CCNA Cyber Ops (Version 1.1) – Chapter 6: Principles of Network Security

itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-6-principles-of-network-security.html

June 12, 2019

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What is the evolution of network security?
- What are the various types of attack tools used by threat actors?
- What is malware?
- What are some common network attacks?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

threat
vulnerability
attack surface
exploit
risk
risk acceptance
risk avoidance
risk limitation
risk transfer
countermeasure
impact
hacker
white hat hackers
gray hat hackers
black hat hackers
script kiddies
vulnerability brokers
hacktivists
cybercriminals
state-sponsored hackers
attack indicators
password crackers
wireless hacking tools

network scanning
packet crafting tools
packet sniffers
rootkit detectors
fuzzers
forensic tools
debuggers
hacking operating systems
encryption tools
vulnerability exploitation tools
vulnerability scanners
virus
Trojan horse
worms
social engineering
spyware
adware
scareware
phishing
reconnaissance
access attacks
pass-the-hash
man-in-the-middle attack
spoofing
pretexting
quid pro quo
tailgating
baiting
visual hacking
spear phishing
whaling
pharming
watering hole
vishing
smishing
zombies
bots
botnet
handlers
botmaster
buffer overflow attack

Introduction (6.0)

The motivation for attacking networks can be financial gain, corporate- or state-sponsored espionage, activism, or simply malicious intent. The people and groups that engage in attacks on our network infrastructures are commonly referred to as threat actors.

This chapter covers the variety of tools and methods threat actors use to launch network attacks.

Attackers and Their Tools (6.1)

In this section, you will learn how networks are attacked.

Who Is Attacking Our Network (6.1.1)

In this topic, you will learn about the evolution of network security.

Threat, Vulnerability, and Risk (6.1.1.1)

We are under attack and attackers want access to our assets. Assets are anything of value to an organization such as data and other intellectual property, servers, computers, smart phones, tablets, and more.

To better understand any discussion of network security, it is important to know the following terms:

- **Threat:** A potential danger to an asset such as data or the network itself.
- **Vulnerability:** A weakness in a system or its design that could be exploited by a threat.
- **Attack surface:** The total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. For example, your operating system and web browser could both need security patches. They are each vulnerable to attacks. Together, they create an attack surface the threat actor can exploit.
- **Exploit:** The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. The attacker does not need an account in the end system to exploit the vulnerability. In a local exploit, the threat actor has some type of user or administrative access to the end system. A local exploit does not necessarily mean that the attacker has physical access to the end system.
- **Risk:** The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset. There are four common ways to manage risk:

- **Risk acceptance:** This is when the cost of risk management options outweighs the cost of the risk itself. The risk is accepted without action.
- **Risk avoidance:** This is an action that avoids any exposure to the risk. This is usually the most expensive risk mitigation option.
- **Risk limitation:** This limits a company's risk exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance. It is the most commonly used risk mitigation strategy.
- **Risk transfer:** The risk is transferred to a willing third party such as an insurance company.

Other commonly used network security terms include

- **Countermeasure:** The protection solution that mitigates a threat or risk.
- **Impact:** The resulting damage to the organization that is caused by the threat.

Note
A local exploit requires inside network access such as a user with an account onthe network. A remote exploit does not require an account on the network to exploit that network's vulnerability.

Hacker vs. Threat Actor (6.1.1.2)

As we know, hacker is a common term used to describe a threat actor. However, the term "hacker" has a variety of meanings:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient
- A network professional who uses sophisticated programming skills to ensure that networks are not vulnerable to attack
- A person who tries to gain unauthorized access to devices on the Internet
- Individuals who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers

The following terms are often used to describe hackers:

- **White hat hackers:** These are ethical hackers who use their programming skills for good, ethical, and legal purposes. White hat hackers may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be threatened. Some organizations award prizes or bounties to white hat hackers when they inform them of a vulnerability.
- **Gray hat hackers:** These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. An example would be someone who compromises a network without permission and then discloses the vulnerability publicly. A gray hat hacker may disclose a vulnerability to the affected organization after having compromised their network. This allows the organization to fix the problem.
- **Black hat hackers:** These are unethical criminals who violate computer and network security for personal gain, or for maliciousness reasons such as attacking networks. Black hat hackers exploit vulnerabilities to compromise computer and network systems.Good or bad, hacking is an important aspect of network security. In this course, the term threat actor is used when referring to those individuals or groups that could be classified as gray or black hat hackers.

Evolution of Threat Actors (6.1.1.3)

Hacking started in the 1960s with phone freaking, or phreaking, which refers to using various audio frequencies to manipulate phone systems. At that time, telephone switches used various tones, or tone dialing, to indicate different functions. Early threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.

In the mid-1980s, computer dial-up modems were used to connect computers to networks. Threat actors wrote “war dialing” programs which dialed each telephone number in a given area in search of computers, bulletin board systems, and fax machines. When a phone number was found, password-cracking programs were used to gain access. Since then, general threat actor profiles and motives have changed quite a bit.

Modern threat actor terms include the following:

- **Script kiddies:** Started in the 1990s and are usually teenagers running existing scripts, tools, and exploits to cause harm, but typically not for profit.
- **Vulnerability brokers:** These are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

- **Hacktivists:** These are gray hat hackers who rally and protest against different political and social ideas. Hacktivists publicity protest against organizations or governments by posting numerous articles and videos, leaking sensitive information, and performing distributed denial-of-service (DDoS) attacks.
- **Cybercriminals:** These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cybercriminals are responsible for stealing billions of dollars from consumers and businesses.
- **State-sponsored hackers:** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gatherintelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

Cybercriminals (6.1.1.4)

Cybercriminals are threat actors who are motivated to make money using any means necessary. While sometimes cybercriminals work independently, they are more often financed and sponsored by criminal organizations. It is estimated that globally, cybercriminals steal billions of dollars from consumers and businesses every year.

Cybercriminals operate in an underground economy where they buy, sell, and trade exploits and tools. They also buy and sell the private information and intellectual property they steal from victims. Cybercriminals target small businesses and consumers, as well as large enterprises and industries.

Cybersecurity Tasks (6.1.1.5)

Threat actors do not discriminate. They target the vulnerable end devices of home users and small-to-medium sized businesses, as well as large public and private organizations.

To make the Internet and networks safer and more secure, we must all develop good cybersecurity awareness. Cybersecurity is a shared responsibility which all users must practice. For example, we must report cybercrime to the appropriate authorities, be aware of potential threats in email and the web, and guard important information from theft.

Organizations must take action and protect their assets, users, and customers.

Cyber Threat Indicators (6.1.1.6)

Many network attacks can be prevented by sharing information about attack indicators. Each attack has unique identifiable attributes. These are known as cyber threat indicators or simply attack indicators.

For instance, a user receives an email claiming they have won a big prize. Clicking on the link in the email results in an attack. The attack indicators couldinclude the fact the user did not enter that contest, the IP address of the sender, the email subject line, the included link to click, or an attachment to download, among others.

Governments are now actively promoting cybersecurity. For instance, the U.S. Department of Homeland Security (DHS) and U.S. Computer Emergency Readiness Team (US-CERT) are leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost. DHS and US-CERT use a system called Automated Indicator Sharing (AIS). AIS enables the sharing of attack indicators between the U.S. government and the private sector as soon as the threat is verified.

The DHS also promotes cybersecurity to all users. For instance, they have an annual campaign in October called "Cybersecurity Awareness Month." This campaign was developed to promote and raise awareness about cybersecurity. The DHS also promotes the "Stop. Think. Connect." campaign to encourage all citizens to be safer and more secure online. The campaign provides material on a wide variety of security topics, including:

- Best Practices for Creating a Password
- Best Practices for Using Public Wi-Fi
- Five Every Day Steps Towards Online Safety
- How to Recognize and Prevent Cybercrime
- Five Steps to Protecting Your Digital Home

Activity 6.1.1.7: What Color Is My Hat?
Refer to the online course to complete this Activity.

Threat Actor Tools (6.1.2)

In this topic, you will learn about the various types of attack tools used by threat actors.

Introduction of Attack Tools (6.1.2.1)

To exploit a vulnerability, an attacker must have a technique or tool that can beused. Over the years, attack tools have become more sophisticated, and highly automated, requiring less technical knowledge to use them than in the past.

Figures 6-1 and 6-2 compare the sophistication of attack tools versus the technical knowledge required to use them in 1985 and today.

