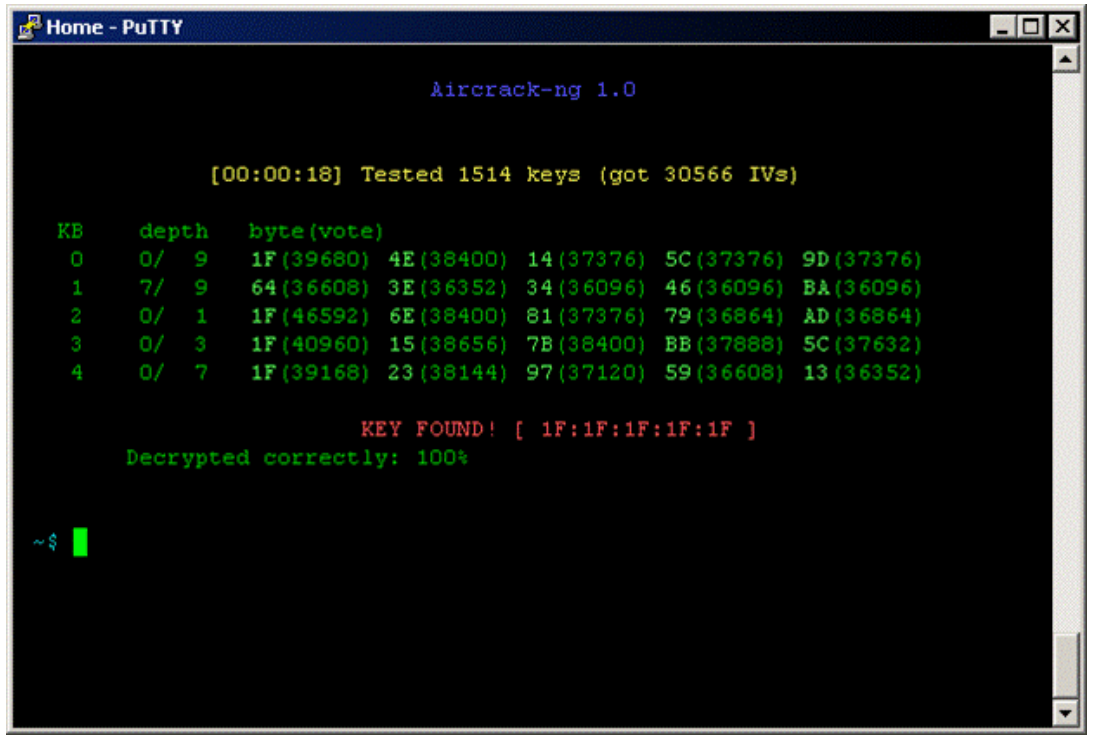
2. **Standardisasi IEEE 802.11b**

   Standar 802.11b saat ini yang paling banyak digunakan satu. Menawarkan thoroughput maksimum dari 11 Mbps (6 Mbps dalam praktik) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia. Transmisi data 5,4 hingga 11 Mbps

3. **Standardisasi IEEE 802.11g**

   Standar 802.11g menawarkan bandwidth yang tinggi (54 Mbps throughput maksimum, 30 Mbps dalam praktik) pada rentang frekuensi 2,4 GHz. Standar 802.11g mundur-kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b

Pada dasarnya ini mengumpulkan dan menganalisa paket-paket yang dienkripsi kemudian menggunakan berbagai alat yang retas password dari paket-paket.



Fitur dari Aircrack

- Mendukung dengan Brute force dan Kamus serangan retak teknik
- Tersedia untuk Windows dan Linux (Meskipun aircrack tersedia untuk Windows tetapi ada isu-isu yang berbeda dengan software ini jika kita menggunakan ini dalam lingkungan Windows, jadi terbaik ketika kita menggunakannya di lingkungan Linux)
- Tersedia dalam live CD
- **Situs untuk Download:**
- http://www.aircrack-ng.org/

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Situs untuk Download:

http://Ophcrack.SourceForge.net/

References :

- https://www.computerweekly.com/photostory/2240149679/11-security-audit-essentials/12/11-Password-cracking-tools
- http://id.wondershare.com/password/password-cracker-tools.html
- https://id.wikipedia.org/wiki/IEEE_802.11
- https://id.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- http://www.aircrack-ng.org/
- http://Ophcrack.SourceForge.net/

SEKIAN & TERIMA KASIH
KELOMPOK I

Nama : Caesario Rian Saputra

Nim : 182420131

Review It Audit tools ACL (Audit Comand Language)

Apa Itu ACL :

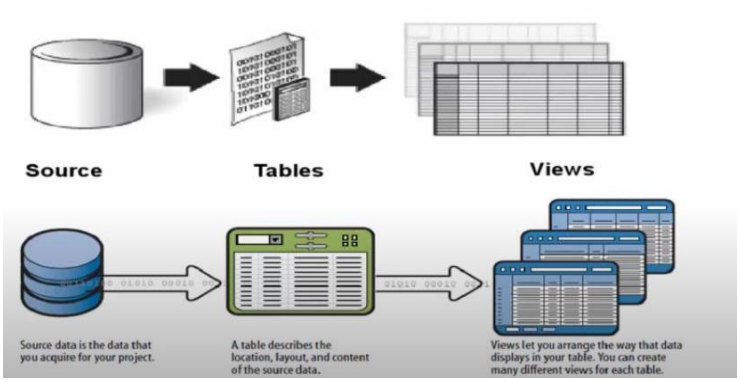
- ACL (Audit Command Language) merupakan salah satu generalized audit software produksi ACL Servies Ltd, Canada
- Software ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit
- ACL dirancang untuk membaca data hanya secara "READ ONLY"
- ACL umumnya digunakan oleh auditor sebagai alat bantu untuk melakukan data analysis, continous monitoring & froud detection

Kemampuan dan kelebihan ACL:

- Universal Data Access
- Jumlah Data Besar
- Kecepatan Waktu Process
- Integritas Data
- Automasi
- Multi File Process
- Log file Navigation
- Fungsi Analisis yang lengkap
- Pelaporan yang handal
- It audit

Proses Data ACL :

- Data dari komputer mini atau mainframe dikonversi menjadi kode EBCDIC (Extended Binary Coded Decimal Interchange Code)
- Data di konversi ke dalam bentuk Text



Manfaat ACL :

- Dapat membantu dalam mengAkses data baik langsung (Direct) kedalam system jaringan ataupun tidak langsung (InDirect) melalui media lain seperti softcopy dalam bentuk teks file/report.
- Menempatkan kesalahan dan potensial fraud sebagai pembanding dan menganalisa file-file menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- Aging dan menganalisa Account Receivable/Payable atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor Invoice/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan supplier.
- Melakukan proses Data Cleansing dan Data Matching atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh End-User.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (Fraud Detection) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

IT AUDIT SOFTWARE

Nama Kelompok :

1.Dhea Noranita Putri (182420112)
2.Reynaldi (182420111)
3.Dini Rahmadia (182420134)
4.Mezi Puspayani (182420120)

MTI REG B 2019
Magister Tehnik Informatika
Universitas Bina Darma
Palembang

Apa itu Nessus ?

- **Nessus** *dibuat oleh Renaud Deraison pada tahun 1998. Nessus adalah* salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan.
- Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem. Sebelum Nessus versi 3, aplikasi ini bersifat open source dan menjadi salah satu primadona di dunia open source. Namun sekarang mulai Nessus versi 3 oleh Teenable Security dijadikan sebagai aplikasi propietary dan closed source

Fitur – fitur yang dimiliki Nessus :

1. Plug-in architecture
   Setiap security test ditulis sebagai external plugin. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca kode dari nessusd engine.
2. NASL (Nessus Attack Scrpiting Language)
   NASL adalah sebuah bahasa yang didesain untuk menulis program security test dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulils program security test.
3. Up-to-date security vulnerability database.

Fitur – fitur yang dimiliki Nessus :

4. Client-sever architecture
   Nessus security scanner terdiri dari dua bagian yaitu: sebuah server yang
   berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagai
   frontend. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari
   fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC,
   dengan server yang melakukan serangan ke jaringan yang dituju.
5. Dapat mengetes jumlah host yang banyak dalam waktu yang sama.
6. Smart service recognation.
   Nessus tidak mempercayai host yang dituju menggunakan port standar yang
   ditentukan oleh IANA. Ini berarti Nessus dapat mengenali sebuah Web server
   yang berjalan pada port yang bukan merupakan port standar (contohnya pada port8080), atau sebuah FTP server yang berjalan pada port 31337.

Fitur – fitur yang dimiliki Nessus :

7. Multiple Services
   Apabila ada dua buah Web server pada host yang dituju maka Nessus akan mengetes kedua Web server tersebut.
8. Complete reports.
   Nessus tidak hanya memberi tahu kelemahan dari jaringan yang dituju tetapi juga memberikan cara yang dapat digunakan untuk mencegah the bad guy utnuk mengeksploitasi kelemahan dari jaringan dan juga memberikan level resiko dari setiap masalah yang ditemukan.
9. Exportable reports.
   Unix client dapat mengekspor laporan sebagai Ascii text, HTML, LaTeX, dll.

Nessus dapat digunakan untuk melakukan audit sebagai berikut:

- Credentialed and un-credentialed port scanning.
- Network based vulnerability scanning.
- Credentialed based patch audits for Windows and most UNIX platforms.
- Redentialed configuration auditing of most Windows and UNIX platforms.
- Robust and comprehensive credentialed security testing of 3rd party applications.
- Custom and embedded web application vulnerability testing.
- SQL database configuration auditing.
- Software enumeration on Unix and Windows.
- Testing anti-virus installs for out-of date signatures and configuration errors.

Download Nessus :

- Kita bisa mendapatkan software nessus pada laman https://www.tenable.com/downloads/nessus?loginAttempted=true
- Website Resmi

http://www.tenable.com/products/nessus-vulnerability-scanner.

Kelebihan Nessus :

- Advanced vulnerability scanning dan configuration audit.
- Mampu mendeteksi process/program mencurigakan dan juga worms.
- Mampu melakukan multiple network scanning (IP, IPv6, Hybrid).
- Automatic scanning scheduler.
- Custom report & Notification.

Kekurangan Nessus :

- Sulit menemukan issue tertentu karna biasanya hasil scanningnya merupakan general case. Biasanya butuh versi profesional untuk fitur yang lebih baik.

Tutorial menginstal dan mengunakan Nessus :

- Anda dapat dapat mempelajari lewat video dari laman ini :

https://www.youtube.com/watch?v=35a0VhzIO2Y

- Anda juga dapat mempelajari langkah-langkanya dengan mendowload dari pdf berikut ini :

https://www.academia.edu/37659321/PROSES_AUDIT_SERVER_DENGAN_NESSUS

TERIMA KASIH

IT AUDIT SOFTWARE

Nama Kelompok :
1.Dhea Noranita Putri (182420112)
2.Reynaldi (182420111)
3.Dini Rahmadia (182420134)
4.Mezi Puspayani (182420120)

MTI REG B 2019
Magister Tehnik Informatika
Universitas Bina Darma
Palembang

Apa itu Nessus ?

- **Nessus** *dibuat oleh Renaud Deraison pada tahun 1998. Nessus adalah* salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan.

Nessus Terbagi Menjadi 3 Tipe, Yaitu :

- **Nessus Home** : digunakan untuk personal
- **Nessus Profesional** : Digunakan untuk penggunaan komersial.
- **Nessus Manager / Nessus Cloud** : Fungsinya Vulnerability Manajemen untuk expert Security teams.

Fungsi nessus?

fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem

Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem. Sebelum Nessus versi 3, aplikasi ini bersifat open source dan menjadi salah satu primadona di dunia open source. Namun sekarang mulai Nessus versi 3 oleh Teenable Security dijadikan sebagai aplikasi propietary dan closed source

Fitur – fitur yang dimiliki Nessus :

1. **Plug-in architecture**
   Setiap security test ditulis sebagai external plugin. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca
   kode dari nessusd engine.
2. **NASL (Nessus Attack Scrpiting Language)**
   NASL adalah sebuah bahasa yang didesain untuk menulis program security test
   dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulils program security test.
3. **Up-to-date security vulnerability database**.

