CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

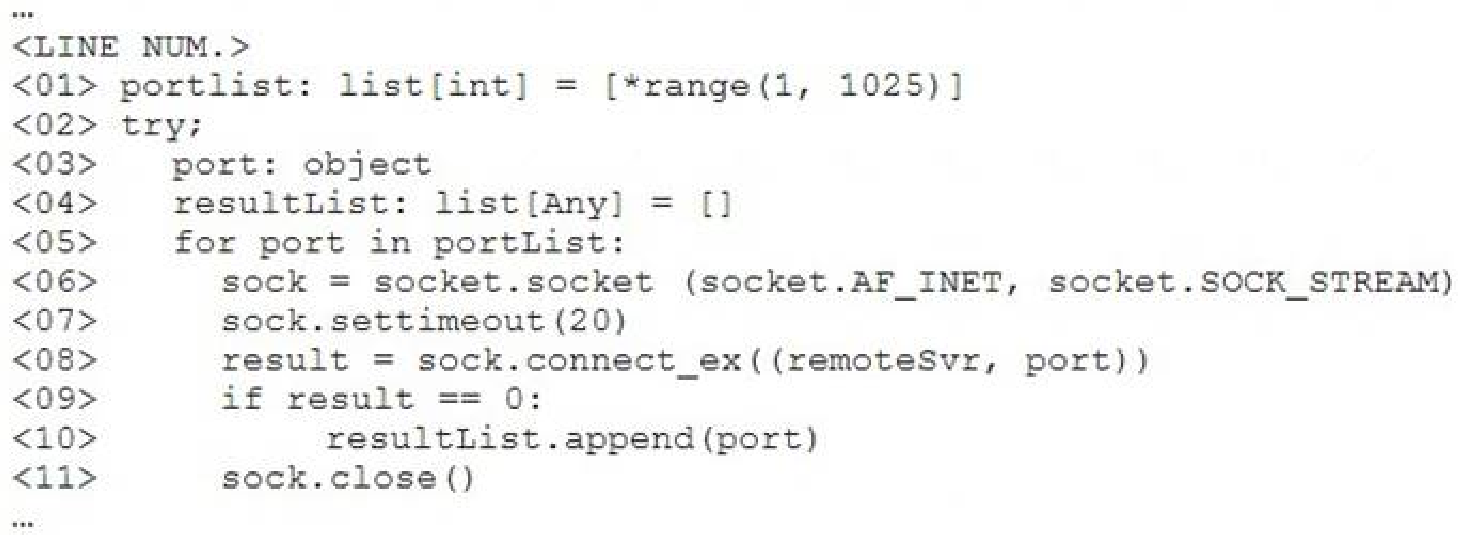
NEW QUESTION 1
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

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

Answer: A

Explanation:
Immunity Debugger is a tool that can be used to deconstruct 64-bit Windows binaries and see the underlying code. Immunity Debugger is a powerful debugger that integrates with Python and allows users to write their own scripts and plugins. It can be used for reverse engineering, malware analysis, vulnerability research, and exploit development

NEW QUESTION 2
A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:



```
...
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try;
<03>   port: object
<04>   resultList: list[Any] = []
<05>   for port in portList:
<06>     sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>     sock.settimeout(20)
<08>     result = sock.connect_ex((remoteSvr, port))
<09>     if result == 0:
<10>         resultList.append(port)
<11>     sock.close()
...
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
B. *range(1, 1025) on line 1 populated the portList list in numerical order.
C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM
D. The remoteSvr variable has neither been type-hinted nor initialized.

Answer: B

Explanation:
Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) https://nmap.org/book/man-port-specification.html

NEW QUESTION 3
A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Launch an external scan of netblocks.
B. Check WHOIS and netblock records for the company.
C. Use DNS lookups and dig to determine the external hosts.
D. Conduct a ping sweep of the company's netblocks.

Answer: C

NEW QUESTION 4
A company recently moved its software development architecture from VMs to containers. The company has asked a penetration tester to determine if the new containers are configured correctly against a DDoS attack. Which of the following should a tester perform first?

A. Test the strength of the encryption settings.
B. Determine if security tokens are easily available.
C. Perform a vulnerability check against the hypervisor.
D. .Scan the containers for open ports.

Answer: D

Explanation:
The first step that a tester should perform to determine if the new containers are configured correctly against a DDoS attack is to scan the containers for open ports. Open ports are entry points for network communication and can expose services or applications that may be vulnerable to DDoS attacks. Scanning the containers for open ports can help the tester identify which services or applications are running on the containers, and which ones may need to be secured or disabled to prevent DDoS attacks. Scanning the containers for open ports can also help the tester discover any unauthorized or malicious services or applications that may have been installed on the containers by previous attackers or compromised containers. Scanning the containers for open ports can be done by using tools such as Nmap, which can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The other options are not the first steps that a tester should perform to determine if the new containers are configured correctly against a DDoS attack. Testing the strength of the encryption settings is not relevant to DDoS attacks, as encryption does not prevent or mitigate DDoS attacks, but rather protects data confidentiality and integrity. Determining

if security tokens are easily available is not relevant to DDoS attacks, as security tokens are used for authentication and authorization, not for preventing or mitigating DDoS attacks. Performing a vulnerability check against the hypervisor is not relevant to DDoS attacks, as the hypervisor is not directly exposed to network traffic, but rather manages the virtual machines or containers that run on it.

NEW QUESTION 5
During the reconnaissance phase, a penetration tester obtains the following output:

```
Reply from 192.168.1.23: bytes=32 time<54ms TTL=128
Reply from 192.168.1.23: bytes=32 time<53ms TTL=128
Reply from 192.168.1.23: bytes=32 time<60ms TTL=128
Reply from 192.168.1.23: bytes=32 time<51ms TTL=128
```

Which of the following operating systems is MOST likely installed on the host?

A. Linux
B. NetBSD
C. Windows
D. macOS

Answer: C

Explanation:
The output shows the result of a ping command, which sends packets to a host and receives replies. The ping command can be used to determine if a host is alive and reachable on the network. One of the information that the ping command displays is the Time to Live (TTL) value, which indicates how many hops a packet can travel before it is discarded. The TTL value can also be used to guess the operating system of the host, as different operating systems have different default TTL values. In this case, the TTL value is 128, which is the default value for Windows operating systems. Linux and macOS have a default TTL value of 64, while NetBSD has a default TTL value of 255.

NEW QUESTION 6
Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

A. chmod u+x script.sh
B. chmod u+e script.sh
C. chmod o+e script.sh
D. chmod o+x script.sh

Answer: A

NEW QUESTION 7
A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks. To avoid disrupting this user’s work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

A. Add a web shell to the root of the website.
B. Upgrade the reverse shell to a true TTY terminal.
C. Add a new user with ID 0 to the /etc/passwd file.
D. Change the password of the root user and revert after the test.

Answer: C

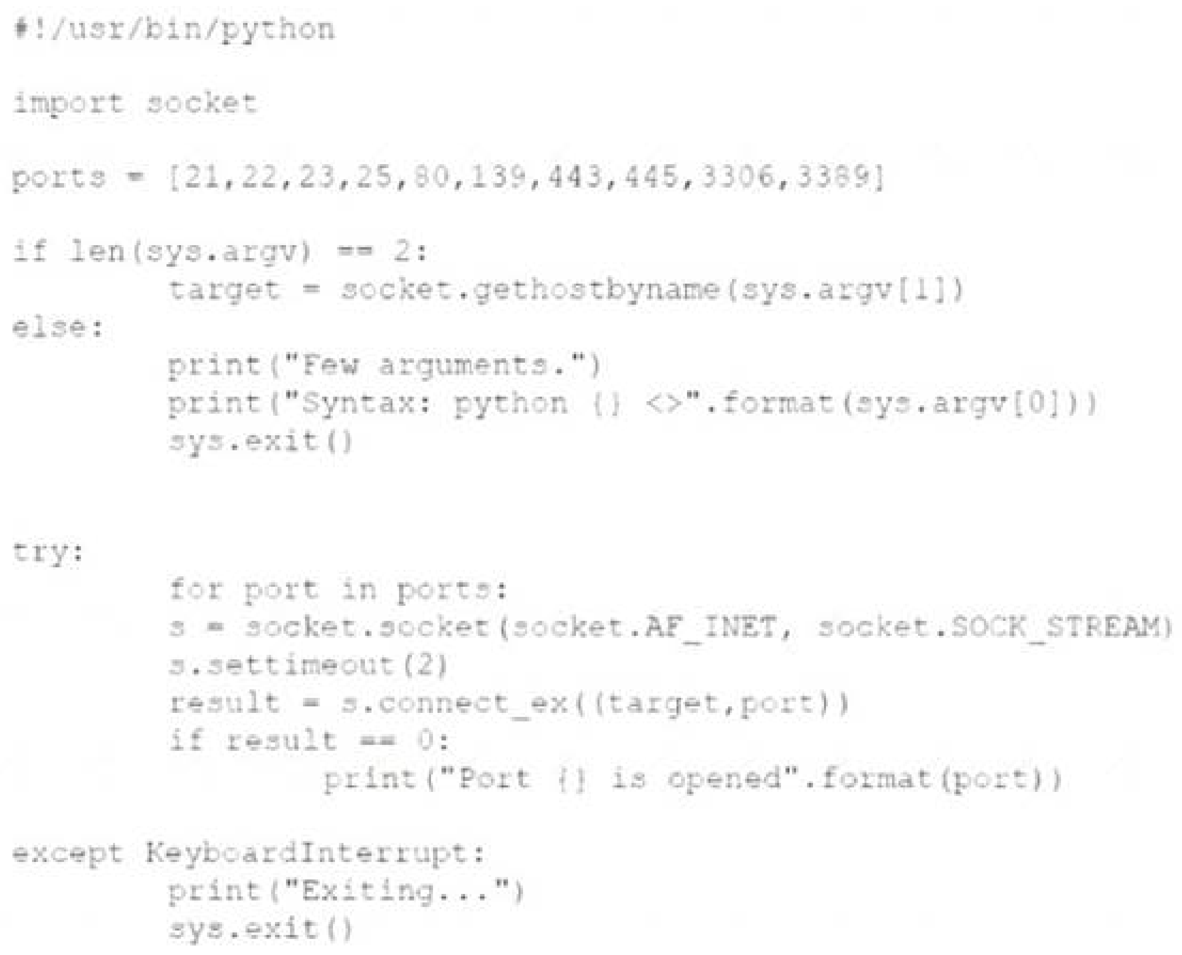
Explanation:
The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won’t disrupt the other user’s work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is “johndoe”, the line to add would be “johndoe:x:0:0:John Doe:/root:/bin/bash”. After the user is added, the penetration tester can use the “su” command to switch to the new user and gain root privileges.

NEW QUESTION 8
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

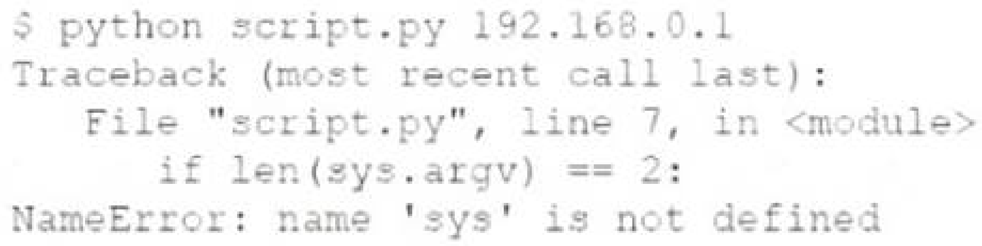
Answer: B

NEW QUESTION 9
A penetration tester created the following script to use in an engagement:



```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("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)
        result = s.connect_ex((target,port))
        if result == 0:
                print("Port {} is opened".format(port))

except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

However, the tester is receiving the following error when trying to run the script:



```
$ python script.py 192.168.0.1
Traceback (most recent call last):
   File "script.py", line 7, in <module>
      if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

A. The sys variable was not defined.
B. The argv variable was not defined.
C. The sys module was not imported.
D. The argv module was not imported.

Answer: C

Explanation:
The sys module is a built-in module in Python that provides access to system-specific parameters and functions, such as command-line arguments, standard input/output, and exit status. The sys module must be imported before it can be used in a script, otherwise an error will occur. The script uses the sys.argv variable, which is a list that contains the command-line arguments passed to the script. However, the script does not import the sys module at the beginning, which causes the error “NameError: name ‘sys’ is not defined”. To fix this error, the script should include the statement “import sys” at the top. The other options are not valid reasons for the error.

NEW QUESTION 10
A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:
U3VQZXIkM2NyZXQhCg==
Which of the following commands should the tester use NEXT to decode the contents of the file?

A. echo U3VQZXIkM2NyZXQhCg== | base64 €"d
B. tar zxvf password.txt
C. hydra €"l svsacct €"p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Answer: A

NEW QUESTION 10
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 11
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

Explanation:
The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

NEW QUESTION 13
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

A. A quick description of the vulnerability and a high-level control to fix it
B. Information regarding the business impact if compromised
C. The executive summary and information regarding the testing company
D. The rules of engagement from the assessment

Answer: A

Explanation:
The systems administrator and the technical stuff would be more interested in the technical aspect of the findings

NEW QUESTION 14
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 18
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

Explanation:
s for why the penetration tester wants this command executed.

NEW QUESTION 22
Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB
B. Metasploit
C. Shodan
D. Retina

Answer: A

Explanation:
"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"
Exploit-DB is a website that collects and archives exploits for various software and hardware products, including network infrastructure devices. Exploit-DB allows users to search for exploits by product name, vendor, type, platform, CVE number, or date. Exploit-DB is a useful resource for obtaining payloads against specific network infrastructure products. Metasploit is a framework that contains many exploits and payloads, but it is not a resource for obtaining them. Shodan is a search engine that scans the internet for devices and services, but it does not provide exploits or payloads. Retina is a vulnerability scanner that identifies weaknesses in network devices, but it does not provide exploits or payloads.

NEW QUESTION 26
Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The

penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

A. Alert the target company of the discovered information.
B. Verify the discovered information is correct with the manufacturer.
C. Scan the equipment and verify the findings.
D. Return to the dumpster for more information.

Answer: C

Explanation:
The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information1, or Metasploit, which can exploit hosts and networks using various payloads or modules2. The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

NEW QUESTION 31
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.
Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

NEW QUESTION 33
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62
Which of the following commands can be used to further attack the website?

A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
B. ../../../../../../../../../../etc/passwd
C. /var/www/html/index.php;whoami
D. 1 UNION SELECT 1, DATABASE(),3-

Answer: D

NEW QUESTION 36
A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room
B. Climbing in an open window of the adjoining building
C. Presenting a false employee ID to the night guard
D. Obstructing the motion sensors in the hallway of the records room

Answer: B

Explanation:
The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D. Option C is also not allowed, as it involves social engineering, which is not part of the scope. Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room. This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

NEW QUESTION 41
A company that developers embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse- engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

A. The reverse-engineering team may have a history of selling exploits to third parties.
B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.

C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
D. The reverse-engineering team will be given access to source code for analysis.

Answer: A

NEW QUESTION 42
A penetration tester conducted an assessment on a web server. The logs from this session show the following:
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ‘ ; DROP TABLE SERVICES; -
Which of the following attacks is being attempted?

A. Clickjacking
B. Session hijacking
C. Parameter pollution
D. Cookie hijacking
E. Cross-site scripting

Answer: C

NEW QUESTION 45
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

Explanation:
These two options best describe the OWASP Top 10, which stands for Open Web Application Security Project Top 10 and is a list of the most critical web application security risks based on data from various sources and experts. The list is updated periodically to reflect changes in technology and threat landscape. The list also ranks the risks in order of importance based on their prevalence, impact, and ease of exploitation or remediation. The other options are not accurate descriptions of the OWASP Top 10. The list does not cover all the risks of web applications, but rather focuses on the most common and severe ones. The list is not a web application security standard, but rather a guideline or reference for developers, testers, and security professionals. The list is not a risk-governance and compliance framework, but rather a resource or tool for identifying and mitigating web application vulnerabilities. The list is not a checklist of Apache vulnerabilities, but rather a general list of web application risks that apply to any web server or platform.

NEW QUESTION 47
A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

A. nmap -sn 10.12.1.0/24
B. nmap -sV -A 10.12.1.0/24
C. nmap -Pn 10.12.1.0/24
D. nmap -sT -p- 10.12.1.0/24

Answer: A

NEW QUESTION 50
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 53
Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements
B. To discuss the findings and dispute any false positives
C. To determine any processes that failed to meet expectations during the assessment
D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Answer: C

NEW QUESTION 55
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: AD

Explanation:
* A. IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company’s web presence. IP addresses can reveal the location, network, and service provider of the company’s web servers, while subdomains can indicate the different functions and features of the company’s website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company’s domain name.
* D. Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company’s web presence. Search engines can provide a wealth of information, such as the company’s profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results the title of the web pages.

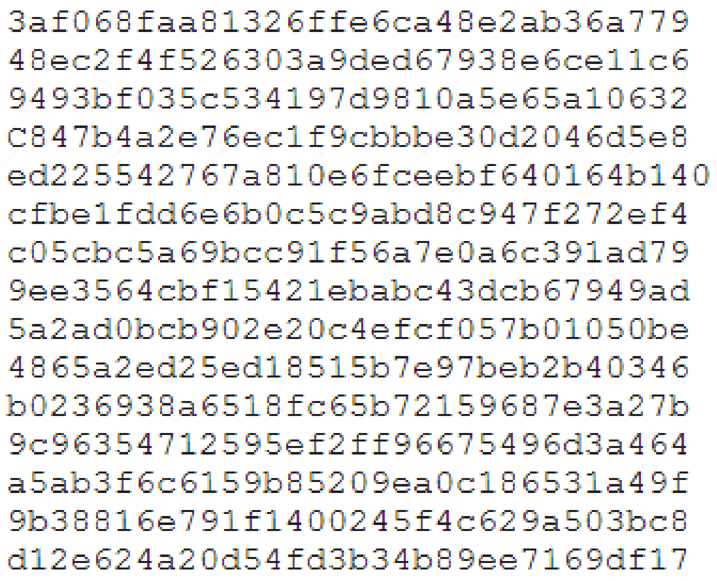
NEW QUESTION 56
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly
B. Monthly
C. Quarterly
D. Annually

Answer: C

Explanation:
Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard1. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.
https://www.pcicomplianceguide.org/faq/#25
PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

NEW QUESTION 57
During an engagement, a penetration tester found the following list of strings inside a file:



```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
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 58
A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

A. Weak authentication schemes
B. Credentials stored in strings
C. Buffer overflows
D. Non-optimized resource management

Answer: C

Explanation:
fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

NEW QUESTION 63
When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

A. security compliance regulations or laws may be violated.
B. testing can make detecting actual APT more challenging.
C. testing adds to the workload of defensive cyber- and threat-hunting teams.
D. business and network operations may be impacted.

