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

2.5.1

Video - Denial of Service Attacks

2.5.2

DoS and DDoS Attacks

A Denial of Service (DoS) attack creates some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:

- **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
- **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.

Click each button for an illustration and explanation of DoS and DDoS attacks.

DoS Attack DDoS Attack

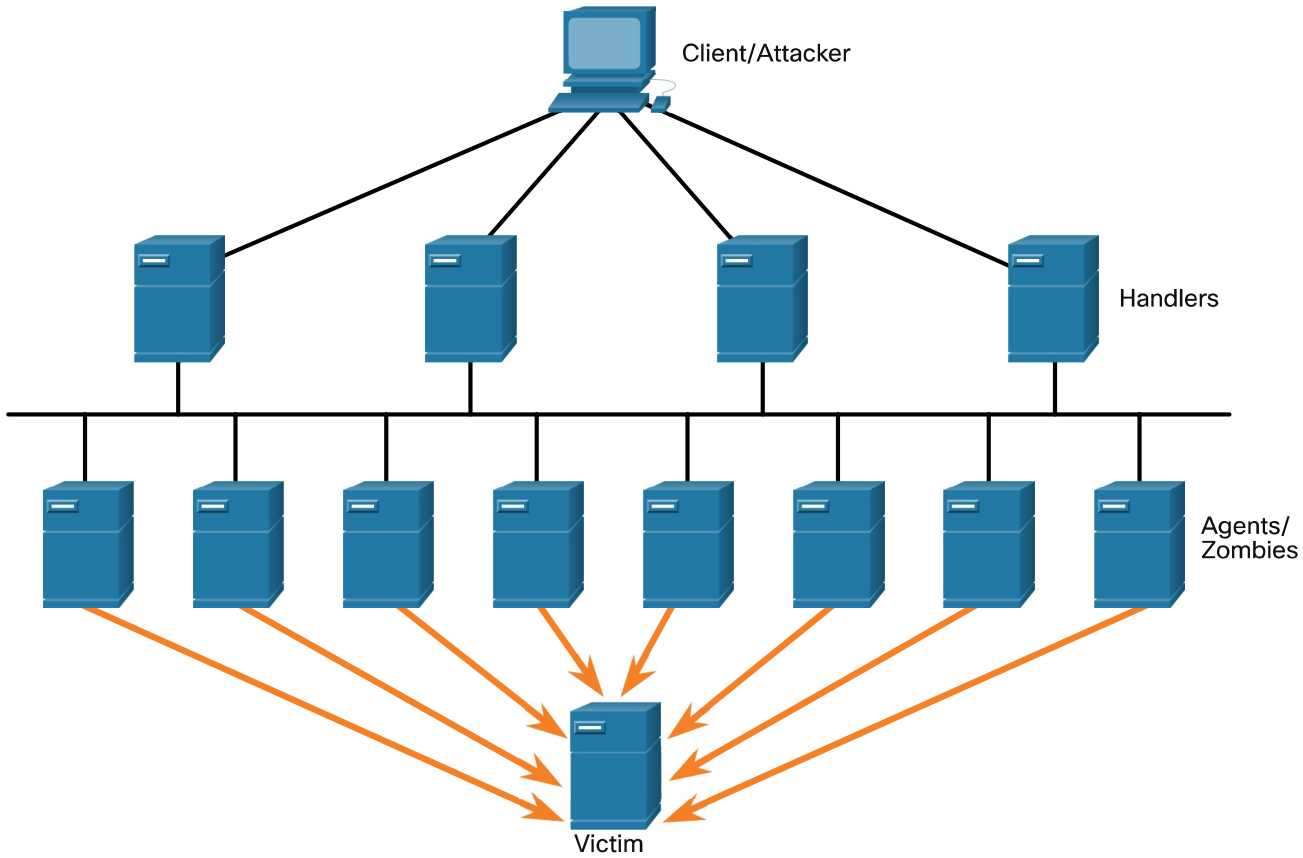
A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, A threat actor builds a network of infected hosts, known as zombies. The threat actor uses a command and control (CnC) system to send control messages to the zombies. The zombies constantly scan and infect more hosts with bot malware. The bot malware is designed to infect a host, making it a zombie that can communicate with the CnC system. The collection of zombies is called a botnet. When ready, the threat actor instructs the CnC system to make the botnet of zombies carry out a DDoS attack.

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

2.5.3

Components of DDoS Attacks

If threat actors can compromise many hosts, they can perform a Distributed DoS Attack (DDoS). 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 the figure. A DDoS attack can use hundreds or thousands of sources, as in IoT-based DDoS attacks.



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

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

Component	Description
zombies	This 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 is designed to infect a host and communicate with a handler system. Bots can also log keystrokes, gather passwords, capture and analyze packets, and more.

Component	Description
botnet	This refers to a group of zombies that have been infected using self-propagating malware (i.e., bots) and are controlled by handlers.
handlers	This refers to a primary **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 who is in control of the botnet and handlers.

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

2.5.4

Video - Mirai Botnet

Mirai is malware that targeted Internet of Things (IoT) devices that are configured with default login information. Closed-circuit television (CCTV) cameras made up the majority of Mirai's targets. Using a brute force dictionary attack, Mirai ran through a list of default usernames and passwords that were widely known on the internet.