Fitur – fitur yang dimiliki Nessus :

4. Client-sever architecture

Nessus security scanner terdiri dari dua bagian yaitu: sebuah server yang berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagaifrontend. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC,dengan server yang melakukan serangan ke jaringan yang dituju.

Fitur – fitur yang dimiliki Nessus :

5. **host yang banyak dalam waktu yang sama.**

6. Smart service recognation.
Nessus tidak mempercayai host yang dituju menggunakan port standar yang
ditentukan oleh IANA. Ini berarti Nessus dapat mengenali sebuah Web server
yang berjalan pada port yang bukan merupakan port standar (contohnya pada port8080), atau sebuah FTP server yang berjalan pada port 31337.

Fitur – fitur yang dimiliki Nessus :

7. **Multiple Services**
   Apabila ada dua buah Web server pada host yang dituju maka Nessus akan mengetes kedua Web server tersebut.
8. **Complete reports.**
   Nessus tidak hanya memberi tahu kelemahan dari jaringan yang dituju tetapi juga memberikan cara yang dapat digunakan untuk mencegah the bad guy utnuk
   mengeksploitasi kelemahan dari jaringan dan juga memberikan level resiko dari setiap masalah yang ditemukan.

Fitur – fitur yang dimiliki Nessus :

9. **Unix client** dapat mengekspor laporan sebagai Ascii text, HTML, LaTeX, dll.

Cara Kerja/pengoperasian Nessus :

- 1. memulai scanning
- 2. sebelum memulai scanning harus membuat template /policy untuk mendefinisikan scanning
- 3. jika sudah terbuat, maka akan muncul all policies
- 4. kemudian pilih menu scans>new scans
- 5. pada sub general isi nama sesuai keinginan

Cara Kerja/pengoperasian Nessus :

- 6. pada contoh ini akan melakukan scanning pada mesin so 7 dengan alamat IP 192.168.1.2 kemudian save
- Selesai
- Hasil yang di dapat adalah menampilkan semua informasi kerentanan atau celah yang dapat dimanfaatkan oleh seseorang hacker . Kita bias melihat apakah tingkat dari celah itu sedang, kritis atau hanya sekedar informasi saja

Nessus dapat digunakan untuk melakukan audit sebagai berikut:

- Credentialed and un-credentialed port scanning.
- Network based vulnerability scanning.
- Credentialed based patch audits for Windows and most UNIX platforms.
- Redentialed configuration auditing of most Windows and UNIX platforms.
- Robust and comprehensive credentialed security testing of 3rd party applications.
- Custom and embedded web application vulnerability testing.
- SQL database configuration auditing.
- Software enumeration on Unix and Windows.
- Testing anti-virus installs for out-of date signatures and configuration errors.

Download Nessus :

- Kita bisa mendapatkan software nessus pada laman https://www.tenable.com/downloads/nessus?loginAttempted=true
- Website Resmi

http://www.tenable.com/products/nessus-vulnerability-scanner.

Kelebihan Nessus :

- Advanced vulnerability scanning dan configuration audit.
- Mampu mendeteksi process/program mencurigakan dan juga worms.
- Mampu melakukan multiple network scanning (IP, IPv6, Hybrid).
- Automatic scanning scheduler.
- Custom report & Notification.

Kekurangan Nessus :

- Sulit menemukan issue tertentu karna biasanya hasil scanningnya merupakan general case. Biasanya butuh versi profesional untuk fitur yang lebih baik.

Kesimpulan :

- Nessus merupakan sebuah program yang dapat digunakan untuk mencari kelemahan pada sebuah sistem komputer. Nessus juga dapat melakukan pengecekan terhadap kerentanan system komputer, dan meningkatkan keamanan sistem yang kita miliki.
- Nessus juga memberikan Informasi dalam menampilkan secara detail apa yang menjadi penyebab kelemahan sistem serta saran untuk mengatasi kelemahan tersebut. Informasi yang ditampilkan sudah dikelompokkan berdasarkan penyebab terjadinya kelemahan.
- Semua kategori kelemahan hasil dari scan menggunakan Nessus ditampikan penjelesan tentang kelemahan yang ada. Penjelasan mengenai kelemahan sistem tersebut bisa dijadikan acuan untuk administrator untuk memperbaiki kelemahan sistem yang muncul sebelum di unggah di web server.

Kesimpulan :

- **Saran**
- Semakin banyak vulnerabilitas dan ancaman yang dapat terjadi di dalam suatu sistem, sudah seharusnya semakin tinggi pula kesadaran kita untuk dapat memproteksi sistem dan informasi yang berada di dalamnya. Sebuah teknik untuk melindungi suatu sistem dinamakan dengan tindakan pencegahan sehingga kita perlu melakukan tindakan pencegahan salah satunya menggunakan tools keamanan seperti nessus

Tutorial menginstal dan mengunakan Nessus :

- Anda dapat dapat mempelajari lewat video dari laman ini :

https://www.youtube.com/watch?v=35a0VhzIO2Y

- Anda juga dapat mempelajari langkah-langkanya dengan mendowload dari pdf berikut ini :

https://www.academia.edu/37659321/PROSES_AUDIT_SERVER_DENGAN_NESSUS

TERIMA KASIH

W3AF

Universitas Bina Darma

KELOMPOK 4

MTI.20A

1. Ekariva Annas Asmara (182420133)
2. Hari Febriadi (182420127)
3. Mifathul Fallah (182420132)
4. Fajar Prayoga (182420136)

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Aplikasi yang akan saya bahas adalah **W3AF**, aplikasi yang bisa di jalankan di linux dan di windows ini sangat banyak di gemari oleh sang **H4Ck3R**, walau lebih banyak yang menggunakannya di linux namun tidak sedikit pula yang menggunakannya di windows. Tetapi

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

W3af adalah ***Web Aplication Attack And Audit Framework***. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu **Kelemahan** website.

Aplikasi ini di buat menggunakan bahasa pemprograman **python**. Sebenarnya pengetahuan saya tentang aplikasi ini sangatlah minim, jadi buat kalian yang ingin menggunakannya dan menguasainya kunjungi situs resminya di : **w3af.org**.

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Berikut tampilan GUI untuk w3af yang saya install pada windows XP :

Universitas Bina Darma

KOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Universitas Bina Darma

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Sumber : https://infobacktrack.wordpress.com/category/deface/

Dalam uji coba ini saya menggunakan backtrack 5, dan secara default sudah terinstall. Untuk bagian menunya bisa dilihat seperti banner diatas. Jika anda menggunakan ubuntu, bisa langsung di ketik

sudo apt-get install w3af

Oke, saya anggap smua sudah memulai tampilan awalnya yah. disini saya mengetik help.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Universitas Bina Darma

KELOMPOK 4

MTI.20A

Sumber : https://infobacktrack.wordpress.com/category/deface/

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Code :

```
1. w3af >> help
2. The following commands are available:
3. helpn                : You are here. help (command) prints
                          more specific help.
4. url-settings         : Configure the URL opener.
5. misc-settings        : Configure w3af misc settings.
6. session              : Load and save sessions.
7. plugins              : Enable, disable and configure plugins.
8. start                : Start site analysis.
9. exploit              : Exploit a vulnerability.
10. tools               : Enter the tools section.
11. tools               : Enter the tools section.
12. exit                : Exit w3af.
```

KELOMPOK 4

Configuration & Menentukan Target. Dalam pengujian ini, saya menggunakan **web FPI** sebagai target. Ingat, disini saya hanya sebatas menguji coba tanpa ada niat lebih lanjut.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Code :

```
w3af>>> target
1. w3afconfig:target>>> help
   |-------------------------------------------------------------------------|
2. view | List the available options and their values. |
3. set | Set a parameter value. |
   |-------------------------------------------------------------------------|
4. back | Go to the previous menu. |
5. exit | Exit w3af. |
6. assert | Check assertion. |
   |-------------------------------------------------------------------------|
w3afconfig:target>>> set target http://www.fpi.or.id/
w3afconfig:target>>> view
```

```
w3af>>> target
w3af/config:target>>> help
|-------------------------------------------------------------------------|
| view          | List the available options and their values.
| set           | Set a parameter value.
|-------------------------------------------------------------------------|
| back          | Go to the previous menu.
| exit          | Exit w3af.
| assert        | Check assertion.
|-------------------------------------------------------------------------|
w3af/config:target>>> set target http://www.fpi.or.id/
w3af/config:target>>> view
```


Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Dan hasil configurasi targetnya adalah :

```
w3af/config:target>>> view
+-----------------+-----------------------+-----------------------------------------------------+
| Setting         | Value                 | Description                                         |
+-----------------+-----------------------+-----------------------------------------------------+
| targetOS        | unknown               | Target operating system (unknown/unix/windows)      |
| targetFramework | unknown               | Target programming framework                        |
|                 |                       | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)    |
| target          | http://www.fpi.or.id/ | A comma separated list of URLs                      |
+-----------------+-----------------------+-----------------------------------------------------+
w3af/config:target>>>
```

Configurasi Plugin :

```
w3af/config:target>>> back
w3af>>> plugins
w3af/plugins>>> help
+-------------+-----------------------------------------------------+
| list        | List available plugins.                             |
+-------------+-----------------------------------------------------+
| back        | Go to the previous menu.                            |
| exit        | Exit w3af.                                          |
| assert      | Check assertion.                                    |
+-------------+-----------------------------------------------------+
| discovery   | View, configure and enable discovery plugins        |
| output      | View, configure and enable output plugins           |
| mangle      | View, configure and enable mangle plugins           |
| evasion     | View, configure and enable evasion plugins          |
| bruteforce  | View, configure and enable bruteforce plugins       |
| audit       | View, configure and enable audit plugins            |
| grep        | View, configure and enable grep plugins             |
+-------------+-----------------------------------------------------+
w3af/plugins>>>
```

Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

w3afconfig : target >>> back
w3af >>> plugins
w3af/plugins >>> help

List	: List available plugins.
Back	: Go to the previous menu.
Exit	: Exit w3af.
Assert	: Check assertion.
Discovery	: View, configure and enable discovery plugins
Output	: View, configure and enable output plugins
Mangle	: View, configure and enable mangle plugins
Evasion	: View, configure and enable evasion plugins
Bruteforce	: View, configure and enable bruteforce plugins
Audit	: View, configure and enable audit plugins
Grep	: View, configure and enable grep plugins

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Memilih Serangan

Disini saya menggunakan audit xss,xsrf,sqli.

