Review: Quiz 07 - Network Forensic (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1

Alice works for VCS Company as a senior security analyst. As part of the yearly security audit, Alice scans her network for vulnerabilities. Using Nmap, Alice conducts an XMAS scan, and most of the ports scanned do not respond. In what state are these ports? *

- Closed
- Open ✓
- Stealth
- Filtered

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2

An investigator is reviewing the firewall logs of a company and notices ICMP packets larger than 65,536 bytes. What type of activity is the investigator observing? *

- Smurf
- Ping of death ✓
- Fraggle
- Nmap scan

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3

What header field in the TCP/IP protocol stack involves the hacker exploit known as the **Ping of Death?** *

- (●) ICMP header field ✓
- ( ) TCP header field
- ( ) IP header field
- ( ) UDP header field

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4

While attempting to run an Nmap port scan on a web server, which of the following commands would scan common ports with minimal noise to evade IDS detection? *

- ( ) nmap -A - Pn
- ( ) nmap -sP -p-65535 -T5
- (●) nmap -sT -O -T0 ✓
- ( ) nmap -A --host-timeout 99 -T1

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5

Alice is scanning a target network. She initiates a TCP connection by sending an SYN packet to a target machine and receives a SYN/ACK packet in response. Instead of completing the three-way handshake with an ACK packet, she sends an RST packet. What type of scan is Alice likely performing, and what is her goal? *

- (●) They are performing an SYN scan to stealthily identify open ports without fully establishing a connection. ✓
- ( ) They are performing a network scan to identify live hosts and their IP addresses.
- ( ) They are performing a TCP connect scan to identify open ports on the target machine.
- ( ) They are performing a vulnerability scan to identify any weaknesses in the target system.

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

6

Alice is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of her scans, she is considering several host discovery techniques. She expects several unused IP addresses at any given time within the private address range of the LAN, but she also anticipates restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation? *

- ICMP ECHO Ping Sweep
- ICMP Timestamp Ping
- TCP SYN Ping
- ARP Ping Scan ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use? *

- -sA ✓
- -sX
- -sT
- -sF

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

8

When using Nmap, the attacker receives the following results.What command-line parameter could you use to determine the type and version number of the web server? *

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

- -sV ✓
- -sS
- -Pn
- -V

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

9

A DoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers open multiple connections and keep waiting for the requests to complete. Which attack is being described here? *

- TCP SYN Flood
- Slowloris ✓
- Ping of Death
- ICMP Flood

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10

Alice, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Alice used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Alice retrieve the required information? *

- nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p <Port List> <Target IP>
- nmap -Pn -sU -p 44818 --script enip-info <Target IP> ✓
- nmap -Pn -sT -p 46824 <Target IP>
- nmap -Pn -sT -p 102 --script s7-info <Target IP>

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11

Facebook recently hired Alice as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. Alice decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan? *

- nmap -sn -PO < target IP address >
- nmap -sn -PS < target IP address > ✓
- nmap -sn -PA < target IP address >
- nmap -sn -PP < target IP address >

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12

During a penetration testing assignment, Alice used a set of scanning tools to create a profile of the target organization. She wanted to scan for live hosts, open ports, and services on a target network. Alice used Nmap for network inventory and Hping3 for network security auditing. However, she wanted to spoof IP addresses for anonymity during probing. Which command should Alice use to perform this task? *

- Hping3 -1 10.0.0.25 -ICMP
- Hping3 -2 10.0.0.25 -p 80
- Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
- Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13

While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue? *

- Contact your Internet Service Provider (ISP) for assistance ✓
- Install a newer version of the server software
- Implement IP address whitelisting
- Increase the server's bandwidth

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14

A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. Your server, reinforced with advanced security measures, can handle 'h' packets per second before it starts showing signs of strain. If 'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects 'r' as a composite number and 'h' as a prime number, making attack detection more challenging. Considering 'r = 2010' and different values for 'h', which of the following scenarios would potentially cause the server to falter? *

- (●) **h = 1987** (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness ✓
- ( ) **h = 1999** (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive
- ( ) **h = 1993** (prime): Despite being less than 'r', the server's prime number capacity keeps it barely operational, but the risk of failure is imminent
- ( ) **h = 2003** (prime): The server can manage more packets than the attacker is sending; hence, it stays operational

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15

You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of IoT devices for public utilities like traffic control, water supply, and power grid management. The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation? *

- ( ) Implement regular firmware updates for all IoT devices.
- ( ) Establish strong, unique passwords for each IoT device.
- ( ) Deploy network intrusion detection systems (IDS) across the IoT network.
- (●) Implement IP address whitelisting for all IoT devices. ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

- ICMP Timestamp Ping Scan
- ICMP ECHO Ping Scan
- TCP SYN Ping Scan
- UDP Ping Scan ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17

Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage 'f' SYN packets per second, and the system is designed to handle this number without any performance issues. If 's' exceeds 'f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (2^k), where 'k' represents each additional SYN packet above the 'f' limit. Now, considering 's = 500' and different 'f' values, in which scenario is the server most likely to experience overload and significantly increased response times? *

- **f = 510:** The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system remains stable, and the response time remains unaffected.
- **f = 495:** The server can handle 495 SYN packets per second. The response time drastically rises (2^5 = 32 times the normal), indicating a probable system overload.
- **f = 505:** The server can handle 505 SYN packets per second. In this case, the response time increases, but not as drastically (2^5 = 32 times the normal), and the system might still function, albeit slowly.
- **f = 490:** The server can handle 490 SYN packets per second. With 's' exceeding 'f' by 10, the response time shoots up (2^10 = 1024 times the usual response time), indicating a system overload. ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

18

Alice works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Alice going to perform? *

- Tracert
- Smurf scan
- Ping trace
- ICMP ping sweep ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

19

What type of attack occurs when an attacker forces a router to stop forwarding packets by flooding it with many open connections simultaneously, effectively disabling all the hosts behind the router? *

- Digital attack
- Denial of Service ✓
- Physical attack
- ARP redirect

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20

As a penetration tester for Google, your next step is to initiate a DoS attack on their network. Why would you want to perform a DoS attack on a system you are testing? *

- Show outdated equipment so it can be replaced
- List weak points on their network ✓
- Use attack as a launching point to penetrate deeper into the network
- Demonstrate that no system can be protected against DoS attacks