Answer: D

NEW QUESTION 65
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 66
During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ------------company systems?

A. Aside-channel attack
B. A command injection attack
C. A watering-hole attack
D. A cross-site scripting attack

Answer: C

Explanation:
The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

NEW QUESTION 69
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 70
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

Explanation:
The best method available to pivot and gain additional access to the network is to span deauthentication packets to the wireless clients. This will cause them to disconnect from their wireless access point and reconnect using their hard-wired connection, which may have less restrictive ACLs. The penetration tester can then capture their traffic or attempt to compromise their systems.

NEW QUESTION 71
Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

A. NIST SP 800-53
B. ISO 27001
C. GDPR

Answer: C

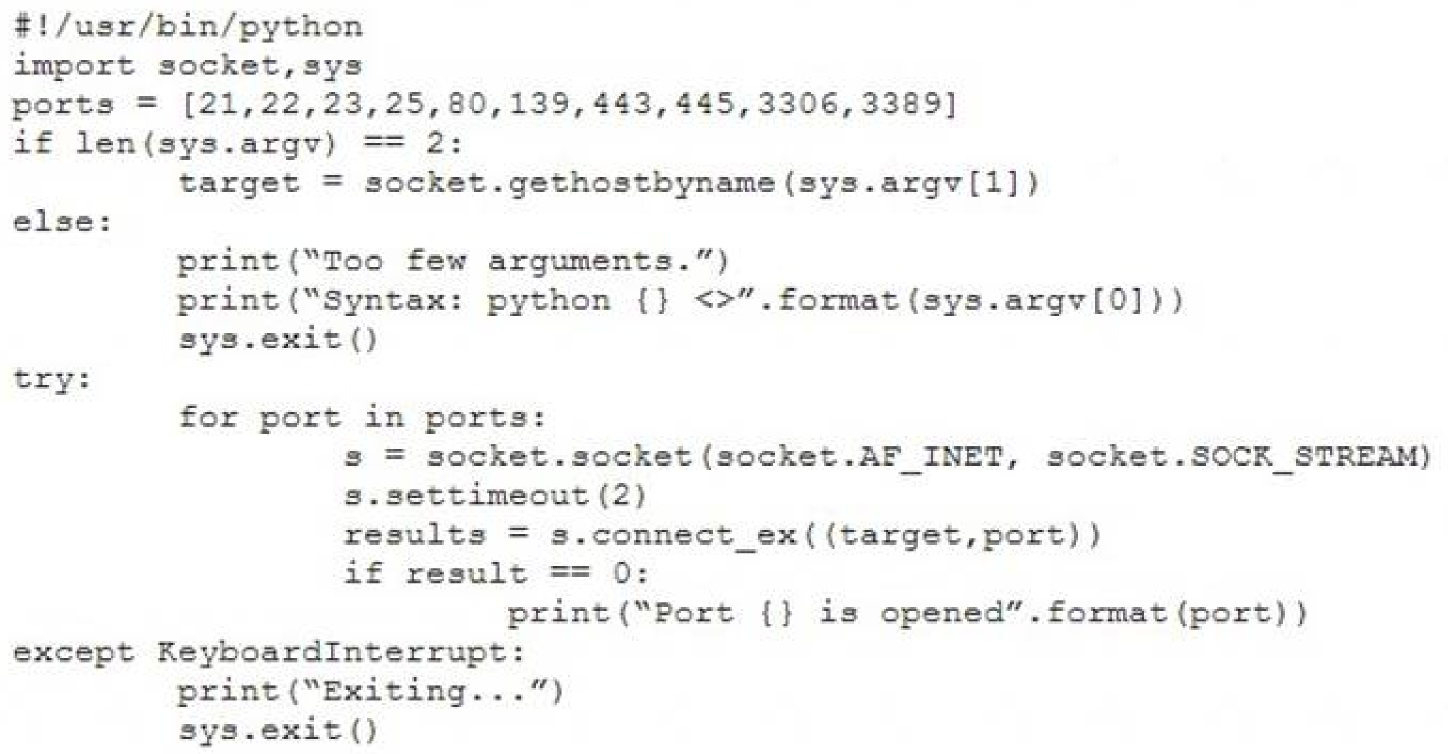
Explanation:
GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.

NEW QUESTION 73
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 77
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

Explanation:
The script will perform a port scan on the target IP address, looking for open ports on a list of common ports. A port scan is a technique that probes a network or a system for open ports, which can reveal potential vulnerabilities or services running on the host.

NEW QUESTION 81
A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?

A. Steganography
B. Metadata removal
C. Encryption
D. Encode64

Answer: B

Explanation:
All other answers are a form of encryption or randomizing the data.

NEW QUESTION 85
Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

A. The team exploits a critical server within the organization.

B. The team exfiltrates PII or credit card data from the organization.
C. The team loses access to the network remotely.
D. The team discovers another actor on a system on the network.

Answer: D

NEW QUESTION 88
During an assessment, a penetration tester was able to access the organization's wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption
B. Using directional antennae
C. Using WEP encryption
D. Disabling Wi-Fi

Answer: A

Explanation:
If a penetration tester was able to access the organization’s wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrack-ng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

NEW QUESTION 89
An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

A. nmap -"T3 192.168.0.1
B. nmap - "P0 192.168.0.1
C. nmap - T0 192.168.0.1
D. nmap - A 192.168.0.1

Answer: C

NEW QUESTION 90
Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

A. Shodan
B. Nmap
C. WebScarab-NG
D. Nessus

Answer: B

NEW QUESTION 92
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

Explanation:
Open-source research and traffic sniffing are two activities that have a minimal chance of detection, as they do not involve sending any packets or requests to the target network or system. Open-source research is the process of gathering information from publicly available sources, such as websites, social media, blogs, forums, etc. Traffic sniffing is the process of capturing and analyzing network packets that are transmitted over a shared medium, such as wireless or Ethernet.

