EXIN Ethical Hacking Foundation

Sample Exam

Edition 201606

ETHICAL HACKING

Content

Introduction

This is the sample exam EXIN Ethical Hacking Foundation. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

Good luck!

Sample exam

1 of 40

What is the primary goal of an Ethical Hacker?

A. Avoiding detection
B. Determining return on investment (ROI) for security measures
C. Resolving security vulnerabilities
D. Testing security controls

2 of 40

What are examples of network sniffing tools?

A. Bash, Nano, VI
B. Nmap, Metasploit, Nessus
C. Wireshark, Tshark, TCPdump

3 of 40

An ethical hacker is hired by an organization to gain remote access to their internal network. He has not received any information about the internal network of the organization.

What kind of test is carried out here?

A. black box testing
B. grey box testing
C. white box testing

4 of 40

What is a function of the R57 shell?

A. Implementing a web-based version of Metasploit
B. Viewing and transferring files
C. Viewing the webcams of visitors towards the website

5 of 40

Mary has added an apostrophe after an ?id= parameter within the URL of a webpage. She now sees an error, saying there was a syntax error.

What did Mary find?

A. Cross-Site Scripting vulnerability
B. PostgreSQL database exploit
C. SQL Injection

6 of 40

A site uses dynamically generated content. By making use of a specific technique, it is possible to steal login credentials of the user.

Which technique is meant here?

A. Session Hijacking
B. SQL injection
C. Cross Site Scripting (XSS)

7 of 40

What can be used to create a connection between your machine and the website you have your R57 shell running on?

A. Eval function
B. Backconnect shell
C. Reverse shell

8 of 40

While in Meterpreter, you found an interesting file named passwords.xls. You want to retrieve this file within Meterpreter but are unsure how to do it.

What should you use?

A. 'download' command within Meterpreter
B. VNC, as it is the fastest way to copy data
C. It's not possible to download files from within the Meterpreter shell

9 of 40

You have found a live system on IP address 192.168.10.113.

Which nmap command lets you detect the Operating System of a target?

A. `nmap -O 192.168.10.113`
B. `nmap -Os 192.168.10.113`
C. `nmap -os 192.168.10.113`

10 of 40

A service scan including fingerprint showed that a target machine is running Apache 2.2.14.

What could be the next step to check if this service is vulnerable?

A. Check online resources such as Exploit-DB, OSVDB for known vulnerabilities.
B. Use Kismet to determine Apache configuration and patch level.
C. Use netcat to gain access to the machine through this service.

11 of 40

You know the table and column names from a database, you can expand your SQL Injection to retrieve data.

What should you use?

A. UNION GET
B. UNION SELECT
C. UNION CONCAT

12 of 40

A hacker is trying to capture traffic from his wireless network adapter.

What network adapter should he look for in Wireshark?

A. eth0
B. l0
C. wlan0

13 of 40

Before beginning the ethical hack at a client, a penetration tester should always be prepared for any legal issues.

What should the penetration tester do to prevent legal liability?

A. Analyze the environment of the client to see if there are any vulnerabilities that might cause issues before the actual ethical hack.
B. Sign a contract with the client before performing the ethical hack.
C. Talk to the client before the test and make sure whether the test has to be a black, grey or white box test.

14 of 40

At what point in the Ethical Hacking process is the attacker most likely to use a port scanning tool?

A. Attack execution
B. Attack preparation
C. Information gathering
D. Report writing

15 of 40

What is a c99 shell used for?

A. It is a command line tool that allows remote connections to a database server.
B. It is a PHP backdoor that allows for the uploading, deletion and execution of files.
C. It is malware used to crash servers that run Microsoft Windows Server 2008 R2.

16 of 40

A hacker has managed to partly follow the process of cracking a WEP key. She has created an ARP packet which should now be injected towards the access point.

Which application should she use to inject the ARP packet?

A. airbase-ng
B. aireplay-ng
C. wesside-ng

17 of 40

A penetration tester wants to know what IP addresses are currently active on the network. He uses nmap to do so.