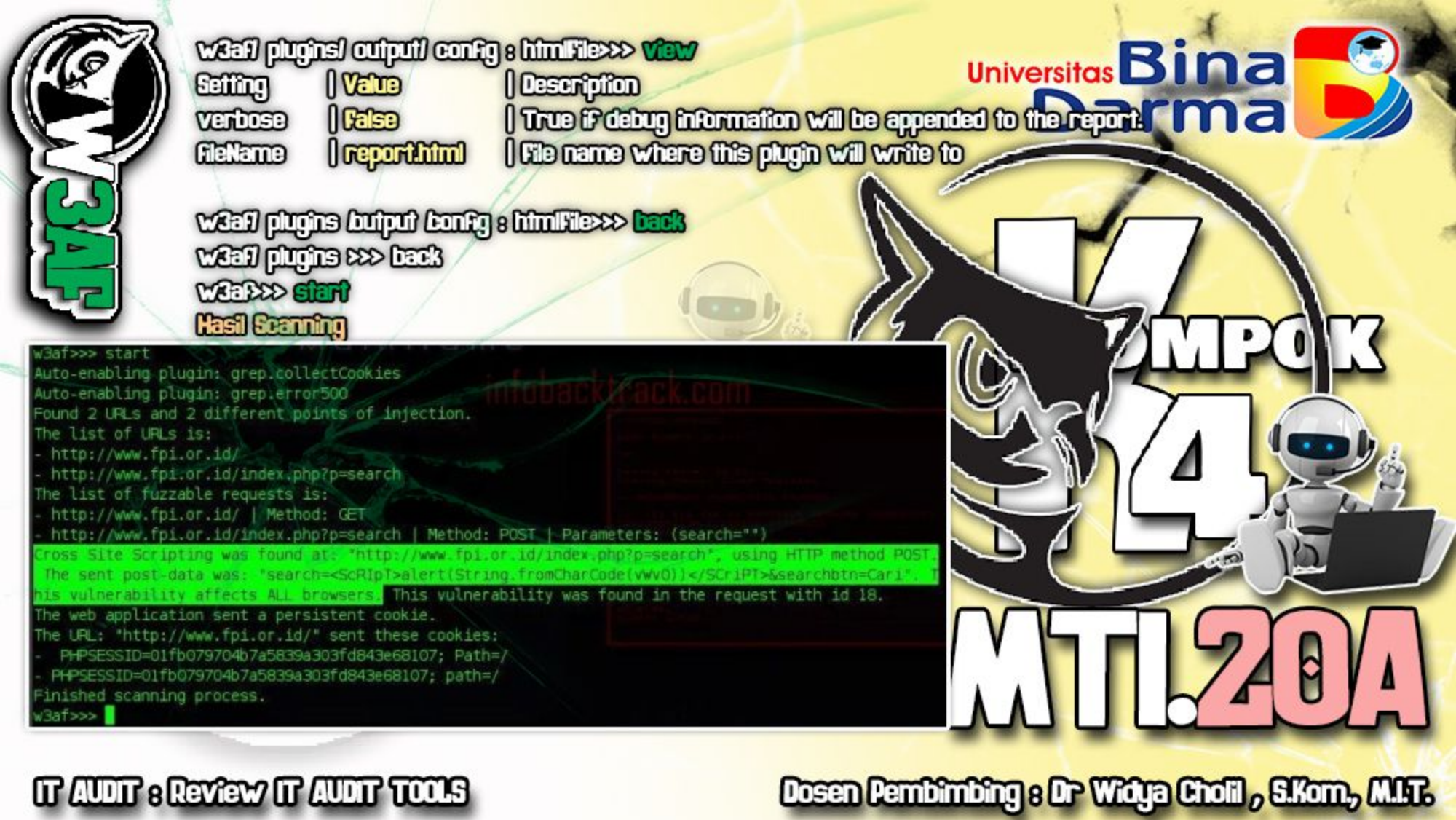
```
w3af>>> plugins
w3af/plugins>>> help
|-------------------------------------------------------------------------|
| list              | List available plugins.                             |
|-------------------------------------------------------------------------|
| back              | Go to the previous menu.                            |
| exit              | Exit w3af.                                          |
| assert            | Check assertion.                                    |
|-------------------------------------------------------------------------|
| discovery         | View, configure and enable discovery plugins        |
| output            | View, configure and enable output plugins           |
| mangle            | View, configure and enable mangle plugins           |
| evasion           | View, configure and enable evasion plugins          |
| bruteforce        | View, configure and enable bruteforce plugins       |
| audit             | View, configure and enable audit plugins            |
| grep              | View, configure and enable grep plugins             |
|-------------------------------------------------------------------------|
w3af/plugins>>> audit xss,xsrf,sqli
w3af/plugins>>> output console,htmlFile
w3af/plugins>>> output config htmlFile
```

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.


w3af/plugins/output/config : htmlFile>>> view
Setting | Value | Description
verbose | False | True if debug information will be appended to the report.
fileName | report.html | File name where this plugin will write to
w3af/plugins/output/config : htmlFile>>> back
w3af/plugins >>> back
w3af>>> start
Hasil Scanning
w3af>>> start
Auto-enabling plugin: grep.collectCookies
Auto-enabling plugin: grep.error500
Found 2 URLs and 2 different points of injection.
The list of URLs is:
- http://www.fpi.or.id/
- http://www.fpi.or.id/index.php?p=search
The list of fuzzable requests is:
- http://www.fpi.or.id/ | Method: GET
- http://www.fpi.or.id/index.php?p=search | Method: POST | Parameters: (search="")
Cross Site Scripting was found at: "http://www.fpi.or.id/index.php?p=search", using HTTP method POST. The sent post-data was: "search=<ScRIpT>alert(String.fromCharCode(vWv0))</SCriPT>&searchbtn=Cari". This vulnerability affects ALL browsers. This vulnerability was found in the request with id 18.
The web application sent a persistent cookie.
The URL: "http://www.fpi.or.id/" sent these cookies:
- PHPSESSID=01fb079704b7a5839a303fd843e68107; Path=/
- PHPSESSID=01fb079704b7a5839a303fd843e68107; path=/
Finished scanning process.
w3af>>>
Universitas Bina Darma
KELOMPOK 4
MTI.20A
IT AUDIT : Review IT AUDIT TOOLS
Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

SIMPULAN

- Dari hasil scanning diatas, dapat di Simpulkan bahwa web tersebut memiliki kelemahan pada XSS.
- Potensi serangan yang dapat dilakukan attacker adalah melakukan pemanggilan Get Web Shell, setelah pemanggilan web shell, maka web tersebut dapat diambil alih.

w3af

Web Application Attack and Audit Framework

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

FUNGSI TOOL W3AF DALAM IT AUDIT

- IT Audit membuat kerangka Konseptual, sehingga audit dapat berjalan sesuai dengan yang diharapkan, Kerangka konseptual dijelaskan sebagai berikut :
  - ✓ **Membuat Perencanaan**
    - Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell
  - ✓ **Mengolah ancaman**
    - Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman
  - ✓ **Kesimpulan**
    - Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

Universitas Bina Darma

Terima Kasih

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

w3af

Web Application Attack and Audit Framework

Fajar Prayoga
182420136
MTI.20A
IT AUDIT
By : Dr Widya Cholil, S.Kom., MIT

RINGKASAN HASIL PRESENTASI KELOMPOK 1-4

Kelompok 1

Ringkasan Materi Password cracking tools /Alat pemecahan kata password

Password cracking adalah proses melibatkan memulihkan password dari lokasi penyimpanan atau data, dikirimkan oleh sistem komputer pada jaringan. Password cracking istilah merujuk kepada kelompok teknik yang digunakan untuk mendapatkan password dari sistem data.

Tujuan dan alasan password cracking meliputi memperoleh akses tidak sah ke sistem komputer atau dapat pemulihan password. Alasan untuk menggunakan teknik password cracking untuk menguji kekuatan password sehingga hacker tidak bisa hack ke dalam sistem.

Aircrack: Alat Cracking Cepat dan efektif WEP/WPA

AirCrack digunakan untuk memecahkan enkripsi WEP dan WPA di jaringan nirkabel. Agar AirCrack dapat bekerja secara efektif, prasyaratnya adalah untuk menangkap paket yang cukup dari udara dan memungkinkan program untuk mengeksekusi algoritma untuk memecahkan kunci nirkabel. AirCrack paling sesuai dengan standar 802.11a / b / g.

OphCrack: Alat untuk Windows sandi cracking

Ophcrack adalah alat open source gratis yang dapat digunakan untuk memecahkan kata password Windows menggunakan tabel pelangi. Ophcrack dibundel gratis untuk Windows XP dan Windows Vista. Ini juga menganalisis kekuatan kata password melalui analisis grafik waktu nyata. Ekstensi untuk meretas kata password sederhana menggunakan brute force.

Fitur OphCrack

- Tersedia untuk Windows tetapi juga tersedia untuk Linux, Mac, Unix dan OS X
- Menggunakan LM hash Windows dan NTLM hash Windows Vista.
- Pelangi tabel tersedia gratis dan mudah untuk Windows
- Untuk menyederhanakan proses cracking Live CD tersedia

Fajar Prayoga
182420136
MTI.20A
IT AUDIT
By : Dr Widya Cholil, S.Kom., MIT

Kelompok 2

Ringkasan Materi Metasploit

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).
Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

Kelompok 3

Ringkasan Materi Maltego

Maltego ini disebut OSINT (Open Source Intelligence Gathering) sebuah alat untuk melakukan *footprinting*, digunakan untuk mengumpulkan informasi sebanyak mungkin dengan tujuan forensik, *pen testing*, atau *ethical hacking*. Aplikasi yang digunakan untuk memetakan jaringan komunikasi Yang berada di internet tujuannya adalah mengumpulkan informasi tentang target dan menampilkan informasi tersebut dalam format yang mudah dimengerti, memvisualisasikan informasi tersebut ke dalam sebuah format graph, sangat cocok untuk *link analysis* dan *data mining*.

Fajar Prayoga
182420136
MTI.20A
IT AUDIT
By : Dr Widya Cholil, S.Kom., MIT

Fungsi dari maltego adalah memudahkan seseoorang yang mencari informasi tentang apa yang mereka selidiki atau mereka incar sebagai target, contoh ketika seorang mencari informasi dari sebuah domain menggunakan maltego, maka maltego akan menampikan bebrap informasi seperti berikut:

- Block IP hosting
- Domain registe
- Email user & admin
- Phone number
- Peta jaringan

Maltego dibedakan menjadi versi komersial (commercial edition) dan versi gratis (community edition). Versi gratis yang tersedia di Kali Linux hanya dapat menampilkan maksimal 12 hasil transformasi, Sebagai sebuah front-end untuk server OSINT, Maltego versi gratis hanya dapat memakai layanan server milik Paterva. Karena versi yang disediakan oleh Kali Linux adalah versi gratis dari Maltego.

Kelompok 4

Ringkasan Materi W3af

W3af adalah Web Aplication Attack And Audit Framework. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengekploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu kelemahan website.

w3af (Web Application Attack and Audit Framework) hampir mirip dengan metasploit, bedanya hanya pada objek yang dikerjakan. w3af fokus pada bagian aplikasi web, sedangkan metasploit lebih ke sistem operasi secara keseluruhan. w3af gratis dan opensource, terdiri dari beberapa bagian plugin untuk serangan yaitu mangle, grep, discovery, audit, evasion, dan bruteforce.

Aplikasi ini dibuat menggunakan bahasa pemrograman python. Untuk persiapan menggunakan w3af, banyak program berbasis python yang harus diinstal seperti python-soappy, python-pyopenssl, dll.

FUNGSI TOOL W3AF DALAM IT AUDIT

IT Audit membuat kerangka Konseptual, sehingga audit dapat berjalan sesuai dengan yang diharapkan, Kerangka konseptual dijelaskan sebagai berikut :

- **Membuat Perencanaan**
  Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell
- **Mengolah ancaman**
  Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman
- **Kesimpulan**
  Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

W3AF

Universitas Bina Darma

KELOMPOK 4

MTI.20A

1. Ekariva Annas Asmara (182420133)
2. Hari Febriadi (182420127)
3. Mifathul Fallah (182420132)
4. Fajar Prayoga (182420136)

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Aplikasi yang akan saya bahas adalah **W3AF**, aplikasi yang bisa di jalankan di linux dan di windows ini sangat banyak di gemari oleh sang **H4Ck3R**, walau lebih banyak yang menggunakannya di linux namun tidak sedikit pula yang menggunakannya di windows. Tetapi

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

W3af adalah ***Web Aplication Attack And Audit Framework***. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu **Kelemahan** website.

Aplikasi ini di buat menggunakan bahasa pemprograman **python**. Sebenarnya pengetahuan saya tentang aplikasi ini sangatlah minim, jadi buat kalian yang ingin menggunakannya dan menguasainya kunjungi situs resminya di : **w3af.org**.