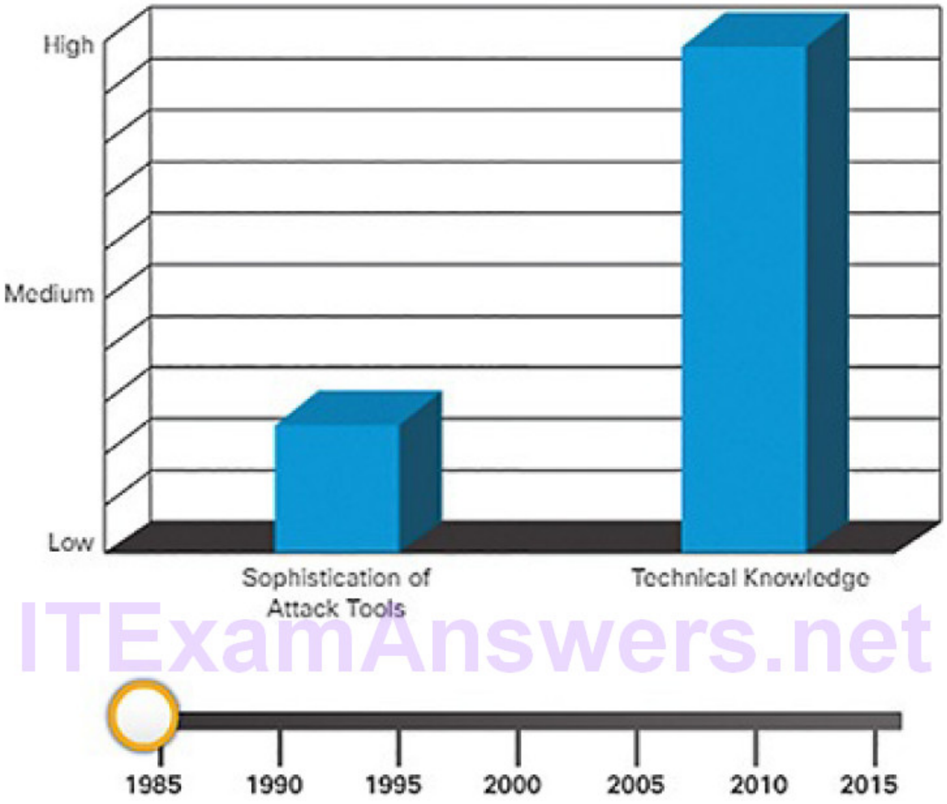


Figure 6-1 Comparing Attack Tools and Technical Knowledge—1985

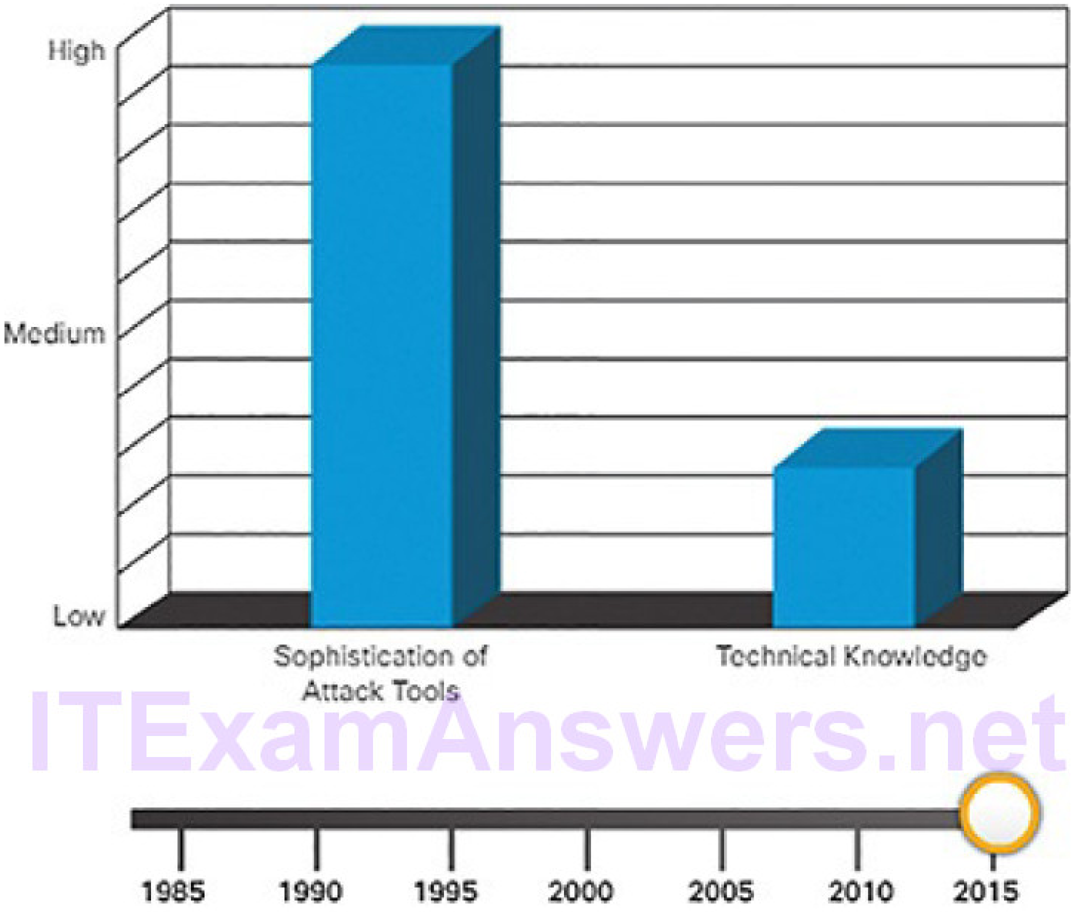


Figure 6-2 Comparing Attack Tools and Technical Knowledge—Today

Evolution of Security Tools (6.1.2.2)

Ethical hacking involves many different types of tools to test and keep the network and its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. However, many of these tools can also be used by threat actors for exploitation.

Threat actors have also created various hacking tools. These tools are explicitly written for nefarious reasons. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.

The following list highlights categories of common network penetration testing tools. Notice how some tools are used by white hats and black hats. Keep in mind that the list is not exhaustive as new tools are continually being developed.

Password crackers: Passwords are the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, LophtCrack, THC Hydra, RainbowCrack, and Medusa.

Wireless hacking tools: Wireless networks are more susceptible to network security threats. Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.

Network scanning and hacking tools: Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.

Packet crafting tools: These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Hping, Nping, and Nemesis.

Packet sniffers: These tools are used to capture and analyze packets withintraditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.

Rootkit detectors: These tools are directory and file integrity checkers used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF OpenBSD Packet Filter.

Fuzzers to search vulnerabilities: Fuzzers are tools used by hackers when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.

Forensic tools: These tools are used by white hat hackers to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and EnCase.

Debuggers: These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.

Hacking operating systems: These are specially designed operating systems preloaded with tools and technologies optimized hacking. Examples of specially designed hacking operating systems include Kali Linux, Backtrack 5r3, SELinux, Knoppix, and BackBox Linux

Encryption tools: These tools safeguard the contents of an organization's data at rest and data in motion. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include TrueCrypt, OpenSHH, OpenSSL, Tor, OpenVPN, and Stunnel.

Vulnerability exploitation tools: These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Vulnerability scanners: These tools scan a network or system to identify open ports. They can also be used to scan known vulnerabilities and scan virtual machines (VMs), BYOD devices, and client databases. Examples of tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

Note
Many of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.

Categories of Attacks (6.1.2.3)

Threat actors can use the previously mentioned tools or a combination of tools to create various attacks. The following list of attacks is not exhaustive as new ways to attack networks are continually discovered.

Eavesdropping attack: This is when a hacker captures and "listens" to network traffic. This attack is referred to as sniffing or snooping.

Data modification attack: If hackers have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.

IP address spoofing attack: A hacker constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Password-based attacks: If hackers discover a valid user account, the attackers have the same rights as the real user. Hackers could obtain lists of valid user and computer names and network information. They could also modify server and network configurations, and modify, reroute, or delete data.

Denial-of-service (DoS) attack: A DoS attack prevents normal use of a computer or network by valid users. After gaining access to your network, a DoS attack can crash applications or network services, flood a computer, or flood the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-middle attack: This attack occurs when hackers have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.

Compromised-key attack: If a hacker obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.

Sniffer attack: A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If thepackets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

It is important to understand that threat actors use a variety of security tools to carry out these attacks.

Activity 6.1.2.4: Classify Hacking Tools
Refer to the online course to complete this Activity.

Common Threats and Attacks (6.2)

In this section, you will learn the various types of threats and attacks.

Malware (6.2.1)

In this topic, you will learn about malware.

Types of Malware (6.2.1.1)

End devices are especially prone to malware attacks. Malware is short for malicious software or malicious code. It is code or software that is specifically designed to damage, disrupt, steal, or generally inflict some other “bad” or illegitimate action on data, hosts, or networks. It is important to know about malware because threat actors and online criminals frequently try to trick users into installing malware to help exploit security gaps. In addition, malware morphs so rapidly that malware-related security incidents are extremely common because antimalware software cannot be updated quickly enough to stop the new threats.

The three most common types of malware are viruses, worms, and Trojan horse attacks, as shown in Figure 6-3.

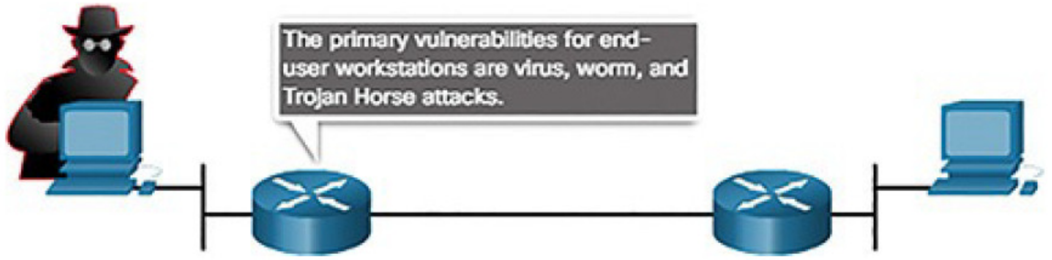

The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks.

Figure 6-3 Types of Malware

Viruses (6.2.1.2)

A virus is a type of malware that propagates by inserting a copy of itself into another program. Viruses then spread from one computer to another, infecting the computers. Most viruses require human help to spread. For example, when someone connects an infected USB drive to their PC, the virus will enter the PC. The virus may then infect a new USB drive, and spread to new PCs. Viruses can lay dormant for an extended period and then activate at a specific time and date.

A simple virus may install itself at the first line of code in an executable file. When activated, the virus might check the disk for other executables so that it can infect all the files it has not yet infected. Viruses can be harmless, such as those that display a picture on the screen, or they can be destructive, such as those that modify or delete files on the hard drive. Viruses can also be programmed to mutate to avoid detection.

Most viruses are now spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are now the most common type of virus.

Trojan Horses (6.2.1.3)

The term Trojan horse originated from Greek mythology. Greek warriors offered the people of Troy (the Trojans) a giant hollow wooden horse as a gift. The Trojans brought the giant horse into their walled city, unaware that it contained many Greek warriors. At night, after most Trojans were asleep, the warriors burst out of the horse, opened the city gates, and allowed a sizeable force to enter and take over the city.

Trojan horse malware is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it. Often, Trojans are found attached to online games.

Users are commonly tricked into loading and executing the Trojan horse on their systems. While playing the game, the user will not notice a problem. In the background, the Trojan horse has been installed on the user's system. The malicious code from the Trojan horse continues operating even after the game has been closed.

The Trojan horse concept is flexible. It can cause immediate damage, provide remote access to the system, or provide access through a back door. It can also perform actions as instructed remotely, such as "send me the password file once per week." This tendency of malware to send data back to the cybercriminal highlights the need to monitor outbound traffic for attack indicators.

