Hands-On Ethical Hacking and Network Defense, 3rd Edition

Chapter 3

Network and Computer Attacks

Objectives

After completing this chapter, you will be able to:

- Describe the different types of malicious software and what damage they can do
- Describe methods of protecting against malware attacks
- Describe the types of network attacks
- Identify physical security attacks and vulnerabilities

Malicious Software (Malware)

- Network attacks prevent a business from operating
- Malicious software (malware)
  - Virus
  - Worm
  - Trojan program
- Goals
  - Main goal is to make money
- Malware was once targeted specifically at Windows, Linux, and other traditional OSs
  - Now target tablets, smartphones, and other devices

Viruses

- Virus – a program that attaches itself to a file or another program
  - Needs host to replicate
  - Does not stand on its own
  - No foolproof prevention method
- Examples:
  - Phishing – e-mail sender who uses social engineering to lure a user to follow a malicious link
  - Ransomware – a type of virus that locks a target system until a ransom is paid

Viruses

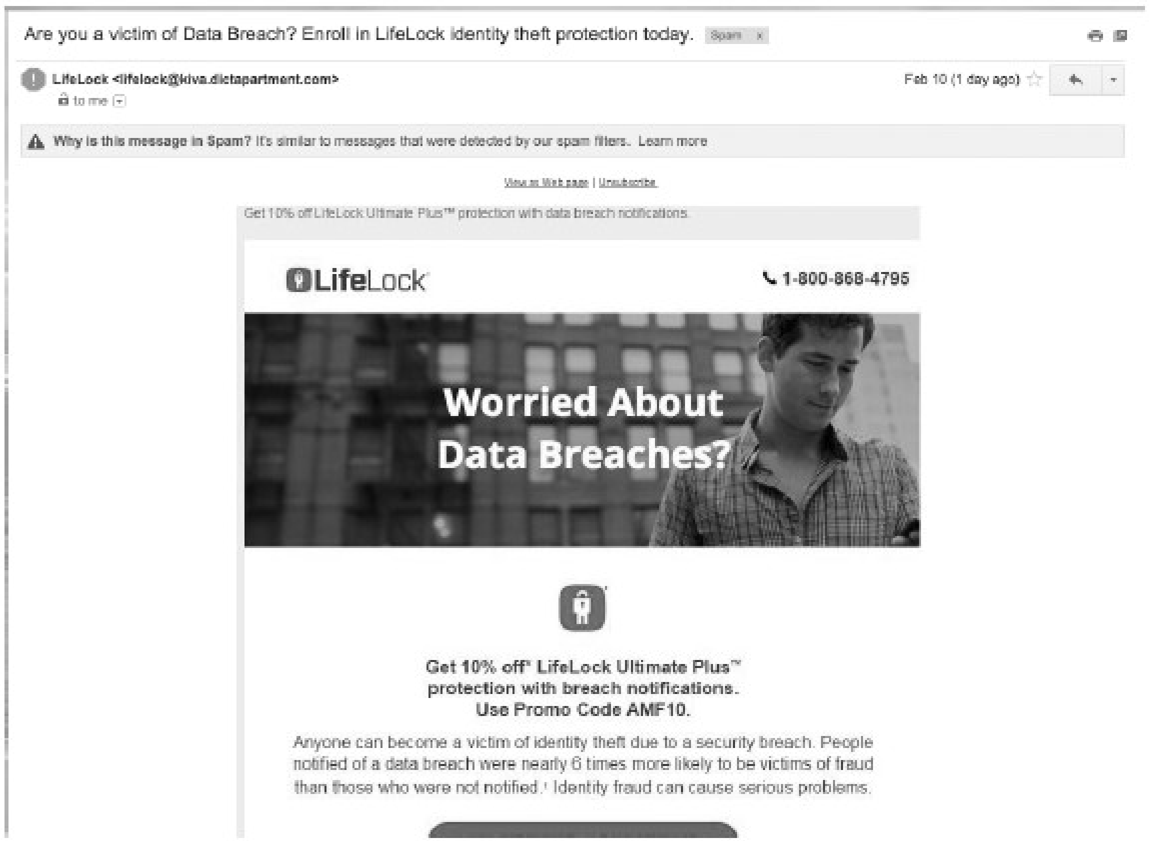

Figure 3-1 A phishing e-mail message

Viruses

- Antivirus programs
  - Detection based on virus signatures
    - Signatures are kept in virus signature file
    - Must update periodically
    - Some offer automatic update feature

