Attacks and Malicious Code

• Chapter 3
Learning Objectives

• Explain denial-of-service (DoS) attacks
• Explain and discuss ping-of-death attacks
• Identify major components used in a DDoS attack and how they are installed
• Understand major types of spoofing attacks
• Discuss man-in-the-middle attacks, replay attacks, and TCP session hijacking
Learning Objectives

• Detail three types of social-engineering attacks and explain why they can be incredibly damaging
• List major types of attacks used against encrypted data
• List major types of malicious software and identify a countermeasure for each one
Denial-of-Service Attacks

- Any malicious act that causes a system to be unusable by its real user(s)
- Take numerous forms
- Are very common
- Can be very costly
- Major types
  - SYN flood
  - Smurf attack
SYN Flood

- Exploits the TCP three-way handshake
- Inhibits server’s ability to accept new TCP connections
TCP Three-Way Handshake

Figure 3-1  TCP three-way handshake
<table>
<thead>
<tr>
<th>E-commerce server</th>
<th>Half-open connections queue</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1- Full</td>
</tr>
<tr>
<td></td>
<td>2- Full</td>
</tr>
<tr>
<td></td>
<td>3- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>.- Full</td>
</tr>
<tr>
<td></td>
<td>x- Full</td>
</tr>
</tbody>
</table>

SYN/ACK replies sent back (to spoofed source address), but no response!

Can't connect

SYN packets with spoofed source

Figure 3-2 SYN flood attack
Figure 3-3  Defending against the SYN flood
Smurf

- Non-OS specific attack that uses the network to amplify its effect on the victim
- Floods a host with ICMP
- Saturates Internet connection with bogus traffic and delays/prevents legitimate traffic from reaching its destination
Figure 3-4  Smurf attack
IP Fragmentation Attacks: Ping of Death

• Uses IP packet fragmentation techniques to crash remote systems
Ping of Death

Maximum size normal packets

65,536 bytes → 65,536 bytes → 65,536 bytes

Ping-of-death packets

100,000+ bytes → 100,000+ bytes

Target computer’s operating system can’t accept or resolve specially constructed oversized packets and crashes

Figure 3-5 Ping of death
Distributed Denial-of-Service Attacks

- Use hundreds of hosts on the Internet to attack the victim by flooding its link to the Internet or depriving it of resources
- Used by hackers to target government and business Internet sites
- Automated tools; can be executed by script kiddies
- Result in temporary loss of access to a given site and associated loss in revenue and prestige
1. Scan for systems to hack

2. Install software to scan for, compromise, and infect agents

3. Agents get loaded with remote control attack software

4. Client issues commands to handlers which control agents in a mass attack

Figure 3-6  Distributed denial-of-service attack
Conducting DDoS Attacks

<table>
<thead>
<tr>
<th>Tools</th>
<th>Flooding or Attack Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trin00</td>
<td>UDP</td>
</tr>
<tr>
<td>Tribe flood network</td>
<td>UDP, ICMP, SYN smurf</td>
</tr>
<tr>
<td>Stacheldracht and variants</td>
<td>UDP, ICMP, SYN smurf</td>
</tr>
<tr>
<td>TFN 2K</td>
<td>UDP, ICMP, SYN smurf</td>
</tr>
<tr>
<td>Shaft</td>
<td>UDP, ICMP, SYN combo</td>
</tr>
<tr>
<td>Mstream</td>
<td>Stream (ACK)</td>
</tr>
<tr>
<td>Trinity, Trinity v3</td>
<td>UDP, SYN, RST, Random Flag, ACK, Fragment</td>
</tr>
</tbody>
</table>
DDoS Countermeasures

- Security patches from software vendors
- Antivirus software
- Firewalls
- Ingress (inbound) and egress (outbound) filtering
Ingress and Egress Filtering

Figure 3-7  Ingress and egress filtering
Preventing the Network from Inadvertently Attacking Others

• Filter packets coming into the network destined for a broadcast address
• Turn off directed broadcasts on internal routers
• Block any packet from entering the network that has a source address that is not permissible on the Internet (see Figures 3-8 and 3-9)
Preventing the Network from Inadvertently Attacking Others