Custom-written Trojan horses, such as those with a specific target, are difficult to detect.

Trojan Horse Classification (6.2.1.4)

Trojan horses are usually classified according to the damage that they cause, or the manner in which they breach a system:

Remote-access Trojan horse: This enables unauthorized remote access.
Data-sending Trojan horse: This provides the threat actor with sensitive data, such as passwords.
Destructive Trojan horse: This corrupts or deletes files.
Proxy Trojan horse: This will use the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP Trojan horse: This enables unauthorized file transfer services on end devices.
Security software disabler Trojan horse: This stops antivirus programs or firewalls from functioning.
DoS Trojan horse: This slows or halts network activity through a denial of service (DoS) attack.

Worms (6.2.1.5)

Computer worms are similar to viruses because they replicate and can cause the same type of damage. Specifically, worms replicate themselves by independentlyexploiting vulnerabilities in networks. Worms can slow down networks as they spread from system to system.

Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network.

Worms are responsible for some of the most devastating attacks on the Internet. In 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.

The initial infection of the SQL Slammer worm, known as the worm that ate the Internet, was a DoS attack that exploited a buffer overflow bug in Microsoft's SQL Server. At its peak, the number of infected servers doubled in size every 8.5 seconds. This is why it was able to infect 250,000+ hosts within 30 minutes. When it was released on the weekend of January 25, 2003, it disrupted the Internet, financial institutions, ATM cash machines, and more. Ironically, a patch for this vulnerability had been released 6 months earlier. The infected servers did not have the updated patch applied. This was a wake-up call for many organizations to implement a security policy requiring that updates and patches be applied in a timely fashion.

Worms share similar characteristics. They all exploit an enabling vulnerability, have a way to propagate themselves, and contain a payload.

Worm Components (6.2.1.6)

Despite the mitigation techniques that have emerged over the years, worms have continued to evolve and pose a persistent threat. Worms have become more sophisticated over time, but they still tend to be based on exploiting weaknesses in software applications.

Most worm attacks consist of the following three components:

Enabling vulnerability: A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.

Propagation mechanism: After gaining access to a device, the worm replicates itself and locates new targets.

Payload: Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor access to theinfected host or to create a DoS attack.

Worms are self-contained programs that attack a system to exploit a known vulnerability. Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again. Their propagation mechanisms are commonly deployed in a way that is difficult to detect.

Figure 6-4 displays the propagation technique used by the Code Red worm.

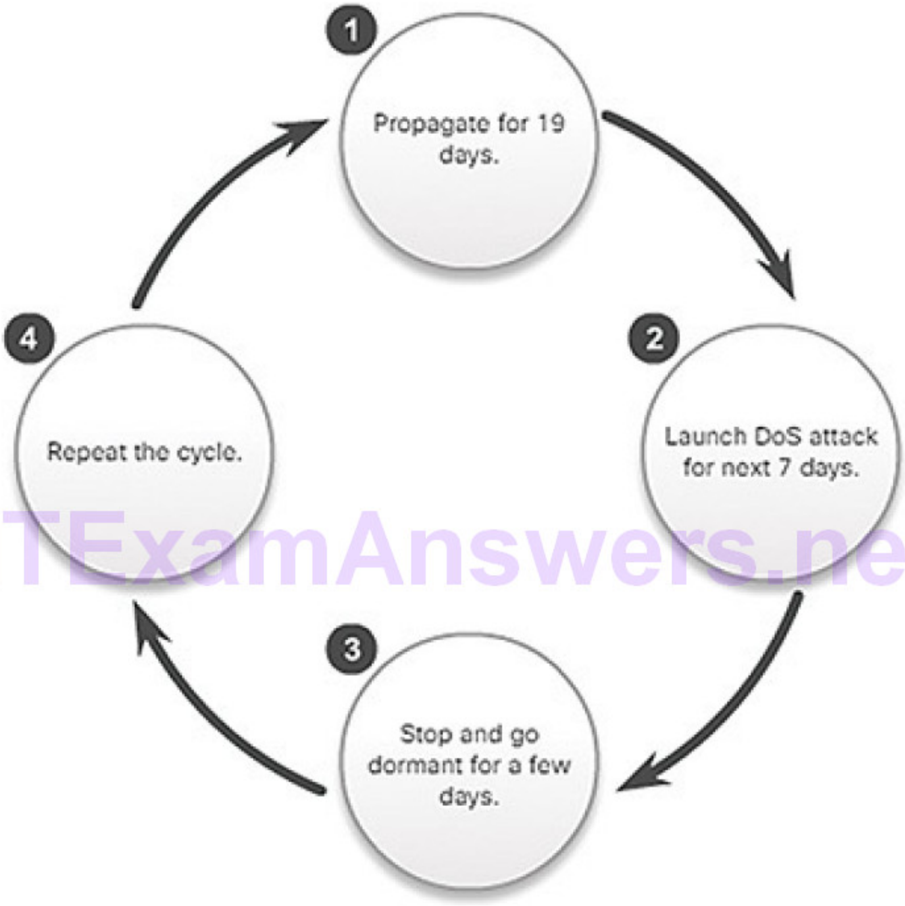

1
Propagate for 19 days.
2
Launch DoS attack for next 7 days.
3
Stop and go dormant for a few days.
4
Repeat the cycle.

Figure 6-4 Code Red Worm Propagation

Note
Worms never really stop spreading on the Internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.

Ransomware (6.2.1.7)

Threat actors have used viruses, worms, and Trojan horses to carry theirpayloads and for other malicious reasons. However, malware continues to evolve.

Currently, the most dominating malware is ransomware. Ransomware is malware that denies access to the infected computer system or its data. The cybercriminals then demand payment to release the computer system.

Ransomware has evolved to become the most profitable malware type in history. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent.

There are dozens of ransomware variants. Ransomware frequently uses an encryption algorithm to encrypt system files and data. The majority of known ransomware encryption algorithms cannot be easily decrypted, leaving victims with little option but to pay the asking price. Payments are typically paid in bitcoin because users of bitcoin can remain anonymous. Bitcoin is an open source, digital currency that nobody owns or controls.

Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns. Social engineering is also used, such as when cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user's computer.

Other Malware (6.2.1.8)

These are some examples of the varieties of modern malware:

Spyware: This malware is used to gather information about a user and send the information to another entity without the user's consent. Spyware can be a system monitor, Trojan horse, Adware, tracking cookies, or key loggers, or a combination of these tools.

Adware: This malware typically displays annoying pop-ups to generate revenue for its author. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware: This malware includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. It is generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogusthreat.

Phishing: This malware attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.

Rootkit: This malware is installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.

This list will continue to grow as the Internet evolves. New malware will always be developed. A major goal of cybersecurity operations is to learn about new malware and how to promptly mitigate it.

Common Malware Behaviors (6.2.1.9)

Cybercriminals continually modify malware code to change how it spreads and infects computers. However, most produce similar symptoms that can be detected through network and device log monitoring.

Computers infected with malware often exhibit one or more of the following symptoms:

- Appearance of strange files, programs, or desktop icons
- Antivirus and firewall programs are turning off or reconfiguring settings

- Computer screen is freezing or system is crashing
- Emails are spontaneously being sent without your knowledge to your contact list
- Files have been modified or deleted
- Increased CPU and/or memory usage
- Problems connecting to networks
- Slow computer or web browser speeds
- Unknown processes or services running
- Unknown TCP or UDP ports open
- Connections are made to hosts on the Internet without user action
- Strange computer behavior

Note
Malware behavior is not limited to the preceding list.

Activity 6.2.1.10: Identify the Malware Type
Refer to the online course to complete this Activity.

Lab 6.2.1.11: Anatomy of Malware
In this lab, you will research and analyze some recent malware.

Common Network Attacks (6.2.2)

In this topic, you will learn about common network attacks.

Types of Network Attacks (6.2.2.1)

Malware is a means to get a payload delivered. When it is delivered and installed, the payload can be used to cause a variety of network-related attacks from the inside. Threat actors can also attack the network from outside.

Why do threat actors attack networks? There are many motives, including money, greed, revenge, or political, religious, or sociological beliefs. Network security professionals must understand the types of attacks used to counter these threats to ensure the security of the LAN.

To mitigate attacks, it is useful to first categorize the various types of attacks. By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

Although there is no standardized way of categorizing network attacks, the method used in this course classifies attacks in three major categories.

- Reconnaissance attacks
- Access attacks
- DoS attacks

Reconnaissance Attacks (6.2.2.2)

Reconnaissance is known as information gathering. It is analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something. What the thief is actually doing is looking for vulnerable homes to break into such as unoccupied residences, residences with easy-to-open doors or windows, and those residences without security systems or security cameras.

Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. When directed at an endpoint on the network, such as PCs and servers, a recon attack is also called host profiling. This is because the attacker can get a profile of the system, including operating system type and version. If a system is not fully patched, the attacker will then look for known vulnerabilities to exploit.

Recon attacks precede intrusive access attacks or DoS attacks, and often employ the use of widely available tools.

Sample Reconnaissance Attacks (6.2.2.3)

These are some of the techniques used by malicious threat actors conducting reconnaissance attacks:

Perform an information query of a target: The threat actor is looking for initial information about a target. Readily available tools are used including a Google search of the organization’s website. Public information about the target network is available from DNS registries using **dig, nslookup,** and **whois** utilities.

