

Exam Report: 12.1.11 Practice Questions

Date: 5/11/2020 1:27:16 pm
Time Spent: 7:27

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 54%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following best describes the HTTP Request/Response TRACE?

- ☐ Stores web pages and distributes them to clients.
- ☐ Only transfers the status line and the header section.
- ➡ ☒ Performs a loopback test to a target resource.
- ☐ Establishes a communication tunnel to the server.

Explanation

The TRACE command performs a loopback test to a target resource.

The POST command is used to send data to the server using HTML forms.

The HEAD command requests information from the server, but only transfers the status line and the header section.

A web server is a system used to store and distribute web pages to clients.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVERS_HACKING_FACTS_01_EH1]

▼ Question 2: Correct

Which of the following HTTP response messages would you receive if additional action needs to be taken to complete the request?

- ☐ 4xx: Client Error
- ➡ ☒ 3xx: Redirection
- ☐ 1xx: Informational
- ☐ 2xx: Success

Explanation

The HTTP response message 3xx: *Redirection* indicates that additional action needs to be taken to complete the request.

The HTTP response message 1xx: *Informational* indicates the request has been received and the process is continuing.

The HTTP response message 2xx: *Success* indicates the action was received, understood, and accepted.

The HTTP response message 4xx: *Client Error* indicates that the request included a bad syntax or other

error and cannot be completed.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVERS_HACKING_FACTS_02_EH1]

▼ Question 3: Correct

Which of the following explains why web servers are often targeted by attackers?

- ☐ Web servers are placed behind firewalls to make them less accessible to users.
- ☐ Web servers are standalone servers that seldom interact with other network resources.
- ☐ Web servers are simple devices with few complex features, making their attack surfaces easy to exploit.
- ➡ ☒ Web servers provide an easily found, publicly accessible entrance to a network that users are encouraged to enter into and browse.

Explanation

Web servers provide an entrance to a network that users are encouraged to enter into, browse, and get comfortable with.

Web servers are placed in front of firewalls or in a DMZ to make them accessible to users.

Web servers interact with other servers, like database servers, when creating content requested by users.

Web servers have complex modules and plug-ins that may contain exploitable features.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVERS_HACKING_VULNERABILITIES_01_EH1]

▼ Question 4: Incorrect

Which of the following best describes Microsoft Internet Information Services (IIS)?

- ☒ ~~A database server technology~~
- ➡ ☐ A web server technology
- ☐ An email server technology
- ☐ A name server technology

Explanation

Microsoft Internet Information Services (IIS) is a web server technology.

Microsoft DNS, OpenDNS, and SaveDNS are examples of name server technologies.

Oracle, MySQL, and PostgreSQL are examples of database server technologies.

Apache James, Postfix, and Exim are examples of email server technologies.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVERS_HACKING_WEB_SERVERS_01_EH1]

▼ Question 5: Incorrect

Which of the following is an open-source web server technology?

- ➡ ☐ Apache Web Server
- ☐ Nginx
- ☐

☒ ~~LightSpeed Web Server~~

☐ Microsoft Internet Information Services (IIS)

Explanation

Apache Web Server (or Apache HTTP Server) is an open-source web server that is the most widely used web server technology.

Microsoft Internet Information Services (IIS) is neither open-source nor the most widely used web server technology.

Nginx is an open-source web server but isn't the most widely used web server technology.

LightSpeed Web Server is neither open-source nor the most widely used web server technology.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVERS_HACKING_WEB_SERVERS_02_EH1]

▼ Question 6: Correct

Which of the following steps in the web server hacking methodology involves setting up a web server sandbox to gain hands-on experience attacking a web server?

- ➡ ☒ Mirroring
- ☐ Session hijacking
- ☐ Footprinting
- ☐ Vulnerability scanning

Explanation

The mirroring step involves setting up a web server sandbox that is similar to the web server being attacked to gain hands-on experience.

Footprinting is the technique of gathering information about the web server to find ways to penetrate the server.

Vulnerability scanning is the inspection of the potential points of exploit on the web server.

Session hijacking is the exploitation of a web session to gain unauthorized access to the web server.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVER_ATTACKS_METHODODOLOGY_01_EH1]

▼ Question 7: Correct

Which of the following is a password cracking tool that can make over 50 simultaneous target connections?

- ☐ TCH-Hydra
- ☐ Metasploit
- ☐ Wfetch
- ➡ ☒ Brutus

Explanation

Brutus is a password cracking tool that can make over 50 simultaneous target connections.

