Exam Report: 5.1.10 Practice Questions

Date: 5/2/2020 5:47:35 pm
Time Spent: 4:34

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

A technician is using a modem to dial a large block of phone numbers in an attempt to locate other systems connected to a modem. Which type of network scan is being used?

- Fingerprinting
- Wardialing
- Stealth
- Ping sweep

Explanation

Wardialing uses a modem. The scan dials a large block of phone numbers and attempts to locate other systems connected to a modem. If the scan gets a response, it accepts the connection. Modems are still often used for fax machines, multi-purpose copiers, and as a backup for high-speed internet.

A ping sweep is used to scan a range of IPs to look for live systems. Ping sweeps help to build a network inventory, but can also alert the security system, which could result in an alarm being triggered or your attempts being blocked.

A stealth scan, also known as a half-open scan, sends a SYN packet to a port. The three-way handshake does not occur because the original system does not reply with the final ACK. At this point, you have discovered an open port, but because an ACK packet was not sent, a connection was not actually made, and there is no security log.

Fingerprinting relies on small differences in packets created by various operating systems. Differences can be noticed by examining the TTL values, TCP window size, DHCP requests, ICMP requests, HTTP packets, and open port patterns.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_NETWORK_SCAN_01_EH1]

Question 2: Incorrect

A ping sweep is used to scan a range of IP addresses to look for live systems. A ping sweep can also alert a security system, which could result in an alarm being triggered or an attempt being blocked. Which type of scan is being used?

- ~~Port scan~~
- Network scan
- Decoy scan
- Vulnerability scan

Explanation

A network scan is designed to locate all the live hosts on a network. This type of scan will identify the systems that may be attacked later or those that may be scanned a little more closely.

A vulnerability scan is used to find system weaknesses, such as open ports, access points, and other potential threats. This type of scan is quite commonly done as a proactive measure, with the goal of catching problems internally before an attacker is able to locate those same vulnerabilities and act on them.

A decoy scan works by sending more than on packet per port. All of these packets carry spoofed source IP addresses except on packets that carry the original scanner IP address.

A port scan is the process of sending carefully crafted messages or packets to a target computer with the intent of learning more about it.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_NETWORK_SCAN_02_EH1]

Question 3: Incorrect

Randy is an ethical hacker student. He has learned how nmap flag manipulation can help find open ports. Although the name of the operating system did not jump right out at him, he might be able to figure it out by reviewing packet information. In a packet, Randy can see a TTL of 255 and a window size of 4128. What type of scanning process is Randy using?

- Fingerprinting
- ~~Ping sweep~~
- Wardialing
- Beyond Trust

Explanation

You may be able to figure out which operating system a target is running by reviewing packet information. Fingerprinting relies on small differences in packets created by various operating systems. Differences can be noticed by examining the TTL values, TCP window size, DHCP requests, ICMP requests, HTTP packets, and open port patterns.

Wardialing uses a modem. The scan dials a large block of phone numbers and attempts to locate other systems connected to a modem. If the scan gets a response, it accepts the connection. Modems are still often used for fax machines, multi-purpose copiers, and as a backup for high-speed internet.

A ping sweep is used to scan a range of IPs looking for live systems. Ping sweeps help to build a network inventory, but can also alert the security system, which could result in an alarm being triggered or your attempts being blocked.

Beyond Trust provides a network security scanner that helps to identify vulnerabilities and prioritize solutions. This software is available as a standalone application or as part of their larger vulnerability management solution.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_OP_SYS_FINGERPRINT_01_EH1]

Question 4: Incorrect

Which of the following scans is used to actively engage a target in an attempt to gather information about it?

- TCP scan
- ~~Vulnerability scan~~
- Network scan
- Port scan

Explanation

A port scan is the process of sending carefully crafted messages or packets to a target computer with the intent of learning more about it using a tool such as nmap.

A network scan is designed to locate all the live hosts on a network. This type of scan will identify systems that may be attacked later or systems that should be scanned a little more closely.

A vulnerability scan is used to find system weaknesses, such as open ports, access points, and other potential threats. This type of scan is quite commonly done as a proactive measure, with the goal of catching problems internally before an attacker is able to locate those same vulnerabilities and act on them.

A decoy scan works by sending more than one packet per port. All of these packets carry spoofed source IP addresses except one packet, which carries the original scanner IP address.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_PORT_SCAN_01_EH1]

Question 5: Correct

A hacker finds a target machine but wants to avoid getting caught, so the hacker finds another system to take the blame. This system is frequently called a zombie machine because it's disposable and creates a good distraction. Which of the following port scans is being used?

