

Exam Report: 5.2.9 Practice Questions

Date: 1/20/2020 4:59:56 pm
Time Spent: 15:13

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 87%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following is the best countermeasure against man-in-the-middle attacks?

- ☐ MIME email
- ☐ PPP
- ➡ ☒ IPsec
- ☐ UDP

Explanation

IPsec is the best countermeasure against man-in-the middle attacks from the selections listed here. Use IPsec to encrypt data in a VPN tunnel as it passes between two communication partners. Even if someone intercepts the traffic, they will be unable to extract the contents of the messages because they are encrypted.

All email is MIME email, so this is not a countermeasure against man-in-the middle attacks.

References

LabSim for Security Pro, Section 5.2.
[All Questions SecPro2017_v6.exm SPOOF_POISON_01]

▼ Question 2: Correct

What is modified in the most common form of spoofing on a typical IP packet?

- ☐ Destination address
- ☐ Hash total
- ➡ ☒ Source address
- ☐ Protocol type field value

Explanation

The most common form of spoofing on a typical IP packet is modification of the source address. In this way, the correct source device address is hidden.

Modifications of the destination address would be pointless because the packets would not be sent to the intended victim or target. Modification of the protocol type field value is not typical, but doing so would cause the recipient to process the contents of the packet under different protocol rules than what the actual contents should be processed under, such as processing the packet as a UDP packet when it is actually an IGMP packet. Modification of the hash total would cause the packet to be dropped when it reached its destination because the target's computation of the hash would not match the stated hash in the header. This indicates that packet's integrity was compromised.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_02]

▼ Question 3: Correct

Which type of activity changes or falsifies information in order to mislead or re-direct traffic?

- ☐ Sniffing
- ☐ Spamming
- ➡ ☒ Spoofing
- ☐ Snooping

Explanation

Spoofing changes or falsifies information in order to mislead or re-direct traffic.

Snooping is the act of spying into private information or communications. One type of snooping is *sniffing*. Sniffing captures network packets to examine the contents of communications. *Spamming* is sending a victim unwanted and unrequested email messages.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_03]

▼ Question 4: Correct

Which of the following describes a man-in-the-middle attack?

- ☐ Malicious code is planted on a system, where it waits for a triggering event before activating.
- ☐ A person convinces an employee to reveal their login credentials over the phone .
- ➡ ☒ A false server intercepts communications from a client by impersonating the intended server.
- ☐ An IP packet is constructed that is larger than the valid size.

Explanation

A false server intercepting communications from a client by impersonating the intended server is a form of a man-in-the-middle attack.

Convincing an employee to reveal his login credentials over the phone is an example of a social engineering attack. Constructing an IP packet that is larger than the valid size is a land attack (a form of DoS). Planting malicious code that waits for a triggering event before activating is a logic bomb.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_06]

▼ Question 5: Correct

Capturing packets as they travel from one host to another with the intent of altering the contents of the packets is a form of which attack type?

- ☐ Spamming
- ➡ ☒ Man-in-the-middle attack
- ☐ Passive logging
- ☐ DDoS

Explanation

Capturing packets between two existing communication partners is a form of a man-in-the middle attack. As this attacks type's name implies, traffic is intercepted somewhere in the middle of the communicating

partners. The best way to protect against man-in-the middle attacks is to use session encryption or line encryption solutions.

Passive logging is a means of recording information about network traffic or operations in a system without affecting either in any way.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_07]

▼ Question 6: Correct

When the TCP/IP session state is manipulated so that a third party is able to insert alternate packets into the communication stream, what type of attack has occurred?

- ☐ Masquerading
- ☐ Replay
-  ☒ Hijacking
- ☐ Spamming

Explanation

A *hijacking* attack is one where the TCP/IP session state is manipulated so that a third party is able to insert alternate packets into the communication stream. Session hijacking has become difficult to accomplish due to the use of time stamps and randomized packet sequencing rules employed by modern operating systems.


References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_08]

▼ Question 7: Correct

What is the goal of a TCP/IP hijacking attack?

- ☐ Destroying data.
- ☐ Preventing legitimate authorized access to a resource.
-  ☒ Executing commands or accessing resources on a system the attacker does not otherwise have authorization to access.
- ☐ Establishing an encryption tunnel between two remote systems over an otherwise secured network.

Explanation

The goal of a TCP/IP hijacking attack is to execute commands or access resources on a system the attacker does not otherwise have authorization to access. When an attacker successfully performs TCP/IP hijacking, they take over control of the hijacked communication session. Whatever access the original user had, the attacker can now exploit. However, the attack only grants access within the confines of the hijacked session. Just because a hacker gains the victim's access to a server, it does not automatically grant the attacker the victim's access to a different server.

A virus's goal is often to destroy data. A denial of service attack's goal is often to prevent legitimate access to a resource. An internal VPN's goal is often to establish an encryption tunnel between two remote systems over an otherwise secured network.

References


LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_09]

▼ Question 8: Correct

Which of the following is **not** a protection against session hijacking?



-  ☒ DHCP
- ☐ reservations
- ☐ Time stamps
- ☐ Packet sequencing
- ☐ Anti-IP spoofing

Explanation

DHCP reservations are not a protection against session hijacking. If a valid MAC address can be discovered, then an IP address is handed out freely to the spoofed client by the DHCP server.

Packet sequencing and time stamps prevent session hijacking by disallowing packets that are out of order or have expired. Anti-IP spoofing checks the identity of the host before allowing communication to occur, even if the IP address is known.


References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_10]

▼ Question 9: Correct

Which of the following is the most effective protection against IP packet spoofing on a private network?