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Berikut tampilan GUI untuk w3af yang saya install pada windows XP :

Universitas Bina Darma

KOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Universitas Bina Darma

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Sumber : https://infobacktrack.wordpress.com/category/deface/

Dalam uji coba ini saya menggunakan backtrack 5, dan secara default sudah terinstall. Untuk bagian menunya bisa dilihat seperti banner diatas. Jika anda menggunakan ubuntu, bisa langsung di ketik

sudo apt-get install w3af

Oke, saya anggap smua sudah memulai tampilan awalnya yah. disini saya mengetik help.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Universitas Bina Darma

KELOMPOK 4

MTI.20A

Sumber : https://infobacktrack.wordpress.com/category/deface/

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Code :

```
1. w3af >> help
2. The following commands are available:
3. helpn                : You are here. help (command) prints
                          more specific help.
4. url-settings         : Configure the URL opener.
5. misc-settings        : Configure w3af misc settings.
6. session              : Load and save sessions.
7. plugins              : Enable, disable and configure plugins.
8. start                : Start site analysis.
9. exploit              : Exploit a vulnerability.
10. tools               : Enter the tools section.
11. tools               : Enter the tools section.
12. exit                : Exit w3af.
```

KELOMPOK 4

Configuration & Menentukan Target. Dalam pengujian ini, saya menggunakan **web FPI** sebagai target. Ingat, disini saya hanya sebatas menguji coba tanpa ada niat lebih lanjut.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Code :

```
w3af>>> target
1. w3afconfig:target>>> help
   |-------------------------------------------------------------------------|
2. view | List the available options and their values. |
3. set | Set a parameter value. |
   |-------------------------------------------------------------------------|
4. back | Go to the previous menu. |
5. exit | Exit w3af. |
6. assert | Check assertion. |
   |-------------------------------------------------------------------------|
w3afconfig:target>>> set target http://www.fpi.or.id/
w3afconfig:target>>> view
```

```
w3af>>> target
w3af/config:target>>> help
|-------------------------------------------------------------------------|
| view          | List the available options and their values.
| set           | Set a parameter value.
|-------------------------------------------------------------------------|
| back          | Go to the previous menu.
| exit          | Exit w3af.
| assert        | Check assertion.
|-------------------------------------------------------------------------|
w3af/config:target>>> set target http://www.fpi.or.id/
w3af/config:target>>> view
```


Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Dan hasil configurasi targetnya adalah :

```
w3af/config:target>>> view
+-----------------+-----------------------+-----------------------------------------------------+
| Setting         | Value                 | Description                                         |
+-----------------+-----------------------+-----------------------------------------------------+
| targetOS        | unknown               | Target operating system (unknown/unix/windows)      |
| targetFramework | unknown               | Target programming framework                        |
|                 |                       | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)    |
| target          | http://www.fpi.or.id/ | A comma separated list of URLs                      |
+-----------------+-----------------------+-----------------------------------------------------+
w3af/config:target>>>
```

Configurasi Plugin :

```
w3af/config:target>>> back
w3af>>> plugins
w3af/plugins>>> help
+-------------+-----------------------------------------------------+
| list        | List available plugins.                             |
+-------------+-----------------------------------------------------+
| back        | Go to the previous menu.                            |
| exit        | Exit w3af.                                          |
| assert      | Check assertion.                                    |
+-------------+-----------------------------------------------------+
| discovery   | View, configure and enable discovery plugins        |
| output      | View, configure and enable output plugins           |
| mangle      | View, configure and enable mangle plugins           |
| evasion     | View, configure and enable evasion plugins          |
| bruteforce  | View, configure and enable bruteforce plugins       |
| audit       | View, configure and enable audit plugins            |
| grep        | View, configure and enable grep plugins             |
+-------------+-----------------------------------------------------+
w3af/plugins>>>
```

Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

w3afconfig : target >>> back
w3af >>> plugins
w3af/plugins >>> help

List	: List available plugins.
Back	: Go to the previous menu.
Exit	: Exit w3af.
Assert	: Check assertion.
Discovery	: View, configure and enable discovery plugins
Output	: View, configure and enable output plugins
Mangle	: View, configure and enable mangle plugins
Evasion	: View, configure and enable evasion plugins
Bruteforce	: View, configure and enable bruteforce plugins
Audit	: View, configure and enable audit plugins
Grep	: View, configure and enable grep plugins

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Memilih Serangan

Disini saya menggunakan audit xss,xsrf,sqli.

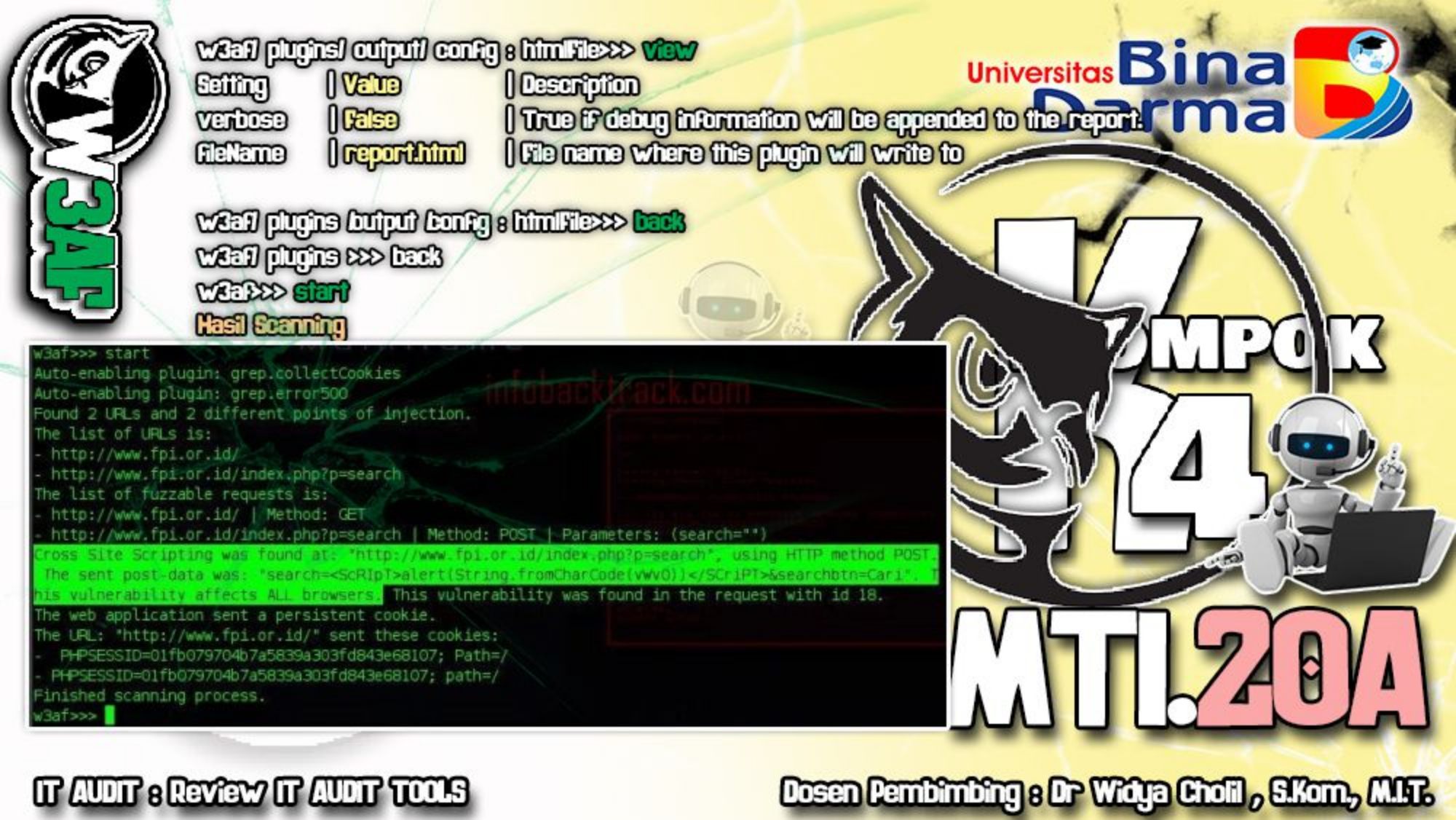
```
w3af>>> plugins
w3af/plugins>>> help
|-------------------------------------------------------------------------|
| list              | List available plugins.                             |
|-------------------------------------------------------------------------|
| back              | Go to the previous menu.                            |
| exit              | Exit w3af.                                          |
| assert            | Check assertion.                                    |
|-------------------------------------------------------------------------|
| discovery         | View, configure and enable discovery plugins        |
| output            | View, configure and enable output plugins           |
| mangle            | View, configure and enable mangle plugins           |
| evasion           | View, configure and enable evasion plugins          |
| bruteforce        | View, configure and enable bruteforce plugins       |
| audit             | View, configure and enable audit plugins            |
| grep              | View, configure and enable grep plugins             |
|-------------------------------------------------------------------------|
w3af/plugins>>> audit xss,xsrf,sqli
w3af/plugins>>> output console,htmlFile
w3af/plugins>>> output config htmlFile
```

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.


w3af/plugins/output/config : htmlFile>>> view
Setting | Value | Description
verbose | False | True if debug information will be appended to the report.
fileName | report.html | File name where this plugin will write to
w3af/plugins/output/config : htmlFile>>> back
w3af/plugins >>> back
w3af>>> start
Hasil Scanning
w3af>>> start
Auto-enabling plugin: grep.collectCookies
Auto-enabling plugin: grep.error500
Found 2 URLs and 2 different points of injection.
The list of URLs is:
- http://www.fpi.or.id/
- http://www.fpi.or.id/index.php?p=search
The list of fuzzable requests is:
- http://www.fpi.or.id/ | Method: GET
- http://www.fpi.or.id/index.php?p=search | Method: POST | Parameters: (search="")
Cross Site Scripting was found at: "http://www.fpi.or.id/index.php?p=search", using HTTP method POST. The sent post-data was: "search=<ScRIpT>alert(String.fromCharCode(vWv0))</SCriPT>&searchbtn=Cari". This vulnerability affects ALL browsers. This vulnerability was found in the request with id 18.
The web application sent a persistent cookie.
The URL: "http://www.fpi.or.id/" sent these cookies:
- PHPSESSID=01fb079704b7a5839a303fd843e68107; Path=/
- PHPSESSID=01fb079704b7a5839a303fd843e68107; path=/
Finished scanning process.
w3af>>>
Universitas Bina Darma
KELOMPOK 4
MTI.20A
IT AUDIT : Review IT AUDIT TOOLS
Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

SIMPULAN

- Dari hasil scanning diatas, dapat di Simpulkan bahwa web tersebut memiliki kelemahan pada XSS.
- Potensi serangan yang dapat dilakukan attacker adalah melakukan pemanggilan Get Web Shell, setelah pemanggilan web shell, maka web tersebut dapat diambil alih.

w3af

Web Application Attack and Audit Framework

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

FUNGSI TOOL W3AF DALAM IT AUDIT

- IT Audit membuat kerangka Konseptual, sehingga audit dapat berjalan sesuai dengan yang diharapkan, Kerangka konseptual dijelaskan sebagai berikut :
  - ✓ **Membuat Perencanaan**
    - Identifikasi kelemahan : Kelemahan pada XSS, Potensi serangan, pemanggilan Get Web Shell
  - ✓ **Mengolah ancaman**
    - Baik kualitatif maupun secara kuantitatif audit menentukan arti penting suatu ancaman
  - ✓ **Kesimpulan**
    - Tindakan pengamanan dilakukan untuk menyingkirkan atau mengurangi ancaman

Universitas Bina Darma

Terima Kasih

Dosen Pembimbing : Dr Widya Cholil, S.Kom, M.IT/IT Audit

w3af

Web Application Attack and Audit Framework

METASPLOIT

IT SECURITY AUDIT TOOL

Universitas Bina Darma

TIM PENYUSUN

1. LILY PEBRIANA (182420114)
2. LAILATUR RAHMI (182420118)
3. ARIYANSAH (182420117)
4. MEFTA EKO S. (182420113)
5. GIAN PRATAMA (182420116)
6. AGUS SUMITRO (182420126)

