Exam Report: 10.2.14 Practice Questions

Date: 5/10/2020 11:34:07 am
Time Spent: 1:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 58%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following tasks is being described?

1. Sniff the traffic between the target computer and the server.
2. Monitor traffic with the goal of predicting the packet sequence numbers.
3. Desynchronize the current session.
4. Predict the session ID and take over the session.
5. Inject commands to target the server.

- Session hijacking
- Cookie hijacking
- Passive hijacking
- Application hijacking

Explanation

The steps in the question describe the process used in session hijacking.

Passive hijacking is, essentially, sniffing traffic between the target and the host, and does not complete steps 2-4.

Cookie hijacking is gaining access to a user's session token to gain access to a system or account.

Application hijacking uses cookie hijacking to gain access at the Application level.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_SESSION_HIJACKING_FACT_01_EH1]

Question 2: Correct

Which of the following describes a session ID?

- The source IP address of an encrypted packet sent from a server to a client.
- A unique token that a server assigns for the duration of a client's communications with the server.
- The symmetric key used to encrypt and decrypt communications between a client and a server.
- The destination IP address of an encrypted packet sent from a server to a client.

Explanation

A session ID is a unique token that a server assigns for the duration of a client's communications with the server.

A packets source IP address is the sender's address, not a session

ID.
A packets destination IP address is the receiver's address not a session ID.
A symmetric encryption key used to encrypt and decrypt communications between two computers.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_SESSION_HIJACKING_FACT_02_EH1]

Question 3: Correct

Which of the following is characterized by an attacker using a sniffer to monitor traffic between a victim and a host?

- Active hijacking
- Passive hijacking
- Session key
- Session ID

Explanation

Passive hijacking is when an attacker uses a sniffer to monitor traffic between a victim and a host.

Active hijacking is when an attacker manipulates a client's connection in such a way that ejects the real client and allows the server to think that the attacker is the authenticated user.

A session ID is a unique token that a server assigns for the duration of a client's communications with the server.

A session key is a symmetric encryption key used to encrypt and decrypt communications between two computers.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_SESSION_HIJACKING_FACT_03_EH1]

Question 4: Correct

Jason, an attacker, has manipulated a client's connection to disconnect the real client and allow the server to think that he is the authenticated user. Which of the following describes what he has done?

- Session sniffing
- Active hijacking
- Passive hijacking
- Cross-site scripting

Explanation

Active hijacking is when an attacker manipulates a client's connection to disconnect the real client and allow the server to think that the attacker is the authenticated user.

Passive hijacking is when an attacker uses a sniffer to monitor traffic between a victim and a host.

Session sniffing is basically just an extension of sniffing efforts that we've discussed in the past, except now, we're specifically on the lookout for session IDs.

Cross-site scripting attacks (XSS) involve the injection of malicious Java, Flash, or HTML script into web applications.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_SESSION_HIJACKING_FACT_04_EH1]

Question 5: Incorrect

Which of the following best describes the process of using prediction to gain session tokens in an Application level hijacking attack?

- Review a user's browsing history to enter a previously used URL to gain access to an open session.
- ~~Obtain a user's HTTP cookies to collect session IDs embedded within the file to gain access to a session.~~
- Convince the victim system that you are the server so you can hijack a session and collect sensitive information.
- Collect several session IDs that have been used before and then analyze them to determine a pattern.

Explanation

The easiest way to predict session tokens is to collect several session IDs that have been used before and then analyze them to determine a pattern. Once you know the pattern or algorithm being used, you may be able to predict a future ID.

Convincing the victim system that you are the server is a task associated with UDP session hijacking; this task is not part of using prediction to gain session tokens.

Reviewing a user's browsing history to gain access to previously visited URLs is not a means of using Application level hijacking by predicting session tokens.