• Block at the firewall any packet that uses a protocol or port that is not used for Internet communications on the network
• Block packets with a source address originating inside your network from entering your network
Ingress Filtering of Packets with RFC 1918 Addresses

Interface serial n
  IP access-group 101 in
!
access-list 101 deny IP 10.0.0.0 0.255.255.255 any
access-list 101 deny IP 192.168.0.0 0.0.255.255 any
access-list 101 deny IP 172.16.0.0 0.15.255.255 any
access-list 101 permit IP any any

Figure 3-8  Ingress filtering of packets with RFC 1918 addresses
Filtering of Packets with RFC 2827 Addresses

Figure 3-9 Filtering of packets with RFC 2827 addresses
Spoofing

• Act of falsely identifying a packet’s IP address, MAC address, etc
• Four primary types
  ◦ IP address spoofing
  ◦ ARP poisoning
  ◦ Web spoofing
  ◦ DNS spoofing
IP Address Spoofing

• Used to exploit trust relationships between two hosts
• Involves creating an IP address with a forged source address
Filtering spoofed packets

Host A: 192.168.1.1

Host B: 10.1.1.1

1. SYN flood

2. Attacker creates a packet with the source address of Host B (10.1.1.1)

3. Host A’s reply packets are sent to Host B, which is unable to process them

4. Attacker must guess the contents of Host A’s packet and craft an appropriate reply

Attacker: 172.16.24.1

Figure 3-10 Filtering spoofed packets
ARP Poisoning

• Used in man-in-the-middle and session hijacking attacks; attacker takes over victim’s IP address by corrupting ARP caches of directly connected machines

• Attack tools
  ◦ ARPoison
  ◦ Ettercap
  ◦ Parasite
Web Spoofing

• Convinces victim that he or she is visiting a real and legitimate site
• Considered both a man-in-the-middle attack and a denial-of-service attack
Web Spoofing

Figure 3-11  Web spoofing
DNS Spoofing

- Aggressor poses as the victim’s legitimate DNS server
- Can direct users to a compromised server
- Can redirect corporate e-mail through a hacker’s server where it can be copied or modified before sending mail to final destination
To Thwart Spoofing Attacks

- **IP spoofing**
  - Disable source routing on all internal routers
  - Filter out packets entering local network from the Internet that have a source address of the local network

- **ARP poisoning**
  - Use network switches that have MAC binding features
To Thwart Spoofing Attacks

- Web spoofing
  - Educate users
- DNS spoofing
  - Thoroughly secure DNS servers
  - Deploy anti-IP address spoofing measures
Man in the Middle

• Class of attacks in which the attacker places himself between two communicating hosts and listens in on their session
• To protect against
  ◦ Configure routers to ignore ICMP redirect packets
Man-in-the-Middle Attacks

**Host A**
Thinks it's communicating with Host B

**Attacker**
Sits between the two hosts and is able to monitor and modify their transmissions

**Host B**
Thinks it's communicating with Host A

*Figure 3-12  Man-in-the-middle attacks*
Man-in-the-Middle Applications

- Web spoofing
- TCP session hijacking
- Information theft
- Other attacks (denial-of-service attacks, corruption of transmitted data, traffic analysis to gain information about victim’s network)
Man-in-the-Middle Methods

- ARP poisoning
- ICMP redirects
- DNS poisoning
Replay Attacks

- Attempts to circumvent authentication mechanisms by:
  - Recording authentication messages from a legitimate user
  - Reissuing those messages in order to impersonate the user and gain access to systems
Replay Attack

Figure 3-13  Replay attack
TCP Session Hijacking

- Attacker uses techniques to make the victim believe he or she is connected to a trusted host, when in fact the victim is communicating with the attacker
- Well-known tool
  - Hunt (Linux)
Figure 3-14  Attacker using source Ethernet segment as user
Attacker Using Victim’s TCP Connection

The hunt program is executed

ARP hijacking will be used

The attacker will hijack session 0

The attacker has taken over the session as if he is the victim. He can execute commands using the victim’s privileges

