

Exam Report: 11.2.13 Practice Questions

Date: 5/11/2020 11:47:59 am
Time Spent: 6:39

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following is the process of determining the configuration of ACLs by sending a firewall TCP and UDP packets?

- ☐ Port scanning
- ☐ Banner grabbing
- ☐ Packet filtering

➡ ☒ Firewalking

Explanation

Firewalking is the process of probing a firewall to determine the configuration of ACLs.

Banner grabbing is a simple method that helps identify the firewall's vendor and software version.

Port scanning is used to identify open ports and the services running on them.

Packet filtering firewalls are the simplest and earliest type of firewall. Packet filtering firewalls look at packets' header information to determine legitimate traffic.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls
[e_firewall_eh1.exam.xml Q_FIREWALL_IDENTIFICATION_01_EH1]

▼ Question 2: Incorrect

Which of the following firewall limitations is a critical vulnerability because it means that packet filters cannot tell whether a connection was started inside or outside the organization?

- ➡ ☐ Inability to detect the keep the state status.
- ☒ Inability to protect from internal attacks.
- ☐ Inability to prevent spoofing.
- ☐ Inability to inspect the packet's payload.

Explanation

A packet filtering firewall does not detect or keep the connection state. This inability to keep up with the state status is a critical vulnerability because it means that packet filters cannot tell whether a connection was started inside or outside the organization.

Firewalls can filter by IP addresses but cannot prevent spoofing.

Firewalls can block specific ports and protocols but cannot inspect the packet's payload.

A firewall is unable to protect a system from internal attacks or backdoors.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALL_LIMITATIONS_01_EH1]

▼ Question 3: Incorrect

Which of the following firewall technologies operates at Layers 3 (Network) and 4 (Transport) of the OSI model?

☐ VPN

➡ ☐ Packet filtering

☐ Circuit level gateway

☒ Application level

Explanation

Packet filtering firewalls look at the header information of the packets to determine legitimate traffic. This technology operates at Layers 3 (Network) and 4 (Transport) of the OSI model.

Circuit level gateways are a more complex form of firewall that operates at Level 5 (Session) of the OSI model.

Application level firewalls, also known as application gateways or proxies, can also filter application-specific commands and can be configured as a web proxy. This firewall can tend to be slower because of deep packet inspection at Layer 7 (Application).

A Virtual Private Network (VPN) is a network that provides secure access to a private network through the public network or Internet.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALL_TECHNOLOGY_01_EH1]

▼ Question 4: Correct

Which of the following best describes a proxy server?

☐ Operates at Layers 3 (Network) and 4 (Transport) of the OSI model.

☐ Operates at Level 5 (Session) of the OSI model.

☐ Operates at Layers 5 (Session) and 7 (Application) of the OSI model.

➡ ☒ Operates at Layer 7 (Application) of the OSI model.

Explanation

Proxy servers act as a proxy for internal hosts when connecting to the internet. Proxy servers can also:

- Prevent client systems from communicating directly with an outside source. This reduces exposure and risk.
- Filter traffic by content. This means proxy servers can operate at Layer 7 (the Application layer) of the OSI.
- Speed up browsing by caching frequently visited sites and resources.

Packet filtering technology operates at Layers 3 (Network layer) and 4 (Transport layer) of the OSI model.

Circuit-level gateways are a more complex form of firewall. Circuit-level gateways operate at Level 5 (Session layer) of the OSI model.


References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALL_TECHNOLOGY_02_EH1]

Question 5: Correct

Which of the following best describes a stateful inspection?

- ☐ Designed to sit between a host and a web server and communicate with the server on behalf of the host.
-  ☒ Determines the legitimacy of traffic based on the state of the connection from which the traffic originated.
- ☐ Offers secure connectivity between many entities and uses encryption to provide an effective defense against sniffing.
- ☐ Allows all internal traffic to share a single public IP when connecting to an outside entity.

Explanation

Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated. The stateful firewall maintains a state table that tracks the ongoing record of active connections.

A Virtual Private Network (VPN) is a network that provides secure access to a private network through the public network or Internet. Virtual private networks offer secure connectivity between many entities, both internally and remotely. Their use of encryption provides an effective defense against sniffing.

Network address translation (NAT) separates IP addresses into two sets. This technology allows all internal traffic to share a single public IP when connecting to an outside entity.

A firewall can be implemented on Circuit level gateways or Application level gateways. Both of these firewall designs sit between a host and a web server and communicate with the server on behalf of the host. They can also be used to cache frequently accessed websites for faster web page loading.