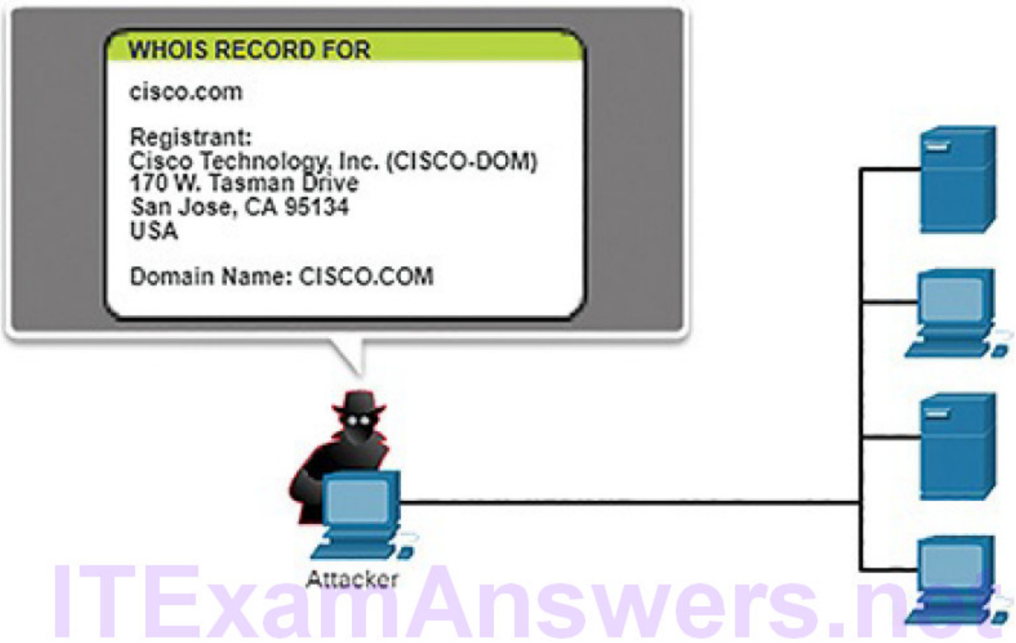
Initiate a ping sweep of the target networks: The threat actor initiates a ping sweep of the target networks revealed by the previous DNS queries to identify target network addresses. The ping sweep identifies which IP addresses are active. This allows creation of a logical topology of the target network.

Initiate a port scan of active IP addresses: The threat actor then initiates port scans on the live hosts identified by the ping sweep to determine which ports or services are available. Port scanning tools such as Nmap, SuperScan, Angry IP Scanner, and NetScanTools initiate connections to the target hosts by scanning for ports that are open on the target computers.

Run vulnerability scanners: The threat actor uses a vulnerability scanningtool such as Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, or Open VAS to query the identified ports. The goal is to identify potential vulnerabilities on the target hosts.

Run exploitation tools: The threat actor now attempts to exploit the identified vulnerabilities in the system. The threat actor uses vulnerability exploitation tools such as Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Figure 6-5 shows an example of a threat actor using the **whois** command to find information about a target.



WHOIS RECORD FOR

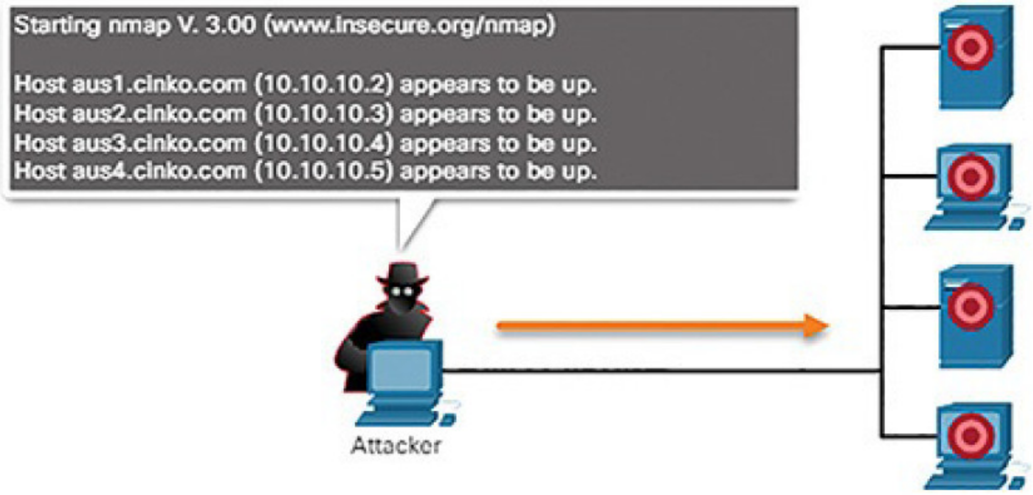
cisco.com

Registrant:
Cisco Technology, Inc. (CISCO-DOM)
170 W. Tasman Drive
San Jose, CA 95134
USA

Domain Name: CISCO.COM

Figure 6-5 Internet Information Queries

Figure 6-6 shows an example of a threat actor doing a ping sweep of the target's network address space to discover live and active IP addresses.

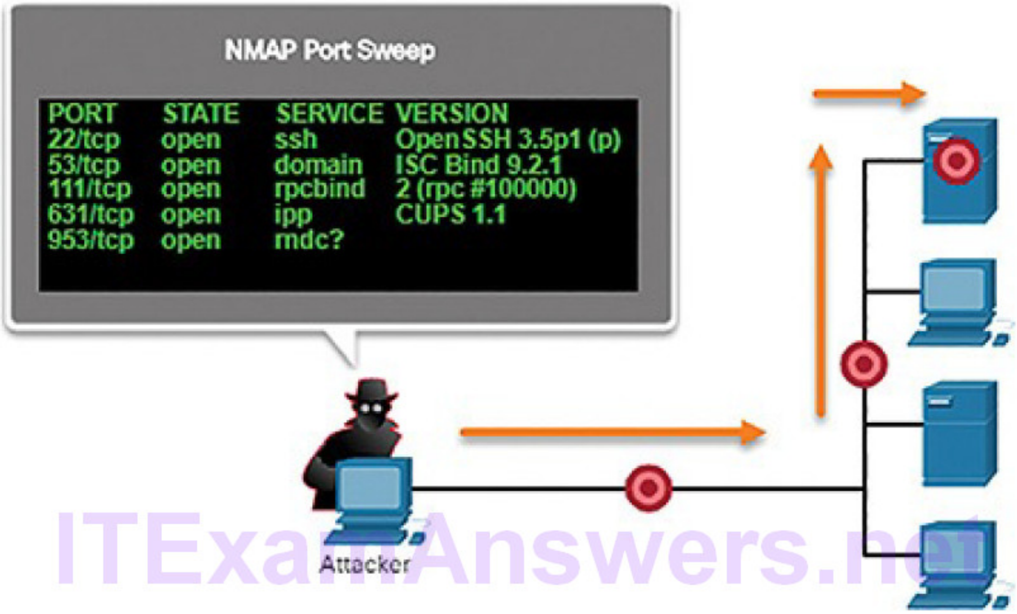


```
Starting nmap V. 3.00 (www.insecure.org/nmap)

Host aus1.cinko.com (10.10.10.2) appears to be up.
Host aus2.cinko.com (10.10.10.3) appears to be up.
Host aus3.cinko.com (10.10.10.4) appears to be up.
Host aus4.cinko.com (10.10.10.5) appears to be up.
```

Figure 6-6 Performing Ping Sweeps

Figure 6-7 shows an example of a threat actor performing a port scan on the discovered active IP addresses using Nmap.



```
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 3.5p1 (p)
53/tcp   open     domain   ISC Bind 9.2.1
111/tcp  open     rpcbind  2 (rpc #100000)
631/tcp  open     ipp      CUPS 1.1
953/tcp  open     rndc?
```

Figure 6-7 Performing Port Scans

Access Attacks (6.2.2.4)

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. The goal of the threat actor may be to steal information or to remotely control the inside host.

There are at least three reasons that threat actors would use access attacks on networks or systems:

- To retrieve data
- To gain access to systems
- To escalate access privileges

Figure 6-8 shows an example of a threat actor using an access attack to gain root privileges to an FTP server.

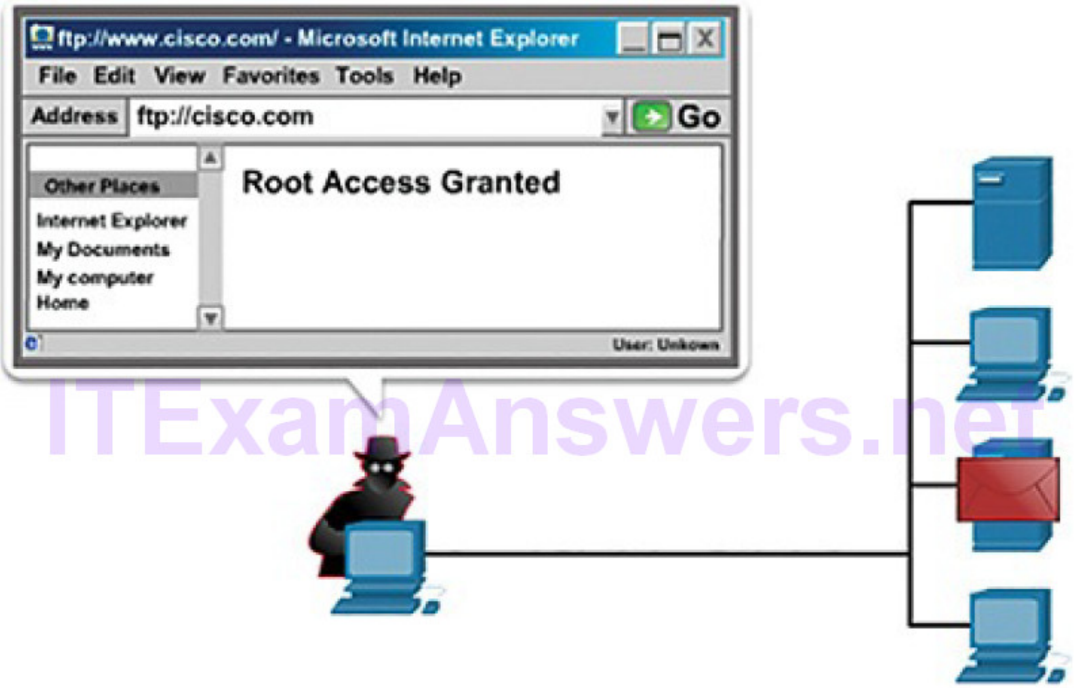


Figure 6-8 Access Attack on an FTP Server

Types of Access Attacks (6.2.2.5)

There are several common types of access attacks:

Password attack: Threat actors attempt to discover critical system passwords using various methods such as phishing attacks, dictionary attacks, brute-force attacks, network sniffing, or social engineering techniques. Brute-force password attacks involve repeated attempts using tools such as Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

Pass-the-hash: The threat actor already has access to the user's machine and uses malware to gain access to the stored password hashes. The threat actor then uses the hashes to authenticate to other remote servers or deviceswithout using brute force. Hashing is discussed in more detail later in the course.