Program Pascasarjana
Magister Teknik Informatika
MTI – 20A

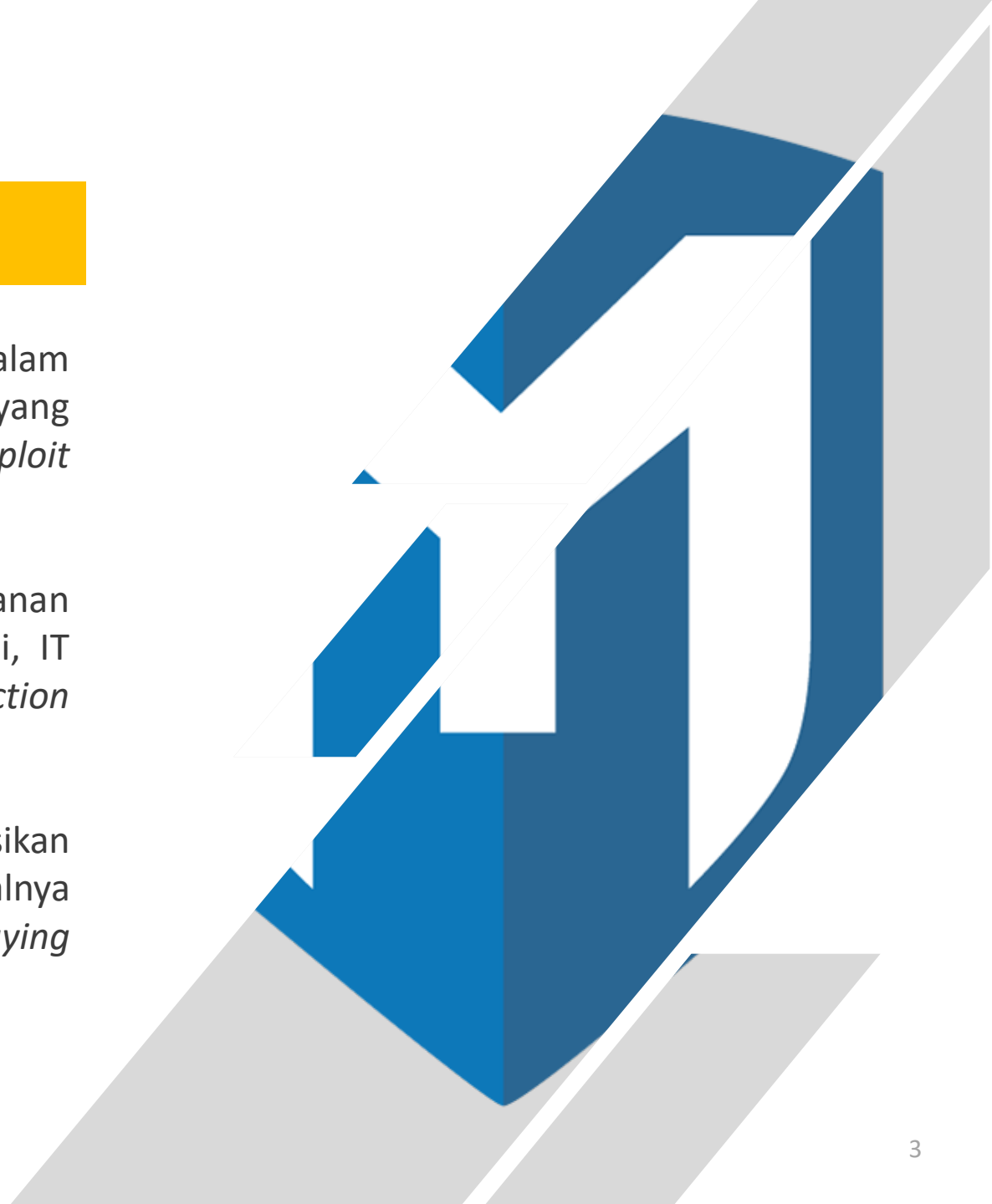
metasploit®

METASPLOIT

Metasploit adalah sebuah *framework* yang cukup populer dalam bidang hacking dan IT Security sebagai *cyber exploitation tools* yang sangat memiliki dukungan untuk membuat suatu *exploit vulnerability* yang belum diketahui pada suatu jaringan.

Metasploit mampu menyediakan informasi tentang kerentanan keamanan yang dapat membantu dalam pengujian penetrasi, IT Audit, maupun pengembangan *signature* IDS (*Intrusion Detection System*).

Metasploit tersedia dalam versi windows, namun direkomendasikan menggunakan versi linux karena banyak fitur Metasploit misalnya *raw IP packet injection, wireless driver exploitation, SMB relaying attacks* yang tidak tersedia pada versi Windows.



TIMELINE METASPLOIT

H.D. Moore menulisnya dalam bahasa PERL

Tim menuliskannya kembali dengan bahasa RUBY

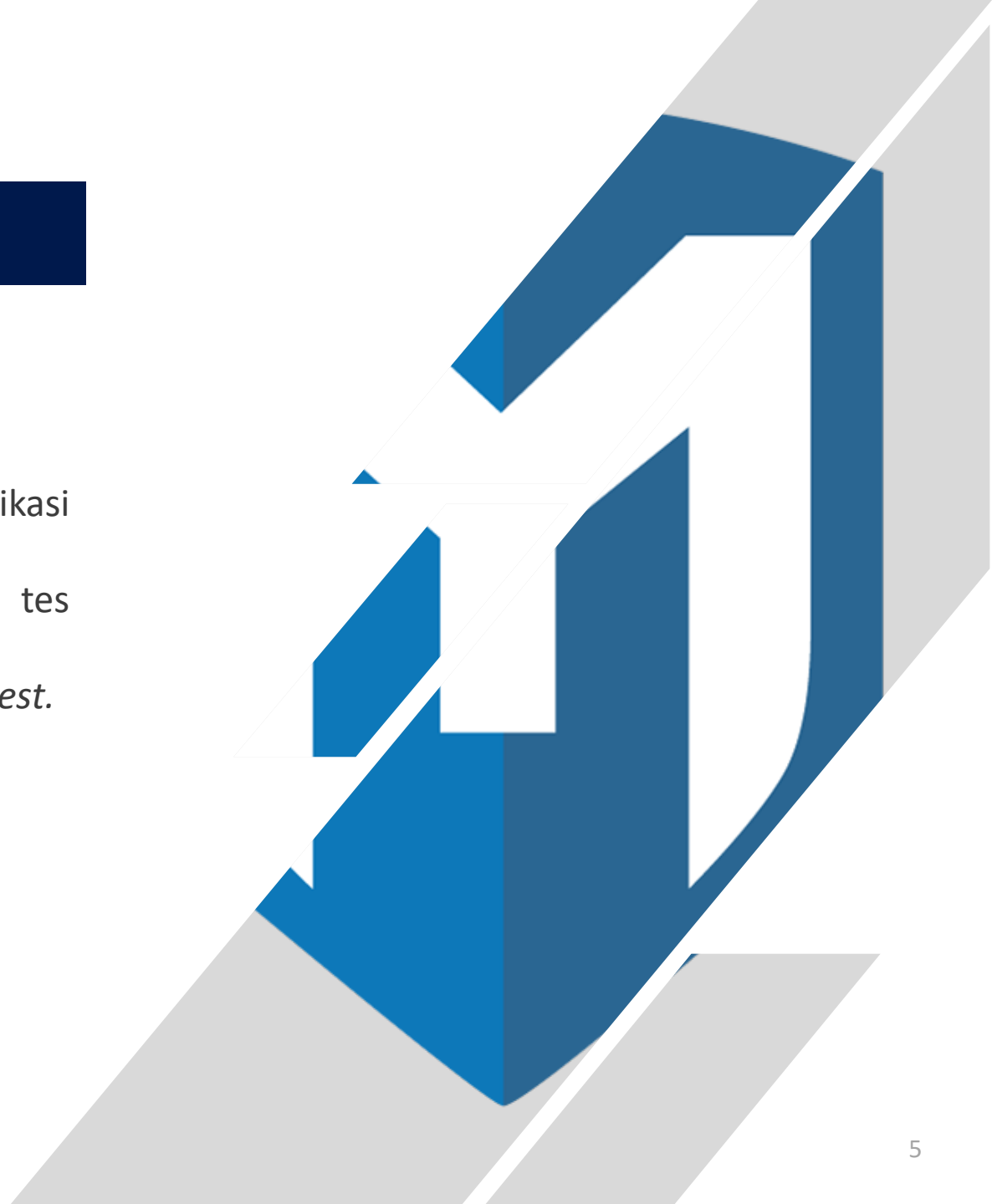
Diakuisi oleh perusahaan RAPID7

Tersedia varian Metasploit Framework & Metasploit Community (gratis), Metasploit Express & Metasploit Professional (komersial).

KEGUNAAN METASPLOIT

Beberapa kegunaan Metasploit :

1. Demo atau presentasi.
2. Digunakan oleh administrator sistem untuk melakukan verifikasi instalasi *patch* sistemnya.
3. Digunakan oleh vendor untuk melakukan penelitian dan tes kelemahan produknya.
4. Dibidang keamanan jaringan untuk melakukan *penetration test.*
5. Riset dan penelitian eksploitasi keamanan.
6. Tes IPS/IDS.
7. Legal Hacking.



MENJALANKAN METASPLOIT

Langkah dasar untuk mengekploitasi suatu sistem menggunakan Metasploit adalah sebagai berikut :

1. Memeriksa apakah sistem target yang dipilih memiliki kerentanan terhadap metode eksploit yang dipilih.
2. Memilih dan mengkonfigurasi eksploit (file kode yang memasuki sistem target dan mampu mengambil keuntungan dari salah satu *bug* yang ada).
3. Memilih metode *encoding* sehingga *intersion-prevention system* (IPS) mengabaikan muatan data yang di *encoding*.
4. Memilih dan mengkonfigurasi *payload* (file kode yang akan dieksekusi pada sistem target setelah berhasil masuk).
5. Melaksanakan exploitasi.

THANK YOU

Universitas Bina Darma

W3AF

Universitas Bina Darma

KELOMPOK 4

MTI.20A

1. Ekariva Annas Asmara (182420133)
2. Hari Febriadi (182420127)
3. Mifathul Fallah (182420132)
4. Fajar Prayoga (182420136)

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Aplikasi yang akan saya bahas adalah **W3AF**, aplikasi yang bisa di jalankan di linux dan di windows ini sangat banyak di gemari oleh sang **H4Ck3R**, walau lebih banyak yang menggunakannya di linux namun tidak sedikit pula yang menggunakannya di windows. Tetapi

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

W3af adalah ***Web Aplication Attack And Audit Framework***. Tujuan proyek ini adalah untuk sebuah kerangka untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Dengan aplikasi ini kita lebih mudah untuk men-scan suatu website sehingga dapat mengetahui celah suatu website.

Aplikasi ini di buat menggunakan bahasa pemprograman **python**. Sebenarnya pengetahuan saya tentang aplikasi ini sangatlah minim, jadi buat kalian yang ingin menggunakannya dan menguasainya kunjungi situs resminya di : **w3af.org**.

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Berikut tampilan GUI untuk w3af yang saya install pada windows XP :

Universitas Bina Darma

KOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Universitas Bina Darma

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

KELOMPOK 4

MTI.20A

Dalam uji coba ini saya menggunakan backtrack 5, dan secara default sudah terinstall. Untuk bagian menunya bisa dilihat seperti banner diatas. Jika anda menggunakan ubuntu, bisa langsung di ketik

```
sudo apt-get install w3af
```

Oke, saya anggap smua sudah memulai tampilan awalnya yah. disini saya mengetik help.

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Console 2007 W3AF

Studi Kasus : Mencari Kelemahan WEB

Target Web : Situs FPI-Online

Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Universitas Bina Darma

Code :

```
1. w3af >> help
2. The following commands are available:
3. helpn                : You are here. help (command) prints
                          more specific help.
4. url-settings         : Configure the URL opener.
5. misc-settings        : Configure w3af misc settings.
6. session              : Load and save sessions.
7. plugins              : Enable, disable and configure plugins.
8. start                : Start site analysis.
9. exploit              : Exploit a vulnerability.
10. tools               : Enter the tools section.
11. tools               : Enter the tools section.
12. exit                : Exit w3af.
```

KELOMPOK 4

Configuration & Menentukan Target. Dalam pengujian ini, saya menggunakan **web FPI** sebagai target. Ingat, disini saya hanya sebatas menguji coba tanpa ada niat lebih lanjut.