Viruses

Virus	Description
CryptoLocker	As of January 2016, this "ransomware" virus is estimated to have infected over 250,000 computers. This malware locks the user's files in an encrypted container and requires the victim to pay ransom for their decryption. Like most malware, it is delivered through an e-mail that is designed to trick the user in to clicking on a malicious link or attachment. Once a machine is infected, the victim has a set amount of time to pay the ransom if they want to retrieve their files. Payment is currently only accepted via BitCoin and averages about $300 USD per victim.
MalumPOS	A recent trend in malware has been to target devices responsible for processing payments, referred to as POS (Point of Sale) systems. The MalumPOS virus was used in mid 2015 to attack POS devices at hotel chains. This virus was programmed to find, intercept, copy, and exfiltrate payment card information (e.g., credit/debit card numbers and other information stored on the magnetic track of a credit card).
Carbanak	This virus is spread via phishing e-mails that almost always target financial institutions. These phishing e-mails contain a word document and a malicious .cpl file (keep this in mind for the upcoming base-64 decoding exercise). Once initial access is gained, the malware runs a number of checks to ensure it's able to gain the proper privileges to further its attack. Once proper privileges are gained or verified, a backdoor is opened to a few remote servers under the control of an unknown (to this point) malicious actor. This malware has been used to facilitate fraudulent transactions in financial institutions' funds transfer systems and ATM machines.
Gumblar	First detected in March 2009, this malware spread by mass-hacking hundreds of thousands of Web sites, which then exploited visiting browsers via Adobe PDF and Flash vulnerabilities. The malware steals FTP credentials that are used to further compromise Web sites that the victim maintains. It also hijacks Google searches and blocks access to antivirus update sites to prevent removal. Recent variations install a backdoor that attempts to connect to a botnet.
Gpcode	This "ransomware" virus detected in 2008 isn't widespread but is unique because it uses practically unbreakable 1024-bit asymmetric key encryption to hide a user's documents on the computer and hold them for ransom until the victim pays to get the encryption key.

Table 3-1 Common computer viruses

Viruses

- Some viruses contained in e-mail attachments were encoded in base 64
- Running a base-64 decoder on suspicious attachments can help determine if malware or viruses are detected
- Examples of what to look for:
  - Hidden computer programs
  - Executable pieces of programming code

Macro Viruses

- Macro virus
  - A virus encoded as a macro in programs that support a macro programming language (e.g., Visual Basic for Applications)
  - Basically a lists of commands
    - Can be used in destructive ways
  - Example: Melissa - appeared in 1999
- Even nonprogrammers can create macro viruses
  - Instructions posted on Web sites
    - Security professionals learn from thinking like attackers

Worms

- Worm
  - A program that replicates and propagates without a host
  - Infamous examples:
    - Stuxnet
    - Code Red
    - Conficker
- Theoretically can infect every computer in the world over a short period

Worms

Worm	Description
Flame (aka sKyWiper)	Often touted as the most complex malware ever created, Flame was discovered in May of 2012. It used advanced techniques to infect both local and remote computers. Its capabilities included: microphone/webcam spying, keystroke logging, and screen capturing.
Stuxnet	In 2010, this malicious code was found on the Industrial Control Systems (ICS) in a nuclear production facility in Iran. Believed to have been delivered via USB, the worm may have used newly discovered Windows exploits to propagate itself, according to later analysis. Once the malware spread to a system that was running specific control software, the malware took control of the attached uranium refinement equipment, causing centrifuges to spin erratically and then fail. This is analogous to making a washing machine spin so fast that the motor burns out!

Table 3-2 **Common computer worms (*continues*)**

Worms

Worm	Description
Duqu	Detected in October of 2011, it had similar design features to Stuxnet but with a different objective. Instead of causing damage to uranium refinement equipment, its goal was to steal data from users. This malware targeted government agencies in Europe and the Middle East, where the majority of infections occurred.
Storm	Detected in January 2007, this worm is spread by automatically generated e-mail messages. It is estimated that this botnet Trojan program and its variants infected millions of systems.
Waledac	This e-mail worm harvests and forwards passwords and spreads itself in an e-mail with an attachment called eCard.exe. It has many variants that can be controlled remotely. A recent variant used a geographic IP address lookup to customize the e-mail message so that it looked like a Reuters news story about a dirty bomb that exploded in a city near the victim.
Conficker	Detected in late 2008, this botnet worm and its variants propagated through the Internet by using a Microsoft network service vulnerability. It updates itself dynamically but can be detected remotely with a standard port scanner, such as Nmap, and a special Conficker signature plug-in.
Slammer	Detected in 2003, this worm was purported to have shut down more than 13,000 ATMs of one of the largest banks in America by infecting database servers located on the same network.

