Hands-On Ethical Hacking and Network Defense, Edition 4

Chapter 3: Network and Computer Attacks

Module Objectives

- By the end of this module, you should 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

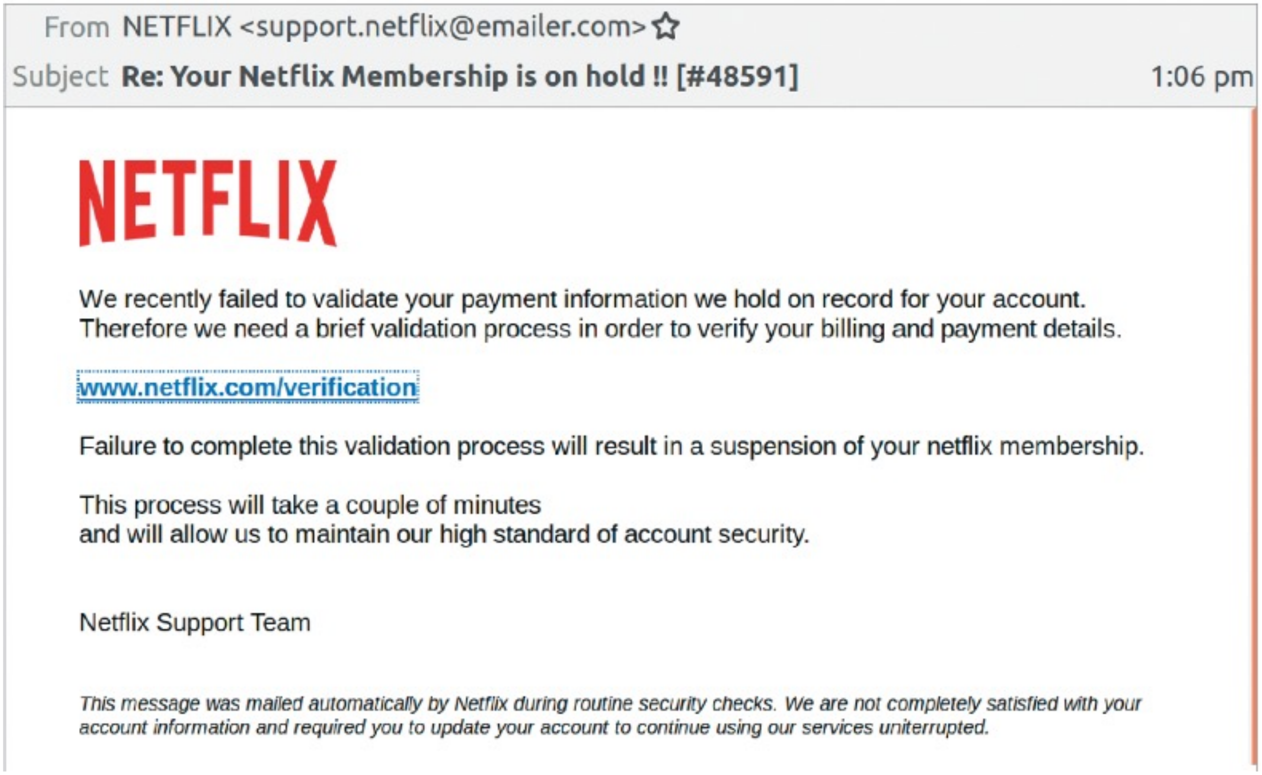
Malicious Software (Malware)

- Network attacks are initiated to steal data that can be used or sold for financial gain or to carry out a sociopolitical agenda
- Malicious software (**malware**)
  - Virus
  - Worm
  - Trojan program
- Main goal
  - To make money
- Malware was once targeted specifically at Windows, Linux, and other traditional OSs
  - Now, it is written to target tablets, smartphones, and other Internet-connected devices

Viruses (1 of 4)