FQR3SBC
Social Engineering

• Class of attacks that uses trickery on people instead of computers
• Goals
  ○ Fraud
  ○ Network intrusion
  ○ Industrial espionage
  ○ Identity theft
  ○ Desire to disrupt the system or network
## Dumpster Diving

### Table 3-2 Useful information gathered from trash bins

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal phone directories</strong></td>
<td>Names and numbers of people to target and impersonate—many usernames are based on legal names</td>
</tr>
<tr>
<td><strong>Organizational charts</strong></td>
<td>Information about people who are in positions of authority within the organization</td>
</tr>
<tr>
<td><strong>Policy manuals</strong></td>
<td>How secure (or insecure) the company really is</td>
</tr>
<tr>
<td><strong>Calendars</strong></td>
<td>Which employees are out of town at a particular time</td>
</tr>
<tr>
<td><strong>Outdated hardware</strong></td>
<td>Hard drives may be restored to provide all sorts of useful information</td>
</tr>
<tr>
<td><strong>System manuals, network diagrams, and other sources of technical information</strong></td>
<td>The exact information that attackers may seek, including the IP addresses of key assets, network topologies, locations of firewalls and intrusion detection systems, operating systems, applications in use, and more</td>
</tr>
</tbody>
</table>
Online Attacks

• Use chat and e-mails venues to exploit trust relationships
Social Engineering Countermeasures

- Take proper care of trash and discarded items
- Ensure that all system users have periodic training about network security
Attacks Against Encrypted Data

- Weak keys
- Mathematical attacks
- Birthday attack
- Password guessing
- Brute force
- Dictionary
Weak Keys

- Secret keys used in encryption that exhibit regularities in encryption, or even a poor level of encryption
Mathematical Attack

• Attempts to decrypt encrypted data using mathematics to find weaknesses in the encryption algorithm
• Categories of cryptanalysis
  ◦ Cyphertext-only analysis
  ◦ Known plaintext attack
  ◦ Chosen plaintext attack
Birthday Attack

• Class of brute-force mathematical attacks that exploits mathematical weaknesses of hash algorithms and one-way hash functions
Password Guessing

• Tricks authentication mechanisms by determining a user’s password using techniques such as brute force or dictionary attacks
Figure 3-15  Multilayered approach to virus scanning
Brute Force

• Method of breaking passwords that involves computation of every possible combination of characters for a password of a given character length
Dictionary

- Method of breaking passwords by using a predetermined list of words as input to the password hash
- Only works against poorly chosen passwords
Software Exploitation

• Utilizes software vulnerabilities to gain access and compromise systems
• Example
  ◦ Buffer overflow attach
• To stop software exploits
  ◦ Stay appraised of latest security patches provided by software vendors
## Malicious Software

### Table 3-3  Malware differences

<table>
<thead>
<tr>
<th>Type</th>
<th>Propagation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>Copies itself into other executable programs and scripts</td>
<td>Melissa</td>
</tr>
<tr>
<td>Worm</td>
<td>Exploits vulnerabilities with the intent of propagating itself across the network</td>
<td>Code Red, Code Red II, Nimda</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>Uses social engineering techniques to trick users into running the malware’s executable</td>
<td>ILOVEYOU, Naked Wife, Anna Kournikova</td>
</tr>
</tbody>
</table>
Viruses

- Self-replicating programs that spread by “infecting” other programs
- Damaging and costly
<table>
<thead>
<tr>
<th>Type</th>
<th>Primary Period</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot sector</td>
<td>1980s to mid-90s</td>
<td>Spread by infecting floppy or hard disk boot sectors; when an infected disk is booted, the virus is loaded into memory and attempts to infect any and all floppy disks inserted into the computer</td>
</tr>
<tr>
<td>File infector</td>
<td>mid-90s</td>
<td>A class called “parasitic viruses” because they must infect other programs, file infectors copy themselves into other programs. When an infected file is executed, the virus is loaded into memory and tries to infect other executables. File types commonly infected include: *.exe, *.drv, *.dll, *.bin, *.ovl, *.sys, *.com</td>
</tr>
<tr>
<td>Multipartite</td>
<td>mid-90s</td>
<td>Propagated using both boot sector and file infector methods</td>
</tr>
<tr>
<td>Macro viruses</td>
<td>Current</td>
<td>Currently accounting for the vast majority of viruses, macro viruses are application specific as opposed to OS specific and propagate very rapidly via e-mail. Many macro viruses are Visual Basic scripts that exploit commonly used Microsoft applications such as Word, Excel, and Outlook.</td>
</tr>
</tbody>
</table>
## Virus Databases