Table 3-2 Common computer worms (*continued*)

Worms

- Some infamous worms have cost businesses billions of dollars as a result of:
  - Lost productivity caused by computer downtime
  - Time spent on recovery lost data, reinstalling programs and OSs
  - Hiring or contracting IT personnel
- Security professionals are working to protect automated teller machines (ATMs)
  - Cyberattack against ATMs are a serious concern

Trojan Programs

- Insidious attack against networks and computers
  - Disguise themselves as useful programs
  - Can install backdoors and rootkits
    - Allow attackers remote access
    - Rootkits are created after an attack and usually hide itself in the OS tools
- A good software or hardware firewall
  - Identifies traffic on unfamiliar ports
- Trojan programs can use known ports
  - TCP port 80 (HTTP) or UDP port 53 (DNS)

Trojan Programs

Trojan program	TCP ports used
W32.Korgo.A	13, 2041, and 3067
Backdoor.Rtkit.B	445
Backdoor.Systsec, Backdoor.Zincite.A	1034
W32.Beagle.Y@mm	1234
W32.Mytob.MX@mm	7000
Agobot, Backdoor.Hacarmy.C, Linux.Backdoor.Kaitenh, Backdoor.Clt, Backdoor.IRC.Flood.E, Backdoor.Spigot.C, Backdoor.IrcContact, Backdoor.DarkFtp, Backdoor.Slackbot.B	6667
Backdoor.Danton	6969
Backdoor.Nemog.C	4661, 4242, 8080, 4646, 6565, and 3306

Table 3-3 Trojan programs and ports

Spyware

- Sends information from infected computer to attacker
  – Confidential financial data
  – Passwords
  – PINs
  – Any other stored data
- Can register each keystroke entered
  – Prevalent technology
- Educate users about spyware

Spyware

Figure 3-2 A spyware initiation program

Adware

- Similar to spyware
  - Installed without users being aware
- Sometimes displays a banner
- Main purpose
  - Determine user’s purchasing habits
    - Tailors advertisement
- Main problem
  - Slows down computers

Protecting Against Malware Attacks

- Difficult task
  - New viruses, worms, and Trojan programs appear daily
- Antivirus programs
  - Can detect many malware programs
- Educate users about these attacks
  - Users who aren't trained thoroughly can open holes into a network that no technology can protect against

Protecting Against Malware Attacks

Figure 3-3 Detecting a virus

Source: McAfee

Educating Your Users

- Structural training
  - Includes all employees and management
  - E-mail monthly security updates
  - Recommend virus signature database updating
    - Activate automatic updates
- Whitelisting
  - Allows only approved programs to run on computers
- Another recommendation to make is to update virus signature files as soon as they are available from the vendor

Educating Your Users

- Two popular spyware and adware removal programs:
  - SpyBot Search and Destroy
  - Malwarebytes Anti-Malware (MBAM)
- Firewalls
  - Software (personal) and hardware (enterprise)

Avoiding Fear Tactics

- Avoid scaring users into complying with security measures
  - Sometimes used by unethical security testers
    - Against the OSSTMM's Rules of Engagement
- Promote awareness rather than instilling fear
  - Users should be aware of potential threats
  - Build on users' knowledge
    - Makes training easier

Intruder Attacks on Networks and Computers

- Attack
  - Any attempt by an unauthorized person to access, damage, or use network resources
  - Usually happens when a weakness or a vulnerability is exploited
- Exploit
  - A specially crafted string of data intended to take advantage of a vulnerability
- Network security
  - Concern with security of network infrastructure

Intruder Attacks on Networks and Computers

- Computer security
  - Concerned with security of a stand alone computer
    - Not part of a network infrastructure
- Computer crime
  - Fastest growing type of crime worldwide

Denial-of-Service Attacks

- Denial-of-service (DoS) attack
  - Prevents legitimate users from accessing network resources
  - Some forms do not involve computers
- Attackers do not attempt to access information
  - May just want to cripple the network
- Installing an attack yourself is not wise
  - Only explain how the attack could happen

Denial-of-Service Attacks

- Ping of Death Attacks
  - Type of DoS attack
    - Not as common as during the late 1990s
  - How it works
    - Attacker creates a large ICMP packet
      - More than allowed 65,535 bytes
    - Large packet is fragmented into small packets
      - Reassembled at destination
    - Destination point cannot handle reassembled oversize packet
      - Causes it to crash or freeze

