Handling Denial-of-Service Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what Denial of Service incidents are.

Explain what the different types of Denial of Service incidents that IH&R team members may detect during an investigation are.

Identify what steps the IH&R team should take to contain and eradicate Denial of Service incidents.

Define what the steps that the IH&R team should take to ensure recovery from Denial of Service incidents.

External Resources:

Handling Denial of Service Incidents

What is a Denial of Service (DoS) Incident? -

In a DoS attack, attackers flood a victim’s system with non-legitimate service requests or traffic to overload its resources. The goal of a DoS attack is not to gain unauthorized access to a system or to corrupt data; it is to keep the legitimate users away from using the system.

NOTE: A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a victim’s system or network resources, launched indirectly through many compromised computers (bots/zombies).

The services under attack are those of the “primary victim,” whereas the compromised systems used to launch the attack are the “secondary victims.”

What are the different types of DoS/DDoS Incidents?

▪ Volumetric Attacks - Exhaust the bandwidth either within the target network/service, or between the target network/service and the rest of the internet, and result in traffic blockage preventing access to legitimate users. Volumetric DDoS attacks generally target protocols that are stateless and do not have built-in congestion avoidance.

There are two types of bandwidth depletion attacks:

o Flood attack - bots/zombies sending large volumes of traffic against victim’s systems in order to overwhelm and consume all the available bandwidth.

o Amplification attack - bots/zombies send messages to a broadcast IP address; this method amplifies malicious traffic that consumes the victim systems’ bandwidth.

Volumetric attack techniques:

o User Datagram Protocol (UDP) flood attack
o Internet Control Message Protocol (ICMP) flood attack
o Ping of Death attack
o Smurf attack
o Malformed IP packet flood attack
o Spoofed IP packet flood attack

▪ Protocol Attacks - consume the connection state tables present in the network infrastructure devices such as load-balancers, firewalls, and application servers, and no new connections will be allowed since the device will be waiting for existing connections to close or expire. The magnitude of attack is measured in packets per second (pps) or connections per second (cps).

Protocol attack techniques:

o SYN flood attack
o ACK flood attack
o TCP connection flood attack
o TCP state exhaustion attack
o Fragmentation attack
o RST attack

▪ Application Layer Attacks - Attacker tries to exploit the vulnerabilities in application layer protocol or in the application itself to prevent the access of the application to the legitimate user. These attacks destroy a specific aspect of an application or service and are effective with one or few attacking machines producing a low traffic rate (very hard to detect and mitigate). The magnitude of attack is measured in requests-per-second (rps).

Application layer attack techniques:

o HTTP flood attack
o Slowloris attack

▪ Permanent Denial-of-Service Attack Permanent DoS (PDoS) attacks (phlashing) - targets hardware causing irreversible damage to the hardware. The PDoS attack exploits security flaws in a device, thereby allowing the remote administration on the management interfaces of the victim’s hardware, such as printers, routers, or other networking devices.

▪ Distributed Reflection Denial of Service (DRDoS) attack (“spoofed” attack) - use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application. The DRDoS attack exploits the TCP three-way handshake vulnerability. This attack involves the attacker machine, intermediary victims (zombies), secondary victims (reflectors), and the target machine. The attacker launches this attack by sending requests to the intermediary hosts, which in turn reflects the attack traffic against the target.

What is the process involved in executing a DRDoS attack? -

- The attacker commands the intermediary victims (zombies) to send a stream of TCP SYN packets with the primary target's IP address as the source IP address to other non-compromised machines (secondary victims or reflectors) getting them to establish a connection with the primary target.

- As a result, the reflectors send a huge volume of TCP SYN-ACK traffic to the primary target to establish a new connection with it.

- The primary target discards the SYN-ACK packets received from the reflectors, as it did not send the actual SYN packet.

- The reflectors keep waiting for the TCP ACK response from the primary target.

- Assuming that the packet lost its path, these bunches of reflector machines resend their TCP SYN-ACK packets to the primary target in an attempt to establish the connection, until time-out occurs.

- The combined bandwidth of these reflector machines overwhelms the target machine.

How can we detect DoS/DDoS Incidents? -

Three types of detection techniques:

- Activity Profiling - done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information. Packet header information includes the destination and sender IP addresses, ports, and transport protocols used. An attack is indicated by

o An increase in activity levels among the network flow clusters
o An increase in the overall number of distinct clusters (DDoS attack)

- Sequential Change-point Detection - filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks. If there is a drastic change in traffic flow rate, a DoS attack may be occurring. This technique uses the Cumulative Sum (Cusum) algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series.

NOTE: The sequential change-point detection technique identifies the typical scanning activities of the network worms.

- Wavelet-based Signal Analysis - analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. These techniques check frequency components present at a specific time and provide a description of those components. Presence of an unfamiliar frequency indicates suspicious network activity. A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.

What are other DoS/DDoS detection techniques? -

Other techniques for detecting DoS/DDoS attack are as follows:

- Analyzing the network traffic that contains high number of Address Resolution Protocol (ARP) requests

- Checking the Network Address Translation (NAT)/Port Address Translation (PAT) address-translation tables for large numbers of entries

- Checking whether the router's IP input, ARP input, IP cache ager, and Cisco Express Forwarding (CEF) processes are using abnormally high amounts of memory

- Checking whether the router's ARP, IP input, CEF, and inter-process communication (IPC) processes are running at a much higher CPU utilization rate

- Checking for high numbers of similar kinds of packets from the same or different IP addresses that can result in TCP or UDP flooding

How do we contain DoS/DDoS Incidents? -

DoS/DDoS response strategies are as follows:

```
▪ Absorb the Attack
▪ Divert the Attack
▪ Block the Attack
▪ Degrade non-essential service(s)
▪ Shutdown
▪ Load Balancing
▪ Throttling
▪ Drop requests
```

What about Post Attack Forensics? -

Forensic techniques that an incident responder can execute:

```
▪ Traffic Pattern Analysis
▪ Packet Traceback
▪ Event Log Analysis
```

What about Eradicating DoS/DDoS Incidents: Blocking Potential Attacks? -

```
▪ Ingress/Egress filtering
▪ TCP Intercept (Cisco)
▪ Rate Limiting - configured to limit the rate of requests at layers 4 and 5
of the OSI model
```

What about Eradicating DoS/DDoS Incidents: Disabling Botnets? -

```
▪ RFC 3704 filtering by denying traffic with spoofed addresses. Filter
requires packets sourced from valid, allocated address space. A “bogon list”
consists of all unused or reserved IP addresses that should not come in from
the internet.

▪ IPS Source / IP Reputation Filtering

▪ Black hole filtering of incoming traffic that is discarded or dropped
without informing the source that the data did not reach its intended recipient

▪ Enable IP Source Guard (Cisco) or similar features in other routers to
filter traffic based on the DHCP snooping binding database or IP source
bindings, preventing a bot from sending spoofed packets
```

What about Recovery after DoS/DDoS Incidents? -

The IH&R team should perform the following activities to recover the network
from DoS/DDOS attacks:

```
▪ Determine the extent of impact on different sources, their ability to
function and risks involved in using the compromised resources

▪ Devise various methods of recovery depending on different factors such as
severity of incident, systems affected, systems and devices required to keep
business running, and backup resources available

▪ Communicate with the incident response team to select best recovery plan and
obtain required permissions from cybersecurity authorities

▪ Use the backup resources efficiently to replace the compromised systems

▪ Check the functionality of all the restored systems

▪ Implement additional monitoring to look for related activity in future

▪ Regularly update security policies
```