NEW QUESTION 95
A compliance-based penetration test is primarily concerned with:

A. obtaining PII from the protected network.
B. bypassing protection on edge devices.
C. determining the efficacy of a specific set of security standards.
D. obtaining specific information from the protected network.

Answer: C

NEW QUESTION 100
Penetration tester is developing exploits to attack multiple versions of a common software package. The versions have different menus and)ut.. they have a

common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

A. Conditional
B. Library
C. Dictionary
D. Sub application

Answer: B

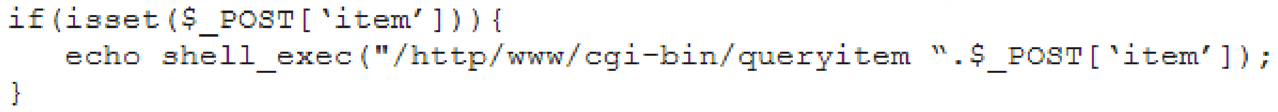
Explanation:
The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example. Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements. Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

NEW QUESTION 101
A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment
B. Report distribution
C. Testing restrictions
D. Liability

Answer: B

NEW QUESTION 102
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

Explanation:
Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server. Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts. cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the “item” variable.

NEW QUESTION 105
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 107
A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

A. Shoulder surfing
B. Call spoofing
C. Badge stealing

D. Tailgating
E. Dumpster diving
F. Email phishing

Answer: CD

NEW QUESTION 108
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.

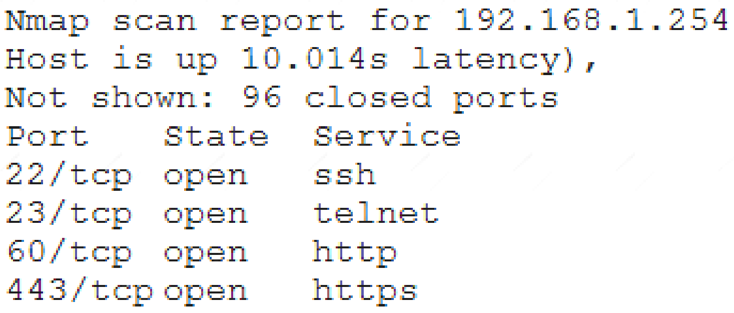
NEW QUESTION 113
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

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 116
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 119
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

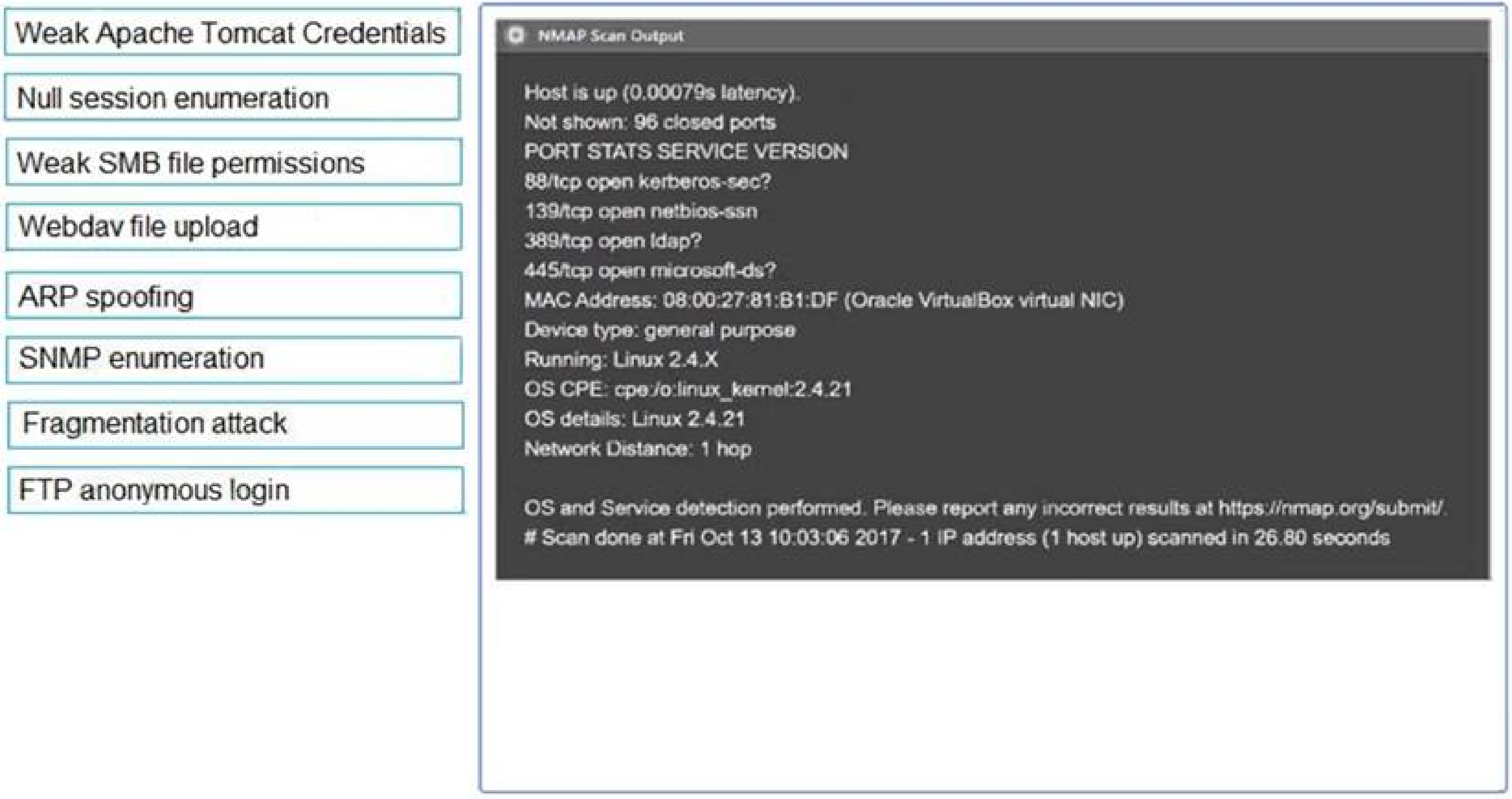
Explanation:
W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

NEW QUESTION 123
A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.
Which of the following should the tester verify FIRST to assess this risk?