- **Virus:** A program that attaches itself to a file or another program, often sent via email
  - Can’t replicate itself or operate without the presence of a host
  - Does not stand on its own
- Examples
  - Phishing: Sender of a phishing email uses social engineering to lure a user into following a malicious link to a fake website
  - **Ransomware:** A type of virus that locks a target system until a ransom is paid
- Bad news about viruses
  - No foolproof prevention method

Viruses (2 of 4)



From NETFLIX <support.netflix@emailer.com> ☆

Subject **Re: Your Netflix Membership is on hold !! [#48591]** 1:06 pm

NETFLIX

We recently failed to validate your payment information we hold on record for your account. Therefore we need a brief validation process in order to verify your billing and payment details.

www.netflix.com/verification

Failure to complete this validation process will result in a suspension of your netflix membership.

This process will take a couple of minutes
and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uniterrupted.

Figure 3-1 Phishing email message

Viruses (3 of 4)

- Antivirus software
  - Compares signatures and common malicious programmatic behaviors of known viruses against every file on a computer
    - Signatures are kept in a **virus signature file**
      - Must update regularly
    - Many antivirus software packages offer automatic updates
- Network security devices
  - Can monitor entire networks and intercept malware before it reaches users
- **Sandboxing**
  - Allows users to run programs in a secure, isolated operating area that prevents malicious files from being written to the hard drive

Common Computer Viruses (1 of 3)

Virus	Description
Ryuk	The Ryuk ransomware virus was responsible for more than one-third of all ransomware attacks in 2020. Ryuk is used in attacks targeting companies, hospitals, and government municipalities. Ryuk encrypts critical files and typically demands a multimillion-dollar ransom.
FormBook	FormBook is a malware family of data stealers and form grabbers. It attempts to steal the contents of the Windows Clipboard, log what you type on the keyboard, and steal data while you browse the web. It is sold as “malware-as-a-service” on hacking forums. Hackers can purchase a subscription and use the FormBook tool. FormBook is usually distributed through spam email containing malicious attachments.
CryptoLocker	CryptoLocker is less prevalent now but is considered the father of many ransomware viruses. CryptoLocker has become a term referring to families of ransomware viruses. In 2016, it was estimated to have infected more than 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 email message that is designed to trick users into clicking a malicious link or attachment. Once a machine is infected, victims have a set amount of time to pay the ransom if they want to retrieve their files.

Common Computer Viruses (2 of 3)

Virus	Description
MalumPOS	Malware has targeted 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 strip of a credit card). POS attacks were rare in 2020, but a new strain seems to target personally identifying information only instead of full payment card information.
Carbanak	This virus is spread via phishing emails that almost always target financial institutions. These phishing emails contain a Word document and a malicious .cpl file. (Keep this in mind for the upcoming base-64 decoding exercise.) When it first accesses a system, the malware runs a number of checks to ensure it can gain the proper privileges to further its attack. When proper privileges are obtained or verified, the malware opens a backdoor 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.

Common Computer Viruses (3 of 3)

Virus	Description
Gumblar	First detected in March 2009, this malware spread by mass-hacking hundreds of thousands of websites, which then exploited visiting browsers via Adobe PDF and Flash vulnerabilities. It has made a resurgence in 2020, crashing thousands of blogs and websites that use WordPress, Drupal, Joomla, and other PHP-based constructs. The malware steals FTP credentials and uses them to further compromise websites 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 or PGPCoder	This ransomware virus was detected in 2008 and was still active in 2020. Although not widespread, it 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 for the encryption key.