HTTP cookies are the most common location to find session IDs. This is not the process of using prediction to determine future session IDs or tokens.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_CLIENT_NETWORK_ATTACKS_APP_LEVEL_01_EH1]

Question 6: Correct

Which term describes the process of sniffing traffic between a user and server, then re-directing the traffic to the attacker's machine, where malicious traffic can be forwarded to either the user or server?

- Man-in-the-middle
- Session hijacking
- Cross-site scripting
- DNS spoofing

Explanation

A man-in-the-middle attack is the process of sniffing traffic between a user and sever and then re-directing the traffic to the attacker's machine, where malicious traffic can be forwarded to either the user or server.

Session hijacking is the process of taking over an established connection between a host and a web server. The session token can be stolen, or a predicted session token can be used.

Cross-site scripting attacks involve the injection of malicious Java, Flash, or HTML script into web applications.

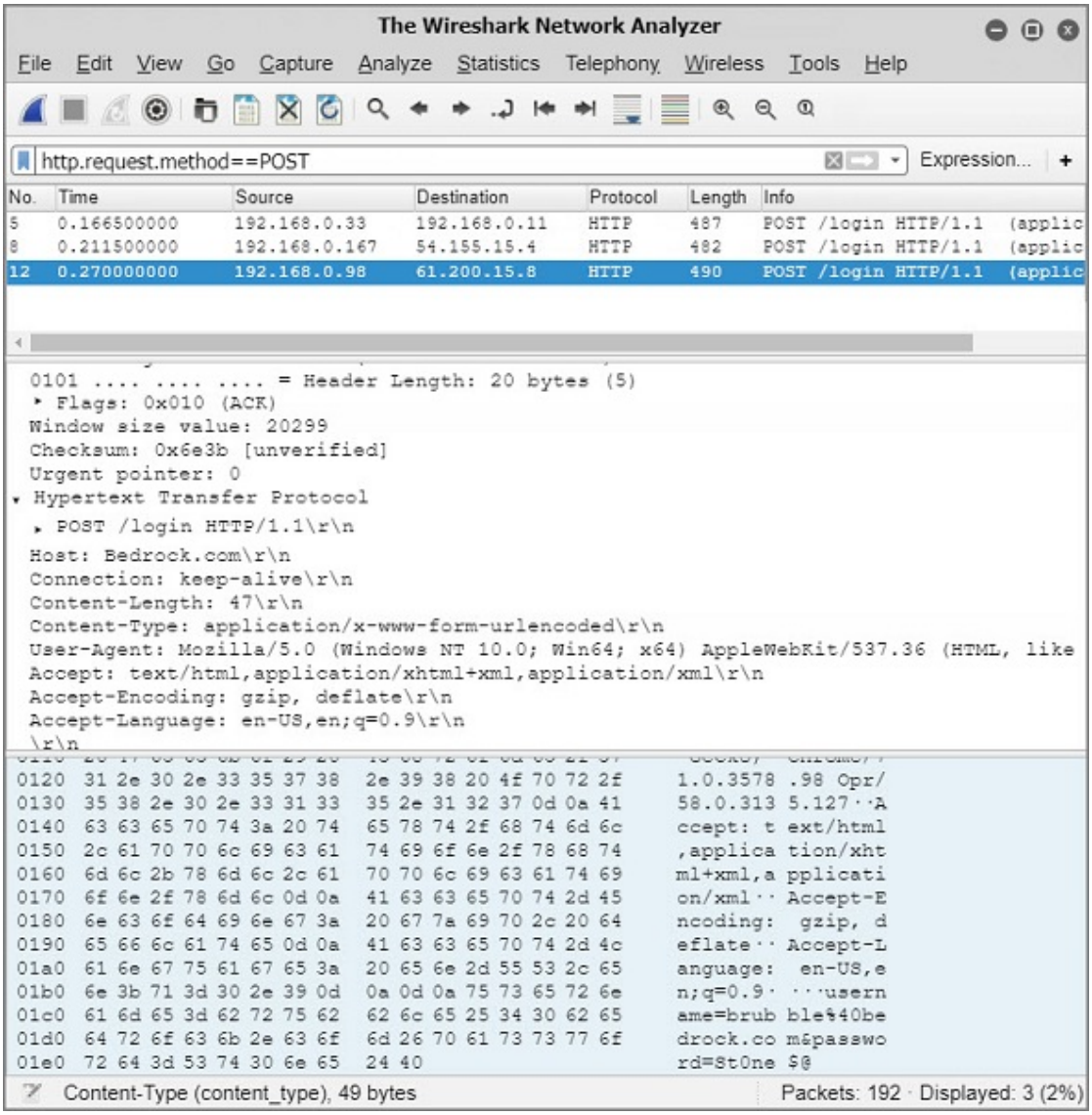
In DNS spoofing, an attacker will alter the DNS server in a way that will redirect traffic to a malicious website that can gather sensitive information about a user or that can install malware onto the target machine.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_CLIENT_NETWORK_ATTACKS_NET_LEVEL_01_EH1]