Metasploit is a penetration testing toolkit that contains remote exploits for various platforms.

Wfetch is a tool that targets websites that have Active Server Pages (ASP) or wireless protocols.

TCH-Hydra is a password cracking tool that supports several different protocols.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVER_ATTACKS_TOOLS_01_EH1]

▼ Question 8: Incorrect

Which of the following types of web server attacks is characterized by altering or vandalizing a website's appearance in an attempt to humiliate, discredit, or annoy the victim?

- ➡ ☐ Website defacement
- ☐ Footprinting
- ☒ Cross-site scripting
- ☐ Directory traversal

Explanation

Website defacement is a fairly unique attack where a website is vandalized so that the site's appearance is altered or defaced in an attempt to humiliate, discredit, or even just annoy the victim.

Directory traversal targets directories and executables outside of the web server directories.

Cross-site scripting benefits from scripting defects on a website. Instead of targeting the application or the data itself, the attack targets the user.

Footprinting is not a type of web server attack. An attacker may use footprinting to learn about and identify a web server prior to an attack.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVER_ATTACKS_TYPES_01_EH1]

▼ Question 9: Incorrect

Which of the following best describes a phishing attack?

- ➡ ☐ A user is tricked into believing that a legitimate website is requesting their login information.
- ☐ An attacker alters the XSS to run a Trojan horse with the victim's web browser.
- ☐ In this attack, attackers use various weaknesses to hack into seemingly secure passwords.
- ☒ This attack is used to intercept communications between an authorized user and the web server.

Explanation

In a phishing attack, a user is tricked into believing that a legitimate website is requesting their login information. Instead, the user is redirected to a malicious website that steals the user's login information.

A man-in-the-middle attack is used to intercept communications between an authorized user and the web server.

A web server password cracking attack uses various weaknesses to hack into seemingly secure passwords.

A cross-site scripting attack alters XSS to run a Trojan horse with the victim's web browser.

References

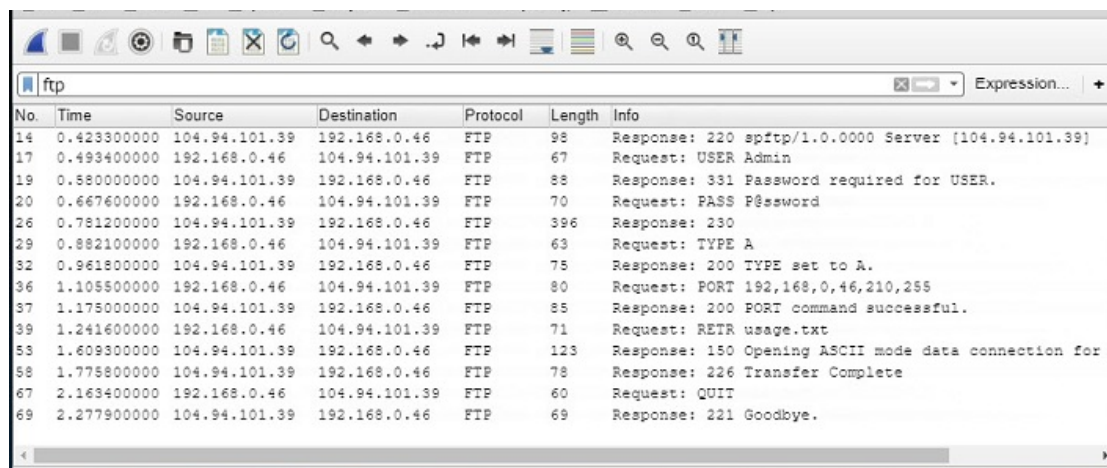
TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVER_ATTACKS_TYPES_02_EH1]

▼ Question 10: Incorrect

As part of your penetration test, you have captured an FTP session, as shown below. Which of the following concerns or recommendations will you include in your report?