What nmap switch does he need to perform this test?

A. -sU
B. -sO
C. -sP

18 of 40

A client has said that he created a case-insensitive filter for 'script' from being inserted in any forms to prevent an XSS PoC.

How can you bypass this?

A. `<sCrIPt>alert(1);</ScRiPT>`
B. `<javascript>alert(1);</script>`
C. `<img src=x onerror=alert(1)>`

19 of 40

A hacker managed to find an XSS vulnerability. Now she wants to take over sessions.

Where does she need the data retrievable from?

A. document.session
B. session.cookie
C. document.cookie

20 of 40

When creating an XSS PoC, what is the function that provides a pop-up?

A. `popup()`
B. `alert()`
C. `window.popup()`

21 of 40

A penetration tester is asked to scan a machine, but is only allowed to check if TCP/IP ports 21, 22, 80 and 443 are open.

What should she use?

A. `nmap -vv -A -p 21,22,80,https <target>`
B. `nmap -vv -p 21,22,80,443 <target>`
C. `nmap -sV ftp, ssh, http, https <target>`

22 of 40

A website's URL contains `'index.php?page=home.php'`. The page=parameter allows remote URLs to be passed and it loads them.

What is this an example of?

A. Remote File Inclusion
B. Remote File Injection
C. Remote File Impersonation

23 of 40

Someone has breached a website and managed to keep it a secret. The hack was not part of an assignment and there was no permission.

What is this person called?

A. Black hat hacker
B. Hacktivist
C. Scriptkiddie
D. White hat hacker

24 of 40

You are performing a penetration test and are asked to test the authentication strength of a storage device. You have not received the IP address of the host, but you were told that the system sends a message to the network's broadcast every five minutes.

What could you use to find the IP address of the host?

A. Ncrack
B. Netdiscover
C. Wireshark

25 of 40

An Ethical Hacker is asked to perform a penetration test for a client and all he has received is a URL.

What kind of test is this?

A. Black box penetration test
B. Black hat hacking test
C. White box penetration test

26 of 40

Penetration testers sometimes use shells to communicate and find vulnerabilities in systems. One type of shells is so-called 'Bind Shells'. In certain scenario's these are ineffective.

Why is that?

A. Firewalls will block any traffic on a port the Bind Shells tries to communicate on.
B. Windows 7 and above cannot run shell commands anymore if the user is not an administrator.
C. Bind Shells only run on terminal based operating systems.

27 of 40

A penetration tester is testing a web application. To check for vulnerabilities she decides to check if SQL injections are possible.

Which character is typically used first by the penetration tester?

A. Dollar sign
B. Semicolon
C. Single quote

28 of 40

You are not sure what the MAC address is of your WiFi network.

After being advised to use Airodump-NG, what network should you look for?

A. BSSID
B. ESSID
C. SSID

29 of 40

You are trying to find out which of your plugged in network adapters supports WiFi.

What command should you use in your terminal window?

A. `iwconfig`
B. `wificards`
C. `wireshark`

30 of 40

What is ESSID?

A. MAC address of a connected client
B. MAC address of a target access point
C. Network name

31 of 40

A tester is conducting a penetration test on a web server. She begins the test with a banner grabbing attack. She has already verified that the web server is running a Linux distribution. However, the HTTP banner reports that it is running IIS version 8.

What type of defense is the web server administrator using?

A. Folder redirection
B. Port obfuscation
C. Process redirection
D. Service spoofing

32 of 40

You have saved the output of an Nmap scan in XML format.

What should you use to import the scan results within Metasploit?

A. `db_import`
B. `nmap_import`
C. `scan_import`

33 of 40

Metasploit makes use of several modules in order to test for vulnerabilities. One of these modules allows the penetration tester to automatically serve browser exploits.

What is the name of this module used in Metasploit?

A. browser_exploiter
B. browser_autopwn
C. metasploit_autopwn

34 of 40

An ethical hacker is trying to breach a website through SQL Injection. He also changed his User-Agent HTTP header, sent by his browser.