Viruses (4 of 4)

- Some viruses contained in email attachments were encoded in base 64
- Running a base-64 decoder on suspicious email attachments can help determine if malware or viruses are detected
- Examples of what to look for:
  - Hidden computer programs
  - Executable pieces of programming code known as **shell**
    - Creates an interface to an OS for issuing system commands
    - Should not appear in an email attachment

Macro Viruses

- Macro virus
  - A virus coded as a macro in programs that support a macro programming language (e.g., Visual Basic for Applications)
  - Macro: Basically, a list of commands
    - Can be coded to carry out several malicious actions
    - Example
      - Melissa: Appeared in 1999
- Viruses were created by programmers in the past
  - Today, even nonprogrammers can create viruses easily
  - Instructions on how to create a virus step by step are posted on websites
    - Security professionals learn from thinking like attackers

Worms

- **Worm**: A program that replicates and propagates itself without having to attach itself to a host
- Infamous examples:
  - Stuxnet
  - Code Red
  - Conficker
- Theoretically, a worm that replicates itself multiple times to every user it infects can infect every computer in the world over a short period
- Some infamous worms have cost businesses billions of dollars because of:
  - Lost productivity caused by computer downtime and time spent recovering lost data
  - Reinstalling programs and operating systems
  - Hiring or contracting IT personnel

Common Computer Worms (1 of 2)

Worm	Description
WannaCry	WannaCry is a ransomware cryptoworm that began its attack in 2017. It targeted vulnerabilities in the Microsoft Windows file-sharing protocol server message block (SMB), which allowed it to spread from system to system. Once on a system, it would then release its ransomware attack. Within a day, WannaCry had infected more than 230,000 computers in about 150 countries.
Flame (also called KyWiper)	Often touted as the most complex malware ever created, Flame was discovered in May 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 (ICSs) in a nuclear production facility in Iran. Believed to have been delivered via USB drive, 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.

Common Computer Worms (2 of 2)

Worm	Description
Duqu	Detected in October of 2011, Duqu had design features similar 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 spread through automatically generated email messages. It is estimated that this botnet Trojan program and its variants infected millions of systems.
Waledac	This email worm harvests and forwards passwords and spreads itself in an email 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 email 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.

Trojan Programs

- Responsible for the most insidious attacks against networks and computers worldwide
  - Disguise themselves as useful programs
  - Can install **backdoors** or **rootkits** on a computer
    - Backdoors or rootkits give attackers a means of regaining access to the attacked computer later
    - A rootkit is created after an attack and usually hides itself in the OS tools
- A good software or hardware firewall
  - Identifies traffic using unfamiliar ports
- Common ports used by Trojans
  - TCP port 80 (HTTP) or UDP port 53 (DNS)

