Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

June 5, 2023

# Chapter 7 - 9 Review

## Question

### 7.1 Define a denial-of-service (DoS) attack

A denial-of-service (DoS) attack is defined as “an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space” (Stallings & Brown, 2018. p. 226). In other words, this means that a DoS attack has the goal of using up the resources of a system in order to prevent the usage of the system or impair it for other users such as slowing down the connection to its servers or network. There is also something called a distributed denial-of-service attack, DDoS, which has the same goal as a DoS attack but uses multiple sources to try to prevent or impair the system, network or resources.

### 7.2 What types of resources are targeted by such DoS attacks?

The categories or types of resources which are targeted by DoS attacks are: network bandwidth, system resources, and application resources (Stallings & Brown, 2018. p. 226).

## 7.3 What is the goal of a flooding attack?

Flooding attacks have a variety of forms which they are able to take on based on the network protocol, which is being used to perform the attack, however, the general goal of a flood attack is to overload the network capacity on a link to a server (Stallings & Brown, 2018. p. **). The other potential goal of a flooding attack is to overload the server's ability to handle and respond to its traffic (Stallings & Brown, 2018. p. **). Flood attacks are typically performed by flooding the target with malicious packets which competes with real, valid traffic causing dropped packets (Stallings & Brown, 2018. p. 233).

## 7.4 What types of packets are commonly used for flooding attacks?

Flooding attacks will typically use ICMP, UDP, or TCP SYNC packets (Stallings & Brown, 2018. p. 233).

ICMP – ICMP flooding was typically used because network administrations would traditionally allow this type of packet into their network as the ping command is a useful diagnostic tool, however, recently network admins have started to block these types of packets to pass through firewalls (Stallings & Brown, 2018. p. 233). As a result of the block of ICMP ping packets being blocked attackers have switched to TCP/IP packets which are not being blocked (Stallings & Brown, 2018. p. 233).

UDP – With UDP flooding the attacker will direct the packets to a specific port on the network, such as the diagnostic echo service which are often enabled on servers by default (Stallings & Brown, 2018. p. 233 - 234).

TCP SYN – With TCP SYN flooding the TCP packets are getting sent to the targeted system and would look like a normal TCP connection request (Stallings & Brown, 2018. p. 234).

---

**8.1 List and briefly define four classes of intruders.**

Four classes of intruders are: cyber criminals, activists, state-sponsored organizations, and others (Stallings & Brown, 2018. p. 252).

Cyber criminals – Cyber criminals are often individuals, or they are members of an organized crime group, their goal is to get a financial reward through performing activities such as identity theft, theft of financial credentials, corporate espionage, data theft, or data ransoming (Stallings & Brown, 2018. p. 252 - 253).

Activists – Activists can be individuals working as an insider or are a member of a larger group of outside attackers, they are motivated by social or political causes rather than financial gain, they also have titles such as hacktivist (Stallings & Brown, 2018. p. 253). Often with their attacks activists try to promote it and publicize it in a way that they try to gain attention to promote their cause, they do this through website defacement,

DoS attacks, or the theft and distribution of data which give negative publicity or compromise their targets (Stallings & Brown, 2018. p. 254).

State-sponsored organizations – State-sponsored organizations are groups of hackers which are sponsored by governments with the goal of conducting espionage or other sabotage activities (Stallings & Brown, 2018. p. 254).

Others – There are also other types of hackers who cannot necessarily be put into one group of the above types of intruders, however, there are many other groups which simply are not listed, some of these are people who are simply motivated by the technical challenge or by peer-group esteem and reputation (Stallings & Brown, 2018. p. 254).

## 8.4 Describe the three logical components of an IDS

The three logical components of an IDS, Intrusion Detection System, are: sensors, analyzers, and user interfaces (Stallings & Brown, 2018. p. 256).

Sensors – Sensors are what collects the data for the IDS (Stallings & Brown, 2018. p. 256). The input data for the sensor can be any part of a system which can contain evidence for an intrusion (Stallings & Brown, 2018. p. 256). There are many different types of inputs for sensors such as network packets, log files, and system call traces (Stallings & Brown, 2018. p. 256). The sensor after it has collected this data forwards it to the analyzer (Stallings & Brown, 2018. p. 256).

Analyzers – The analyzers receive its input from the sensors or from other analyzers, the analyzer then determines if an intrusion has actually occurred (Stallings & Brown, 2018. p. 256). An analyzer output can also include the evidence which the analyzer used to determine if the intrusion occurred or not, an analyzer can also provide guidance of what to do in its output for what steps to take (Stallings & Brown, 2018. p. 256). The inputs for the analyzers can also be stored for further analysis and review (Stallings & Brown, 2018. p. 256).

User interfaces – The analyzers then sends their data to a user interface which is a part of the IDS and enables the users to view its output and control the behavior of the system (Stallings & Brown, 2018. p. 257).