What can he achieve with this action?

A. He acquires a matching SSL connection.
B. He obtains better performance of the website so that it responds faster to his requests.
C. He prevents forensics from revealing his real browser that was used during the attack

35 of 40

A network administrator noticed some suspicious traffic on the company's network. He decides to investigate it. After successfully pinging the source of the traffic he uses a utility to find the associated MAC address.

Which utility does he use?

A. ARP
B. DNSSpoof
C. PSExec

36 of 40

When typing exploit in Metasploit, the exploit module fails to run and gives an error that says a target has not been selected.

How can this be fixed?

A. Configuring the RHOST variable to provide a target address
B. Checking the available targets by typing `'show targets'`, then select a target by typing `'set TARGET x'`
C. Typing `'check'` to see if the target is vulnerable

37 of 40

When looking at webserver log files, Pete wants to know what browser was used during the attack against his website. Pete should look for information that is generally being sent through the `<answer>` header.

Which `<answer>` header does it concern?

A. Accept-Language:
B. Host:
C. User-Agent:

38 of 40

A company has suffered from a DDoS attack. They have the IP address of the attacker and want to contact their Internet Service Provider to report an abuse.

What must they perform?

A. DNS Lookup
B. GeoIP Location Lookup
C. WHOIS Lookup

39 of 40

A penetration tester is scanning the network environment of his client with a tool. This tool has the following properties:

- It uses a ranking to show the impact of a vulnerability.
- It detects all sorts of vulnerabilities on various operating systems such as Windows, Linux and Mac OS.
- It is able to detect bots, trojans and other malware that might be installed on the computers connected to the network.

What is the name of the tool the penetration tester is using?

A. Nessus
B. Nmap
C. Nikto

40 of 40

What is the name of the Metasploit modules that are **not** used for exploitation?

A. Auxiliaries
B. Payloads
C. shellcodes

Answer key

1 of 40

What is the primary goal of an Ethical Hacker?

A. Avoiding detection
B. Determining return on investment (ROI) for security measures
C. Resolving security vulnerabilities
D. Testing security controls

A. Incorrect. Avoiding detection is one part of Ethical Hacking but not the primary goal.
B. Incorrect. ROI calculation is part of control selection and risk mitigation.
C. Incorrect. Ethical Hacking is finding and documenting vulnerabilities, not resolving them.
D. Correct. The primary job of Ethical Hackers is security testing.

2 of 40

What are examples of network sniffing tools?

A. Bash, Nano, VI
B. Nmap, Metasploit, Nessus
C. Wireshark, Tshark, TCPdump

A. Incorrect. These are random Linux / UNIX tools.
B. Incorrect. These are all-in-one exploit tools (Metasploit, Nessus) and scanning tools (Nmap).
C. Correct. These are sniffing tools. Penetration Testing – A Hands-On Introduction to Ethical Hacking, chapter 7.

3 of 40

An ethical hacker is hired by an organization to gain remote access to their internal network. He has not received any information about the internal network of the organization.

What kind of test is carried out here?

A. black box testing
B. grey box testing
C. white box testing

A. Correct. The ethical hacker doesn't know anything about the internal network. He simulates being a black hat hacker, working from outside the company.
B. Incorrect. In this case the ethical hacker is given a minimum of information.
C. Incorrect. In a white box test, all the relevant information about the system/network is available to the hacker.

4 of 40

What is a function of the R57 shell?

A. Implementing a web-based version of Metasploit
B. Viewing and transferring files
C. Viewing the webcams of visitors towards the website

A. Incorrect. There is no web-based version of Metasploit that you can use out-of-the-box. Metasploit is a framework that makes use of database for vulnerability exploitation.
B. Correct. That is a function of the R57 shell.
C. Incorrect. This is not possible with the R57 Shell. This could be done with a tool in combination with Metasploit.

5 of 40

Mary has added an apostrophe after an ?id= parameter within the URL of a webpage. She now sees an error, saying there was a syntax error.