No.	Time	Source	Destination	Protocol	Length	Info
14	0.423300000	104.94.101.39	192.168.0.46	FTP	98	Response: 220 sftp/1.0.0000 Server [104.94.101.39]
17	0.493400000	192.168.0.46	104.94.101.39	FTP	67	Request: USER Admin
19	0.580000000	104.94.101.39	192.168.0.46	FTP	88	Response: 331 Password required for USER.
20	0.667600000	192.168.0.46	104.94.101.39	FTP	70	Request: PASS P@ssword
26	0.781200000	104.94.101.39	192.168.0.46	FTP	396	Response: 230
29	0.882100000	192.168.0.46	104.94.101.39	FTP	63	Request: TYPE A
32	0.961800000	104.94.101.39	192.168.0.46	FTP	75	Response: 200 TYPE set to A.
36	1.105500000	192.168.0.46	104.94.101.39	FTP	80	Request: PORT 192,168,0,46,210,255
37	1.175000000	104.94.101.39	192.168.0.46	FTP	85	Response: 200 PORT command successful.
39	1.241600000	192.168.0.46	104.94.101.39	FTP	71	Request: RETR usage.txt
53	1.609300000	104.94.101.39	192.168.0.46	FTP	123	Response: 150 Opening ASCII mode data connection for u
58	1.775800000	104.94.101.39	192.168.0.46	FTP	78	Response: 226 Transfer Complete
67	2.163400000	192.168.0.46	104.94.101.39	FTP	60	Request: QUIT
69	2.277900000	104.94.101.39	192.168.0.46	FTP	69	Response: 221 Goodbye.

- ☐ FTP request type A allows ASCII files to be downloaded.
- ☒ ~~FTP ports 102 & 160 should be hidden.~~
- ☐ FTP response type 230 should be blocked.

➡ ☐ FTP uses clear-text passwords.

Explanation

FTP is a very insecure protocol, and, as can be seen from the captured session, the username and password can be seen in a clear-text form. This means that FTP users are vulnerable to man-in-the-middle (MITM) attacks that can steal usernames and passwords or modify files as they pass over a network.

If FTP is required, you can block ports, but then FTP is not available.

The FTP Type command is used to set the transfer mode to ASCII meaning that files are transferred as text. This can be a concern, but the fact that the username and password are visible in plan text is a higher concern.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEB_SERVER_ATTACKS_WIRES_CRACK_01_EH1]

▼ Question 11: Correct

Frank wants to do a penetration test. He is looking for a tool that checks for vulnerabilities in web applications, network systems, wireless networks, mobile devices, and defense systems such as IDS or IPS. Which of the following tools would you recommend to him?

- ☐ Syhunt Dynamic
- ☐ Immunity CANVAS
- ➡ ☒ COREImpact Pro
- ☐ Arachni

Explanation

COREImpact Pro is a penetration testing tool that checks for vulnerabilities in web applications, network systems, wireless networks, mobile devices, and defense systems such as IDS or IPS.

Immunity CANVAS provides an exploit development framework for penetration testers.

Arachni is open-source and helps penetration testers evaluate the security of their web applications.

Syhunt Dynamic can automate security testing and help to guard web infrastructure against known security threats.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEBSERVER_COUNTER_PENTEST_TOOLS_01_EH1]

▼ Question 12: Incorrect

Which of the following web server countermeasures is implemented to fix known vulnerabilities, eliminate bugs, and improve performance?

- ☐ Remove inactive accounts.
- ☒ ~~Disable the directory listing option.~~
- ☐ Perform a vulnerability scan.
- ➡ ☐ Install patches and updates.

Explanation

Patches and updates are designed to fix known vulnerabilities, eliminate bugs, and improve performance.

Removing inactive accounts reduces the risk of data breaches.

Disabling the directory listing option reduces the risk of directory traversal attacks.

Performing a vulnerability scan targets the web server with various types of attacks to find weaknesses.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEBSERVER_COUNTER_SECURE_SET_CONFIG_01_EH1]

▼ Question 13: Correct

You are looking for a web server security tool that will detect hidden malware in websites and advertisements. Which of the following security tools would you most likely use?

- ➡ ☒ Hackalert
- ☐ Wikto
- ☐ MBSA
- ☐ Syhunt Dynamic

Explanation

Hackalert is a cloud-based subscription service that detects hidden malware in websites and advertisements.

MBSA, or Microsoft Baseline Security Analyzer, is a patch management tool that checks for updates to the operating system, database components, and SQL server. It also scans for any errors or vulnerabilities in the configuration settings.

Syhunt Dynamic can automate security testing and help to guard web infrastructure against known security threats.

Wikto is a security scanner for Windows web servers. It checks for errors in code and monitors HTTP requests and responses.

References

TestOut Ethical Hacker Pro - 12.1 Web Servers

[e_webservers_eh1.exam.xml Q_WEBSERVER_COUNTER_SECURE_TOOLS_01_EH1]