PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following OT protocols sends information in cleartext?

A. TTEthernet

B. DNP3

C. Modbus

D. PROFINET

Correct Answer: C

Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here\\'s an analysis of each protocol regarding whether it sends information in cleartext:

TTEthernet (Option A):

DNP3 (Option B):

Modbus (Answer: C):

PROFINET (Option D):

Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

QUESTION 2

During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

A. Clear the Windows event logs.

B. Modify the system time.

C. Alter the log permissions.

D. Reduce the log retention settings.

Correct Answer: A

During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are

removed. Here\\'s a detailed explanation of why clearing the Windows event logs is the best method for this scenario:

Understanding Windows Event Logs: Windows event logs are a key forensic artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential

security incidents.

Why Clear Windows Event Logs:

Method to Clear Event Logs:

shell

Copy code

wevtutil cl System wevtutil cl Security wevtutil cl Application uk.co.certification.simulator.questionpool.PList@18e830ed Alternative Options and Their Drawbacks: Case References: In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester\\'s actions remain undetected.

QUESTION 3

A penetration tester cannot find information on the target company\\'s systems using common OSINT methods. The tester\\'s attempts to do reconnaissance against internet- facing resources have been blocked by the company\\'s WAF. Which of the following is the best way to avoid the WAF and gather information about the target company\\'s systems?

A. HTML scraping

B. Code repository scanning

C. Directory enumeration

D. Port scanning

Correct Answer: B

When traditional reconnaissance methods are blocked, scanning code repositories is an effective method to gather information. Here\\'s why:

Code Repository Scanning:

Comparison with Other Methods:

Scanning code repositories allows gathering a wide range of information that can be critical for further penetration testing effort

QUESTION 4

SIMULATION A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets. INSTRUCTIONS Select the appropriate answer(s), given the output from each section. Output 1

Output 1 Output 2 Output 3

```
[*] Target: somecloudomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@somecloudomain.org
security@somecloudomain.org
info@somecloudomain.org
gfareau@somecloudomain.org
avapretta@somecloudomain.org
lastname@somecloudomain.org
researchIT@somecloudomain.org
ghstrowski@somecloudomain.org
conferencespeakers@somecloudomain.org

[*] Hosts found: 9
---------------------
academic-stores.somecloudomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudomain.org:198.134.5.32
connection.somecloudomain.org:13.107.246.51, 13.107.213.51
logins.somecloudomain.org:198.134.5.46
your.somecloudomain.org:52.173.139.125
ITpartners.somecloudomain.org:104.43.140.101
ls.somecloudomain.org:67.199.248.13, 67.199.248.12
stores.somecloudomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudomain.org:23.96.239.26
```

