Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/13/2022 7:45:24 pm • Time spent: 01:56

Score: 90%

Passing Score: 80%

Question 1: ✓ Correct

Which of the following is the term used to describe what happens when an attacker sends falsified messages to link their MAC address with the IP address of a legitimate computer or server on a network?

- ➡ ● ARP poisoning
- ○ Port mirroring
- ○ MAC flooding
- ○ MAC spoofing

EXPLANATION

Address Resolution Protocol (ARP) poisoning is when an attacker sends fake ARP messages to link their MAC address with the IP address of a legitimate computer or server on the network. Once their MAC address is linked to an authentic IP address, the attacker can receive any messages directed to the legitimate address. As a result, the attacker can intercept, modify, or block communications to the legitimate MAC address.

Port mirroring creates a duplicate of all network traffic on a port and sends it to another device.

MAC flooding is when an attacker intentionally floods a content-addressable memory table with Ethernet frames, each originating from different MAC addresses. Once the table starts to overflow, the switch responds by broadcasting all incoming data to all ports, basically turning itself into a hub instead of a switch.

MAC spoofing is done to enable the bypass of access control lists on servers or routers by either hiding a computer on a network or by allowing it to impersonate another network device.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_arp_pois_01_secp7.question.fex

▾ Question 2: ✓ Correct

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

○ Null session

○ Hijacking

➡ ● ARP poisoning

○ MAC flooding

EXPLANATION

ARP spoofing/poisoning associates the attacker's MAC address with the IP address of a victim's device. 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 Fail Open mode, in which all incoming packets are broadcast out of 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 username and password. With hijacking, an attacker steals an open session, inserting himself or herself into the session in place of the original client.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_arp_pois_02_secp7.question.fex

▼ Question 3: ✓ Correct

Which type of denial-of-service (DoS) attack occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses?

○ Spam

➡ ◉ DNS poisoning

○ SYN flood

○ ARP poisoning

EXPLANATION

DNS 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 a primary DNS server.
- The incorrect mapping is made available to client applications through the resolver.
- Traffic is directed to incorrect sites.

ARP poisoning corrupts the ARP cache or sends incorrect ARP data that spoofs MAC addresses, causing devices to send frames to the wrong host or an unreachable host.

Spam sent in such great amounts can consume bandwidth or fill a mailbox, leaving no room for legitimate traffic.

A SYN flood exploits the TCP three-way handshake.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_dns_pois_01_secp7.question.fex

▼ Question 4: ✓ Correct

While using the internet, you type the URL of one of your favorite sites in the browser. Instead of going to the correct site, 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?

○ Man-in-the-middle

○ Spoofing

○ Hijacking

➡ ● DNS poisoning

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. 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 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 in which 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

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_dns_pois_02_secp7.question.fex

▼ **Question 5:** ✓ 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.

Which kind of exploit has been used in this scenario?

○ Domain name kiting

➡ ● DNS poisoning

○ Reconnaissance

○ Man-in-the-middle

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.

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

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_dns_pois_03_secp7.question.fex

Question 6: ✓ Correct

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

➡ ● A false server intercepts communications from a client by impersonating the intended server.

○ Malicious code is planted on a system, where it waits for a triggering event before activating.

○ An IP packet is constructed that is larger than the valid size.

○ A person convinces an employee to reveal his or her login credentials over the phone.

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 or her logon 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). Planted malicious code that waits for a triggering event before activating is a logic bomb.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_mtm_01_secp7.question.fex

▼ Question 7: ✓ 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 type of attack?

- ➡ ● Man-in-the-middle attack
- ○ Passive logging
- ○ Spamming
- ○ DDoS

EXPLANATION

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

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_mtm_02_secp7.question.fex

Question 8: ✓ Correct

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

○ Spamming

➡ ◉ Spoofing

○ Snooping

○ Sniffing

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

☰ 11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_spoof_01_secp7.question.fex

▼ Question 9: ✓ 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 which form of attack?

○ Sniffing

➡ ● Spoofing

○ Snooping

○ Spamming

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

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_spoof_02_secp7.question.fex

Question 10: ✕ Incorrect

Which of the following are network-sniffing tools?

- ● ~~WinDump, KFSensor, and Wireshark~~
- ○ Ettercap, Ufasoft snif, and Shark
- ➡ ○ Cain and Abel, Ettercap, and TCPDump
- ○ Ufasoft snif, TCPDump, and Shark

EXPLANATION

Cain and Abel is a collection of tools that includes ARP poisoning. Cain and Abel redirects packets from a target by forging ARP replies.

Ettercap is a sniffing tool with multiple functions that can be used for ARP poisoning, passive sniffing, packet grabbing, and protocol decoding.

TCPDump is a command line sniffer designed for the Linux environment.

Ufasoft snif is a sniffing tool that has capture, analysis, and decryption features.

WinDump is the Windows version of TCPdump.

Wireshark is a network packet analyzer that tries to capture network packets and display the data they carry in as much detail as possible.

Shark is a tool that is used to create botnets.

KFSensor is a Windows host-based intrusion detection system. It acts as a vulnerable server to attract hackers and record their activities.

REFERENCES

11.6.2 Analyzing Network Attacks Facts

q_analyz_netattacks_tcpdump_secp7.question.fex