References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALL_TECHNOLOGY_03_EH1]

Question 6: Incorrect

Jessica needs to set up a firewall to protect her internal network from the Internet. Which of the following would be the best type of firewall for her to use?

-  ☐ Hardware
- ☐ Software
- ☒ Tunneling
- ☐ Stateful

Explanation

Hardware firewalls are physical devices that are usually placed at the junction or gateway between two networks, generally a private network and a public network such as the internet. Hardware firewalls can be a standalone product or also built into devices like broadband routers.

Software firewalls are generally used to protect individual hosts.

Tunneling is when an attacker wraps a malicious command in an HTTP, ICMP, or ACK tunneling packet that bypasses the firewall and reaches an internal system.

Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALL_TYPE_01_EH1]

Question 7: Incorrect

You are working on firewall evasion countermeasures and are specifically looking for a tool to expose TTL vulnerabilities. Which of the following tools would you use?

- ☒ Tunneling
- ☐ Traffic IQ Professional
- ☐ KFSensor

➡ ☐ Firewalking

Explanation

Firewalking is the process of probing a firewall to determine the configuration of ACLs by sending it TCP and UDP packets.

Traffic IQ Professional enables security professionals to audit and validate security devices' behavior.

Tunneling is when an attacker wraps a malicious command in an HTTP, ICMP, or ACK tunneling packet that bypasses the firewall and reaches an internal system.

KFSensor is a Windows host-based intrusion detection system.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_EVADE_FIREWALLS_COUNTERMEASURE_01_EH1]

▼ Question 8: Incorrect

Which of the following best describes source routing?

- ☐ The packet's sender investigates the route that a packet takes through the network.
- ➡ ☐ The packet's sender designates the route that a packet should take through the network.
- ☒ The packet's sender has no control over the route that a packet takes through the network.
- ☐ The packet's sender eliminates the route that a packet should take through the network.

Explanation

In source routing, packet's sender designates the route that a packet should take through the network. The purpose is to specify a route that bypasses the firewall. Using this technique, the attacker attempts to evade the firewall restrictions.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_EVADE_FIREWALLS_EVASION_TECH_01_EH1]

▼ Question 9: Incorrect

Nmap provides many commands and scripts that are used to evade firewalls and intrusion detection systems. Which of the following is the proper nmap command to use the decoy option?

- ☐ **nmap -f 10.10.10.1**
- ☐ **nmap -P0 -sI 1.1.1.1:1234 10.10.10.1**
- ➡ ☐ **nmap -D RND:25 10.10.10.1**
- ☒ ~~**nmap -sA 10.10.10.1**~~

Explanation

Nmap has a decoy option. Use the -D parameter to perform the scan. With -D option, it appears to the remote host that the host(s) you specify as decoys are scanning the target network, too. In the example,

the host, 10.10.10.1, will see 25 port scans, and the remote host, or IDS, has no way of telling which one was real.

The **nmap** TCP ACK Scan (-sA) sends an ACK packet to discover open ports and to determine filtered and unfiltered responses. Firewalls treat ACK packet as the response of the SYN packets; therefore, ACK packets do not create logs.

Use **nmap** to hide your IP address with the -P0 -sI command. The example uses an idle scan technique. It uses port 1234 on 1.1.1.1 IP as a zombie to scan host, 10.10.10.1.

The **nmap -f** parameter splits the request into small segments of IP packets. Fragmentation is useful for evading the firewall.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_EVADE_FIREWALLS_EVASION_TOOL_01_EH1]

▼ Question 10: Incorrect

Which of the following tools enables security professionals to audit and validate the behavior of security devices?

- ➡ ☐ Traffic IQ Professional
- ☐ MTU offset
- ☐ TCP ACK Scan
- ☒ Fragment Packets

Explanation

An example of a dedicated evasion defense tool is Traffic IQ Professional, which enables security professionals to audit and validate the behavior of security devices. They do this by generating the standard application traffic or attack traffic between two virtual machines. This tool can be used to assess, audit, and test the behavioral characteristics of any non-proxy packet filtering device, including Application-layer firewalls, intrusion detection and prevention systems, and routers and switches.

TCP ACK Scan sends an ACK packet to discover open ports and to determine filtered and unfiltered responses. Firewalls treat ACK packets as the response of the SYN packets; therefore, ACK packets do not create logs.

MTU offset lets you specify your own packet offset size with the --mtu option. The offset must be a multiple of eight.