What did Mary find?

A. Cross-Site Scripting vulnerability
B. PostgreSQL database exploit
C. SQL Injection

A. Incorrect. Using an apostrophe [’] to close the SQL query will cause the application to throw a SQL syntax error (if a SQLi vulnerability is present).
B. Incorrect. Using an apostrophe [’] to close the SQL query will cause the application to throw a SQL syntax error (if a SQLi vulnerability is present).
C. Correct. Using an apostrophe [’] to close the SQL query will cause the application to throw a SQL syntax error (if a SQLi vulnerability is present).

6 of 40

A site uses dynamically generated content. By making use of a specific technique, it is possible to steal login credentials of the user.

Which technique is meant here?

A. Session Hijacking
B. SQL injection
C. Cross Site Scripting (XSS)

A. Incorrect. Session Hijacking is something the hacker might want to do after using XSS.
B. Incorrect. SQL injection is creating new queries and trying to get private information from the database.
C. Correct. XSS code makes it possible to place java script code into a site without the user noticing it. The code can show a fake login window that sends the credentials to the hacker. Penetration Testing - A Hands-On Introduction to Hacking, chapter 14, Cross Site Scripting.

7 of 40

What can be used to create a connection between your machine and the website you have your R57 shell running on?

A. Eval function
B. Backconnect shell
C. Reverse shell

A. Incorrect. Eval function has nothing to do with the R57 shell. It does not prompt anything.
B. Correct. R57 is also called "Backconnect shell". It is used for sending malware, spam, etc.
C. Incorrect. R57 is also called "Backconnect shell". It is used for sending malware, spam, etc.

8 of 40

While in Meterpreter, a hacker finds an interesting file named passwords.xls. He wants to retrieve this file within Meterpreter but is unsure how to do it.

What should the hacker use?

A. 'download' command within Meterpreter
B. VNC, as it is the fastest way to copy data
C. It's not possible to download files from within the Meterpreter shell

A. Correct. Penetration Testing - A Hands-On Introduction to Hacking, chapter 13.
B. Incorrect. VNC is used to connect to a remote pc and share a screen for example.
C. Incorrect. The hacker can connect to a remote computer and download files.

9 of 40

You have found a live system on IP address 192.168.10.113.

Which nmap command lets you detect the Operating System of a target?

A. `nmap -O 192.168.10.113`
B. `nmap -Os 192.168.10.113`
C. `nmap -os 192.168.10.113`

A. Correct. The -O tries to get the information of the OS that is used. Penetration Testing - A Hands-On Introduction to Hacking, chapter 5.
B. Incorrect. The -Os is not even a key for nmap.
C. Incorrect. The -os is not even a key for nmap.

10 of 40

A service scan including fingerprint showed that a target machine is running Apache 2.2.14.

What could be the next step to check if this service is vulnerable?

A. Check online resources such as Exploit-DB, OSVDB for known vulnerabilities.
B. Use Kismet to determine Apache configuration and patch level.
C. Use netcat to gain access to the machine through this service.

A. Correct. Penetration Testing - A Hands-On Introduction to Hacking, chapter 6, Web Application Scanning and Researching for Vulnerabilities.
B. Incorrect. Kismet is a wifi vulnerability tool.
C. Incorrect. Netcat is not a tool to check vulnerabilities.

11 of 40

You know the table and column names from a database, you can expand your SQL Injection to retrieve data.

What should you use?

A. UNION GET
B. UNION SELECT
C. UNION CONCAT

A. Incorrect. The SQL UNION operator combines the result of two or more SELECT statements.
B. Correct. The SQL UNION operator combines the result of two or more SELECT statements.
C. Incorrect. The CONCAT function is used to concatenate two strings to form a single string (when we have only one field to receive the data).

12 of 40

A hacker is trying to capture traffic from his wireless network adapter.

What network adapter should he look for in Wireshark?