### Table 3-5: Virus Databases

<table>
<thead>
<tr>
<th>Network Associates (McAfee)</th>
<th><a href="http://vil.nai.com/VIL/default.asp">http://vil.nai.com/VIL/default.asp</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec</td>
<td><a href="http://securityresponse.symantec.com/avcenter/vinfodb.html">http://securityresponse.symantec.com/avcenter/vinfodb.html</a></td>
</tr>
<tr>
<td>Computer Associates</td>
<td>www3.ca.com/virus/encyclopedia.asp</td>
</tr>
<tr>
<td>Trend Micro</td>
<td><a href="http://www.antivirus.com/vinfo/virusencyclo/">www.antivirus.com/vinfo/virusencyclo/</a></td>
</tr>
</tbody>
</table>
## Evolution of Virus Propagation Techniques

<table>
<thead>
<tr>
<th>Virus</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKA</td>
<td>January 1999</td>
<td>Single mailer</td>
</tr>
<tr>
<td>Melissa</td>
<td>March 1999</td>
<td>Mass mailer targeting 50 recipients in a single activation</td>
</tr>
<tr>
<td>Babylonia</td>
<td>December 1999</td>
<td>Mass mailer using plug-in techniques</td>
</tr>
<tr>
<td>LoveLetter</td>
<td>May 2000</td>
<td>Mass mailer targeting all recipients in the victim’s address book, in multiple activations</td>
</tr>
<tr>
<td>MTX</td>
<td>August 2000</td>
<td>Mass mailer incorporating file infector, sharing network, and backdoor features</td>
</tr>
<tr>
<td>Nimda</td>
<td>September 2001</td>
<td>Mass mailer, also incorporating file infector, sharing network, backdoor process, and IIS infector methods</td>
</tr>
</tbody>
</table>
Protecting Against Viruses

• Enterprise virus protection solutions
  ◦ Desktop antivirus programs
  ◦ Virus filters for e-mail servers
  ◦ Network appliances that detect and remove viruses

• Instill good behaviors in users and system administrators
  ◦ Keep security patches and virus signature databases up to date
Backdoor

• Remote access program surreptitiously installed on user computers that allows attacker to control behavior of victim’s computer
• Also known as remote access Trojans
• Examples
  ◦ Back Orifice 2000 (BO2K)
  ◦ NetBus
• Detection and elimination
  ◦ Up-to-date antivirus software
  ◦ Intrusion detection systems (IDS)
Figure 3-16  BO2K configuration screen
Figure 3-17  NetBus commands
Trojan Horses

• Class of malware that uses social engineering to spread
• Types of methods
  ◦ Sending copies of itself to all recipients in user’s address book
  ◦ Deleting or modifying files
  ◦ Installing backdoor/remote control programs
Logic Bombs

• Set of computer instructions that lie dormant until triggered by a specific event
• Once triggered, the logic bomb performs a malicious task
• Almost impossible to detect until after triggered
• Often the work of former employees
• For example: macro virus
  ◦ Uses auto-execution feature of specific applications
Worms

- Self-contained program that uses security flaws such as buffer overflows to remotely compromise a victim and replicate itself to that system
- Do not infect other executable programs
- Account for 80% of all malicious activity on Internet
- Examples: Code Red, Code Red II, Nimda
Defense Against Worms

- Latest security updates for all servers
- Network and host-based IDS
- Antivirus programs
Chapter Summary

• Mechanisms, countermeasures, and best practices for:
  ◦ Malicious software
  ◦ Denial-of-service attacks
  ◦ Software exploits
  ◦ Social engineering
  ◦ Attacks on encrypted data