To see if the target machine does not have the capabilities to handle small fragmented packets, fragmentation is useful for evading the firewall. The -f parameter splits the request into small segments of IP packets.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_EVADE_FIREWALLS_EVASION_TOOL_02_EH1]

▼ Question 11: Correct

Firewalls, whether hardware or software, are only as effective as their _____?

- ☐ Organization
- ☐ Footprint
- ☐ Location
- ➡ ☒ Configuration

Explanation

Firewalls, whether hardware or software, are only as effective as their configuration; configurations are only as effective as the administrators creating them.

Firewall penetration testing should ensure that the firewall security configuration aligns with the organization's security practices and policies.

Firewalls can be placed anywhere on a network but are most commonly located between the external and internal network. They can also be set up between internal networks.

Footprinting is done by running a port scan on the system and accessing banners. This allows the penetration tester to determine the type of firewall used.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALLPENTEST_FACT_01_EH1]

▼ Question 12: Incorrect

Lorena, the CIO, wants to ensure that the company's security practices and policies match well with their firewall security configuration for maximum protection against hacking. Which of the following actions should Lorena take?

- ☒ ~~Implement new security practices and policies.~~
- ☐ Do nothing. The company's data is safe.
- ➡ ☐ Hire a penetration tester.
- ☐ Purchase a different firewall.

Explanation

At the organizational level, firewall penetration testing should ensure that the firewall security configuration aligns with the organization's security practices and policies. Firewalls, whether hardware or software, are only as effective as their configuration. Testing is required to ensure the appropriate rules have been implemented and that those rules operate as intended.

The penetration tester begins by evaluating the organization's security policies, creating threat models, and conducting a risk assessment to further define the systems and resources that should be tested. Then the penetration tester chooses the methods used for the firewall penetration test. Having a strong understanding of the exploits used by attackers and the techniques attackers use to avoid detection is one of the best penetration test practices.

New security practices and policies would be implemented after the penetration test has been completed and based on the recommendations of the penetration tester.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALLPENTEST_FACT_02_EH1]

▼ Question 13: Incorrect

Jin, a penetration tester, was hired to perform a black box penetration test. He decides to test their firewall. Which of the following techniques should he use first?

- ☐ Firewalking
- ☒ ~~DoS attack~~
- ☐ Hoaxing
- ➡ ☐ Footprinting

Explanation

The first technique the penetration tester should use is footprinting. Footprinting is done by running a port scan on the system and accessing banners. This allows the penetration tester to determine the type of firewall used.

Firewalking is an active reconnaissance technique that attempts to determine which Layer 4 (Transport) protocols a specific firewall will allow through.

A hoax is a type of malicious email with some type of urgent or alarming message that deceives the target.

A Denial of Service (DoS) attack is intended to overwhelm a system so that it is inaccessible. DoS attacks are executed by flooding the cloud infrastructure, such as CPU and memory, with so many malicious requests that the server stops processing legitimate requests and users are unable to gain access.


References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALLPENTEST_FACT_03_EH1]

▼ Question 14: Correct

IP address spoofing, fragmentation attacks, using proxy servers, ICMP tunneling, and ACK tunneling are all examples of which of the following firewall penetration testing techniques?

- ☐ Footprinting
- ☐ Banner grabbing
-  ☒ TCP packet filtering
- ☐ Firewalking

Explanation

When using the TCP packet filtering testing technique, the penetration tester can accomplish the following by modifying the TCP packet:

- Spoof the IP address to gain unauthorized access.
- Use fragmentation attacks to force the TCP header information into the next fragment. This allows the penetration tester to bypass the firewall.
- Use proxy servers that block the actual IP address and display another. This allows access to a blocked website or target device.
- Use ICMP tunneling to tunnel a backdoor application in the data portion of ICMP Echo packets.
- Perform ACK tunneling using tools such as AckCmd to tunnel a backdoor application using TCP packets with the ACK bit set.

Footprinting requires running a port scan on the system and accessing banners. This allows the penetration tester to determine the type of firewall being used.

Firewalking is an active reconnaissance technique that attempts to determine which Layer 4 (Transport layer) protocols a specific firewall will allow through.

Banner grabbing is a basic method for retrieving announcements provided by services in response to connection requests. The three main services that send out banners are FTP, Telnet, and web and email servers.

References

TestOut Ethical Hacker Pro - 11.2 Firewalls

[e_firewall_eh1.exam.xml Q_FIREWALLPENTEST_FACT_04_EH1]