- root/default
- root/1111
- root/54321
- admin/admin1234
- admin1/password
- guest/12345
- tech/tech
- support/support

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.

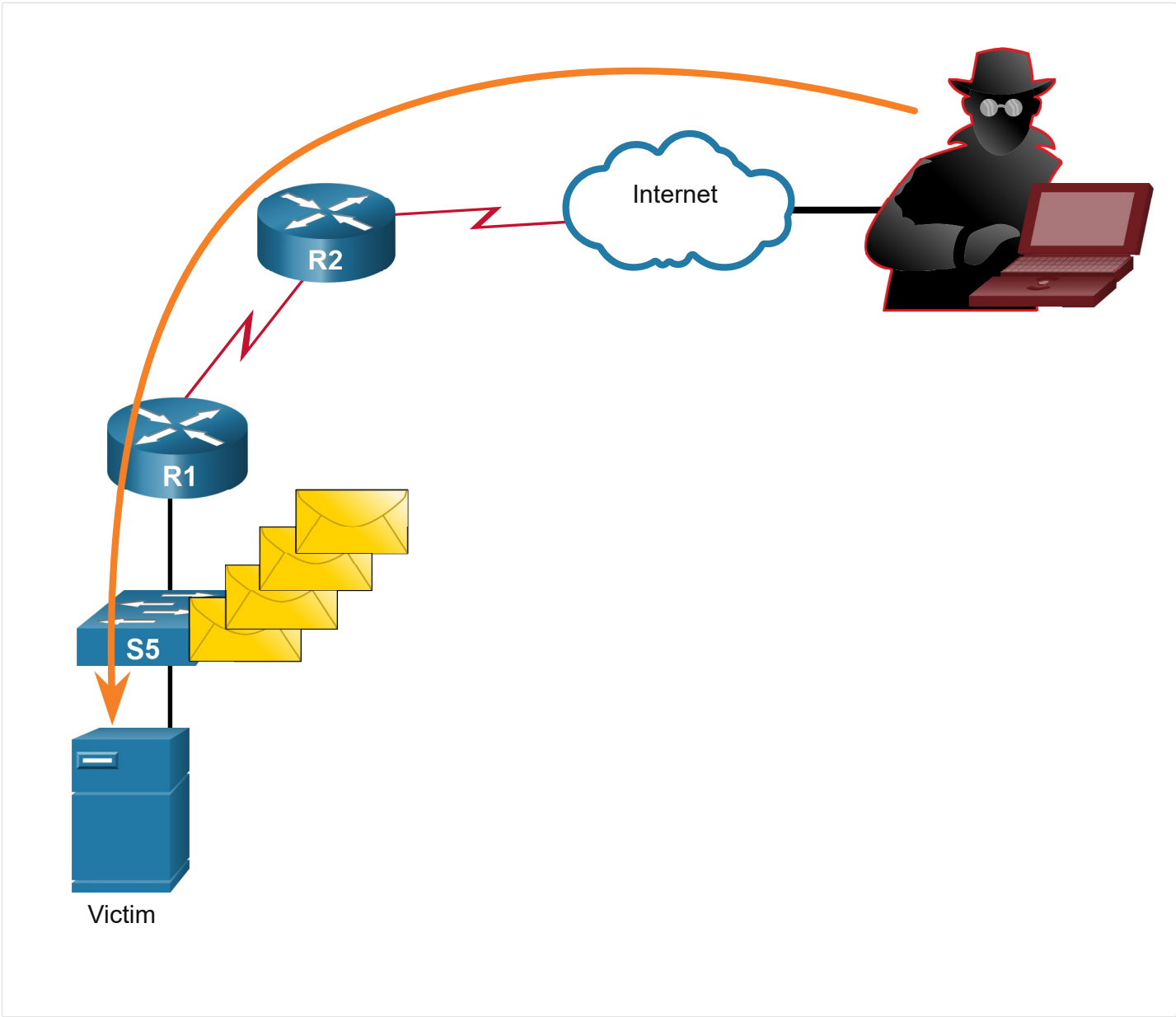
In October 2016 the services of Dyn, a Domain Name System (DNS) provider, were attacked, causing internet outages for millions of users in the United States and Europe.

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.

2.5.5

Buffer Overflow Attack



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. 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.

Buffer overflow attacks are continually evolving. For instance, a remote denial of service 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. Search the Internet on “TALOS-2016-0191 blog” to go to the Cisco Talos threat intelligence website and read a description of such an attack.

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

2.5.6

Evasion Methods

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 evading network and host defenses.

Some of the evasion methods used by threat actors include:

Evasion Method	Description

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.
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.
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.

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

2.5.7

Check Your Understanding - Identify the Types of Network Attacks

Check your understanding of network attacks by answering the following questions.

1. What is the weakest link in network security?

- reconnaissance
- access
- DoS
- social engineering

2. What type of attack is tailgating?

- reconnaissance
- access
- DoS
- social engineering

3. What type of attack is port scanning?

- reconnaissance

- access
- DoS
- social engineering

4. What is the weakest link in network security?

- routers
- people
- TCP/IP
- social engineering

Check
Show Me
Reset

2.4 Common Network Attacks - Reconnaissance, Access, ...
2.6 Network Threats Summary