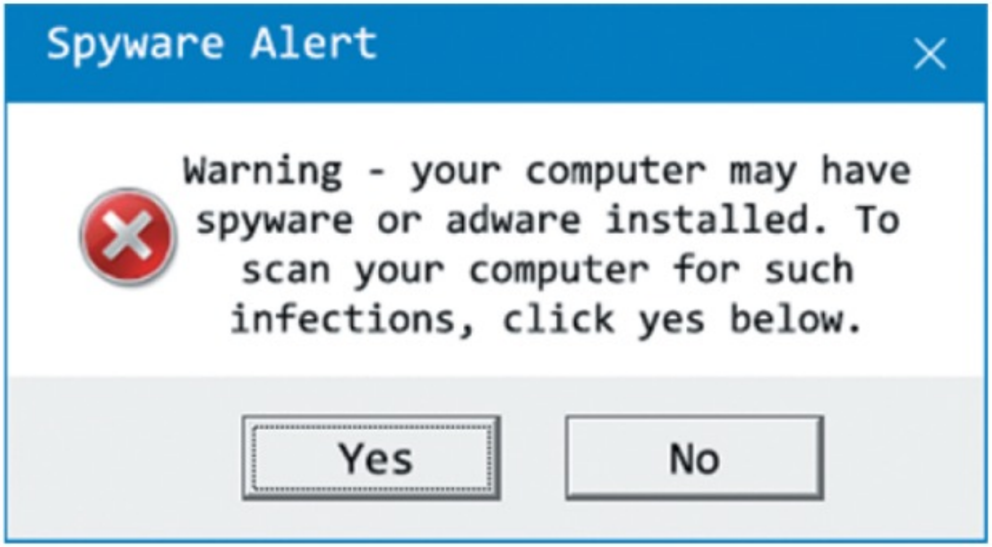
Trojan Programs and Ports

Trojan program	TCP ports used
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
Backdoor.Rtkit.B	445
Backdoor.Systsec, Backdoor.Zincite.A	1034
Emotet	20, 22, 80, 443, 7080, and 50000
Trickbot	447, 8082
W32.Beagle.Y@mm	1234
W32.Korgo.A	13, 2041, and 3067
W32.Mytob.MX@mm	7000

Spyware (1 of 2)

- Sends information from the infected computer to the initiator of the spyware program on your computer
  - Confidential financial data
  - Passwords
  - PINs
  - Any other stored data
- Can register each keystroke entered
  - Prevalent technology
- Records and sends everything a user enters to an unknown person located halfway around the world
- Educate users about spyware

Spyware (2 of 2)



Spyware Alert

Warning - your computer may have spyware or adware installed. To scan your computer for such infections, click yes below.

Figure 3-2 Spyware initiation program

Adware

- Similar to spyware
  - Installed without users being aware of their presence
- Sometimes displays a banner that notifies users of its presence
- Main purpose
  - Determine a user’s purchasing habits
    - Web browsers can then display advertisements tailored to the user
- Security and privacy violation
  - Gathers your purchasing habits
    - Information is likely being sent back to the hackers that deployed the adware

Knowledge Check Activity 3-1

What is the main purpose of malware?

a. Financial gain or destruction
b. Learning passwords
c. Discovering open ports
d. Identifying an operating system

Knowledge Check Activity 3-1: Answer

What is the main purpose of malware?

Answer: a. Financial gain or destruction

The main purpose of malware is to make money. Previously, the main goal was to destroy or corrupt data or to shut down a network or computer system.

Knowledge Check Activity 3-2

Which of the following exploits might hide its destructive payload in a legitimate application or game?

a. Trojan

b. Macro virus

c. Worm

d. Buffer overflow

Knowledge Check Activity 3-2: Answer

Which of the following exploits might hide its destructive payload in a legitimate application or game?

Answer: a. Trojan

Trojans disguise themselves as useful programs and can install a backdoor or rootkit on a computer. A rootkit is created after an attack and usually hides itself in the OS tools, so it's impossible to detect.

Polling Activity 3-1

Which of the following is an example of a macro programming language?

a. C++

b. Shell

c. Basic

d. Visual Basic for Applications

Polling Activity 3-1: Answer

Which of the following is an example of a macro programming language?

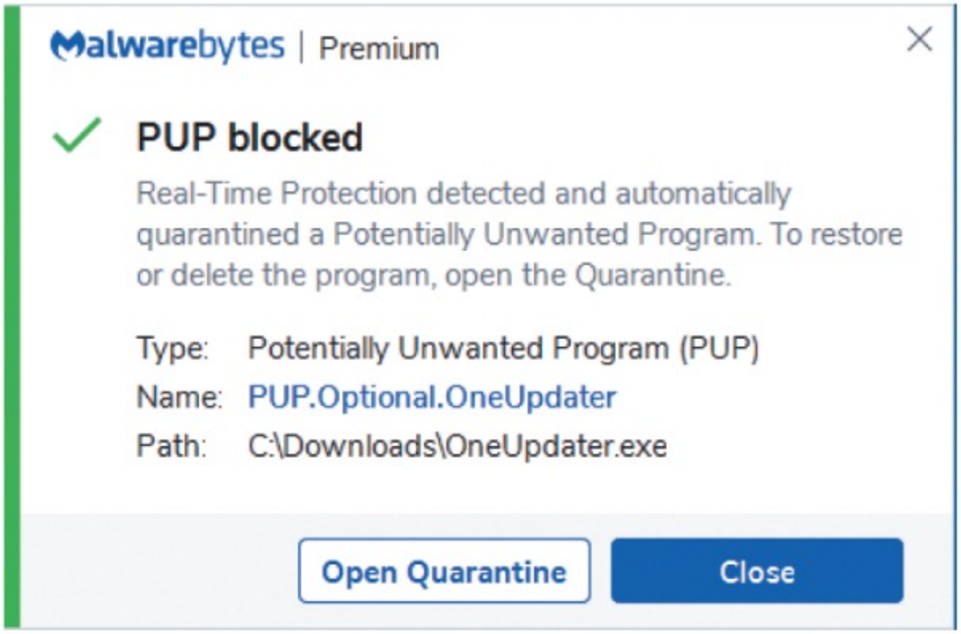
Answer: d. Visual Basic for Applications