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudomain.org`

Output 1 Output 2 Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:   somecloudomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudomain.org
;; global options: +cmd
somecloudomain.org.    300  IN  A 245.62.183.182
somecloudomain.org.    300  IN  A 245.145.184.203
```

Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for somecloudddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: somecloudddomain.org

Select TWO commands that would produce the `nslookup` and `dig` output:

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois somecloudddomain.org

Domain Name: somecloudddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```

A. Check the answer in explanation.

Correct Answer:

Answer: See all the solutions below in Explanation.

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

Select TWO commands that would produce the `nslookup` and `dig` output:

- ☑ `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- ☐ `$ dig @192.168.20.66 somecloudddomain.org +short`
- ☐ `$ dig somecloudddomain.org +noall +short`
- ☑ `> nslookup somecloudddomain.org 8.8.8.8`
- ☐ `> nslookup somecloudddomain.org 192.168.20.66`
- ☐ `> nslookup somecloudddomain.org`

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon

Who registered the domain?

LocalComputerPro's, Inc.

When was the domain registered?

1993-09-22T04:00:38Z

QUESTION 5

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication

B. Public and private keys

C. Password encryption

D. Sessions and cookies

Correct Answer: D

QUESTION 6

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

A. ROE

B. SLA

C. MSA

D. NDA

Correct Answer: D

QUESTION 7

A penetration tester discovers evidence of an advanced persistent threat on the network that is being tested. Which of the following should the tester do next?

A. Report the finding.

B. Analyze the finding.

C. Remove the threat.

D. Document the finding and continue testing.

Correct Answer: A

Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.

Advanced Persistent Threat (APT):

Immediate Reporting:

Other Actions:

Pentest References:

Incident Response: Understanding the importance of immediate reporting and collaboration with the organization\\'s security team upon discovering critical threats like APTs. Ethical Responsibility: Following ethical guidelines and protocols to

ensure the organization can respond effectively to significant threats. By reporting the finding immediately, the penetration tester ensures that the organization\\'s security team is alerted to the presence of an APT, allowing them to initiate an

appropriate incident response.

QUESTION 8

During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop

B. Replay

C. Initialization vector

D. KRACK

Correct Answer: D

KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.

Understanding KRACK:

Attack Steps:

Impact:

Mitigation:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 9

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. certutil ?rlcache ?plit

Correct Answer: A

https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to- download-malware-while-bypassing-av/ --- https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

The certutil command is a Windows utility that can be used to manipulate certificates and certificate authorities. However, it can also be abused by attackers to download files from remote servers using the -urlcache option. In this case, the command downloads accesschk64.exe from http://192.168.2.124/windows-binaries/ and saves it locally. Accesschk64.exe is a tool that can be used to check service permissions and identify potential privilege escalation vectors. The other commands are not relevant for this purpose. Powershell is a scripting language that can be used to perform various tasks, but in this case it uploads a file instead of downloading one. Schtasks is a command that can be used to create or query scheduled tasks, but it does not help with service permissions. Wget is a Linux command that can be used to download files from the web, but it does not work on Windows by default.

QUESTION 10

A penetration tester is performing an assessment for an organization and must gather valid user credentials. Which of the following attacks would be best for the tester to use to achieve this objective?

A. Wardriving

B. Captive portal

C. Deauthentication

D. Impersonation

Correct Answer: D

Impersonation attacks involve the penetration tester assuming the identity of a valid user to gain unauthorized access to systems or information. This method is particularly effective for gathering valid user credentials, as it can involve tactics such as phishing, social engineering, or exploiting weak authentication processes. The other options, such as Wardriving, Captive portal, and Deauthentication, are more focused on wireless network vulnerabilities and are less direct in obtaining user credentials.

QUESTION 11

Which of the following should be included in scope documentation?

A. Service accounts

B. Tester experience

C. Disclaimer

D. Number of tests

Correct Answer: C

A disclaimer is a statement that limits the liability of the penetration tester and the client in case of any unintended

consequences or damages caused by the testing activities. It should be included in the scope documentation to clarify the roles and responsibilities of both parties and to avoid any legal disputes or misunderstandings. Service accounts, tester experience, and number of tests are not essential elements of the scope documentation, although they may be relevant for other aspects of the penetration testing process. References: The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 1: Planning and Scoping Penetration Tests1; The Official CompTIA PenTest+ Student Guide (Exam PT0002), Lesson 1: Planning and Scoping Penetration Tests2; What is the Scope of a Penetration Test?3

QUESTION 12

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client\\'s building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer

B. A mask and personal protective equipment

C. Caution tape for marking off insecure areas

D. A dedicated point of contact at the client

E. The paperwork documenting the engagement

F. Knowledge of the building\\'s normal business hours

Correct Answer: DE

Always carry the contact information and any documents stating that you are approved to do this.

QUESTION 13

During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

A. Segmentation

B. Mobile

C. External

D. Web

Correct Answer: C

An external assessment focuses on testing the security of internet-facing services. Here\\'s why option C is correct:

External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by

attackers from outside the organization\\'s network. Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It\\'s more relevant to internal network

architecture.

Mobile: This assessment targets mobile applications and devices, not general internet-facing services.

Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

References from Pentest:

Horizontall HTB: Highlights the importance of assessing external services to identify vulnerabilities that could be exploited from outside the network. Luke HTB: Demonstrates the process of evaluating public-facing services to ensure their

security.

Conclusion:

Option C, External, is the most appropriate type of assessment for targeting internet-facing services used by the client.

QUESTION 14

A penetration tester identified numerous flaws that could lead to unauthorized modification of critical data.

Which of the following would be best for the penetration tester to recommend?

A. Flat access

B. Role-based access control

C. Permission-based access control

D. Group-based control model

Correct Answer: B

RBAC is best for preventing unauthorized modification by assigning permissions to roles rather than individuals, ensuring that only authorized users can access critical data based on their role within the organization.

QUESTION 15

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing

B. Recon-ng

C. Social media

D. Password dumps

Correct Answer: C

When developing a phishing campaign, the tester should first use social media to gather information about the targets.

Social Media:

Process:

Other Options:

Pentest References:

Spear Phishing: A targeted phishing attack aimed at specific individuals, using personal information to increase the credibility of the email. OSINT (Open Source Intelligence): Leveraging publicly available information to gather intelligence on

targets, including through social media. By starting with social media, the penetration tester can collect detailed and personalized information about the targets, which is essential for creating an effective spear phishing campaign.