PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.

B. Verify the client has granted network access to the hot site.

C. Determine if the failover environment relies on resources not owned by the client.

D. Establish communication and escalation procedures with the client.

Correct Answer: A

The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.

QUESTION 2

A penetration tester uncovered a flaw in an online banking web application that allows arbitrary requests to other internal network assets through a server-side request forgery. Which of the following would BEST reduce the risk of attack?

A. Implement multifactor authentication on the web application to prevent unauthorized access of the application.

B. Configure a secret management solution to ensure attackers are not able to gain access to confidential information.

C. Ensure a patch management system is in place to ensure the web server system is hardened.

D. Sanitize and validate all input within the web application to prevent internal resources from being accessed.

E. Ensure that enhanced logging is enabled on the web application to detect the attack.

Correct Answer: D

QUESTION 3

A penetration tester ran an Nmap scan on an Internet-facing network device with the –F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:

nmap –O –A –sS –p- 100.100.100.50

Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

A. A firewall or IPS blocked the scan.

B. The penetration tester used unsupported flags.

C. The edge network device was disconnected.

D. The scan returned ICMP echo replies.

Correct Answer: A

Reference: https://phoenixnap.com/kb/nmap-scan-open-ports

QUESTION 4

Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?

A. dig company.com MX

B. whois company.com

C. cur1 www.company.com

D. dig company.com A

Correct Answer: A

The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command dig company.com MX would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like company-com.mail.protection.outlook.com, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

QUESTION 5

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly

B. Monthly

C. Quarterly

D. Annually

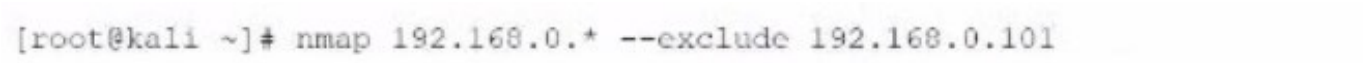
Correct Answer: C

Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard1. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network. https://www.pcicomplianceguide.org/faq/#25 PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

QUESTION 6

Given the following Nmap scan command:

[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101



Which of the following is the total number of servers that Nmap will attempt to scan?

A. 1

B. 101

C. 255

D. 256

Correct Answer: C

The Nmap scan command given will scan all the hosts in the 192.168.0.0/24 subnet, except for the one with the IP address 192.168.0.101. The subnet has 256 possible hosts, but one of them is excluded, so the total number of servers that

Nmap will attempt to scan is 255.

References:

Nmap Commands - 17 Basic Commands for Linux Network, Section: Scan Multiple Hosts, Subsection: Excluding Hosts from Search Nmap Cheat Sheet 2023: All the Commands and More, Section: Target Specification, Subsection: -exclude

QUESTION 7

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap

B. Nikto

C. Cain and Abel

D. Ethercap

Correct Answer: B

https://hackertarget.com/nikto-website-scanner/

QUESTION 8

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Netcat and cURL

C. Burp Suite and DIRB

D. Nmap and OWASP ZAP

Correct Answer: B

Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server. Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts. cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the "item" variable.

QUESTION 9

A penetration tester captured the following traffic during a web-application test:

```
GET http://172.16.0.10:3000/rest/basket/2 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI
iLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOi
JhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9k
ZWZhdWx0QWRtaW4uc3nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyM
DIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxldGVkQXQ
iOm5lbGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6NTYxMjM3MzU2Mn0.fKRquassopr9J5JO5YN1_Rji06e8zNGiE7vc0EfGM
JyKF0v_fAgv0yN9zTaYo1sU2dedd tkDVgwN9BiajjU-0B6eW9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8pSlpLqMlEiG-hwffOubKWiYBacH8-1d_SOK6ClgePjT7zxfcEqkM
Connection: keep-alive
Referer: http://172.16.0.10:3000/
Cookie: io=qiEk8j0ODPvlatUPAAAC; language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp
1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExv
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4uc5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0
aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxl
idGVkQXQiOm5lbGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6NTYxMjM3MzU2Mn0.fKRquassopr9J5JO5YN1_Rji06e8zNGiE7w
c0EfGMJyKF0v_fAgv0yN9zTaYo1sU2dcddtkDVgwN9BiajjU-0B6eW9Tj9d50hUGAJrE4tdmzPA8i4qlhtWz8pSlpLqMlEiG-hwffOubKWiYBacH8-1d_SOK6ClgePjT7zxfcEqkM
Content-Length: 0
Host: 172.16.0.10:3000
```

Which of the following methods should the tester use to visualize the authorization information being transmitted?

A. Decode the authorization header using UTF-8.

B. Decrypt the authorization header using bcrypt.

C. Decode the authorization header using Base64.

D. Decrypt the authorization header using AES.

Correct Answer: C

QUESTION 10

A penetration tester is testing a company\\'s public API and discovers that specific input allows the execution of arbitrary commands on the base operating system. Which of the following actions should the penetration tester take next?

A. Include the findings in the final report.

B. Notify the client immediately.

C. Document which commands can be executed.

D. Use this feature to further compromise the server.

Correct Answer: B

The Nmap command uses the Xmas scan technique, which sends packets with the FIN, PSH, and URG flags set. This is an attempt to bypass firewall rules and elicit a response from open ports. However, if the target responds with an RST packet, it means that the port is closed. Open ports will either ignore the Xmas scan packets or send back an ACK packet. Therefore, the information most likely indicates that all of the ports in the target range are closed. References: [Nmap Scan Types], [Nmap Port Scanning Techniques], [CompTIA PenTest+ Study Guide: Exam PT0-002, Chapter 4: Conducting Passive Reconnaissance, page 127]

QUESTION 11

A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

A. Configure wireless access to use a AAA server.

B. Use random MAC addresses on the penetration testing distribution.

C. Install a host-based firewall on the penetration testing distribution.

D. Connect to the penetration testing company\\'s VPS using a VPN.

Correct Answer: D

The best way to provide confidentiality for the client while using a wireless connection is to connect to the penetration testing company\\'s VPS using a VPN. This will encrypt the traffic between the penetration tester and the VPS, and prevent any eavesdropping or interception by third parties. A VPN will also allow the penetration tester to access the client\\'s network securely and bypass any firewall or network restrictions.

QUESTION 12

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA

B. MSA

C. SOW

D. MOU

Correct Answer: C

As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client\\'s information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

QUESTION 13

The attacking machine is on the same LAN segment as the target host during an internal penetration test. Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?

A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt

B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt

C. nmap PnsV OiL target.txt A target_text_Service

D. nmap sSPn n iL target.txt A target_txtl

Correct Answer: A

According to the Official CompTIA PenTest+ Self-Paced Study Guide1, the correct answer is A. nmap -sn -n -exclude 10.1.1.15 10.1.1.0/24 -oA target_txt. This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine\\'s IP address (10.1.1.15) from the scan (- exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

QUESTION 14

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client\\'s website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

A. -8 -T0

B. --script "http*vuln*"

C. -sn

D. -O -A

Correct Answer: B

Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n - T4 --open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with

the following options:

-p 445 specifies the port number to scan.

-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.

-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.

-Open only shows hosts that have open ports, which can reduce the output and focus on relevant results. The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time

sensitive.

QUESTION 15

Which of the following would a company\\'s hunt team be MOST interested in seeing in a final report?

A. Executive summary

B. Attack TTPs

C. Methodology

D. Scope details

Correct Answer: B