A. Whether sensitive client data is publicly accessible
B. Whether the connection between the cloud and the client is secure
C. Whether the client's employees are trained properly to use the platform
D. Whether the cloud applications were developed using a secure SDLC

Answer: A

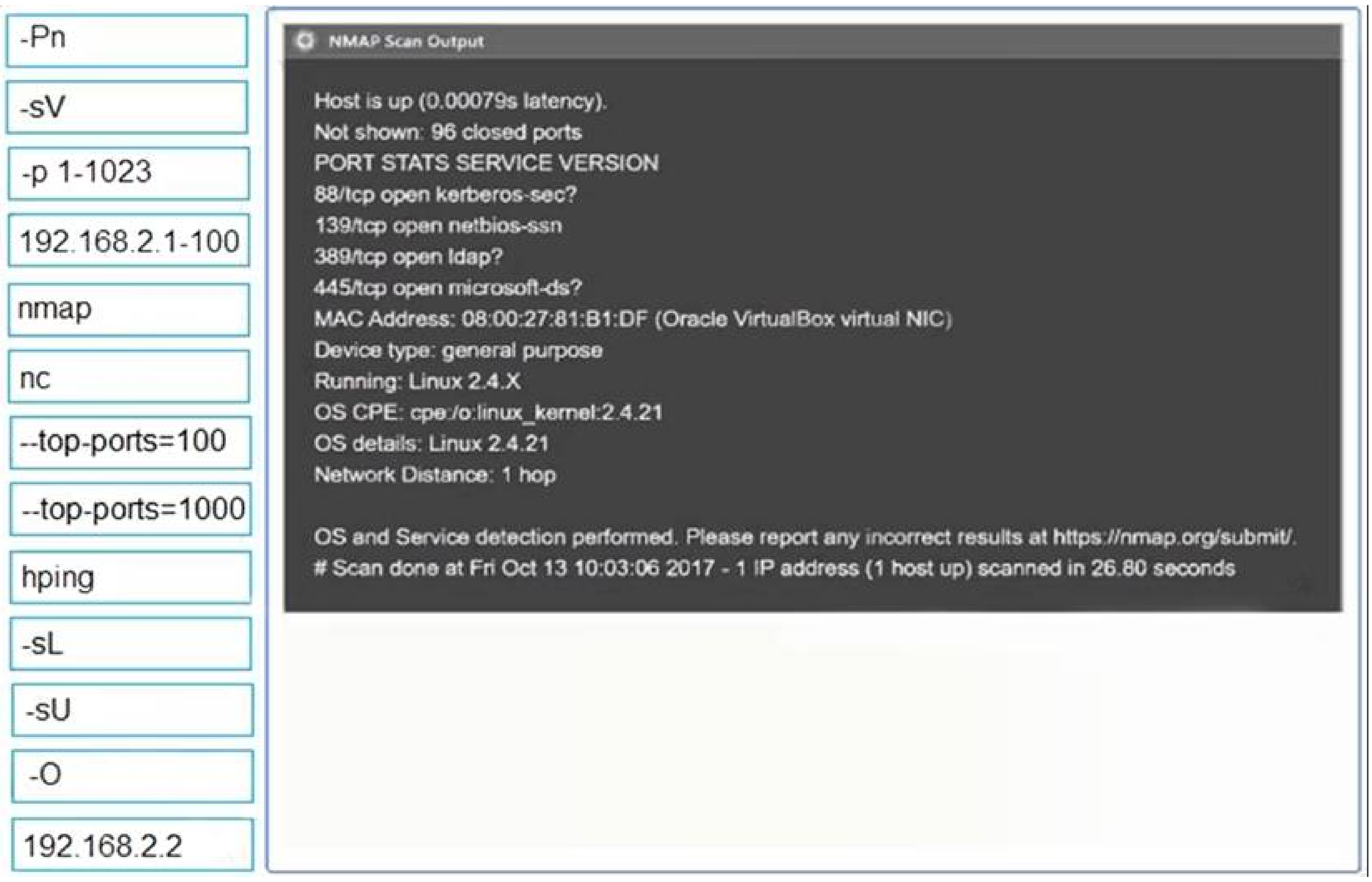
NEW QUESTION 124
SIMULATION
Using the output, identify potential attack vectors that should be further investigated.



Weak Apache Tomcat Credentials
Null session enumeration
Weak SMB file permissions
Webdav file upload
ARP spoofing
SNMP enumeration
Fragmentation attack
FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```



-Pn
-sV
-p 1-1023
192.168.2.1-100
nmap
nc
--top-ports=100
--top-ports=1000
hping
-sL
-sU
-O
192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

```
ports – [21, 22]
```

```
{:ports => 21:ports => 22}
```

```
#!/usr/bin/python
```