Trust exploitation: Threat actors use a trusted host to gain access to network resources. For example, an external host that accesses an internal network over VPN is trusted. If that host is attacked, the attacker may use the trusted host to gain access to the internal network.

Port redirection: This is when a threat actor uses a compromised system as a base for attacks against other targets.

Man-in-the-middle attack: The threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.

IP, MAC, DHCP spoofing: Spoofing attacks are attacks in which one device attempts to pose as another by falsifying address data. There are multiple types of spoofing attacks. For example, MAC address spoofing occurs when one computer accepts data packets based on the MAC address of another computer that is the actual destination for the data.

Figures 6-9 through 6-11 show an example of trust exploitation.

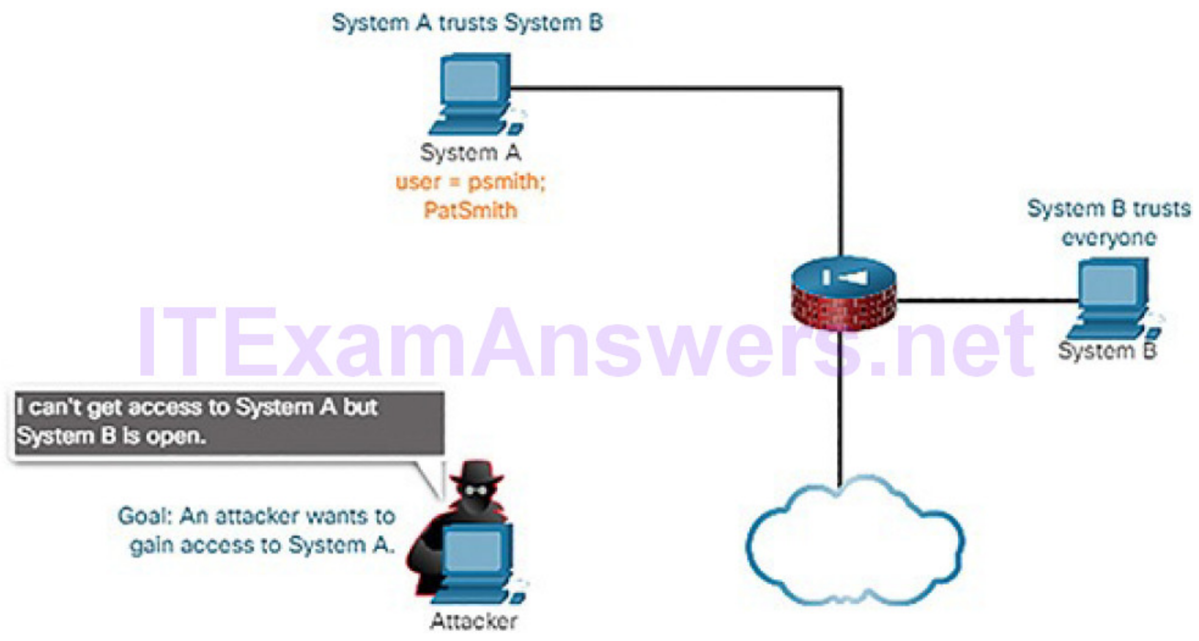

System A trusts System B
System A
user = psmith;
PatSmith
System B trusts everyone
System B
I can't get access to System A but System B is open.
Goal: An attacker wants to gain access to System A.
Attacker

Figure 6-9 Trust Exploitation: Attacker Cannot Access System A

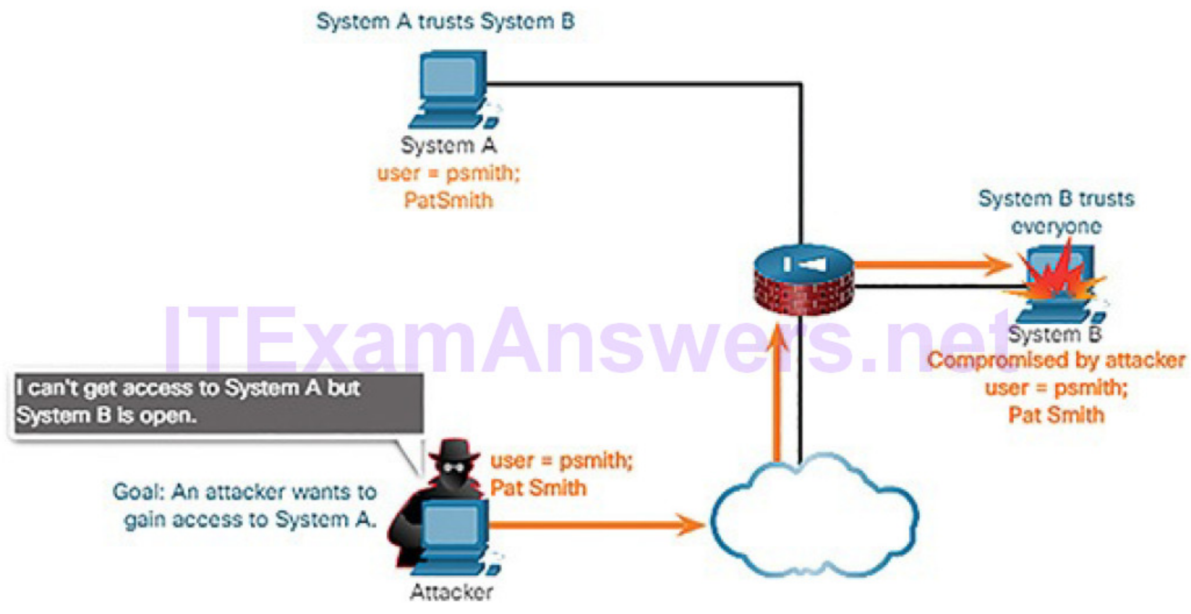


Figure 6-10 Trust Exploitation: Attacker Can Access System B

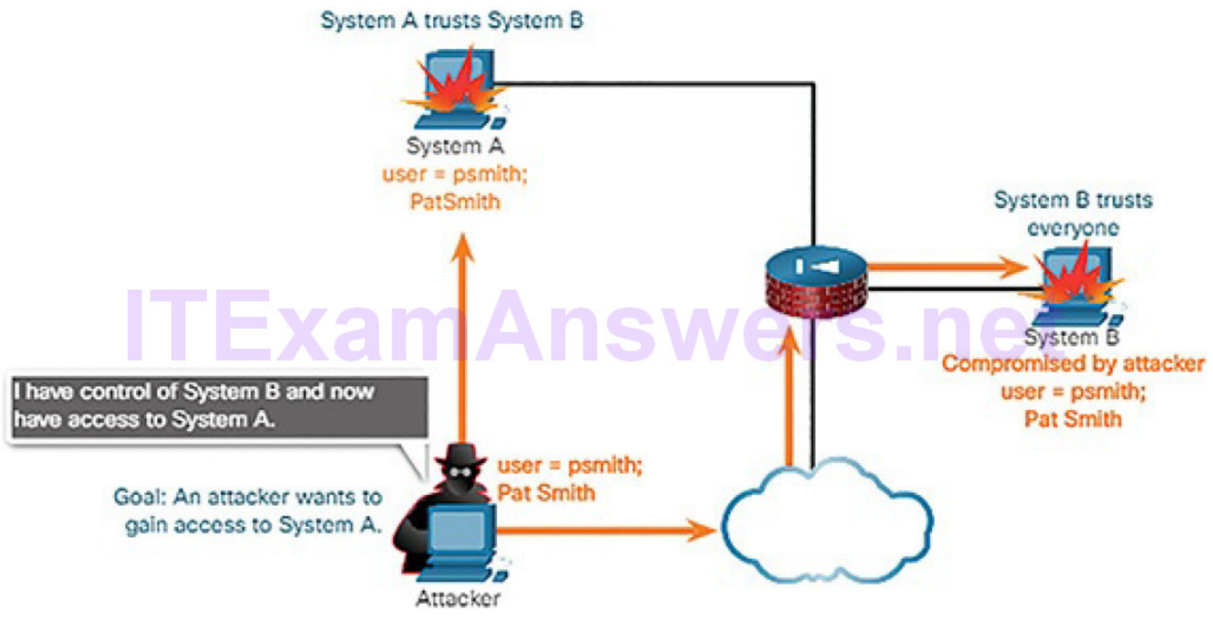


Figure 6-11 Trust Exploitation: Attacker Uses System B to Access System A

The port redirection example in Figure 6-12 displays a threat actor using SSH to connect to compromised Host A. Host A is trusted by Host B; therefore, the threat actor is allowed to use Telnet to access it.