An example of a macro programming language is Visual Basic for Applications (VBA).

Protecting against Malware Attacks (1 of 2)

- 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 (2 of 2)



✓ PUP blocked

Real-Time Protection detected and automatically quarantined a Potentially Unwanted Program. To restore or delete the program, open the Quarantine.

Type: Potentially Unwanted Program (PUP)
Name: PUP.Optional.OneUpdater
Path: C:\Downloads\OneUpdater.exe

Figure 3-3 Detecting a virus

Educating Your Users (1 of 2)

- Conducting structured training
  - Includes all employees and management
  - Email monthly security updates to all employees
  - Recommend virus signature database updating
    - Activate automatic updates
- Actively phishing employees and sending them to training content if they click a link they should not click
- **White-listing**
  - 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 (2 of 2)

- Two popular spyware and adware removal programs:
  - HitmanPro
  - Malwarebytes Anti-Malware (MBAM)
- Training employees on safe email practices and how to recognize and avoid phishing messages
- Installing firewalls
  - Software firewalls (for home and small-business users)
    - For those who don’t have a hardware firewall or an intrusion detection system (IDS)

Avoiding Fear Tactics

- Avoid scaring users into complying with security measures
  - Sometimes used by unethical security testers
    - Against the Open Source Security Testing Methodology Manual’s (OSSTMM) Rules of Engagement
- Promote awareness rather than instill fear
  - Users should be aware of potential threats, not terrified by them
  - Build on the users’ existing knowledge
    - Makes training easier

Discussion Activity 3-1

Antivirus software is one of the main points of defense against malware and network attacks. Perform research to discover five of the best “free” antivirus solutions. In a few paragraphs, describe your findings and discuss which antivirus software you think is the best and explain why.

Discussion Activity 3-1: Answer

Antivirus software is one of the main points of defense against malware and network attacks. Perform research to discover five of the best “free” antivirus solutions. In a few paragraphs, describe your findings and discuss which antivirus software you think is the best and explain why.

Answer: Some of the best antivirus solutions in the market are Avira, Panda, TotalAV, Kaspersky, and Malwarebytes. Avira has one of the best anti-malware engines in the market and is user-friendly. Panda Free Antivirus provides good virus protection and is also lightweight and secure. TotalAV’s identifies the trickiest ransomware and cryptojacking files. Kaspersky Security Cloud is another great antivirus software that also comes with plenty of additional benefits. Malwarebytes Free is a minimalistic and simple antivirus scanner, but it can miss hidden files that brands like Avira and TotalAV can detect.