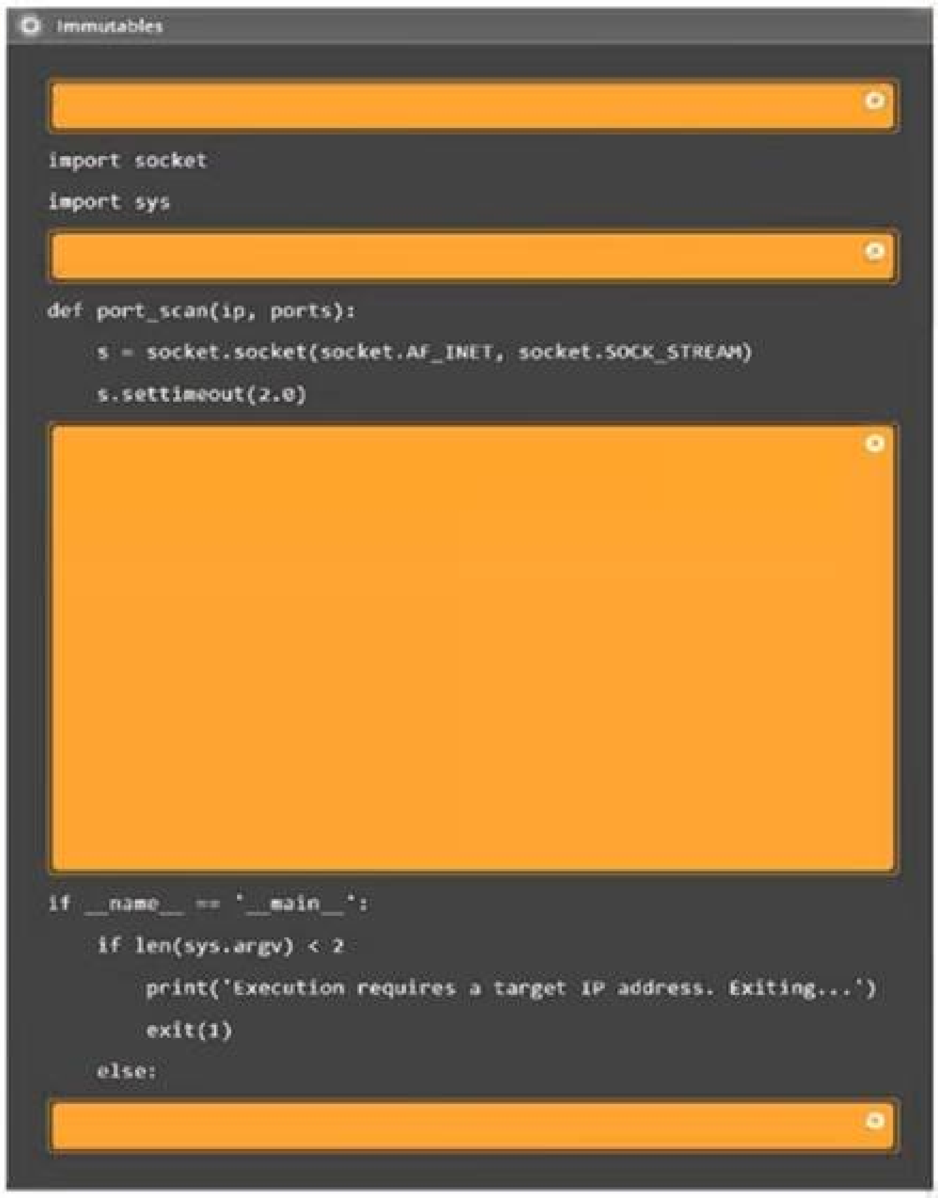
```
for $PORT in $PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s – OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s – TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s – CLOSED" % (ip, port))

    finally:
        s.close()
```

```
export $PORTS = 21,22
```

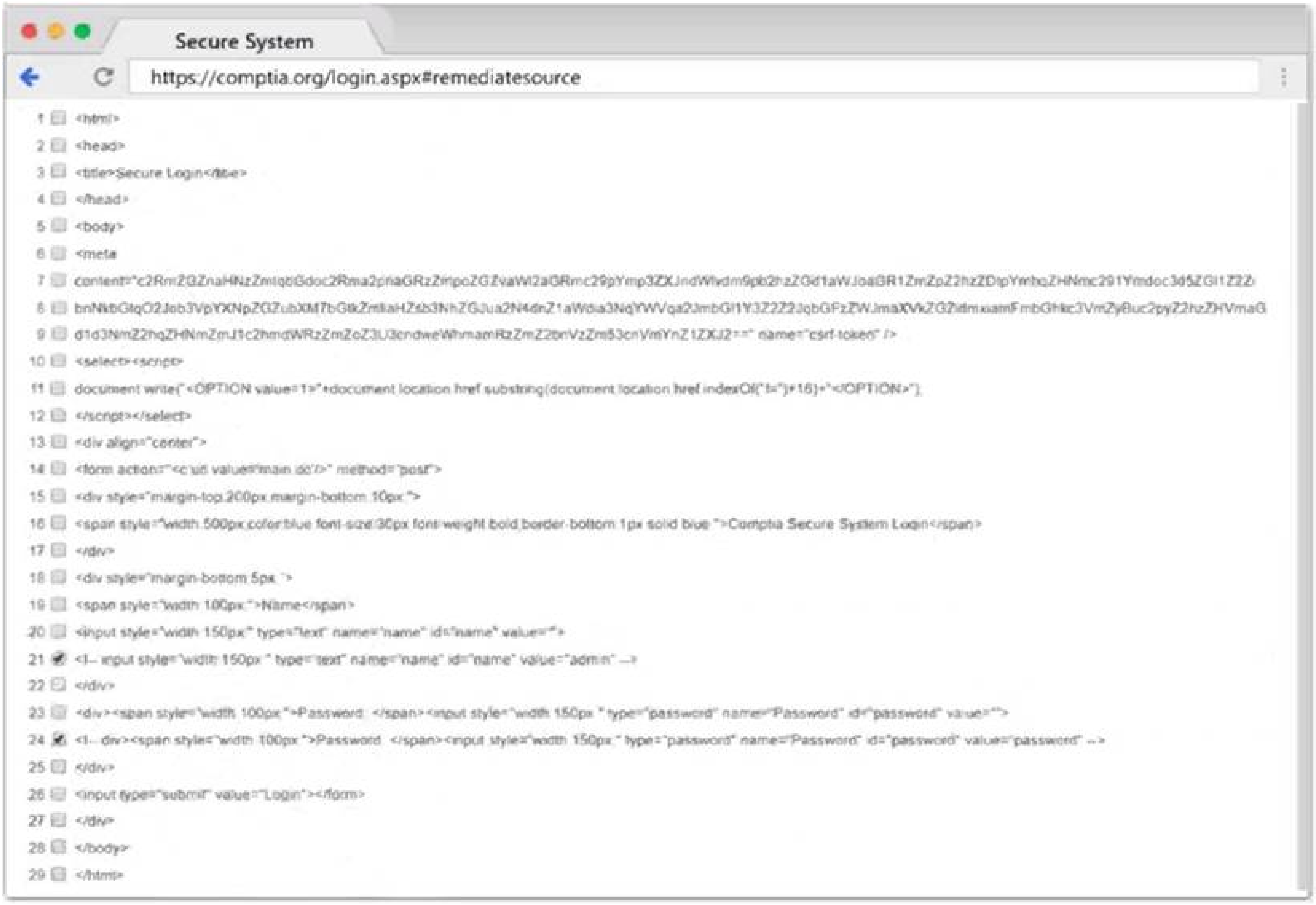
```
#!/usr/bin/ruby
```

```
#!/usr/bin/bash
```