Question 7: Correct

While performing a penetration test, you captured a few HTTP POST packets using Wireshark. After examining the selected packet, which of the following concerns or recommendations will you include in your report?



- ◯ The checksum is unverified.
- ◯ Keep-alive connections are being used.
- ➡ ◉ Passwords are being sent in clear text.
- ◯ The urgent pointer flag is set to 0.

Explanation

Passwords and usernames are being sent in clear text, which can be captured and used for man-in-the-middle attacks.

An urgent pointer set to 0 simply means that there is no urgent data to process and there is no security threat.

Checksums are used to ensure the integrity of data portions for data transmission or storage. A checksum is basically a calculated summary of such a data portion. The fact that the checksum for this packet is not verified is not a major security threat in and of itself.

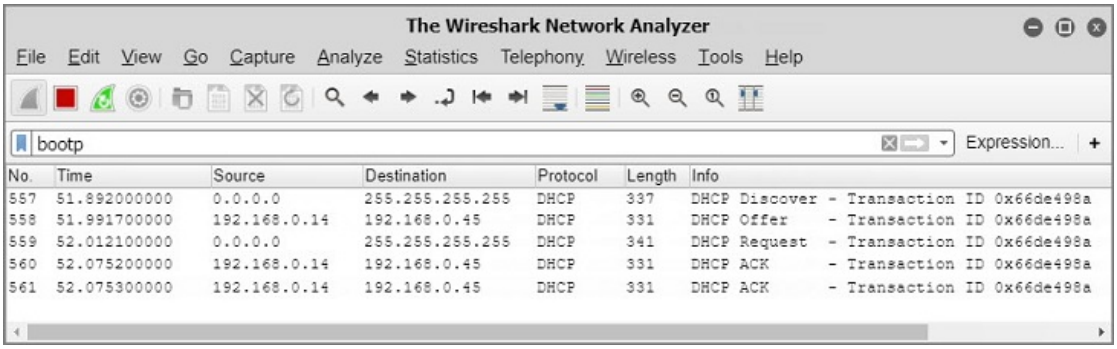
The HTTP keep-alive header maintains a connection between a client and your server, reducing the time needed to serve files. This is not a major threat.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_CLIENT_NETWORK_ATTACKS_WIRE_HTTP_01_EH1]

Question 8: Incorrect

As the cybersecurity specialist for your company, you have used Wireshark to check for man-in-the-middle DHCP spoofing attacks using the bootp filter. After examining the results, what is your best assessment?



- No man-in-the-middle spoofing attacks are currently present.
- A man-in-the-middle spoofing attack is possible due to two DHCP ACK packets.
- ~~A man-in-the-middle spoofing attack is possible due to the DHCP Offer packet captured from the hacker.~~
- Two man-in-the-middle spoofing attacks were captured.

Explanation

Because you received two DHCP ACK packets from the same source IP address, there is a high probability that one of these is a result of a man-in-the-middle spoofing attack.