A. eth0
B. l0
C. wlan0

A. Incorrect. eth0 is always a wired Ethernet adapter. wlan0 is the only wireless adapter choice.
B. Incorrect. wlan0 is the only wireless adapter choice.
C. Correct. wlan0 is the only wireless adapter choice. Penetration Testing – A Hands-On Introduction to Hacking, chapter 7.

13 of 40

Before beginning the ethical hack at a client, a penetration tester should always be prepared for any legal issues.

What should the penetration tester do to prevent legal liability?

A. Analyze the environment of the client to see if there are any vulnerabilities that might cause issues before the actual ethical hack.
B. Sign a contract with the client before performing the ethical hack.
C. Talk to the client before the test and make sure whether the test has to be a black, grey or white box test.

A. Incorrect. Analyzing the environment of the client comes after signing all legal documents such as the NDA. Using hacking tools does not make it legal or not.
B. Correct. Sign a contract. That way both parties (the pentester and client) know what is mutually expected. Penetration Testing - A Hands-On Introduction to Hacking, chapter 0.
C. Incorrect. Although this has to be done this has nothing to do with any legal issues.

14 of 40

At what point in the Ethical Hacking process is the attacker most likely to use a port scanning tool?

A. Attack execution
B. Attack preparation
C. Information gathering
D. Report writing

A. Incorrect. This is the actual attack. Port scanning is information gathering.
B. Incorrect. This phase uses the information from port scanning to select targets.
C. Correct. Port scanning is part of active reconnaissance and scanning.
D. Incorrect. This is summarizing results. Port scanning is gathering data that feeds the report.

15 of 40

What is a c99 shell used for?

A. It is a command line tool that allows remote connections to a database server.
B. It is a PHP backdoor that allows for the uploading, deletion and execution of files.
C. It is malware used to crash servers that run Microsoft Windows Server 2008 R2.

A. Incorrect. It's not used for remote connections to a database server.
B. Correct. It's a backdoor shell that can be uploaded to a site to gain access to files stored on that site. Once it is uploaded, the hacker can use it to edit, delete, or download any files on the site, or upload his own.
C. Incorrect. c99 shell can be classified as malware but it is definitely not.

16 of 40

A hacker has managed to partly follow the process of cracking a WEP key. She has created an ARP packet which should now be injected towards the access point.

Which application should she use to inject the ARP packet?

A. airbase-ng
B. aireplay-ng
C. wesside-ng

A. Incorrect. Airbase is a multi-purpose tool aimed at attacking clients.
B. Correct. Aireplay will inject captured or created packets on a wireless network.
C. Incorrect. wesside is a WEP cracking tool but does not inject captured packets.

17 of 40

A penetration tester wants to know what IP addresses are currently active on the network. He uses nmap to do so.

What nmap switch does he need to perform this test?

A. -sU
B. -sO
C. -sP

A. Incorrect. -sU is used to do a so called UDP scan.
B. Incorrect. -sO tries to determine which IP protocols (TCP, UDP, ICMP) are supported by a system.
C. Correct. -sP scans for active IP addresses on the network. See Penetration Testing - A Hands-On Introduction to Hacking, chapter 5.

18 of 40

A client has said that he created a case-insensitive filter for 'script' from being inserted in any forms to prevent an XSS PoC.

How can you bypass this?

A. `<sCrIPt>alert(1);</ScRiPT>`
B. `<javascript>alert(1);</script>`
C. `<img src=x onerror=alert(1)>`

A. Incorrect. This script will not run because the clients form checks on case sensitive scripts.
B. Incorrect. This will not run because script cannot be run in the form.
C. Correct. This will run. Penetration Testing – A Hands- on Introduction to Hacking, chapter 14.

19 of 40

A hacker managed to find an XSS vulnerability. Now she wants to take over sessions.

Where does she need the data retrievable from?

A. document.session
B. session.cookie
C. document.cookie

A. Incorrect. The document.cookie is the only place where a session is stored.
B. Incorrect. The document.cookie is the only place where a session is stored.
C. Correct. The document.cookie is the only place where a session is stored.

20 of 40

When creating an XSS PoC, what is the function that provides a pop-up?

