Subankamo 300471606

Lab 3 - Denial of Service Attacks (Total: 4 Marks)

Due Date – 30/04/2023

- Follow the instructions in this document,
- Answer the questions in the order they appear in this document,
- Submit the file (.doc, .docx, .pdf) using the ecs submission system (i.e. Lab3). https://apps.ecs.vuw.ac.nz/submit/CYBR371

Instructions:

Sign in into the NETLAB (https://netlab.ecs.vuw.ac.nz/) with the provided credentials and complete the following lab.

A. Denial of Service Attacks

B. ARP Spoofing and MiTM Attacks

- Write the answers to the questions in the order they appear in the lab document files

Questions (Questions are associated with each lab identified by A, B)

- **A1 -** [0.5 Mark] Why aren't new operating systems susceptible to Ping of Death attack? (250 words max)

The Ping of Death attack is a type of computer attack that can make a system crash or reboot by sending packets of data bigger than its capacity. This attack was possible in the past with older systems, but newer operating systems have fixed the problem so they are not vulnerable to this type of attack.

New operating systems are not susceptible to the Ping of Death attack because they have been designed with improved network stack implementations that include input validation checks to prevent buffer overflow attacks. This means that when a Ping packet is received, the operating system will check the size of the packet and reject any packets that are too large or malformed, rather than allowing them to crash the system. Additionally, modern operating systems have built-in firewalls and security features that can detect and block Ping of Death attacks.

- **A2 -** [0.5 Mark] How can you make the Ping of Death packets effective against a target these days? (250 words max)

Ping of Death is an old type of Denial of Service (DoS) attack that takes advantage of a vulnerability in the target operating system's handling of large Internet Control Message Protocol (ICMP) packets. However, even though modern operating systems are no longer vulnerable to this type of attack, attackers can still make use of it in several ways.

-Fragmentation Attack: fragmenting the oversized ICMP packets into smaller fragments that the target system will reassemble - by sending multiple fragmented packets, the attacker can overwhelm the target system and cause it to crash.
-Ping of Death + Distributed Denial of Service (DDoS) attack: multiple systems are used to flood the target system with traffic.
-Ping of Death + Smurf attacks:a large number of ICMP echo requests are sent to a broadcast address with a spoofed IP address that belongs to the target system. This causes all machines on the network to send an echo reply back to the target system, overwhelming it with traffic. Combining Smurf attacks with Ping of Death packets can amplify their impact.

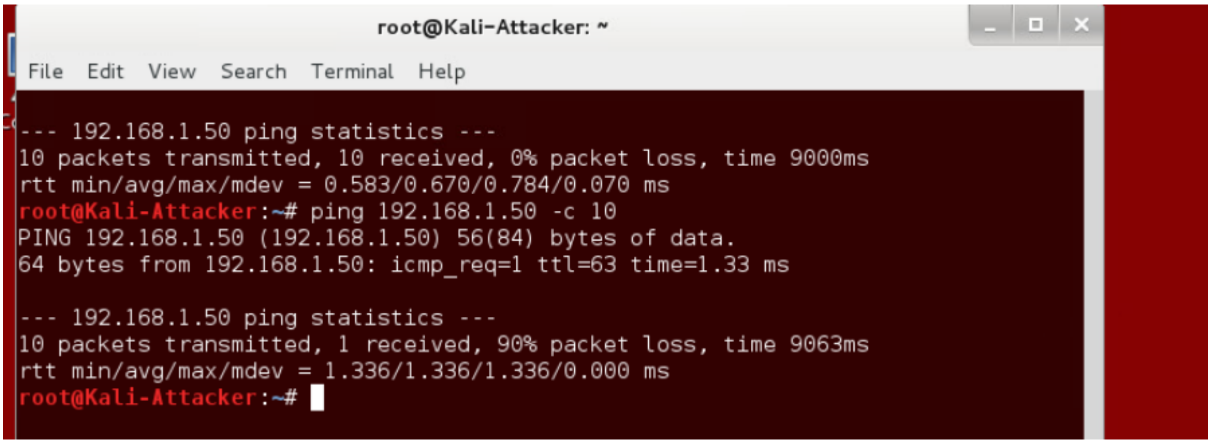
Additionally, attackers can exploit vulnerabilities in specific applications or services running on the target system. For example, sending Ping of Death packets to a web server that is vulnerable to a specific type of attack can cause it to crash.

- **A3** – [1 Mark] Briefly explain the countermeasures to stop and defend against a Smurf attack? (250 words max).

A Smurf attack is a type of DDoS attack that floods a network with traffic by sending ICMP echo requests to the broadcast address, causing all hosts on the network to respond to the target system. To defend against a Smurf attack, network administrators can take several countermeasures:
-disabling IP directed broadcasts (prevent attackers from using the broadcast address to amplify their attack traffic)
-configuring routers to drop ICMP echo requests to the broadcast address (prevent attackers from reaching the hosts on the network)
-implementing ingress and egress filtering, increasing network bandwidth (prevent spoofed packets from entering or leaving their network. This can help to reduce the effectiveness of Smurf attacks and other types of DDoS attacks)
-using DDoS mitigation services (These services use specialised hardware and software to monitor network traffic and automatically block malicious traffic)
These measures can help prevent attackers from using the broadcast address to amplify their attack traffic, reduce the effectiveness of spoofed IP addresses, and block malicious traffic.
-Implement rate limiting (implement rate-limiting policies on the router or firewall to limit the number of ICMP packets that can be sent to the network)

- **A4** - [1 Mark] Did the Smurf attack slow down the network? Compare the average ping response time before and during the Smurf attack.

A Smurf attack can slow down a network by flooding it with large amounts of ICMP echo requests. This can overload network devices, saturate available bandwidth, and cause delays in network communication.
During the attack, the target device is flooded with ICMP echo requests from multiple sources, resulting in an increase in network traffic and delays in network communication.



```
--- 192.168.1.50 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9000ms
rtt min/avg/max/mdev = 0.583/0.670/0.784/0.070 ms
root@Kali-Attacker:~# ping 192.168.1.50 -c 10
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_req=1 ttl=63 time=1.33 ms

--- 192.168.1.50 ping statistics ---
10 packets transmitted, 1 received, 90% packet loss, time 9063ms
rtt min/avg/max/mdev = 1.336/1.336/1.336/0.000 ms
root@Kali-Attacker:~#
```

As we can see the average ping was 0.670 ms but during the smurf attack the average ping was 1.336 ms. This is significantly slower (100% slower) than it was prior to the attack.

- **B1** - [1 Mark] Is Ettercap using ARP spoofing to manipulate http images and JavaScripts? Explain your answer (250 words max).

Yes, Ettercap uses ARP spoofing to perform Man-in-the-Middle (MiTM) attacks, which allow an attacker to intercept and manipulate network traffic between two devices, including HTTP traffic containing images and JavaScripts. When Ettercap is used to perform a MiTM attack, it spoofs the ARP (Address Resolution Protocol) table of the target device, tricking it into sending its traffic through the attacker's machine. This allows the attacker to intercept and manipulate the traffic passing through their machine, including HTTP traffic containing images and JavaScripts. In the case of manipulating images and JavaScripts, Ettercap can intercept the HTTP responses containing these elements, modify them as desired, and then send them back to the target device. This can be used by an attacker to replace images with malicious ones or modify JavaScript files to include malicious code that would be executed by the victim's browser.