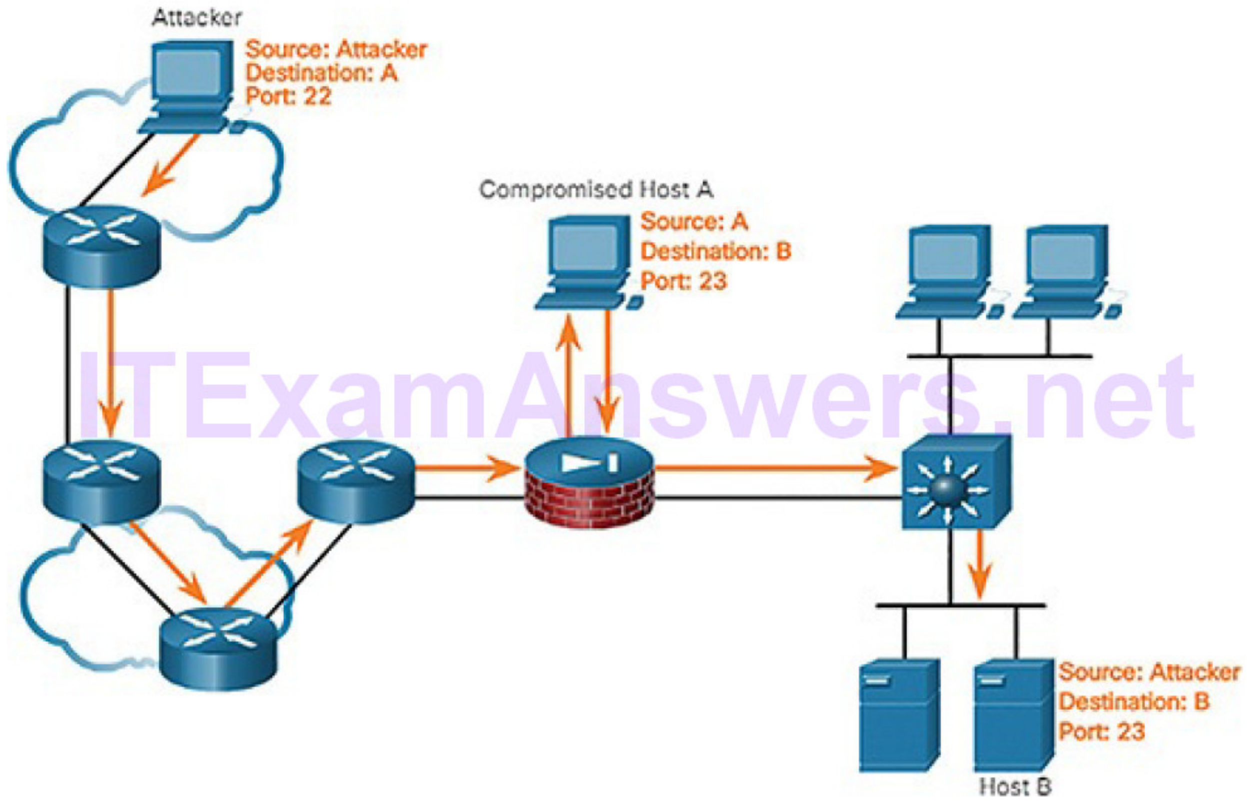


Figure 6-12 Port Redirection Example

Figure 6-13 displays an example of a man-in-the-middle attack.

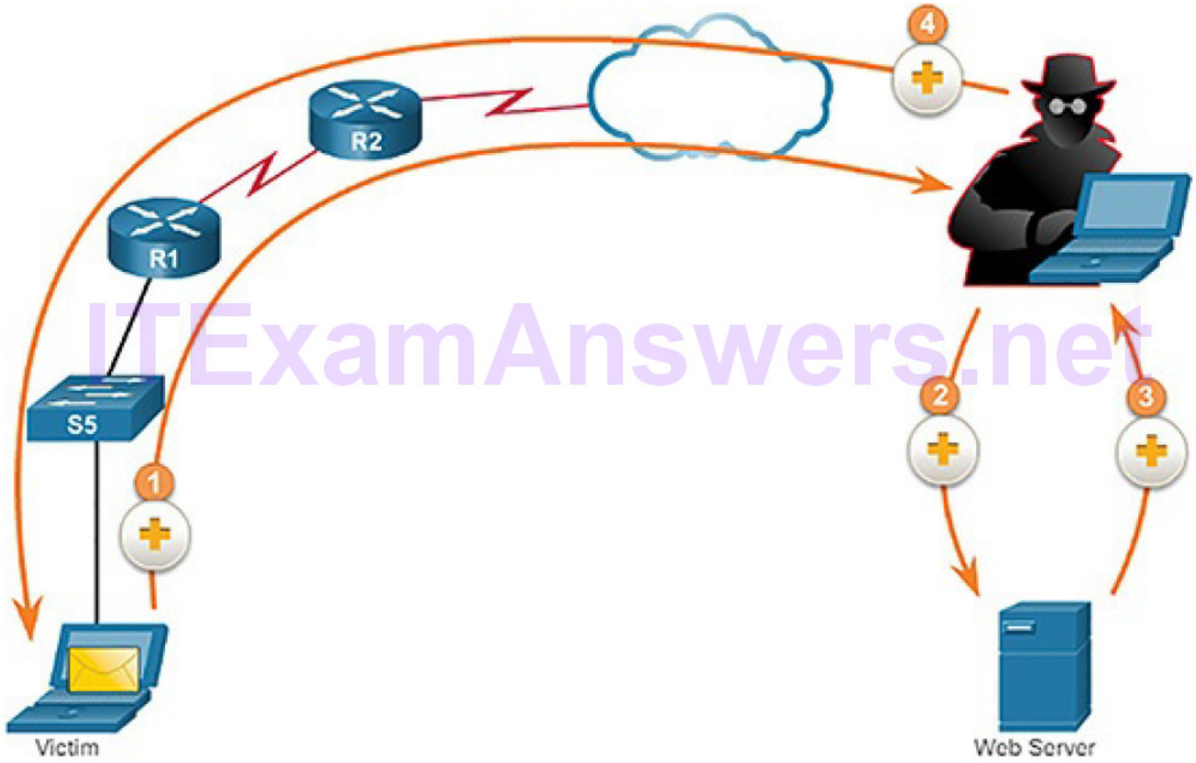


Figure 6-13 Man-in-the-Middle Attack Example

The steps in Figure 6-13 are as follows:

Step 1. When a victim requests a web page, the request is directed to the attacker's computer.
Step 2. The attacker's computer receives the request and retrieves the real page from the legitimate website.
Step 3. That attacker can alter the legitimate web page and apply transformations to the data.
Step 4. The attacker forwards the requested page to the victim.

Social Engineering Attacks (6.2.2.6)

Social engineering is a type of access attack that attempts to manipulate individuals into performing actions or divulging confidential information such as passwords and usernames. It typically involves the use of social skills to manipulate inside network users to divulge information needed to access the network.

Social engineers often rely on people's willingness to be helpful. They also prey on people's weaknesses. For example, a threat actor could call an authorized employee with an urgent problem that requires immediate network access. The threat actor could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

Examples of social engineering attacks include

Pretexting: This is when a threat actor calls an individual and lies to them in an attempt to gain access to privileged data. An example involves a threat actor who pretends to need personal or financial data in order to confirm the identity of the recipient.

Spam: Threat actors may use spam email to trick a user into clicking an infected link, or downloading an infected file.

Phishing: There are many variations of this social engineering technique. A common version is the threat actor sends enticing custom-targeted spam email to individuals with the hope the target users click a link or download malicious code.

Something for something (quid pro quo): This is when a threat actor requests personal information from a party in exchange for something like afree gift.

Tailgating: This is when a threat actor quickly follows an authorized person with a corporate badge into a badge-secure location. The threat actor then has access to a secure area.

Baiting: This is when a threat actor leaves a malware-infected physical device, such as a USB flash drive, in a public location such as a corporate washroom. The finder finds the device and inserts it into their computer. On a Windows host, the autoplay feature may automatically install the malware.

Visual hacking: This is where a threat actor physically observes the victim entering credentials such as a workstation login, an ATM PIN, or the combination on a physical lock. This practice is also referred to as “shoulder surfing.”

Phishing Social Engineering Attacks (6.2.2.7)

Phishing is a common social engineering technique that threat actors use to send emails that appear to be from a legitimate organization (such as a bank). The goal is to get the victim to submit personal or sensitive information such as usernames, passwords, account information, financial information, and more. The email could also attempt to trick the recipient into installing malware on their device.

Variations of phishing attacks include

Spear phishing: This is a targeted phishing attack tailored for a specific individual or organization and is more likely to successfully deceive the target.

Whaling: This is similar to spear phishing but is focused on big targets such as top executives of an organization.

Pharming: This attack compromises domain name services by injecting entries into local host files. Pharming also includes poisoning the DNS by compromising the DHCP servers that specify DNS servers to their clients.

Watering hole: This attack first determines websites that a target group visits regularly. Next, the threat actor attempts to compromise those websites by infecting them with malware that can identify and target only members of the target group.

Vishing: This is a phishing attack using voice and the phone system instead of email.

Smishing: This is a phishing attack using SMS texting instead of email.

The Social Engineering Toolkit (SET) was designed by TrustedSec to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.

Strengthening the Weakest Link (6.2.2.8)

Cybersecurity is only as strong as its weakest link. Since computers and other Internet-connected devices have become an essential part of our lives, they no longer seem new or different. People have become very casual in their use of these devices and rarely think about network security. The weakest link in cybersecurity can be the personnel within an organization, with social engineering as a major security threat. Because of this, one of the most effective security measures that an organization can take is to train its personnel and create a “security-aware culture.”

Lab 6.2.2.9: Social Engineering
In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

Denial-of-Service Attacks (6.2.2.10)

Denial-of-service (DoS) attacks are highly publicized network attacks. A DoS attack results in some sort of interruption of service to users, devices, or applications.

There are two major sources of DoS attacks:

Overwhelming quantity of traffic: This is when a network, host, or application is unable to handle an enormous quantity of data, causing the system to crash or become extremely slow.

Maliciously formatted packets: This is when maliciously formatted packets are forwarded to a host or application and the receiver is unable to handle an unexpected condition. A buffer overflow attack is a method usedin this type of DoS attack. For example, a threat actor forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets. This causes the receiving device to crash or run very slowly.

Figure 6-14 shows an example of a DoS attack.