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**
  - Concerned with the security of computers or devices that are part of a network infrastructure
- **Computer security**
  - Concerned with the security of a stand-alone computing device that is not part of a network infrastructure
- Computer crime
  - Fastest growing type of crime worldwide

Denial-of-Service (DoS) Attack (1 of 2)

- Prevents legitimate users from accessing network resources
- Attackers do not attempt to access the information on a remote computer
  - May just want to cripple the network
- Conducting a DoS attack yourself is not wise
  - Only explain how the attack could be carried out

Denial-of-Service (DoS) Attack (2 of 2)

- **Ping of Death attack**
  - Causes the victim computer to freeze and malfunction
  - Not as common as it was during the late 1990s
  - How it works
    - Attacker creates a large ICMP packet
      - More than the allowed 65,535 bytes
      - Large packet is fragmented into smaller packets
      - Reassembled at its destination
      - User’s system at the destination point cannot handle the reassembled oversize packet
      - Causes it to crash or freeze

Distributed Denial-of-Service Attacks

- **Distributed denial-of-service (DDoS) attack**
  - Attack on the host is launched from multiple servers or workstations
  - Network could be flooded with billions of packets
    - Available network bandwidth could drop
    - Legitimate users may notice a performance degradation
  - Often, participants are not aware their computers are part of the attack
    - They, too, have been attacked
- A Dark DDoS attack
  - A smoke screen to distract network defenders while another, more damaging attack is occurring

Buffer Overflow Attacks

- Attacker finds a vulnerability in poorly written code that doesn’t check for a defined amount of memory space use
- Attacker writes code that overflows buffer
  - Fills buffer with executable program code
  - OS runs this code, and the attacker’s program does something harmful
  - Code elevates the attacker’s permissions to an administrator’s level
    - Or creates a service that allows an attacker to remotely access the target system
- Ensure programmers are aware of how their code might be vulnerable to attack
- DevSecOps
  - Addresses the need for programmers to develop code with security in mind

Buffer Overflow Vulnerabilities (1 of 2)

Buffer overflow	Description
Cisco ASA Internet Key Exchange	Cisco Security Advisory for CVE-2016-1287 discusses a serious buffer overflow vulnerability in the Cisco ASA product line. Attackers could send a specially crafted packet to the affected device, allowing them to gain full administrative privileges. This attack could be carried out from anywhere on the Internet if ASAs are used on a company's perimeter.
GHOST	This vulnerability made headlines across the globe when it was discovered by security researchers at Qualys. Community. 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, a central component of Linux operating systems.
PAN-OS	In 2020, Palo Alto Networks released a fix for a buffer overflow vulnerability in its PAN-OS operating system found in many of its next-generation firewalls. A remote, unauthenticated attacker could use this vulnerability to disrupt system processes or to execute code.

Buffer Overflow Vulnerabilities (2 of 2)

Buffer overflow	Description
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.
VPN Product	In 2020, the NSA alerted administrators about buffer overflow vulnerabilities in three popular VPN products, namely Pulse Secure, Palo Alto GlobalProtect, and Fortinet FortiGate. The vulnerability allowed for arbitrary file downloads and remote code execution on some of these products.
Windows Server Service	Microsoft Security Bulletin MS08-067 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.

Eavesdropping

- An attacker can listen to unencrypted network communications
  - To intercept confidential information or gather credentials that can be used to extend the attack
- Accomplished with sniffing tools
  - Sniffing tools are designed to capture copies of packets being sent across a network
- To defend against the threat of eavesdropping
  - Network equipment and applications should be forced to communicate only over encrypted protocols
    - Use only valid, trusted certificates

Man-in-the-Middle Attacks

- Attackers can inject themselves between two parties or systems communicating with one another
  - To manipulate messages being passed back and forth

Network Session Hijacking

- Enables an 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

Polling Activity 3-2

An exploit that attacks computer systems by inserting executable code in areas of memory because of poorly written code is called which of the following?

a. Buffer overflow

b. Trojan program

c. Virus

d. Worm

Polling Activity 3-2: Answer

An exploit that attacks computer systems by inserting executable code in areas of memory because of poorly written code is called which of the following?

Answer: a. Buffer overflow

In a buffer overflow attack, an attacker finds a vulnerability in poorly written code that doesn’t check for a defined amount of memory space use.