- ☐ Antivirus scanners
- ☐ Digital signatures
-  ☒ Ingress and egress filters
- ☐ Host-based IDS

Explanation

Ingress and egress filters are the most effective protection against IP packet spoofing. Ingress filters examine packets coming into the network, while egress filters examine packets going out of the network. These filters examine packets based on rules that identify any spoofed packets. Any packet suspected of being spoofed on its way into or out of your network is dropped.

Antivirus scanners are useful against viruses. Host-based IDSs are good at detecting host intrusions and security violations. Digital signatures are used to provide a recipient with proof of non-repudiation and integrity of communications.

References


LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_11]

▼ Question 10: Incorrect

While using the internet, you type the URL of one of your favorite sites in the browser. Instead of going to the correct site, however, the browser displays a completely different website. When you use the IP address of the web server, the correct site is displayed.

Which type of attack has likely occurred?

- ☐ Hijacking
- ☒ Spoofing
-  ☐ DNS poisoning
- ☐ Man-in-the-middle

Explanation

Because the correct site shows when you use the IP address, you know that the main website is still functional and that the problem is likely caused by an incorrect domain name mapping. *DNS poisoning*

occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. DNS spoofing is an attack to the cache of a primary DNS server.

- The incorrect mapping is made available to client applications through the resolver.

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks use modified source and/or destination addresses in packets, and can include site spoofing that tricks users into revealing information. A *man-in-the-middle* attack is used to intercept information passing between two communication partners. TCP/IP hijacking is an extension of a man-in-the-middle attack where the attacker steals an open and active communication session from a legitimate user. With spoofing, man-in-the-middle, and hijacking, the attack would be successful regardless of whether the DNS name or the IP address were used.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_12]

▼ Question 11: Correct

Which of the following attacks tries to associate an incorrect MAC address with a known IP address?

- ☐ Null session
- ☐ Hijacking
- ☐ MAC flooding

➡ ☒ ARP poisoning

Explanation

ARP spoofing/poisoning associates the attacker's MAC address with the IP address of victim devices. When computers send an ARP request to get the MAC address of a known IP address, the attacker's system responds with its MAC address.

MAC flooding overloads the switch's MAC forwarding table to make the switch function like a hub. The attacker floods the switch with packets, each containing different source MAC addresses. The flood of packets fills up the forwarding table and consumes so much of the memory in the switch that it causes the switch to enter a state called *failopen mode*, in which all incoming packets are broadcast out all ports (as with a hub), instead of just to the correct ports.

A null session is the ability to log on using a blank user name and password. With *hijacking*, an attacker steals an open session, inserting himself into the session in place of the original client.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_13]

▼ Question 12: Incorrect

What are the most common network traffic packets captured and used in a replay attack?

- ➡ ☐ Authentication
- ☐ Session termination
- ☐ File transfer
- ☒ DNS query

Explanation

Authentication traffic is the most commonly captured type of network traffic packets in replay attacks. If someone is able to replay the stream of authentication packets successfully, they can gain the same access to the system or network as the original user. Fortunately, many authentication security systems include time stamps or dynamic challenge response mechanisms to prevent authentication packets from being replayed.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_14]

▼ Question 13: Correct

When a malicious user captures authentication traffic and replays it against the network later, what is the security problem you are most concerned about?

- ➡ ☒ An unauthorized user gaining access to sensitive resources
- ☐ Denial of service
- ☐ Bandwidth consumption
- ☐ Spam

Explanation

When a malicious user captures authentication traffic and replays it against the network later, the security problem you are most concerned about is an unauthorized user gaining access to sensitive resources. Once a replay attack has been successful, the attacker has the same access to the system as the user from whom the authentication traffic was captured.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_15]

▼ Question 14: Correct

A router on the border of your network detects a packet with a source address that is from an internal client, but the packet was received on the internet-facing interface. This is an example of what form of attack?

- ☐ Spamming
- ➡ ☒ Spoofing
- ☐ Sniffing
- ☐ Snooping

Explanation

This is an example of *spoofing*. Spoofing is the act of changing or falsifying information in order to mislead or re-direct traffic. In this scenario, a packet received on the inbound interface cannot receive a valid packet with a stated source that is from the internal network.

Snooping is the act of spying into private information or communications. One type of snooping is *sniffing*. Sniffing is the act of capturing network packets in order to examine the contents of communications. *Spamming* is sending a victim unwanted and unrequested email messages.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_16]

▼ Question 15: Correct

An attacker uses an exploit to push a modified hosts file to client systems. This hosts file redirects traffic from legitimate tax preparation sites to malicious sites to gather personal and financial information.

What kind of exploit has been used in this scenario? (Choose two. Both responses are different names for the same exploit.)

- ☐ Man-in-the-middle
- ☐ Domain name kiting
- ➡ ☒ DNS poisoning

☐ Reconnaissance☒  Pharming

Explanation

DNS poisoning (also known as *DNS cache poisoning*) occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack:

- Incorrect DNS data is introduced into the cache of a primary DNS server.
- The incorrect mapping is made available to client applications.

Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted by changing the hosts file on a victim's computer.

Reconnaissance is used to gather information for an attack. The goal is to obtain DNS records that identify computer names and IP addresses in a network. Domain name kiting occurs when spammers exploit domain registration by taking advantage of the five-day grace period for a newly registered domain name to acquire domains and never pay for the registration of domain names. They accomplish this by unregistering a domain name just before the grace period is up and then immediately re-registering the domain name. Man-in-the-middle attacks are used to intercept information passing between two communication partners.

References

LabSim for Security Pro, Section 5.2.

[All Questions SecPro2017_v6.exm SPOOF_POISON_17]