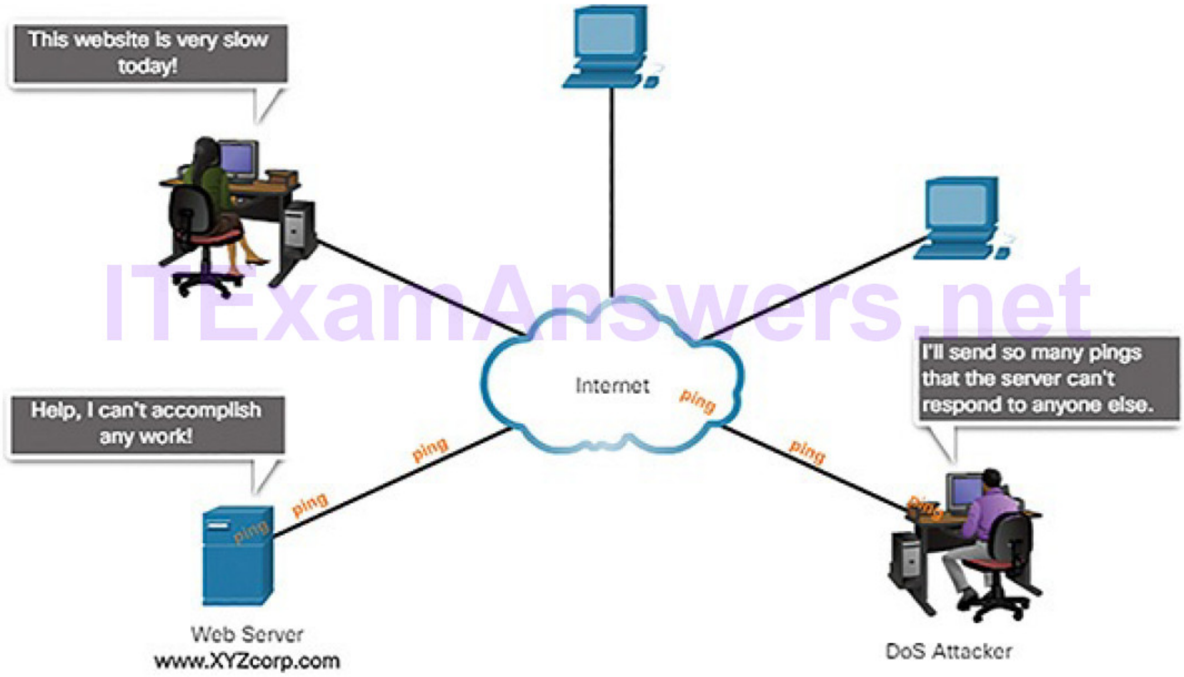

This website is very slow today!
Help, I can't accomplish any work!
Internet
ping
ping
ping
ping
ping
ping
I'll send so many pings that the server can't respond to anyone else.
Web Server
www.XYZcorp.com
DoS Attacker

Figure 6-14 DoS Attack

DoS attacks are considered a major risk because they can easily interrupt business processes or essential network services, and cause significant loss. These attacks are relatively simple to conduct, even by an unskilled threat actor.

DDoS Attacks (6.2.2.11)

If threat actors can compromise many hosts, they can perform a distributed DoS (DDoS) attack. DDoS attacks are similar in intent to DoS attacks, except that a DDoS attack increases in magnitude because it originates from multiple, coordinated sources, as shown in Figure 6-15. A DDoS attack can use hundreds or thousands of sources, as in IoT-based DDoS attacks.

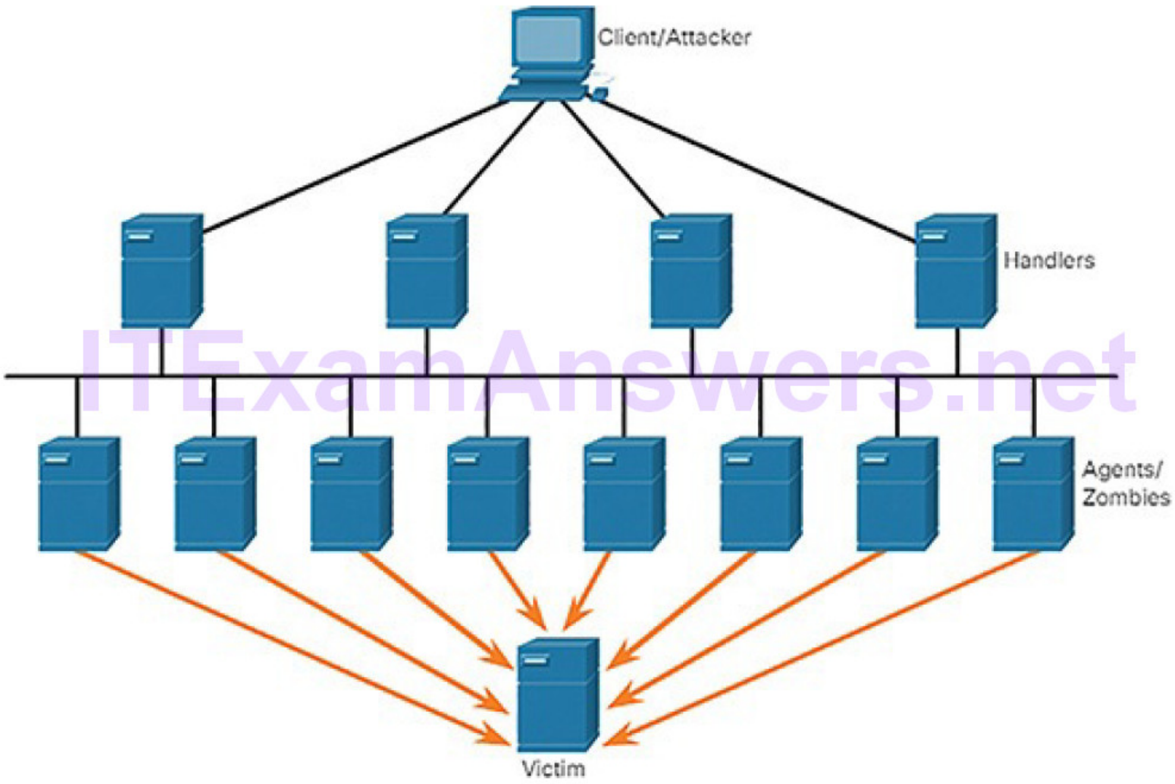


Figure 6-15 Components of a DoS Attack

The following terms are used to describe components of a DDoS attack:

Zombies: Refers to a group of compromised hosts (i.e., agents). These hosts run malicious code referred to as robots (i.e., bots). The zombie malware continually attempts to self-propagate like a worm.

Bots: Bots are malware that are designed to infect a host and communicate with a handler system. Bots can also log keystrokes, gather passwords, capture and analyze packets, and more.

Botnet: Refers to a group of zombies that have been infected using self-propagating malware (i.e., bots) and are controlled by handlers.

Handlers: Refers to a master command-and-control (CnC or C2) server controlling groups of zombies. The originator of a botnet can use Internet Relay Chat (IRC) or a web server on the C2 server to remotely control the zombies.

Botmaster: This is the threat actor in control of the botnet and handlers.

Note
There is an underground economy where botnets can be bought (and sold) for anominal fee. This can provide threat actors with botnets of infected hosts ready to launch a DDoS attack.

Example DDoS Attack (6.2.2.12)

As an example, a DDoS attack could proceed as follows:

1. The threat actor builds or purchases a botnet of zombie hosts.
2. Zombie computers continue to scan and infect more targets to create more zombies.
3. When ready, the botmaster uses the handler systems to make the botnet of zombies carry out the DDoS attack on the chosen target.

Figures 6-16 and 6-17 show an example of a DDoS attack.

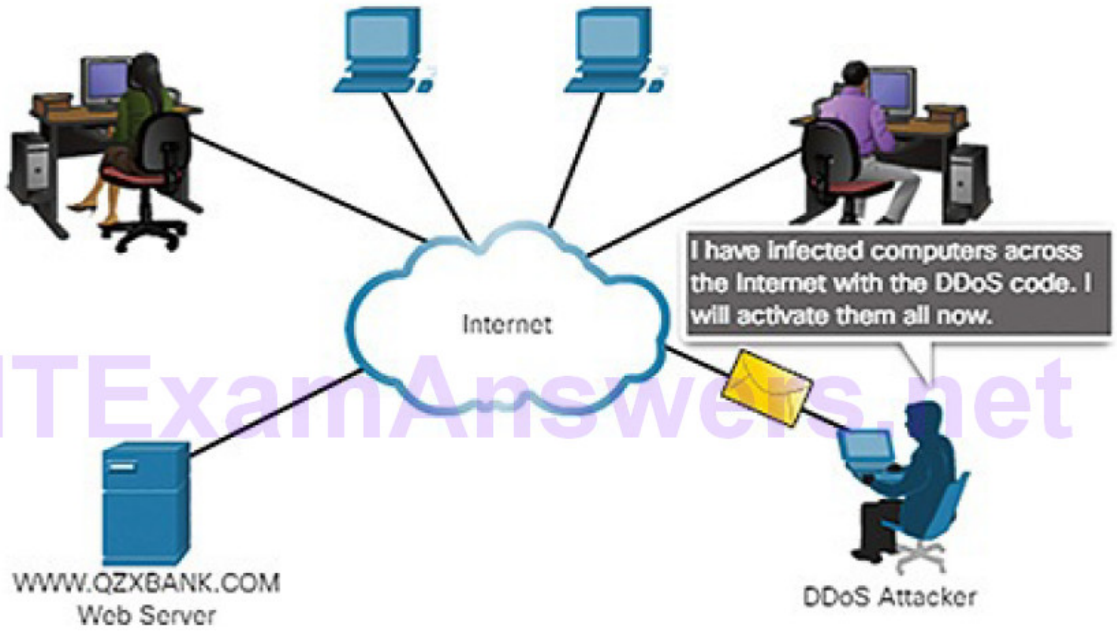

Internet
I have infected computers across the Internet with the DDoS code. I will activate them all now.
WWW.QZXBANK.COM
Web Server
DDoS Attacker