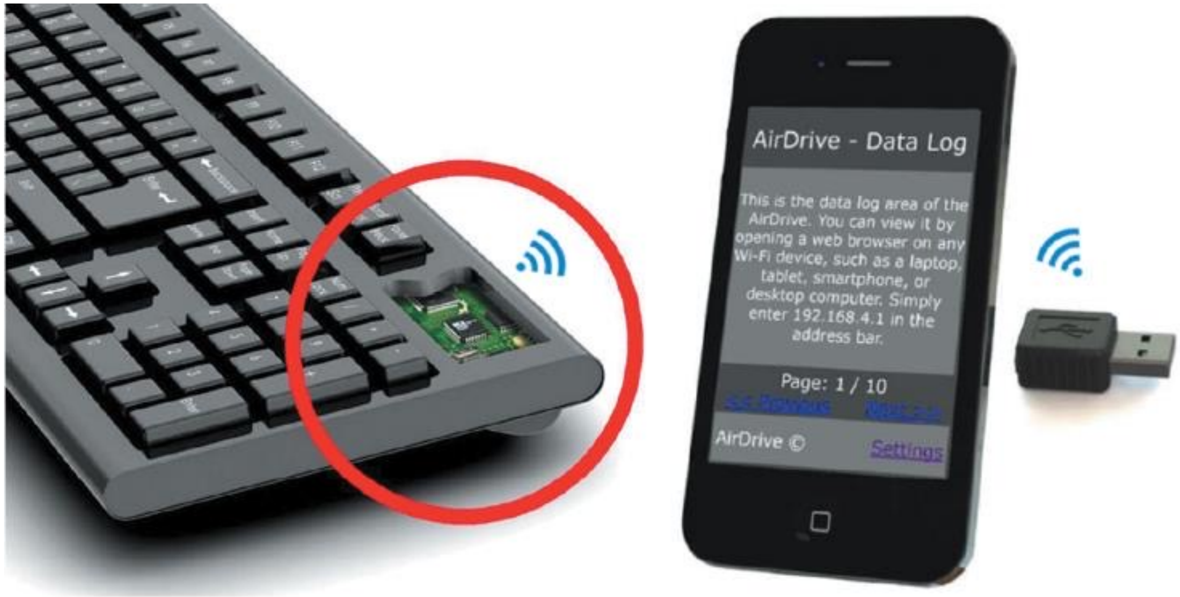
Addressing Physical Security

- Protecting a network requires some basic skills
  - Must secure servers and computers from an attack from within the organization
  - Higher chance that an attacker who breaks into the network is from inside the company rather than outside

Keyloggers (1 of 2)

- Hardware devices or software used to capture keystrokes on a computer
  - Software
    - Behaves like viruses or Trojans
  - Hardware
    - Small device that is easy to install
    - Examples: KeyGrabber and KeyGhost
- Can be used by organizations to monitor the activity of users on their computer systems
- Available as software (spyware) loaded on a computer
  - Retrieved information can be emailed or transferred to a remote location

Keyloggers (2 of 2)



AirDrive - Data Log

This is the data log area of the AirDrive. You can view it by opening a web browser on any Wi-Fi device, such as a laptop, tablet, smartphone, or desktop computer. Simply enter 192.168.4.1 in the address bar.

Figure 3-4 Wi-Fi USB keylogger, keylogger keyboard, and keylogger phone app

Behind Locked Doors

- Lock up your servers
  - Average person
    - Can pick an American home lock in less than five minutes
    - Those who have more time on their hands
      - Can pick a deadbolt lock in under 30 seconds
- Rotary locks are more difficult to crack than deadbolt locks
  - Require pushing in a sequence of numbered bars
  - Neither lock type keeps a record of who entered the locked room
  - Security cards can be used for better security
- Biometric security devices
  - Read fingerprints or retinal scans and are used to restrict access to secure areas
  - Provide a second authentication factor

Self-Assessment

Describe the types of malware attacks and explain how you can protect against each of them.

Summary

- Now that the lesson has ended, you should 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