A. `popup()`
B. `alert()`
C. `window.popup()`

A. Incorrect. Popup () is not a correct javascript method.
B. Correct. Alert () will trigger the alert event which will give a popup window.
C. Incorrect. This will do nothing.

21 of 40

A penetration tester is asked to scan a machine, but is only allowed to check if TCP/IP ports 21, 22, 80 and 443 are open.

What should she use?

A. `nmap -vv -A -p 21,22,80,https <target>`
B. `nmap -vv -p 21,22,80,443 <target>`
C. `nmap -sV ftp, ssh, http, https <target>`

A. Incorrect. It is not possible to scan on a specific type like https or ssh. The tester will have to know which ports are used.
B. Correct. By checking the ports it is possible to see which services (https, ssh, etc.) are running.
C. Incorrect. It is not possible to scan on a specific type like https or ssh. The tester will have to know which ports are used.

22 of 40

A website's URL contains `'index.php?page=home.php'`. The page=parameter allows remote URLs to be passed and it loads them.

What is this an example of?

A. Remote File Inclusion
B. Remote File Injection
C. Remote File Impersonation

A. Correct. Penetration Testing – A Hands-On Introduction to Hacking, chapter 14, Remote File Inclusion.
B. Incorrect. This is not the correct term.
C. Incorrect. This is not the correct term.

23 of 40

Someone has breached a website and managed to keep it a secret. The hack was not part of an assignment and there was no permission.

What is this person called?

A. Black hat hacker
B. Hacktivist
C. Scriptkiddie
D. White hat hacker

A. Correct. A person who hacks without permission is called a Black hat hacker.
B. Incorrect. Valid hacker type, but does not match the description.
C. Incorrect. Valid hacker type, but does not match the description.
D. Incorrect. Valid hacker type, but does not match the description.

24 of 40

You are performing a penetration test and are asked to test the authentication strength of a storage device. You have not received the IP address of the host, but you were told that the system sends a message to the network's broadcast every five minutes.

What could you use to find the IP address of the host?

A. Ncrack
B. Netdiscover
C. Wireshark

A. Incorrect. Ncrack is a high-speed network authentication cracking tool.
B. Incorrect. Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without DHCP server, when you are war driving.
C. Correct. Wireshark can be used to discover an IP address.

25 of 40

An Ethical Hacker is asked to perform a penetration test for a client and all he has received is a URL.

What kind of test is this?

A. Black box penetration test
B. Black hat hacking test
C. White box penetration test

A. Correct. Minimal information is provided to the penetration tester during a black box test.
B. Incorrect. A black hat is a type of hacker, not a type of test.
C. Incorrect. Moderate to advanced details are provided to the penetration tester during a white box test.

26 of 40

Penetration testers sometimes use shells to communicate and find vulnerabilities in systems. One type of shells is so-called 'Bind Shells'. In certain scenario's these are ineffective.

Why is that?

A. Firewalls will block any traffic on a port the Bind Shells tries to communicate on.
B. Windows 7 and above cannot run shell commands anymore if the user is not an administrator.
C. Bind Shells only run on terminal based operating systems.

A. Correct. A bind shell instructs the target machine to open a command shell and listen on a local port. The attack machine then connects to the target machine on the listening port. However, with the advent of firewalls, the effectiveness of bind shells has fallen because any correctly configured firewall will block traffic to some random port like 4444. Penetration Testing - A Hands-On Introduction to Hacking, chapter 4 - Types of shells
B. Incorrect. Bind shells have nothing to do with the user being an administrator.
C. Incorrect. Bind shells run on any operating system or website.

27 of 40

A penetration tester is testing a web application. To check for vulnerabilities she decides to check if SQL injections are possible.

Which character is typically used first by the penetration tester?