Distributed Denial-of-Service Attacks

- Distributed denial-of-service (DDoS) attack
  - Attack on host from multiple servers or workstations
  - Network could be flooded with billions of packets
    - Loss of bandwidth
    - Degradation or loss of speed
  - Often participants are not aware they are part of the attack
    - They, too, have been attacked
- A Dark DDoS attack
  - A smokescreen to distract network defenders while another more damaging attack is occurring

Buffer Overflow Attacks

- Attacker finds a vulnerability in poorly written code
  - Doesn’t check for amount of memory space use
- Attacker writes code that overflows buffer
  - Fills buffer with executable program code
  - OS runs this code
  - Code elevates attacker’s permission
    - Administrator, owner, or creator
- Train programmer in developing applications with security in mind

Buffer Overflow Attacks

Buffer overflow	Description
GHOST	This vulnerability made headlines across the globe when it was discovered by security researchers at Qualys. Under the right conditions, GHOST could be exploited to gain administrative access to a remote system with no credentials. The vulnerability resulted from a weakness with the "glibc" library, central component of Linux operating systems. For more details, visit *https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability*.
Cisco ASA Internet Key Exchange	Cisco Security Advisory for CVE-2016-1287 (*https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike*) discusses this serious buffer overflow vulnerability in Cisco's ASA product line. Attackers could send a specially crafted packet to the affected device, which would allow them to gain full administrative privileges. This attack could be carried out from anywhere on the Internet if ASAs are in use on a company's perimeter.
StageFright Android Overflow Vulnerability	Buffer overflows not only affect traditional operating systems but mobile devices as well. This vulnerability, CVE-2015-1538, was found in Android's media playback libraries. Researchers found that a special MMS (Multimedia Messaging Service) message sent to a target Android device could cause an overflow, which allows for remote code execution without any user interaction.
Windows Server Service	Microsoft Security Bulletin MS08-067 (*www.microsoft.com/technet/security/Bulletin/MS08-067.mspx*) discusses this buffer overflow vulnerability, which makes it possible for attackers to run arbitrary code placed in memory. This vulnerability allowed the infamous Conficker worm to spread.

Table 3-4 Buffer overflow vulnerabilities

Eavesdropping

- An attacker can listen in on unencrypted network communications
  - In order to intercept confidential information or gather credentials that can be used to extend attack
- Accomplished with sniffing tools
  - Designed to capture copies of packets being sent across a network
- To defend against eavesdropping
  - Network equipment and applications should be forced to communicate only over encrypted protocols

Man-in-the-Middle

- Attackers can inject themselves between two parties or systems communicating
  - In order to manipulate messages being passed back and forth

Network Session Hijacking

- Enables attacker to join a TCP session
  - Attacker makes both parties think he or she is the other party
- Complex attack
  - Beyond the scope of this book

Addressing Physical Security

- Protecting a network
  - Requires physical security
- Inside attacks
  - Are more likely than outside attacks

Keyloggers

- Used to capture keystrokes on a computer
  - Software
    - Loaded on to computer
    - Behaves like Trojan programs
  - Hardware
    - Small and easy to install device
    - Goes between keyboard and computer
    - Examples: Key Grabber and KeyGhost
- Available as software (spyware)
  - Retrieved information can be e-mailed or transferred to a remote location