- Idle scan
- Full open scan
- NULL scan
- Xmas tree scan

Explanation

With an idle scan, the hacker finds a target machine but wants to avoid getting caught, so he finds another system to take the blame. This system is frequently called a zombie machine because it's disposable and creates a good distraction for the hacker. The scan directs all requests through the zombie machine. If that zombie machine is flagged, the hacker simply creates another zombie machine and continues with his work.

The full open scan completes a full two-way handshake on all ports. Open ports respond with a SYN/ACK, and closed ports respond with an RST flag, which ends the attempt. The down side of this type of scan (and reason that it's not frequently used) is that somebody now knows you were there.

An Xmas tree scan gets its name because all of the flags are turned on, and the packet is lit up like a Christmas tree. The recipient has no idea what to do with this packet, so either the packet is ignored or dropped. If you get an RST packet, you know the port is closed. If you don't get a response, the port may be open.

A NULL scan sends the packets with no flags set. If the port is open, there will be no response. If the ports are closed, an RST response will be returned.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_PORT_SCAN_02_EH1]

Question 6: Incorrect

Alex, a security specialist, is using an Xmas tree scan. Which of the following TCP flags will be sent back if the port is closed?

- ~~FIN~~
- URG
- RST
- ACK

Explanation

An Xmas tree scan gets its name because all of the flags are turned on, and the packet is lit up like a Christmas tree. The recipient has no idea what to do with this packet, so either the packet is ignored or dropped. If you get an RST flag, you know the port is closed. If you don't get a response, the port may be open.

An ACK would be received if the port was open and acknowledged the receipt of the packet.

A FIN indicates that no additional information will be sent. A closed port would not return a FIN.

AN URG flags a packet as urgent and is not returned by closed ports.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_PORT_SCAN_03_EH1]

Question 7: Incorrect

Which of the following flags is used by a TCP scan to direct the sending system to send buffered data?

- FIN
- PSH
- ~~SYN~~
- URG

Explanation

A TCP scan uses the PSH flag to direct the sending system to send buffered data.

A SYN flag is used to start a connection between hosts.

A FIN indicates that no additional information will be sent. A closed port would not return a FIN.

An URG flags a packet as urgent and is not returned by closed ports.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_TCP_FLAGS_01_EH1]

Question 8: Correct

TCP is a connection-oriented protocol that uses a three-way handshake to establish a connection to a system port. Computer 1 sends a SYN packet to Computer 2. Which packet does Computer 2 send back?

- SYN/ACK
- SYN/RST
- ACK
- RST

Explanation

TCP is a connection-oriented protocol that uses a three-way handshake to establish a connection to a system port. Computer 1 sends a SYN packet to Computer 2. Computer 2 receives the packet and sends a SYN/ACK packet to Computer 1. Computer 1 receives the SYN/ACK packet and replies back with an ACK packet, and the connection is complete.

A SYN flag is used to start a connection between hosts.

An ACK acknowledges the receipt of a packet.

An RST resets a connection.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview

[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_TCP_FLAGS_02_EH1]

Question 9: Correct

What type of scan is used to find system weaknesses such as open ports, access points, and other potential threats?

- Decoy scan
- Network scan
- Port scan
- Vulnerability scan

Explanation

A vulnerability scan is used to find system weaknesses such as open ports, access points, and other potential threats. This type of scan is commonly done as a proactive measure, with the goal of catching problems internally before an attacker is able to locate those same vulnerabilities and act on them.

A network scan is designed to locate all the live hosts on a network. This type of scan will identify the systems that may be attacked later or those that may be scanned a little more closely.

A decoy scan works by sending more than one packet per port. All of these packets carry spoofed source IP addresses except one packet, which carries the original scanner IP address.

A port scan is the process of sending carefully crafted messages or packets to a target computer with the intent of learning more about it.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_PROCESS_VULN_SCAN_01_EH1]

Question 10: Incorrect

You are using an iOS device. You want to scan networks, websites, and ports to find open network devices. Which of the following network mapping tools should you use?

- ~~NetAuditor~~
- Network Topology Manager
- Colasoft
- Scany

Explanation

Scany is a scanner application for iOS devices. It scans networks, websites, and ports to find open network devices. It can obtain domain and network names. It also includes basic networking utilities such as ping, traceroute, and whois.

NetAuditor reports and diagrams network configurations.

Solar Winds Network Topology Manager provides automated network discovery mapping.

Colasoft is a packet crafting software that can be used to modify flags and adjust other packet content.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_TOOLS_NETWORK_MAP_TOOLS_01_EH1]

Question 11: Correct

Which of the following packet crafting software programs can be used to modify flags and adjust other packet content?