A. Dollar sign
B. Semicolon
C. Single quote

A. Incorrect. This is not character to use.
B. Incorrect. This is often the last character to use.
C. Correct. A typical test for SQL injection vulnerabilities is to use a single quotation mark to close the SQL query. If an SQL injection vulnerability is present, the addition of that quotation mark should cause the application to throw an SQL error, because the query will already be closed as part of the underlying code and the extra single quote will cause the SQL syntax to be incorrect. That error will tell us that we can inject SQL queries to the site's database using the tested parameter. Penetration Testing - A Hands-On Introduction to Hacking, chapter 14 -Testing for SQL Injection Vulnerabilities.

28 of 40

You are not sure what the MAC address is of your WiFi network.

After being advised to use Airodump-NG, what network should you look for?

A. BSSID
B. ESSID
C. SSID

A. Correct. The BSSID is the wireless equivalent of a MAC address. Penetration Testing, A Hands-On Introduction to Hacking.
B. Incorrect. The ESSID is the friendly broadcast network name, not the MAC address.
C. Incorrect. This is similar to the ESSID and not the MAC address.

29 of 40

You are trying to find out which of your plugged in network adapters supports WiFi.

What command should you use in your terminal window?

A. `Iwconfig`
B. `wificards`
C. `wireshark`

A. Correct. iwconfig displays the configuration of all connected wireless adapters.
B. Incorrect. This isn't a command.
C. Incorrect. Wireshark will not run in a terminal window. Penetration Testing, A Hands-On Introduction to Hacking.

30 of 40

What is ESSID?

A. MAC address of a connected client
B. MAC address of a target access point
C. Network name

A. Incorrect. ESSID is AP based not client-based.
B. Incorrect. BSSID is the MAC address of an access point.
C. Correct. ESSID is the friendly name of an AP. Penetration Testing, A Hands-On Introduction to Hacking.

31 of 40

A tester is conducting a penetration test on a web server. She begins the test with a banner grabbing attack. She has already verified that the web server is running a Linux distribution. However, the HTTP banner reports that it is running IIS version 8.

What type of defense is the web server administrator using?

A. Folder redirection
B. Port obfuscation
C. Process redirection
D. Service spoofing

A. Incorrect. Folder redirection has nothing to do with web servers.
B. Incorrect. There was no modification to ports in the question statement, and port obfuscation would have no effect on the banner or the OS version.
C. Incorrect. There is no such thing as process redirection. The word redirection may attract unqualified candidates, so this makes it a good distractor.
D. Correct. IIS cannot run on Linux, and the tester has already verified Linux is the OS. So the banner is fake.

32 of 40

You have saved the output of an Nmap scan in XML format.

What should you use to import the scan results within Metasploit?

A. `db_import`
B. `nmap_import`
C. `scan_import`

A. Correct. The 'db_import' command is used to import the scan results in the Metasploit database.
B. Incorrect. The 'nmap_import' command is used to run an Nmap against the targets and the scan results would then be stored automatically in the database.
C. Incorrect. The 'db_import' command is used to import the scan results in the Metasploit database.

33 of 40

Metasploit makes use of several modules in order to test for vulnerabilities. One of these modules allows the penetration tester to automatically serve browser exploits.

What is the name of this module used in Metasploit?

A. browser_exploiter
B. browser_autopwn
C. metasploit_autopwn

A. Incorrect. It's not in metasploit.
B. Correct. See Penetration Testing - A Hands-On Introduction to Hacking, Chapter 10.
C. Incorrect. metasploit_autopwn is often mistaken for browser_autopwn, but metasploit_autopwn is a different module that tries to exploit open ports on systems.

34 of 40

An ethical hacker is trying to breach a website through SQL Injection. He also changed his User-Agent HTTP header, sent by his browser.

What can he achieve with this action?

A. He acquires a matching SSL connection.
B. He obtains better performance of the website so that it responds faster to his requests.
C. He prevents forensics from revealing his real browser that was used during the attack

A. Incorrect. The HTTP header has no relation to SSL connections.
B. Incorrect. Performance has nothing to do with HTTP headers.
C. Correct. Changing the HTTP header will change the information that the server logs about the connection, and therefore the attack. Penetration Testing, A Hands-On Introduction to Hacking, chapter 14.