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Code :

```
w3af>>> target
1. w3afconfig:target>>> help
   |-------------------------------------------------------------------------|
2. view | List the available options and their values. |
3. set | Set a parameter value. |
   |-------------------------------------------------------------------------|
4. back | Go to the previous menu. |
5. exit | Exit w3af. |
6. assert | Check assertion. |
   |-------------------------------------------------------------------------|
w3afconfig:target>>> set target http://www.fpi.or.id/
w3afconfig:target>>> view
```

```
w3af>>> target
w3af/config:target>>> help
|-------------------------------------------------------------------------|
| view          | List the available options and their values.
| set           | Set a parameter value.
|-------------------------------------------------------------------------|
| back          | Go to the previous menu.
| exit          | Exit w3af.
| assert        | Check assertion.
|-------------------------------------------------------------------------|
w3af/config:target>>> set target http://www.fpi.or.id/
w3af/config:target>>> view
```


Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Dan hasil configurasi targetnya adalah :

```
w3af/config:target>>> view
+-----------------+-----------------------+-----------------------------------------------------+
| Setting         | Value                 | Description                                         |
+-----------------+-----------------------+-----------------------------------------------------+
| targetOS        | unknown               | Target operating system (unknown/unix/windows)      |
| targetFramework | unknown               | Target programming framework                        |
|                 |                       | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)    |
| target          | http://www.fpi.or.id/ | A comma separated list of URLs                      |
+-----------------+-----------------------+-----------------------------------------------------+
w3af/config:target>>>
```

Configurasi Plugin :

```
w3af/config:target>>> back
w3af>>> plugins
w3af/plugins>>> help
+-------------+-----------------------------------------------------+
| list        | List available plugins.                             |
+-------------+-----------------------------------------------------+
| back        | Go to the previous menu.                            |
| exit        | Exit w3af.                                          |
| assert      | Check assertion.                                    |
+-------------+-----------------------------------------------------+
| discovery   | View, configure and enable discovery plugins        |
| output      | View, configure and enable output plugins           |
| mangle      | View, configure and enable mangle plugins           |
| evasion     | View, configure and enable evasion plugins          |
| bruteforce  | View, configure and enable bruteforce plugins       |
| audit       | View, configure and enable audit plugins            |
| grep        | View, configure and enable grep plugins             |
+-------------+-----------------------------------------------------+
w3af/plugins>>>
```

Universitas Bina Darma

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

w3afconfig : target >>> back
w3af >>> plugins
w3af/plugins >>> help

List	: List available plugins.
Back	: Go to the previous menu.
Exit	: Exit w3af.
Assert	: Check assertion.
Discovery	: View, configure and enable discovery plugins
Output	: View, configure and enable output plugins
Mangle	: View, configure and enable mangle plugins
Evasion	: View, configure and enable evasion plugins
Bruteforce	: View, configure and enable bruteforce plugins
Audit	: View, configure and enable audit plugins
Grep	: View, configure and enable grep plugins

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Memilih Serangan

Disini saya menggunakan audit xss,xsrf,sqli.

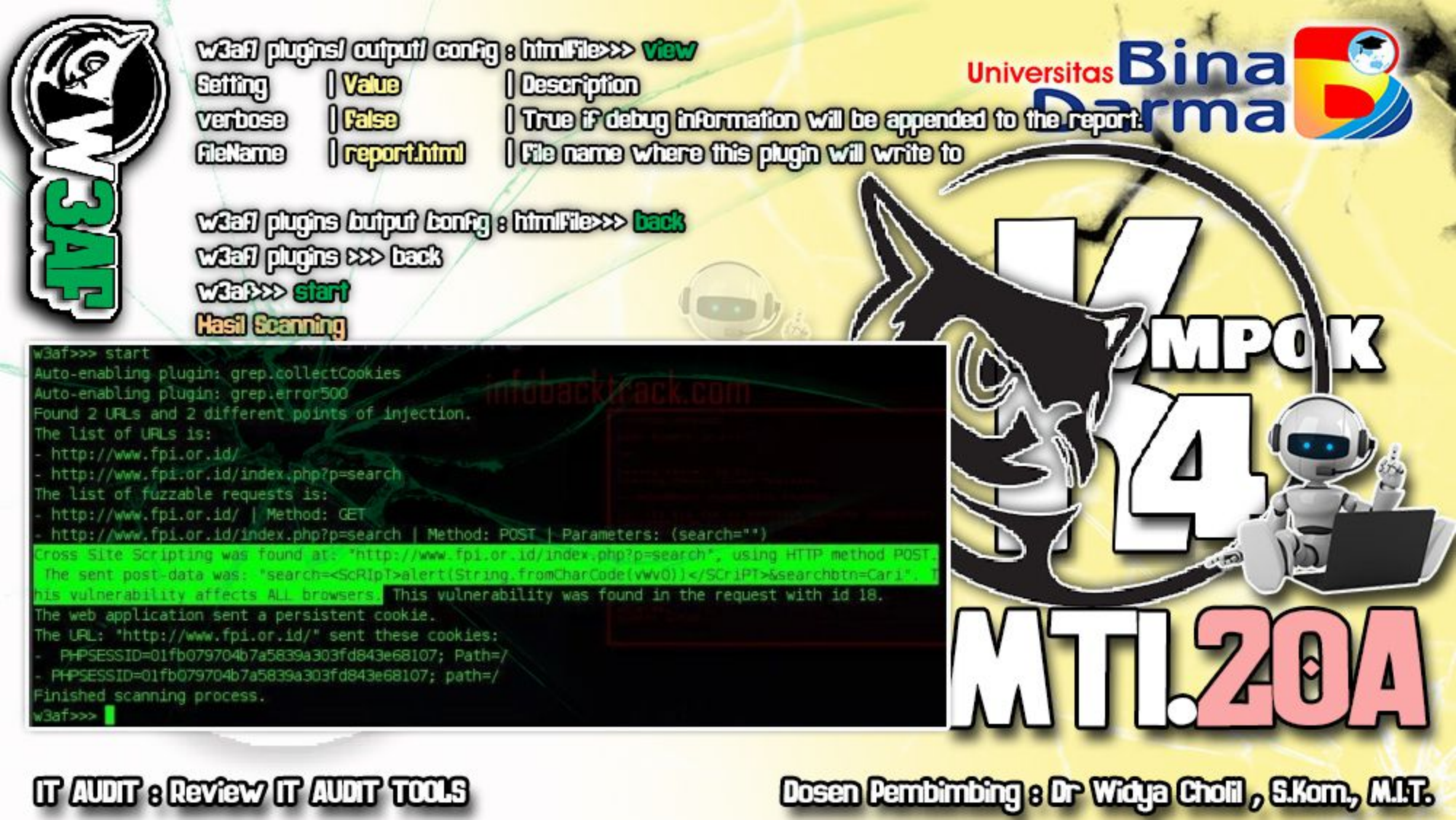
```
w3af>>> plugins
w3af/plugins>>> help
|-------------------------------------------------------------------------|
| list              | List available plugins.                             |
|-------------------------------------------------------------------------|
| back              | Go to the previous menu.                            |
| exit              | Exit w3af.                                          |
| assert            | Check assertion.                                    |
|-------------------------------------------------------------------------|
| discovery         | View, configure and enable discovery plugins        |
| output            | View, configure and enable output plugins           |
| mangle            | View, configure and enable mangle plugins           |
| evasion           | View, configure and enable evasion plugins          |
| bruteforce        | View, configure and enable bruteforce plugins       |
| audit             | View, configure and enable audit plugins            |
| grep              | View, configure and enable grep plugins             |
|-------------------------------------------------------------------------|
w3af/plugins>>> audit xss,xsrf,sqli
w3af/plugins>>> output console,htmlFile
w3af/plugins>>> output config htmlFile
```

Universitas Bina Darma

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.


w3af/plugins/output/config : htmlFile>>> view
Setting | Value | Description
verbose | False | True if debug information will be appended to the report.
fileName | report.html | File name where this plugin will write to
w3af/plugins/output/config : htmlFile>>> back
w3af/plugins >>> back
w3af>>> start
Hasil Scanning
w3af>>> start
Auto-enabling plugin: grep.collectCookies
Auto-enabling plugin: grep.error500
Found 2 URLs and 2 different points of injection.
The list of URLs is:
- http://www.fpi.or.id/
- http://www.fpi.or.id/index.php?p=search
The list of fuzzable requests is:
- http://www.fpi.or.id/ | Method: GET
- http://www.fpi.or.id/index.php?p=search | Method: POST | Parameters: (search="")
Cross Site Scripting was found at: "http://www.fpi.or.id/index.php?p=search", using HTTP method POST. The sent post-data was: "search=<ScRIpT>alert(String.fromCharCode(vWv0))</SCriPT>&searchbtn=Cari". This vulnerability affects ALL browsers. This vulnerability was found in the request with id 18.
The web application sent a persistent cookie.
The URL: "http://www.fpi.or.id/" sent these cookies:
- PHPSESSID=01fb079704b7a5839a303fd843e68107; Path=/
- PHPSESSID=01fb079704b7a5839a303fd843e68107; path=/
Finished scanning process.
w3af>>>
Universitas Bina Darma
KELOMPOK 4
MTI.20A
IT AUDIT : Review IT AUDIT TOOLS
Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Dari hasil scanning diatas, dapat kita ketahui kalau web tersebut memiliki kelemahan pada XSS. Potensi serangan yang dapat dilakukan attacker adalah melakukan

pemanggilan Get Web Shell, setelah pemanggilan web shell, maka web tersebut dapat diambil alih.

Universitas Bina Darma

W3AF

SEKIAN PEMAPARAN DARI KELOMPOK KAMI

TERIMA KASIH

KELOMPOK 4

MTI.20A

IT AUDIT : Review IT AUDIT TOOLS

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

MALTEGO

HARLI SEPTIA FANI (182420122)
PUTRI ARMILIA PRAYESY (182420125)
DEVIAN SAPUTRA (182420128)
I MADE HARYA WIJAYA OKA RAFFLESIA (182420129)
PUTRI ELEINA NURRAHMA (182420138)

MALTEGO

MALTEGO INI DISEBUT **OSINT** (**O**PEN **S**OURCE **I**NTELLIGENCE **G**ATHERING) SEBUAH ALAT UNTUK MELAKUKAN *FOOTPRINTING*, DIGUNAKAN UNTUK MENGUMPULKAN INFORMASI SEBANYAK MUNGKIN DENGAN TUJUAN FORENSIK, *PEN TESTING*, ATAU *ETHICAL HACKING*. APLIKASI YANG DIGUNAKAN UNTUK MEMETAKAN JARINGAN KOMUNIKASI YANG BERADA DI INTERNET TUJUANNYA ADALAH MENGUMPULKAN INFORMASI TENTANG TARGET DAN MENAMPILKAN INFORMASI TERSEBUT DALAM FORMAT YANG MUDAH DIMENGERTI, MEMVISUALISASIKAN INFORMASI TERSEBUT KE DALAM SEBUAH FORMAT GRAPH, SANGAT COCOK UNTUK *LINK ANALYSIS* DAN *DATA MINING*.

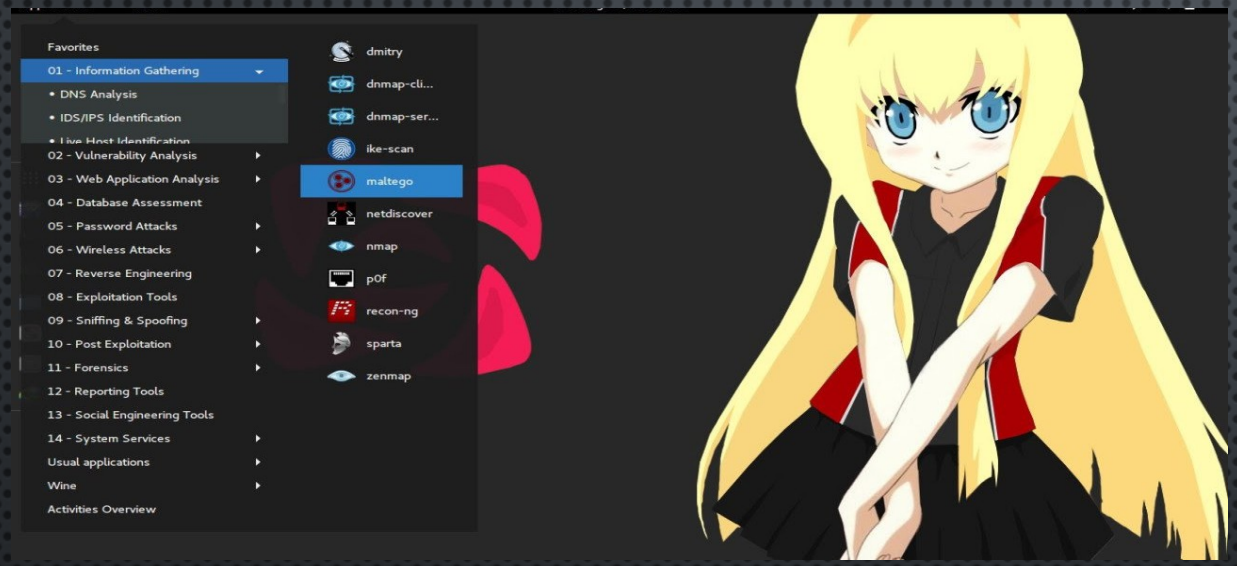
FUNGSI DARI MALTEGO ADALAH MEMUDAHKAN SESEOORANG YANG MENCARI INFORMASI TENTANG APA YANG MEREKA SELIDIKI ATAU MEREKA INCAR SEBAGAI TARGET, CONTOH KETIKA SEORANG MENCARI INFORMASI DARI SEBUAH DOMAIN MENGGUNAKAN MALTEGO, MAKA MALTEGO AKAN MENAMPIKAN BEBRAP INFORMASI SEPERTI BERIKUT:

- BLOCK IP HOSTING
- DOMAIN REGISTE
- EMAIL USER & ADMIN
- PHONE NUMBER
- PETA JARINGAN

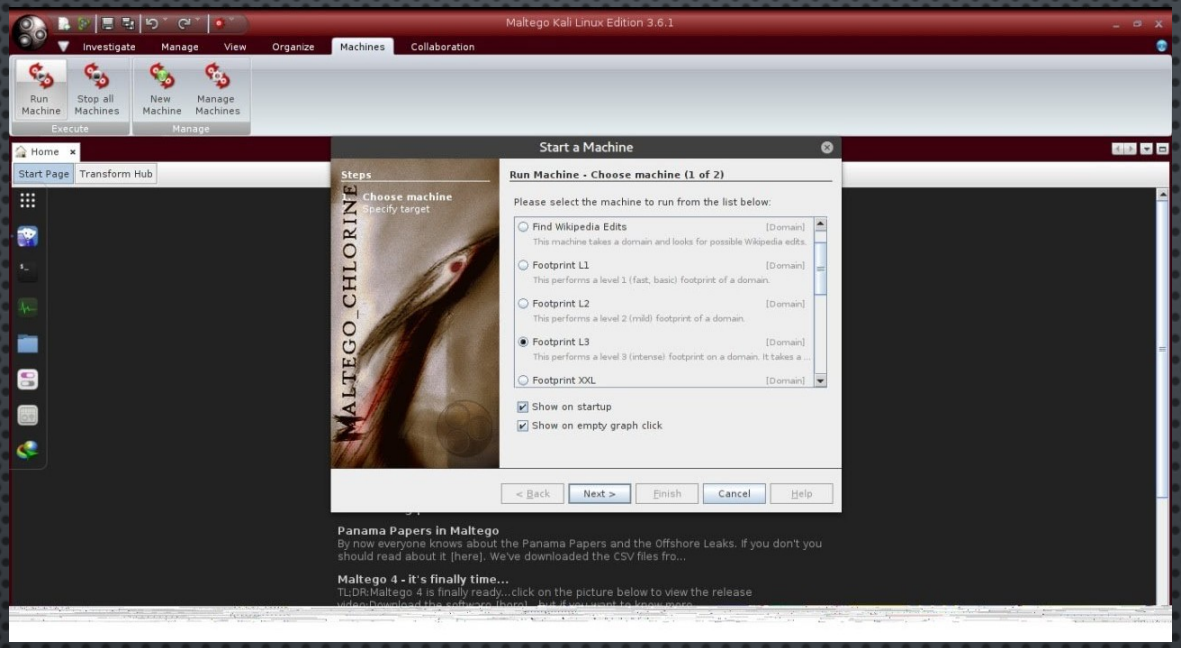
MALTEGO DIBEDAKAN MENJADI VERSI KOMERSIAL (COMMERCIAL EDITION) DAN VERSI GRATIS (COMMUNITY EDITION). VERSI GRATIS YANG TERSEDIA DI KALI LINUX HANYA DAPAT MENAMPILKAN MAKSIMAL 12 HASIL TRANSFORMASI, SEBAGAI SEBUAH FRONT-END UNTUK SERVER OSINT, MALTEGO VERSI GRATIS HANYA DAPAT MEMAKAI LAYANAN SERVER MILIK PATERVA. KARENA VERSI YANG DISEDIAKAN OLEH KALI LINUX ADALAH VERSI GRATIS DARI MALTEGO

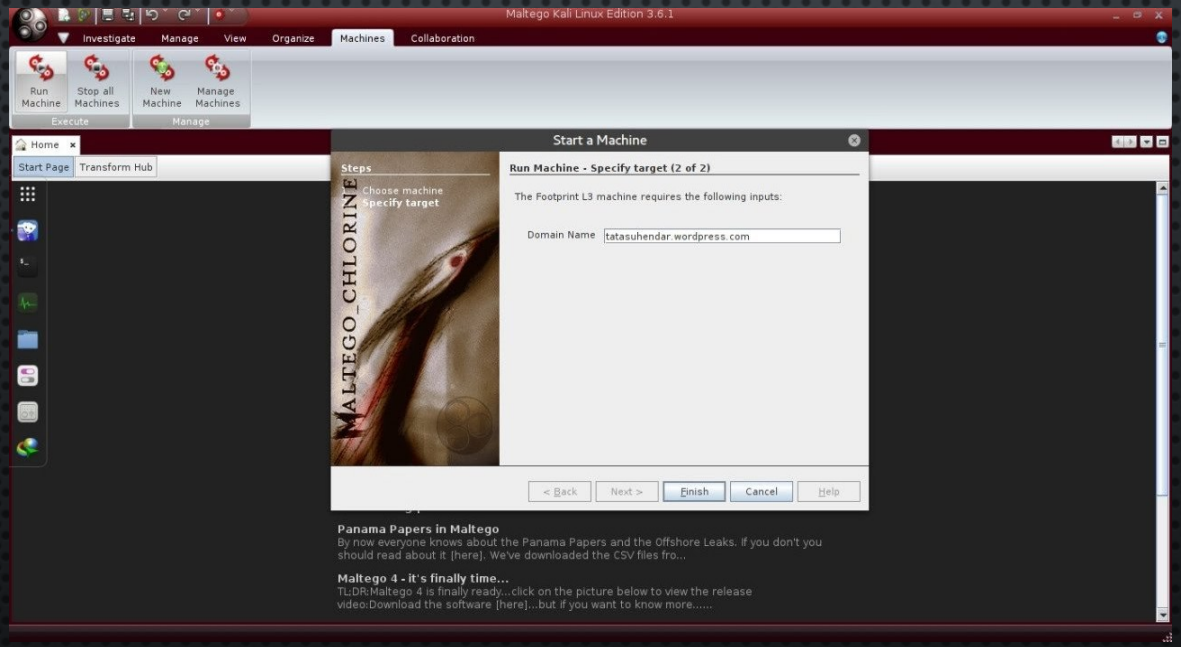
TAHAPAN DALAM PENGGUNAAN MALTEGO

1. BUKA MALTEGO PADA KALI LINUK ANDA, ADA DI MENU INFORMATION GATHERING > MALTEGO

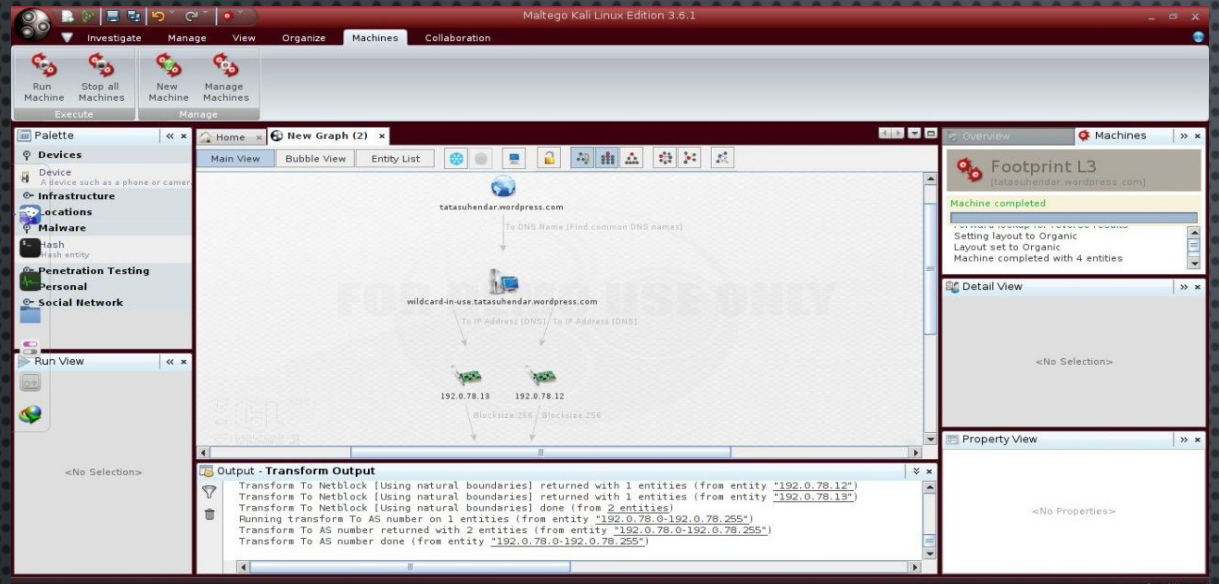


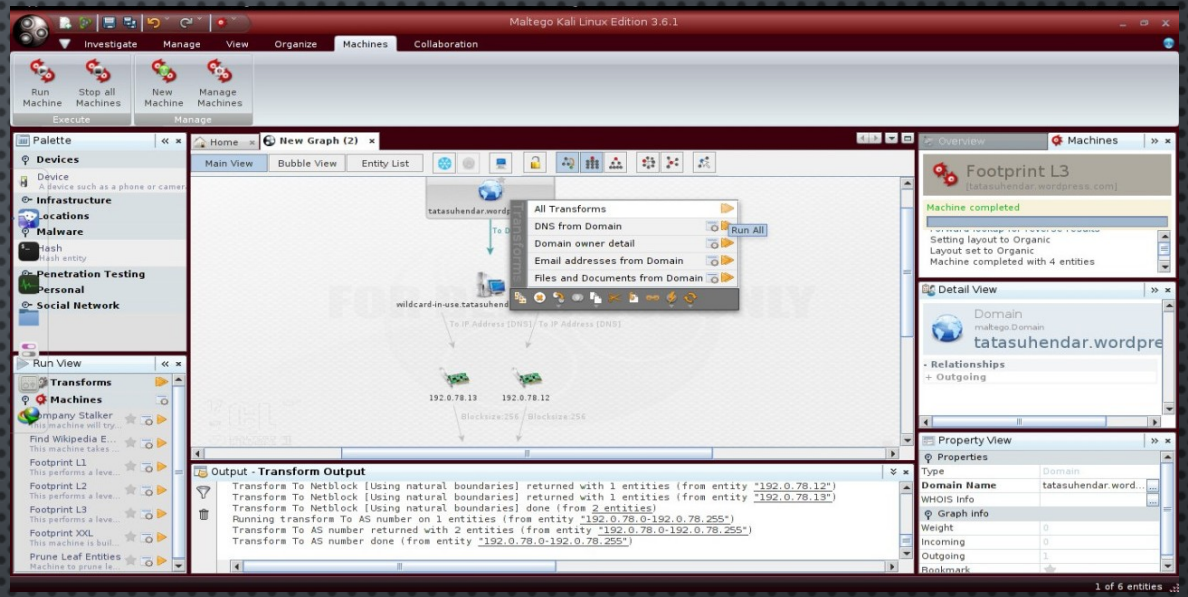
2. LOGIN DENGAN EMAIL DAN PASSWORD YANG TELAH TERDAFTAR
3. SETELAH SELESAI LOGIN MAKA AKAN MUNCUL DIALOG START A MACHINE, PILIH FOOTPRINTING L3 LALU DI STEP KEDUA KITA HARUS MAMASUKAN DOMAIN ATAU LINK WEBSITE TAGE


Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a ...
Footprint XXL [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release