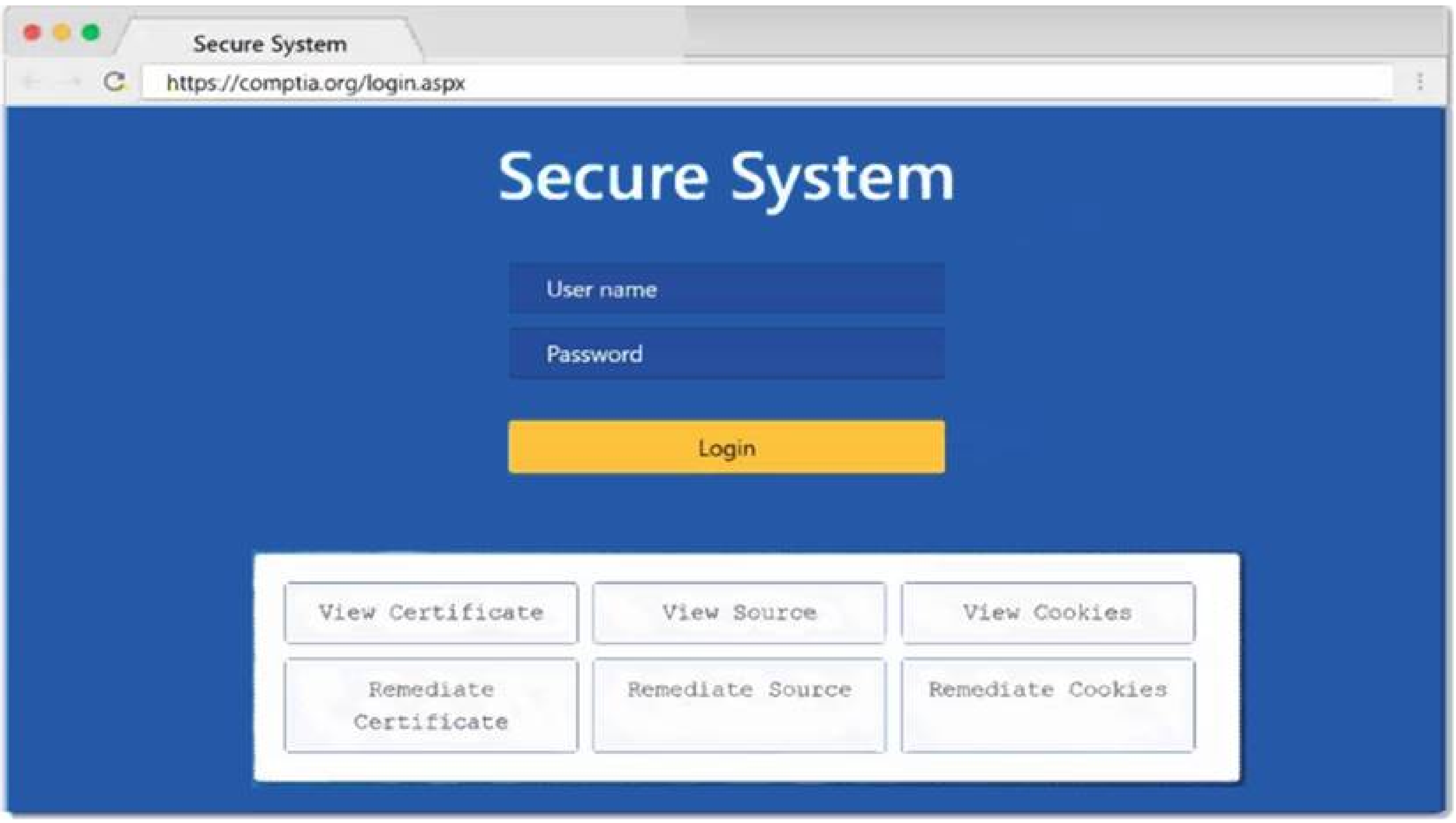
```
for port in ports:
```



```
import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```



```
1 ☐ <html>
2 ☐ <head>
3 ☐ <title>Secure Login</title>
4 ☐ </head>
5 ☐ <body>
6 ☐ <meta
7 ☐ content="c2RmZGZnaHNzZmlqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDlpYmhqZHNmc291Ymdoc3d5ZGl1Z2Zi
8 ☐ bnNkbGlqO2Job3VpYXNpZGZubXM7bGtkZmlaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 ☐ d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
10 ☐ <select><script>
11 ☐ document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("t=")+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" -->
25 ☐ </div>
26 ☐ <input type="submit" value="Login"></form>
27 ☐ </div>
28 ☐ </body>
29 ☐ </html>
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:
1: Null session enumeration Weak SMB file permissions Fragmentation attack
2: nmap
-sV
-p 1-1023
* 192.168.2.2
3: #!/usr/bin/python export $PORTS = 21,22 for $PORT in $PORTS: try:
s.c onnect((ip, port))
print("%s:%s – OPEN" % (ip, port)) except socket.timeout
print("%:%s – TIMEOUT" % (ip, port)) except socket.error as e:
print("%:%s – CLOSED" % (ip, port)) finally
s.close() port_scan(sys.argv[1], ports)

NEW QUESTION 128
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53
B. OWASP Top 10
C. MITRE ATT&CK framework
D. PTES technical guidelines

Answer: C

NEW QUESTION 129
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

Explanation:
Successful exploits could cause network disruptions, service outages, or data corruption, which could affect the connectivity and functionality of the oil rig network. Patch installations, application failures, and bandwidth limitations are less likely to be related to the penetration testing activities.

NEW QUESTION 133
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

Explanation:
The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.

NEW QUESTION 136
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 137
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes
B. IP addresses
C. Encrypted file transfers
D. User hashes sent over SMB

Answer: B

NEW QUESTION 138
The output from a penetration testing tool shows 100 hosts contained findings due to improper patch management. Which of the following did the penetration tester perform?

A. A vulnerability scan
B. A WHOIS lookup
C. A packet capture
D. An Nmap scan

Answer: A

Explanation:
A vulnerability scan is a type of penetration testing tool that is used to scan a network for vulnerabilities. A vulnerability scan can detect misconfigurations, missing patches, and other security issues that could be exploited by attackers. In this case, the output shows that 100 hosts had findings due to improper patch management, which means that the tester performed a vulnerability scan.

NEW QUESTION 141
......