Laud Mills

Part A: Demonstration of a Denial-of-Service attack (DOS) using the tool HPing3 of Kali Linux. Hint: you can type “hping3 --help” on your terminal to check various options.

1. Write down the answers of following based on the command below:

hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.100.7

What is the packet count: -c 20000

What is the data size: -d 120

Which flag is set: -S SYN flag

What is the destination port: -p 80 http

Is 192.168.100.7 a source IP address? No it is rather the destination IP address where packets will be sent.

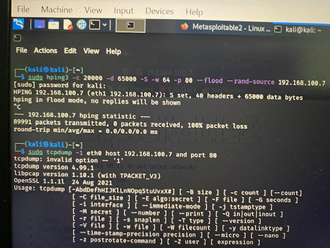
1. Derive a command based on following specification:

* Launch a UDP attack:
* Send packets as fastest as you can
* Keep packet size 65000
* Use IP address of Metasploitable2

Command:

hping3 -c 20000 -d 65000 -S -w 64 -p 80 --flood --rand-source 192.168.100.7

Screenshot:



1. Use the above command but instead of UDP use ICMP packets for flooding in Kali terminal and launch a DOS attack on the DVWA service. Click on various links to check how availability of the website is affected by UDP Flood attack. Show the entire process using screen captures.

Command: sudo hping3 -S 192.168.100.7 -a 192.168.100.55 -p 80 --flood

Screenshot (Kali Linux & Metasploitable2):

A computer screen with a black background

Description automatically generatedA screenshot of a computer

Description automatically generated

Before the Attack After the attack

A computer screen with text on it

Description automatically generated

1. Capture the traffic in Wireshark while launching the above ICMP flood attack (question 2). Take the screenshot of traffic capturing. Find out the source IP address, destination IP address, protocol field from the captured traffic. Generate the io graph in Wireshark that represents number of IP packets transferred in 1 second.

Source IP Address: 192.168.100.55 (spoof IP)

Destination IP Address: 192.168.100.7

Protocol: TCP

Screenshot of Wireshark Traffic Analysis:

A computer screen with text and numbers

Description automatically generated

Screen Shot of Wireshark I/O Graph:

A screen shot of a computer

Description automatically generated

Part B: Risk and Attack Analysis for Web applications security

1. If you are working in a CISCO Router company and you are unable to use name resolution services (DNS) what are the three major steps that a client should focus to troubleshoot? Explain all the three steps in detail.

Verify DNS Configuration: Ensure that the DNS server settings, domain name, and related configurations are correct. Use the show running-config command to check for proper DNS server IP addresses and domain settings. Also, confirm that the router is set to perform DNS lookups (ip domain-lookup).

Verify Network Connectivity: Ensure the router or client can reach the DNS server. Use the ping and traceroute commands to check network connectivity. If there are issues, verify routing, ACLs, or firewalls that may be blocking DNS traffic.

Check DNS Server Functionality: Ensure the DNS server is operational and capable of resolving names. Test the server’s functionality with nslookup or by checking DNS server logs. If the server is unresponsive, misconfigured, or overloaded, address these issues accordingly.

1. Despite the risks and well-known vulnerabilities, businesses and personal users will continue to use the Internet. What are the best practices in routine life to mitigate these risks?

To mitigate the risks and vulnerabilities associated with using the Internet, both businesses and personal users must adopt essential cybersecurity best practices. These include using strong, unique passwords and enabling Multi-Factor Authentication (MFA) for added security. It’s crucial to regularly update all software and systems to patch known vulnerabilities and use antivirus software to detect and prevent malware.

Users should be cautious with emails and links to avoid phishing attacks, and secure Wi-Fi networks with strong encryption to protect against unauthorized access. Encrypting sensitive data and backing it up regularly ensures that information remains safe even if systems are compromised. Monitoring online accounts for suspicious activity and conducting routine audits further enhances security.

Employee education and training on recognizing security threats, along with using Virtual Private Networks (VPNs) for secure browsing, can significantly reduce the chances of cyberattacks. Finally, securing physical access to devices, such as laptops and smartphones, is vital for preventing unauthorized access to sensitive information.

By implementing these best practices, businesses and personal users can significantly reduce their exposure to online threats, ensuring safer and more secure Internet usage.

References:

**National Institute of Standards and Technology (NIST).** (2020). *Cybersecurity framework*. National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>

**Cybersecurity & Infrastructure Security Agency (CISA).** (2023). *Cyber essentials: Basic cyber hygiene for small business*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/cyber-essentials

**Federal Trade Commission (FTC).** (2023). *Protecting your personal information*. Federal Trade Commission. https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

1. Define and justify your answers. The following activities belong to which category.

* True Positive
* False Positive
* True Negative
* False Negative

1. When a legitimate e-mail is incorrectly sent to your spam folder and blocked by IDS.

False Positive. This is because False Positive occurs when a system incorrectly identifies something as a problem or threat when it actually is not.

1. When a spam email appears as spam and filtered by spam filter IDS.

True Positive in the sense that, the spam email is correctly identified as spam by the IDS, which means the system has made the correct decision in flagging the email as spam.

1. When a spam that appears in your e-mail inbox was not caught by your spam filter IDS.

False Negative. This can be likened to failure of the system to detect a danger as it is supposed to be and this can be very costly.

1. When a legitimate email is filtered correctly and sent to the inbox.

True Negative occurs when the system correctly identifies a negative event or condition because the event is legitimate.

1. Understand each of the following scenario in detail and identify the most appropriate type of attack for each of the following scenarios.

|  |  |
| --- | --- |
| **Scenario** | **Attack Type** |
| Via this attack a password with administrator privileges provides an intruder with total unrestricted access to the system or network. | Privilege Escalation |
| A machine is bombarded with ICMP echo replies. | Smurf Attack |
| intruder trying to obtain sensitive information by intercepting, listening and analyzing network communications. | Man-In-The-Middle Attack |
| If the router to the network passes the ping broadcast, all computers on the network will respond with a ping reply to the system. | Denial of Service |
| refers to the ability to gain access to a computer or program that bypasses standard security mechanisms. | Exploiting Vulnerability |
| attack sends spoofed User Datagram Protocol packets to a network’s broadcast address. | Denial of Service |
| involve a coordinated attack from hundreds or thousands of computers across the Internet. | Distributed Denial of Service |
| intruder is able to capture the network data and manipulate it, change it, examine it, and then send it on. | Man-In-The-Middle Attack |
| Programs are designed to guess every possible combination. | Brute Force Attck |
| the attacker imitations the real source of a transmission such as files and emails. | Spoofing |
| a program scans through the entries in a dictionary data file, attempting to guess a password. | Dictionary Attack |

1. Draw a diagram illustrating the Fraggle DoS attack. In your diagram, show all the appropriate IP addresses and packet types. Which specific ports are used to direct these packets ?

Answer:

Port Numbers : Ports 7 and 19

1. Block Diagram :

A diagram of a computer

Description automatically generated