Figure 6-16 DDoS Attack: Infecting Zombies

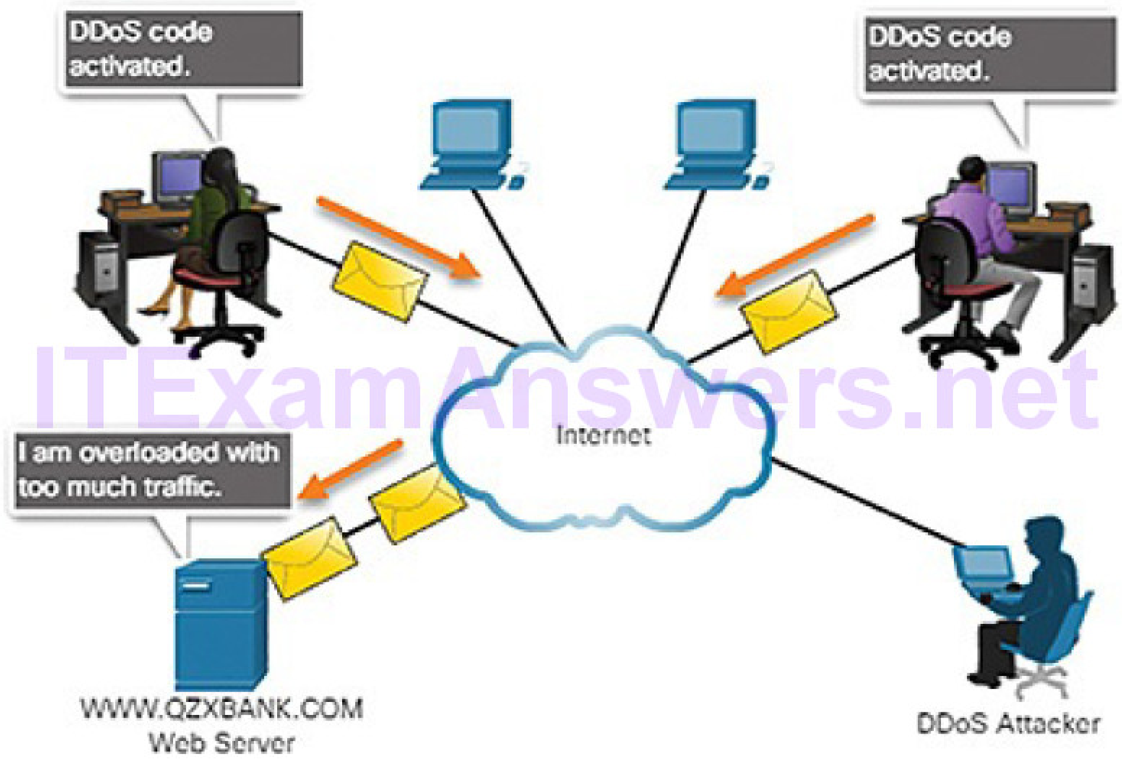


Figure 6-17 DDoS Attack: Zombies Flood Victim Server

Buffer Overflow Attack (6.2.2.13)

The goal of a threat actor when using a buffer overflow attack is to find a system memory-related flaw on a server and exploit it. Exploiting the buffer memory by overwhelming it with unexpected values usually renders the system inoperable, creating a DoS attack.

For example, a threat actor enters input that is larger than expected by the application running on a server. The application accepts the large amount of input and stores it in memory. The result is that it may consume the associated memory buffer and potentially overwrite adjacent memory, eventually corrupting the system and causing it to crash.

An early example of using malformed packets was the Ping of Death. In this legacy attack, the threat actor sent a ping of death, which was an echo request in an IP packet larger than the maximum packet size of 65,535 bytes. The receiving host would not be able to handle a packet of that size and it would crash, as shown in Figure 6-18.

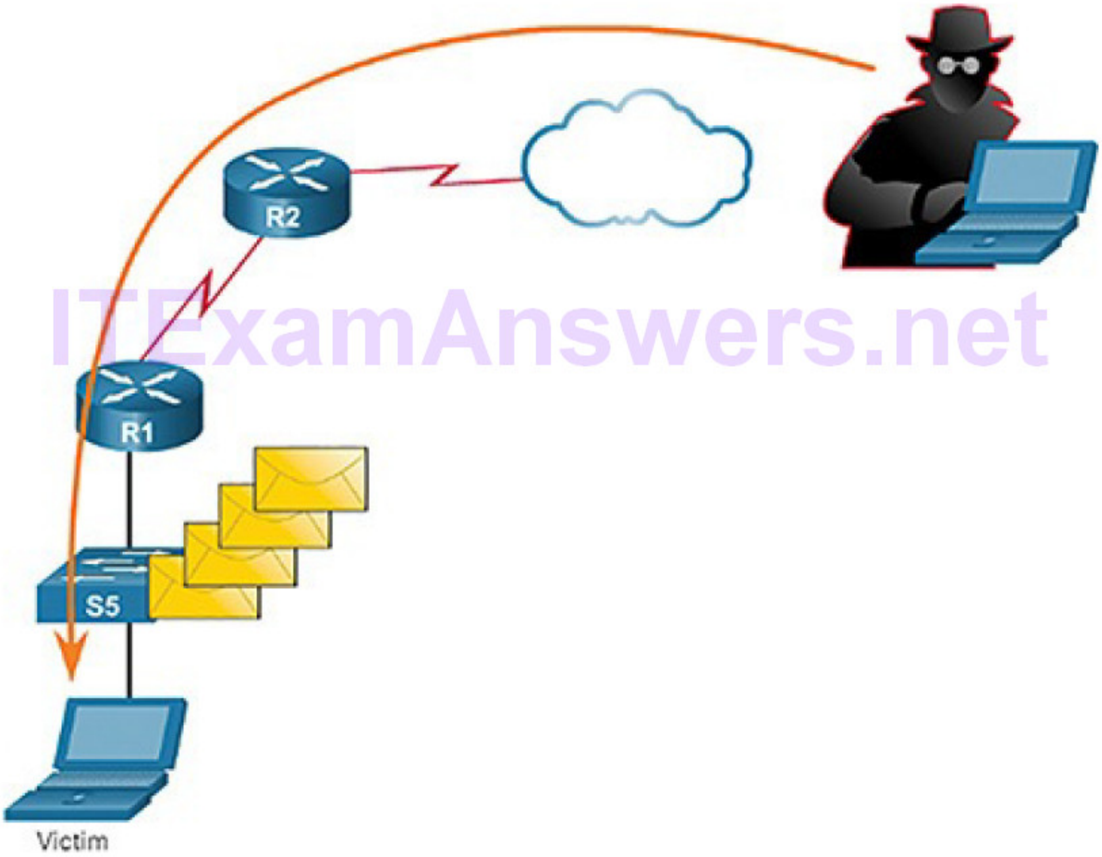


Figure 6-18 Buffer Overflow

Buffer overflow attacks are continually evolving. For instance, a remote DoS attack vulnerability was recently discovered in Microsoft Windows 10. Specifically, a threat actor created malicious code to access out-of-scope memory. When this code is accessed by the Windows AHCACHE.SYS process, it attempts to trigger a system crash, denying service to the user.

Note
It is estimated that one-third of malicious attacks are the result of buffer overflows.

Evasion Methods (6.2.2.14)

Threat actors learned long ago that "to hide is to thrive." This means their malware and attack methods are most effective when they are undetected. For this reason, many attacks use stealthy evasion techniques to disguise an attack payload. Their goal is to prevent detection by network and host defenses.

Some of the evasion methods used by threat actors include:

Encryption and tunneling: This evasion technique uses tunneling to hidethe content, or encryption to scramble its contents, making it difficult for many security detection techniques to detect and identify the malware.

Resource exhaustion: This evasion technique keeps the host too busy to properly use security detection techniques.

Traffic fragmentation: This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.

Protocol-level misinterpretation: This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.

Traffic substitution: In this evasion technique, the threat actor attempts to trick the IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.

Traffic insertion: Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data.

Pivoting: This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to log in to another host using the same credentials.

Rootkits: A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system.

New attack methods are constantly being developed. Network security personnel must be aware of the latest attack methods in order to detect them.

Activity 6.2.2.15: Identify the Types of Network Attack
Refer to the online course to complete this Activity.

Activity 6.2.2.16: Components of a DDoS Attack
Refer to the online course to complete this Activity.

Summary (6.3)

In this chapter, you learned how networks are attacked. You learned the types of threats and attacks used by threat actors. Threat actors are gray or black hat hackers who attempt to gain unauthorized access to our networks. They may also run programs that prevent or slow network access for others. Cybercriminals are threat actors who are motivated solely by financial gain.

Threat actors use a variety of tools, including

- Password crackers
- Wireless hacking tools
- Network scanning and hacking tools
- Packet crafting tools
- Packet sniffers
- Rootkit detectors
- Forensic tools
- Debuggers
- Hacking operating systems
- Encryption tools
- Vulnerability exploitation tools
- Vulnerability scanners

These tools can be used to launch a variety of attacks, including

- Eavesdropping
- Data modification
- IP address spoofing
- Password cracking
- Denial of service
- Man-in-the-middle
- Compromised key
- Network sniffing

Malware, or malicious code, is software that is specifically designed to damage, disrupt, steal, or generally inflict some other "bad" or illegitimate action on data, hosts, or networks. The three most common types of malware are viruses, worms, and Trojan horses:

- A virus is a type of malware that propagates by inserting a copy of itself into another program.
- Worms are similar to viruses because they replicate and can cause the same type of damage. Whereas a virus requires a host program to run, worms can run by themselves.
- A Trojan horse is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.

Malware continues to evolve. The most dominant attack currently is ransomware. Ransomware is malware that denies access to the infected computer system or its data until the owner pays the cybercriminal.

All the various types of tools threat actors use to launch network attacks can be classified as one or more of the following:

Reconnaissance: This is unauthorized discovery and mapping of systems, services, or vulnerabilities.

Access attacks: These exploit known vulnerabilities to gain entry to web accounts, confidential databases, and other sensitive information.

Social engineering: This is an attempt to manipulate individuals into performing actions or divulging confidential information such as passwords and usernames.

Denial of service: This occurs by overwhelming the network with a large quantity of traffic, or maliciously formatting packets that the receiver is unable to handle, causing the device to run very slowly or even crash.

Buffer overflow: This uses a system memory–related flaw on a server to overwhelm it with unexpected values. The goal is to render it inoperable.

To stay hidden and continue their attack, threat actors use a variety of evasion methods, including:

- Encryption and tunneling
- Resource exhaustion
- Traffic fragmentation
- Protocol-level misinterpretation
- Traffic substitution
- Traffic insertion
- Pivoting
- Rootkits

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs are available in the companion CCNA Cybersecurity Operations Lab Manual (ISBN: 9781587134388).

Labs

Lab 6.2.1.11: Anatomy of Malware

Lab 6.2.2.9: Social Engineering