- IP Tools

- Currports
- ping
- Colasoft

Explanation

Colasoft is a packet crafting software program that can be used to modify flags and adjust other packet content.

Currports lists all open UDP and TCP ports on your computer. It also provides information about which process opened the port, which user created the process, and what time it was created.

IP Tools includes 20 different scanning utilities, including an SNMP scanner, UDP scanner, Trace, Finger, Telnet, IP-Monitor, and Trap Watcher. The program supports multitasking so that you can use all utilities at once. IP Tools is designed to work on a Windows system.

Ping uses Internet Control Message Protocol (ICMP) messaging to determine if a remote system is live.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_TOOLS_SCAN_TOOLS_01_EH1]

Question 12: Incorrect

You want a list of all open UDP and TCP ports on your computer. You also want to know which process opened the port, which user created the process, and what time is was created. Which of the following scanning tools should you use?

- Currports
- ~~Angry IP scanner~~
- Hping3
- IP tools

Explanation

Currports lists all open UDP and TCP ports on your computer. It also provides information about which process opened the port, which user created the process, and what time it was created.

Angry IP Scanner is a network scanner. It scans local and remote networks and returns IP ranges via a command line interface.

IP Tools includes 20 different scanning utilities, including an SNMP scanner, UDP scanner, Trace, Finger, Telnet, IP-Monitor, and Trap Watcher. The program supports multitasking so that you can use all utilities at once. IP Tools is designed to work on a Windows system.

Hping3 can create custom packets that can be used to analyze the host. In addition to the normal ICMP pings, Hping3 supports TCP, UDP, has a traceroute mode, and can send and receive files. This tool was primarily designed for the Linux operating system, but does have cross-platform capabilities.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_TOOLS_SCAN_TOOLS_02_EH1]

Question 13: Incorrect

Which of the following best describes the scan with ACK evasion method?

- Helps determine whether the firewall is stateful or stateless and whether or not the ports are open.
- Filters incoming and outgoing traffic, provides you with anonymity, and shields you from possible detection.
- Returns feedback to the fake IP address and ensures there is no record of the IP address sending the requests.

- ~~Sends packets and breaks them apart so intrusion detection systems don't know what they are.~~

Explanation

The Scan with ACK method helps you determine whether the firewall is stateful or stateless and whether or not the ports are open. In an ACK scan, the ACK flag is set. If a port is unfiltered, both open and closed ports return an RST packet. If the port is filtered, it returns either an error message or no response at all.

Fragment packets are probably one of the most commonly used methods for avoiding detection. You are still sending packets; you are just breaking them apart so intrusion detection systems don't know what they are. As long as you're not bombarding the system, the packet segments float by without concern.

Many scanning tools have the functionality to recraft the packet so that the source address reflects a different IP address. The scan is sent to the recipient, the feedback is returned to the fake IP address, and then there is no record of your IP address sending the requests.

A proxy serves as a less vulnerable access point to a network. Typically, proxies are placed in networks to keep external users from accessing the internal network. The proxy filters incoming and outgoing traffic, provides hackers with anonymity, and shields them from detection.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_CONSIDERATIONS_EVASION_01_EH1]

Question 14: Incorrect

Which of the following is a benefit of using a proxy when you find that your scanning attempts are being blocked?

- This scan will help you to determine whether the firewall is stateful or stateless and whether or not the ports are open.
- As long as you are not bombarding the system, the packet segments float by without concern.
- It filters incoming and outgoing traffic, provides you with anonymity, and shields you from detection.
- ~~The scan is sent to the recipient, the feedback is returned to the fake IP address, and then there is no record of your IP address sending the requests.~~

Explanation

A proxy serves as a less vulnerable access point to a network. Typically, proxies are placed in networks to keep external users from accessing the internal network. Proxies filter incoming and outgoing traffic, provide hackers with anonymity, and shield them from detection.

Many scanning tools have the functionality to recraft packets so that the source address reflects a different IP address. The scan is sent to the recipient, the feedback is returned to the fake IP address, and then there is no record of your IP address sending the requests.

A Scan with ACK helps you determine whether a firewall is stateful or stateless and whether or not ports are open. In an ACK scan, only the ACK flag is set. If a port is unfiltered, both open and closed ports return an RST packet. If the port is filtered, it returns either an error message or no response at all.

Fragment packets are probably one of the most commonly used methods for avoiding detection. You are still sending packets; you are just breaking them apart so intrusion detection systems don't know what they are. As long as you don't bombard the system, the packet segments float by without concern.

References

TestOut Ethical Hacker Pro - 5.1 Scanning Overview
[e_scanning_eh1.exam.xml Q_SCAN_CONSIDERATIONS_EVASION_02_EH1]