Keyloggers

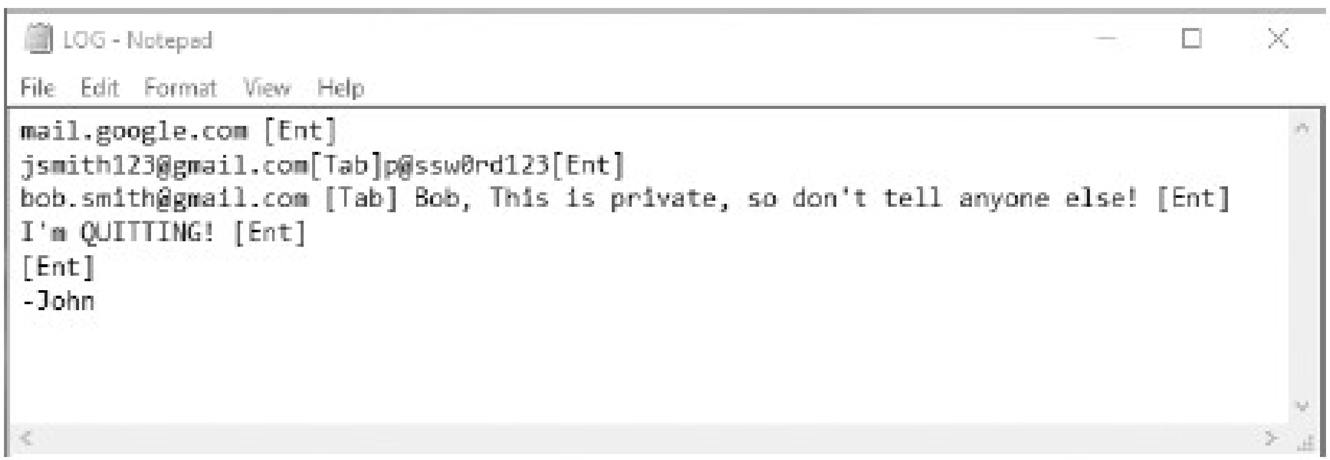

Figure 3-4 An e-mail message captured by Key Grabber

Source: Key Grabber

Keyloggers

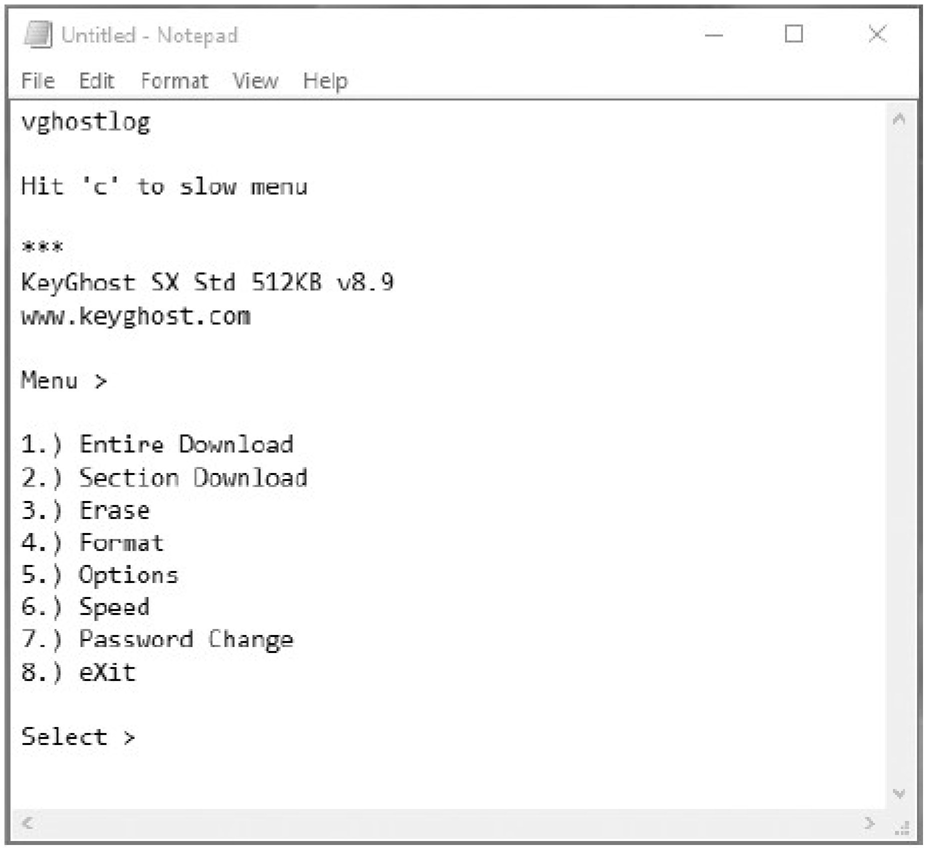

Figure 3-5 The KeyGhost menu

Source: KeyGhost

Behind Locked Doors

- Lock up servers
  - Average person
    - Can pick deadbolt lock in less than five minutes
    - After only a week or two of practice
  - Experienced hackers
    - Can pick deadbolt lock in under 30 seconds
- Rotary locks are harder to pick
  - Require pushing in a sequence of numbered bars
- Keep a record of who enters and leaves the room
  - Security cards can be used for better security

Summary

- Be aware of attacks
  - Network infrastructures and standalone computers
  - Can be perpetrated by insiders or outside attackers
- Malicious software
  - Viruses
  - Worms
  - Trojan programs
  - Spyware
  - Adware

Summary

- Attacks
  - Denial-of-Service (DoS)
  - Distributed Denial-of-Service (DDoS)
  - Buffer overflow
  - Ping of Death
  - Session hijacking
- Keyloggers
  - Monitor computer system
- Physical security
  - Everyone’s responsibility