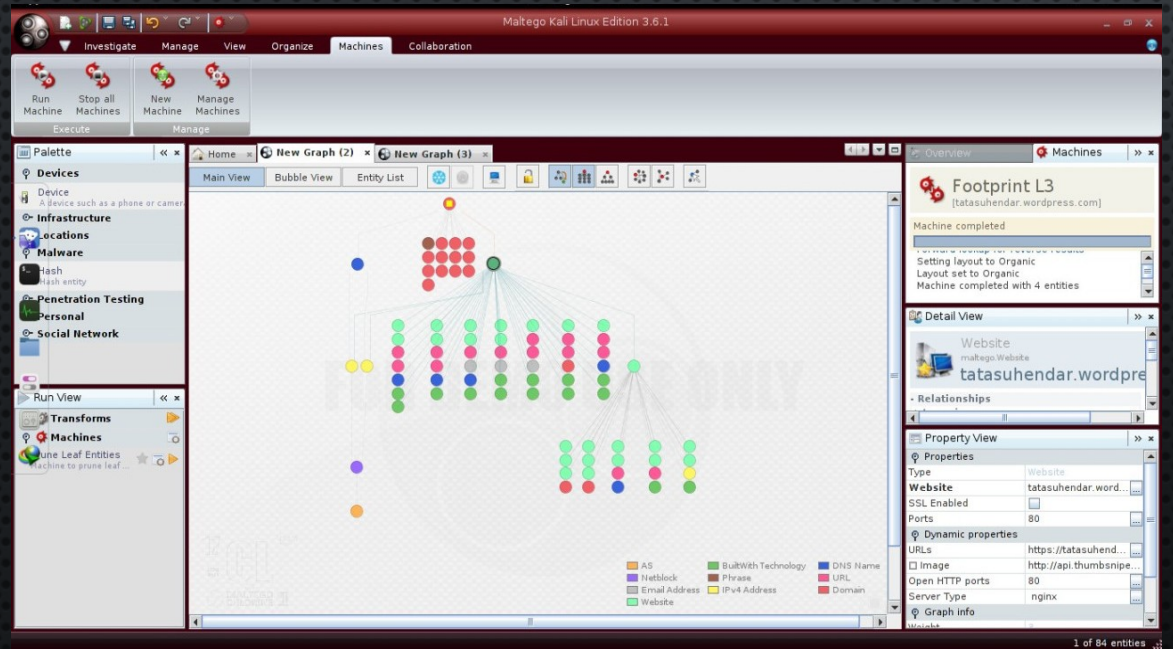

Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Run Machine
Stop all Machines
New Machine
Manage Machines
Execute
Manage
Home
Start Page
Transform Hub
Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Specify target (2 of 2)
The Footprint L3 machine requires the following inputs:
Domain Name
tatasuhendar.wordpress.com
< Back
Next >
Finish
Cancel
Help
Panama Papers in Maltego
By now everyone knows about the Panama Papers and the Offshore Leaks. If you don't you should read about it [here]. We've downloaded the CSV files fro...
Maltego 4 - it's finally time...
TL;DR:Maltego 4 is finally ready...click on the picture below to view the release
video:Download the software [here]...but if you want to know more.....

4. TAMPILAN AWALNYA KURANG LEBIH SEPERTI INI, DAN DISINI KITA BISA MENGGALI INFORMASI DARI TARGET DENGAN KLIK KANAN PADA WEB TARGET DAN RUN ALL TRANSFORMS

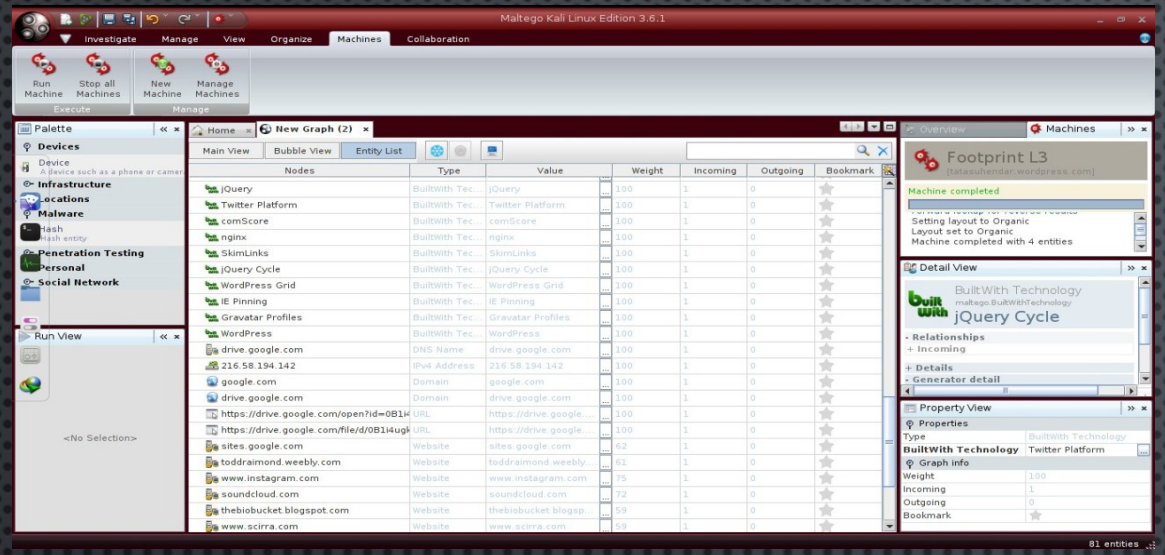




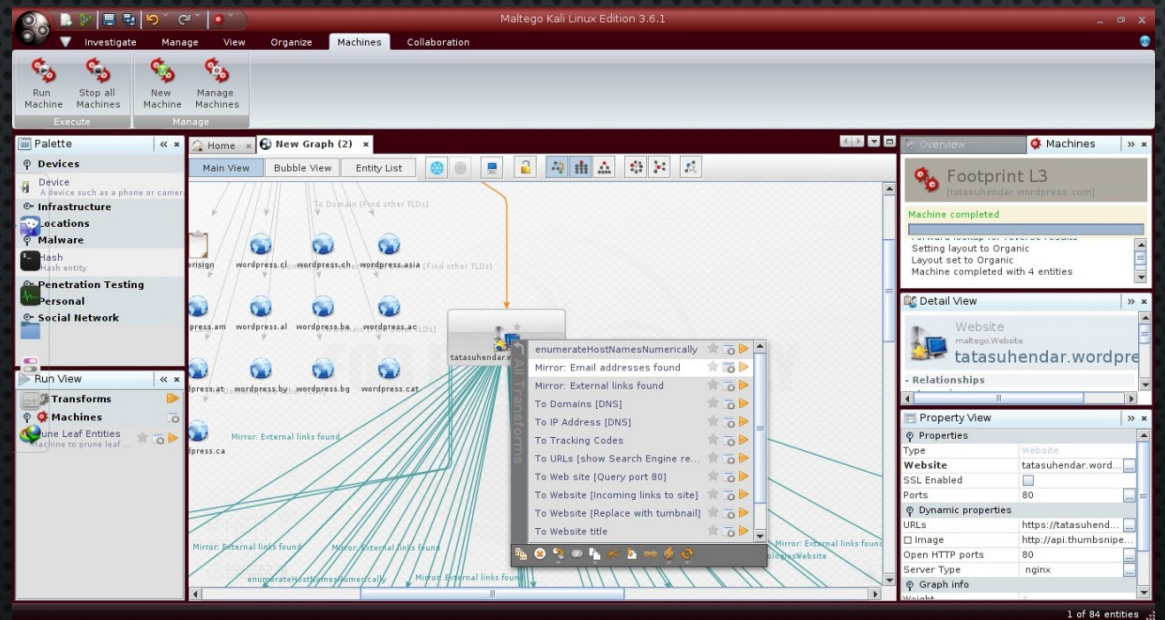
5. BEGINILAH TAMPILAN WEBSITE YANG DITARGETKAN TADI SUDAH DI ALL TRANSFORMS



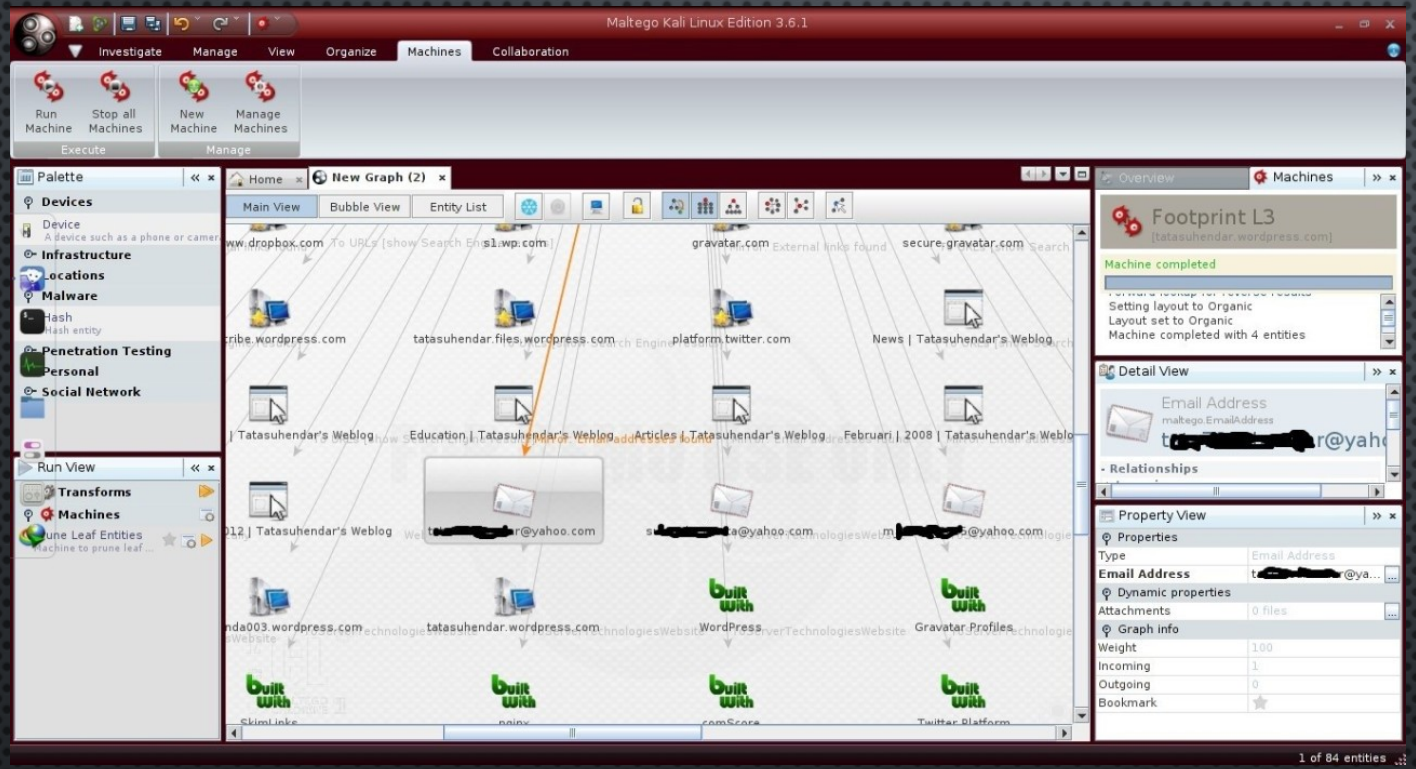
DAN DIBAWAH INI DALAM TAMPILAN ENTRY LIST



6. UNTUK MENCARI INFORMASI TENTANG ALAMAT EMAIL, PILIH IKON WEBNYA LALU KLIK KANAN PILIH“MIRROR: EMAIL ADDRESS FOUND”. INILAH HASILNYA TERDAPAT 3 EMAIL YG TERHUBUNG DENGAN WEB TERSEBUT



7. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA



8. UNTUK MENCARI DATA, DOKUMEN, ATAU YANG LAINNYA CARANYA SAMA SEPERTI MENCARI EMAIL, TINGGAK KLIK KANAN IKON WEBNYA DAN KLIK ALL TRANSFORMS UNTUK MENAMPILKANNYA

SOURCE

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

https://www.gagaltotal666.site/2016/06/cara-menggunakan-maltego-di-kali-linux.html?m=1

https://www.google.com/amp/s/flatisjusticeblog.wordpress.com/2016/08/31/menggali-informasi-menggunakan-maltego-di-kali-linux/amp/

TERIMAKASIH