A DHCP Offer packet is expected.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_CLIENT_NETWORK_ATTACKS_WIRE_MITM_01_EH1]

Question 9: Correct

Which of the following protocols is one of the most common methods used to protect packet information and defend against network attacks in VPNs?

- BLE
- ECC
- IPsec
- SYN

Explanation

Internet Protocol Security (IPsec) is one of the most common methods used to protect packet information and defend against network attacks.

Bluetooth low energy (BLE), also known as Bluetooth Smart, is a wireless personal area network. BLE is not a protocol used for encryption.

Elliptic curve cryptography (ECC) is a public-key cryptography method based on groups of numbers in an elliptical curve. ECC is not a protocol used for encryption.

TCP packets have flag indicators. Two of these indicators are SYN and ACK. SYN starts a connection between two systems. ACK acknowledges that a packet has been received. TCP flags are not used for encryption.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_HIJACK_WEB_COUNTER_ADMIN_ROLE_01_EH1]

Question 10: Incorrect

Which of the following are protocols included in the IPsec architecture?

- ~~IKE, AH, and ACK~~
- SIP, AH, and ESP
- IKE, AH, and ESP
- SIP, AH, and ACK

Explanation

There are several protocols within the IPsec architecture, including:

- The Internet Key Exchange (IKE), which creates the encryption keys.
- Authentication Header (AH), which authenticates the packets' sender.
- Encapsulating Security Payload (ESP), which provides sender authentication and encryption.

TCP packets have flag indicators. Two of these indicators are SYN and ACK. SYN starts a connection between two systems. ACK acknowledges that a packet has been received.

VoIP uses Session Initiation Protocol (SIP) to enable voice and video calls over an IP network.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_HIJACK_WEB_COUNTER_ADMIN_ROLE_02_EH1]

Question 11: Incorrect

A penetration tester discovers a vulnerable application and is able to hijack a website's URL hyperlink session ID. The penetration tester is able to intercept the session ID; when the vulnerable application sends the URL hyperlink to the website, the session IDs are embedded in the hyperlink. Which of the following types of session hijacking countermeasures is the penetration tester using?

- TCP/IP session hijacking
- Man-in-the-middle attack
- ~~UDP session hijacking~~
- Session fixation attack

Explanation

Session fixation attacks target websites where session IDs are provided in the hyperlink. URLs are sent to a user with session IDs already embedded into them. When a user logs in using this URL, their user information becomes aligned with that session ID. An attacker following the same URL would have the same level of access as the targeted user.

A UDP session hijack is a connectionless protocol. Even though it can be used as a countermeasure, there is no connection session to hijack.

A man-in-the-middle attack can be both an Application- or Network-level attack. It involves using methods like ARP poisoning to redirect malicious traffic to either the target machine or server.

The TCP/IP session hijack is where the hacker hijacks the TCP connection session by sniffing and intercepting the target machine's traffic with the server. Then, by modifying the packets and injecting them into the server, the hacker is able to authenticate as if they are the target machine.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_HIJACK_WEB_COUNTER_PENTEST_ROLE_01_EH1]

Question 12: Incorrect

Your network administrator has set up training for all the users regarding clicking on links in emails or instant messages. Which of the following is your network administrator attempting to prevent?

- DNS spoofing
- Session fixation
- ~~Packet sniffing~~
- Packet filtering

Explanation

User education is an important part of security. Because attacks like session fixation rely on a user clicking on a link in an email or instant message, users should be trained not to click on these links.

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network.

DNS spoofing, also known as DNS cache poisoning, targets Active Directory or other DNS-reliant networks.

Packet filtering firewalls look at packets' header information to determine legitimate traffic.

References

TestOut Ethical Hacker Pro - 10.2 Session Hijacking
[e_session_hijacking_eh1.exam.xml Q_HIJACK_WEB_COUNTER_USER_ROLE_01_EH1]