**8.5 Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?**

A host-based IDS is defined as something that “monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity” (Stallings & Brown, 2018. p. 257). This means that a host-based IDS is specific to a single host and the IDS is only performed on that host as well as all evidence and sensors. A host-based IDS also only looks at process identifiers and its calls.

A network-based IDS is defined as something that “monitors network traffic for particular network segments or devices and analyzes network transport, and application protocols to identify suspicious activity” (Stallings & Brown, 2018. p. 257). This means

that a network-based IDS can cover segments of a network or an entire network and analyzes the network traffic specifically.

It is possible to also have a distributed or hybrid Intrusion Detection System, IDS, which combines information from a number of different sensors from a host such as its process identifiers and system calls as well as sensors from the network which looks at traffic (Stallings & Brown, 2018. p. 257). This allows both of the IDS's to be combined into a single system which takes the advantages of both.

---

**9.1 List three design goals for a firewall**

Three design goals for a firewall are as follows:

"1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies […]

3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system […]" (Stallings & Brown, 2018. p. 290).

To summarize, the first goal of a firewall is that all traffic must pass through it, the second goal is that only authorized traffic can pass through it, and the third goal is that the firewall itself is immune to penetration.

## 9.2 List four characteristics used by firewalls to control access and enforce a security policy

Four characteristics used by firewalls to control access and enforce a security policy are as follows: IP address and protocol values, application protocol, user identity, and network activity (Stallings & Brown, 2018. p. 290).

IP Address and Protocol Values – Firewalls use IP addresses and protocol values to control access based on the source or destination addresses and port numbers, the direction of the traffic if it is inbound or outbound, and other network transport layer characteristics (Stallings & Brown, 2018. p. 290). Typically, this type of filtering will be used by the packet filter and stateful inspection firewalls and is used to limit access to specific services (Stallings & Brown, 2018. p. 290).

Application protocol – The application protocol in a firewall is used to control access based authorized application protocol data (Stallings & Brown, 2018. p. 291). This type of filtering will also be done by an application-level gateway which can relay and monitor the exchange of information (Stallings & Brown, 2018. p. 291).

User identity – Firewalls use user identities to control access to the network based on the identity of the user, this is typically done for internal users who are able to

identify themselves using some form of secure authentication such as IPSec (Stallings & Brown, 2018. p. 291).

Network activity – Firewalls use network activity to control access based on considerations such as the time or request (Stallings & Brown, 2018. p. 291).

**9.3 What information is used by a typical packet filtering firewall?**

A typical packet filtering firewall will use the source IP address, the destination IP address, the source and destination transport-level address, the IP protocol field, and the interface (Stallings & Brown, 2018. p. 293).

Source IP address – This is the IP address which originated the IP packet (Stallings & Brown, 2018. p. 293).

Destination IP address – This is the IP address of the system which the IP packet is trying to reach (Stallings & Brown, 2018. p. 293).

Source and destination transport-level address – This is the transport-level, such as TCP or UDP port number which is able to define an application such as SNMP or HTTP (Stallings & Brown, 2018. p. 293).

IP protocol field – This defines the transport protocol being used (Stallings & Brown, 2018. p. 293).

Interface – This is the interface of the firewall the packet came from (Stallings & Brown, 2018. p. 293).

**Problem**

**9.4 Table 9.5 shows a sample of a packet filter firewall ruleset for an imaginary network of IP address that range from 192.168.1.0 to 192.168.1.254. Describe the effect of each rule.**

**Table 9.5 Sample Packet Filter Firewall Ruleset**

| | Source Address | Source Port | Dest Address | Dest Port | Action |
|---|---|---|---|---|---|
| 1 | Any | Any | 192.168.1.0 | >1023 | Allow |
| 2 | 192.168.1.1 | Any | Any | Any | Deny |
| 3 | Any | Any | 192.168.1.1 | Any | Deny |
| 4 | 192.168.1.0 | Any | Any | Any | Allow |
| 5 | Any | Any | 192.168.1.2 | SMTP | Allow |
| 6 | Any | Any | 192.168.1.3 | HTTP | Allow |
| 7 | Any | Any | Any | Any | Deny |

1 – Rule one says that anything coming from any source address from any source port which is trying to communicate with 192.168.1.0 will be allowed as long as its port that it is trying to go to is greater than 1023

2 – Rule 2 says that if the source address is coming from 192.168.1.1 and any port to any destination address or port that it will be denied

3 – Rule 3 says that any source address or port trying to communicate with the address 192.168.1.1 at any port will be denied

4 – Rule 4 says that if the source address is 192.168.1.0 at any port with any destination address or port that it will be allowed

5 – Rule 5 says that any source address on any port which is going to 192.168.1.2 through SMTP will be allowed

6 – Rule 6 says that any source address on any source port going to 192.168.1.3 through HTTP will be allowed

7 – Rule 7 says that any source address with any source port going to any destination address or port will be denied

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

*Dalton Murray*