35 of 40

A network administrator noticed some suspicious traffic on the company's network. He decides to investigate it. After successfully pinging the source of the traffic he uses a utility to find the associated MAC address.

Which utility does he use?

A. ARP
B. DNSSpoof
C. PSExec

A. Correct. ARP shows the MAC addresses for all IP addresses of which network traffic was received. Penetration Testing - A Hands-On Introduction to Hacking, chapter 7.
B. Incorrect. DNSSpoof doesn't provide information on MAC addresses.
C. Incorrect. PSExec doesn't provide information on MAC addresses.

36 of 40

When typing exploit in Metasploit, the exploit module fails to run and gives an error that says a target has not been selected.

How can this be fixed?

A. Configuring the RHOST variable to provide a target address
B. Checking the available targets by typing `'show targets'`, then select a target by typing `'set TARGET x'`
C. Typing `'check'` to see if the target is vulnerable

A. Incorrect. RHOST is only used to set the remote host parameter.
B. Correct. Penetration Testing, A Hands-On Introduction to Hacking, chapter 4 – Module Database
C. Incorrect. “check” is not a valid option.

37 of 40

When looking at webserver log files, Pete wants to know what browser was used during the attack against his website. Pete should look for information that is generally being sent through the `<answer>` header.

Which `<answer>` header does it concern?

A. Accept-Language:
B. Host:
C. User-Agent:

A. Incorrect. User-Agent tells a web server the type and version of the client's browser.
B. Incorrect. User-Agent tells a web server the type and version of the client's browser.
C. Correct. User-Agent tells a web server the type and version of the client’s browser. Penetration Testing, A Hands-On Introduction to Hacking, chapter 7.

38 of 40

A company has suffered from a DDoS attack. They have the IP address of the attacker and want to contact their Internet Service Provider to report an abuse.

What must they perform?

A. DNS Lookup
B. GeoIP Location Lookup
C. WHOIS Lookup

A. Incorrect. This is only used to get DNS tables.
B. Incorrect. This only shows geolocation information for the IP Address.
C. Correct. WHOIS show all the information there is to know about the IP Address.

39 of 40

A penetration tester is scanning the network environment of his client with a tool. This tool has the following properties: - It uses a ranking to show the impact of a vulnerability. It detects all sorts of vulnerabilities on various operating systems such as Windows, Linux and Mac OS. It is able to detect bots, trojans and other malware that might be installed on the computers connected to the network.

What is the name of the tool the penetration tester is using?

A. nessus
B. nmap
C. nikto

A. Correct. Nessus is a vulnerability scanner that uses all the things stated in the question. Penetration Testing, A Hands-On Introduction to Hacking, chapter 6 - Nessus
B. Incorrect. Nmap doesn't scan for vulnerabilities. It is a version scanner.
C. Incorrect. Nikto is a web application scanner only.

40 of 40

What is the name of the Metasploit modules that are **not** used for exploitation?

A. auxiliaries
B. payloads
C. shellcodes

A. Correct. Some modules that are not used for exploitation are known as auxiliary modules; they include vulnerability scanners, fuzzers, and even denial of service modules. A good rule of thumb to remember is that exploit modules use a payload and auxiliary modules do not. Penetration Testing - A Hands-On Introduction to Hacking, chapter 4 - using an auxiliary module.
B. Incorrect. Payloads are the same as shellcode and are used to exploit.
C. Incorrect. Shellcodes are the same as payloads and are used to exploit.

Evaluation

The table below shows the correct answers to the questions in this set of sample questions.

Question	Answer Key	Question	Answer Key
1	D	21	B
2	C	22	A
3	A	23	A
4	B	24	C
5	C	25	A
6	C	26	A
7	B	27	C
8	A	28	A
9	A	29	A
10	A	30	C
11	B	31	D
12	C	32	A
13	B	33	B
14	C	34	C
15	B	35	A
16	B	36	B
17	C	37	C
18	C	38	C
19	C	39	A
20	B	40	A

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER