PT0-002 Q&As

CompTIA PenTest+

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester is working to enumerate the PLC devices on the 10.88.88.76/24 network. Which of the following commands should the tester use to achieve the objective in a way that minimizes the risk of affecting the PLCs?

A. nmap --script=s7-info -p 102 10.88.88.76/24 -T3

B. nmap --script=wsdd-discover -p 3702 -sUlO.88.88.76/24

C. nmap --script=iax2-version -p 4569 -sU -V 10.88.88.76/24 -T2

D. nmap --script=xll-access -p 6000-6009 10.88.88.76/24

Correct Answer: A

The nmap command with the --script=s7-info is specifically designed to interact with Siemens S7 PLCs, which are common industrial control systems. The -p 102 specifies the port associated with Siemens S7 communications. The -T3 timing option is chosen to minimize the risk of impacting the PLCs by not being overly aggressive in the scan timing, which is important in operational technology environments where PLCs can be sensitive to high network traffic. The other options listed do not specifically target PLC devices or use appropriate timing to minimize risk.

QUESTION 2

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

A. Vulnerability scanning

B. Network segmentation

C. System hardening

D. Intrusion detection

Correct Answer: B

Network segmentation is the practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, security level, or access control. Network segmentation can enhance the security of a network by isolating sensitive or critical systems from less secure or untrusted systems, reducing the attack surface, limiting the spread of malware or intrusions, and enforcing granular policies and rules for each segment. To be PCI compliant, which is a set of standards for protecting payment card data, the company should have implemented network segmentation to separate the servers that perform financial transactions from other parts of the network that may be less secure or more exposed to threats. The other options are not specific requirements for PCI compliance, although they may be good security practices in general.

QUESTION 3

A penetration tester breaks into a company\\'s office building and discovers the company does not have a shredding service. Which of the following attacks should the penetration tester try next?

A. Dumpster diving

B. Phishing

C. Shoulder surfing

D. Tailgating

Correct Answer: A

The penetration tester should try dumpster diving next, which is an attack that involves searching through trash bins or dumpsters for discarded documents or items that may contain sensitive or useful information. Dumpster diving can reveal information such as passwords, account numbers, credit card numbers, invoices, receipts, memos, contracts, or employee records. The penetration tester can use this information to gain access to systems or networks, impersonate users or employees, or perform social engineering attacks. The other options are not likely attacks that the penetration tester should try next based on the discovery that the company does not have a shredding service. Phishing is an attack that involves sending fraudulent emails that appear to be from legitimate sources to trick users into revealing their credentials or clicking on malicious links or attachments. Shoulder surfing is an attack that involves observing or spying on users while they enter their credentials or perform other tasks on their devices. Tailgating is an attack that involves following authorized personnel into a restricted area without proper authorization or identification.

QUESTION 4

A penetration tester requested, without express authorization, that a CVE number be assigned for a new vulnerability found on an internal client application. Which of the following did the penetration tester most likely breach?

A. ROE

B. SLA

C. NDA

D. SOW

Correct Answer: A

ROE stands for Rules of Engagement, which are the guidelines and limitations that define the scope, objectives, and methods of a penetration testing engagement. ROE should be agreed upon by both the client and the tester before the testing begins, and they should include the authorization to perform certain actions, such as requesting CVE numbers, disclosing vulnerabilities, or exploiting systems. By requesting a CVE number without express authorization, the penetration tester most likely breached the ROE and violated the client\\'s trust and expectations.

QUESTION 5

Which of the following tools would be best to use to conceal data in various kinds of image files?

A. Kismet

B. Snow

C. Responder

D. Metasploit

Correct Answer: B

Snow is a tool designed for steganography, which is the practice of concealing messages or information within other non-secret text or data. In this context, Snow is specifically used to hide data within whitespace of text files, which can include the whitespace areas of images saved in formats that support text descriptions or metadata, such as certain PNG or JPEG files. While the other tools listed (Kismet, Responder, Metasploit) are powerful in their respective areas (network sniffing, LLMNR/NBT-NS poisoning, and exploitation framework), they do not offer functionality related to data concealment in image files or steganography.

QUESTION 6

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

A. Shodan

B. Nmap

C. WebScarab-NG

D. Nessus

Correct Answer: B

QUESTION 7

DRAG DROP

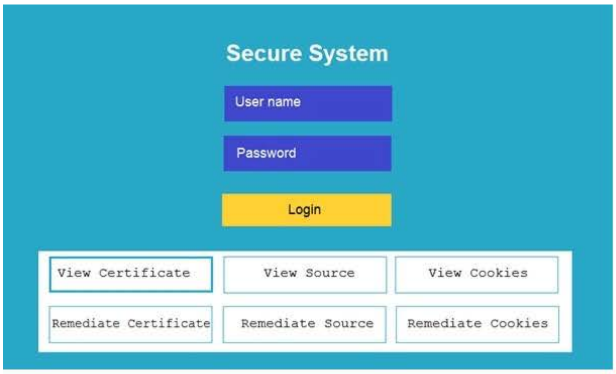
You are a penetration tester reviewing a client\\'s website through a web browser.

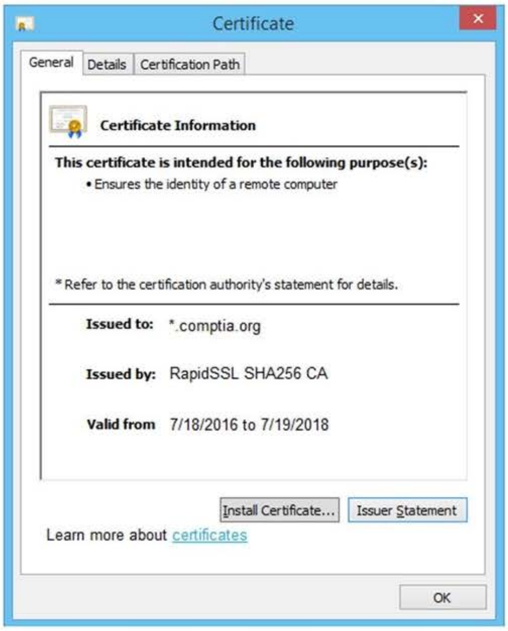
INSTRUCTIONS

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

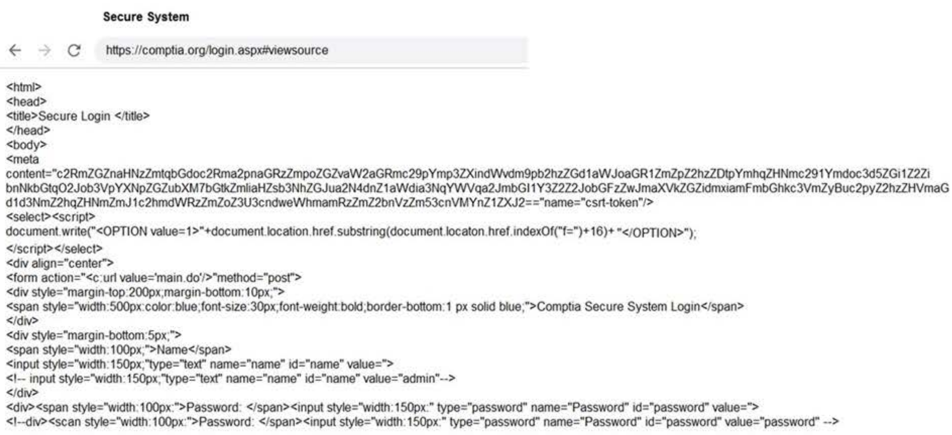
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

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

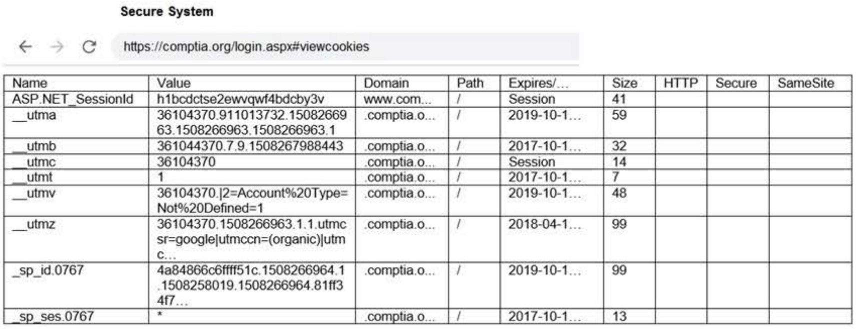
Learn more about certificates



Secure System

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

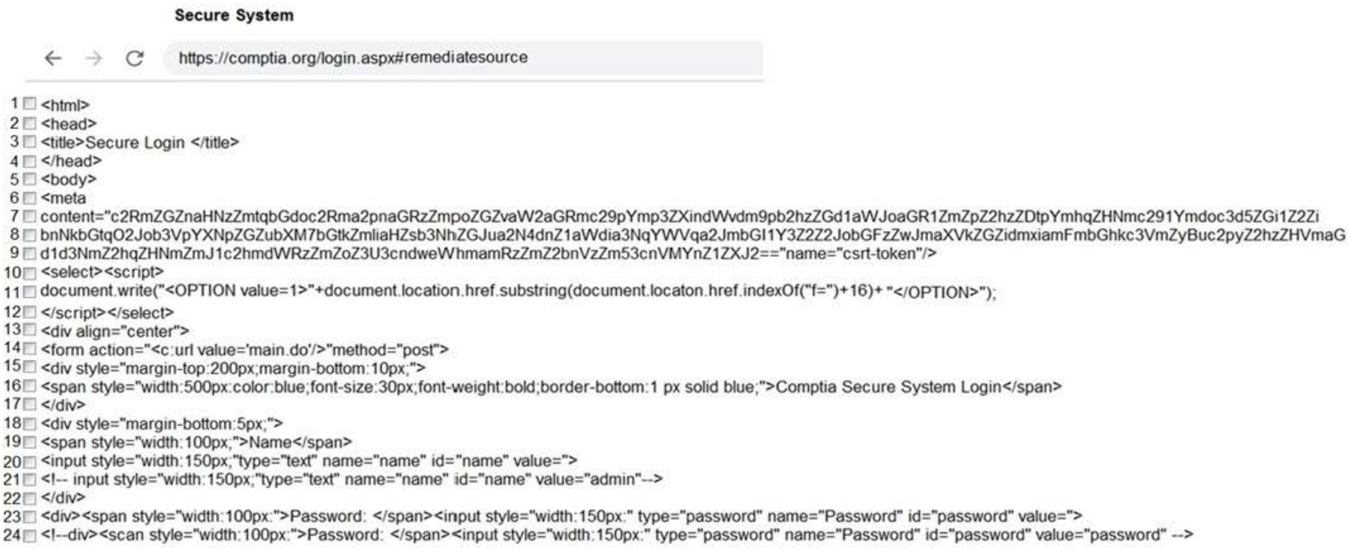
```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
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

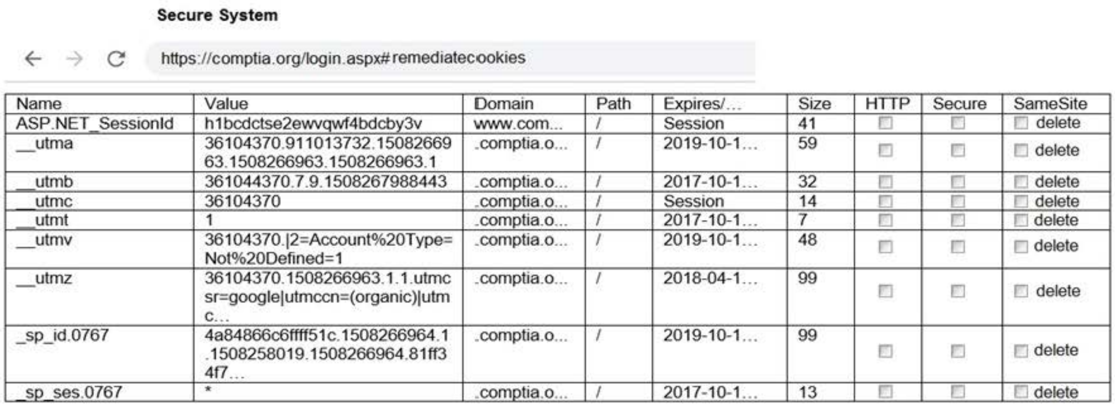
Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			



Secure System

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

```
1 □ <html>
2 □ <head>
3 □ <title>Secure Login </title>
4 □ </head>
5 □ <body>
6 □ <meta
7 □ content="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" -->
```

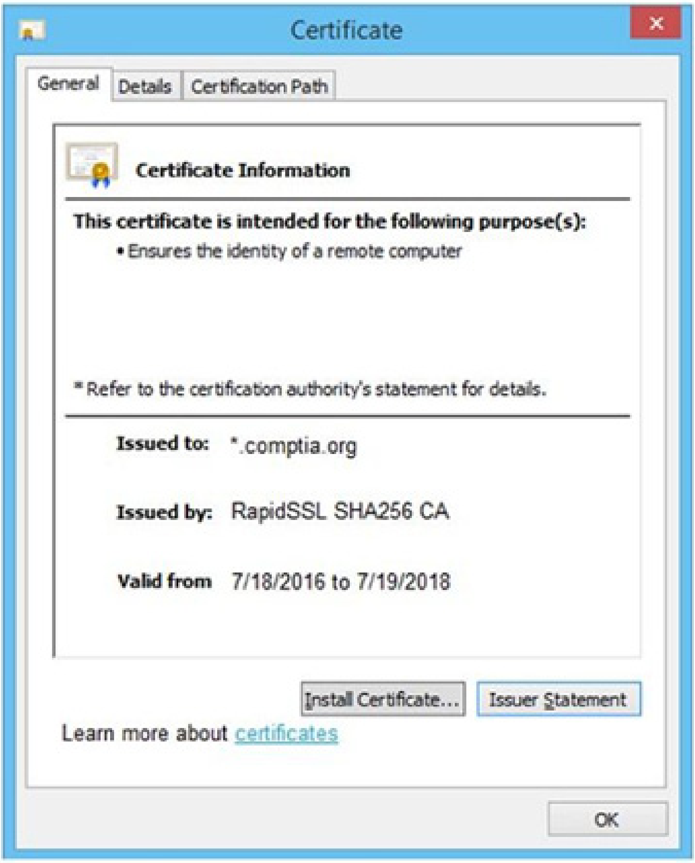


Secure System

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	36104370.911013732.1508266963.1508266963.1508266963.1	.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.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	□	□	□ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.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

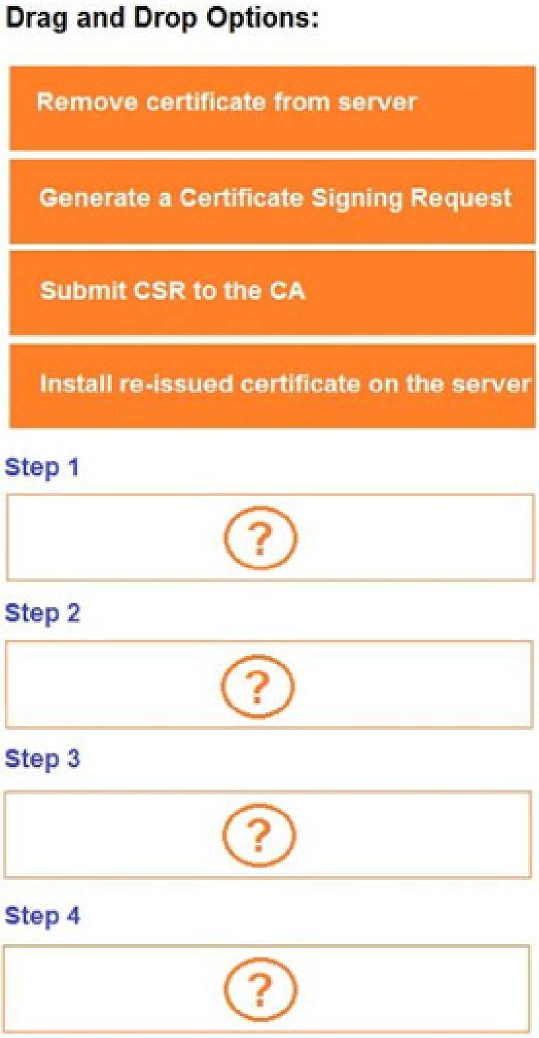
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

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

Learn more about certificates



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

?

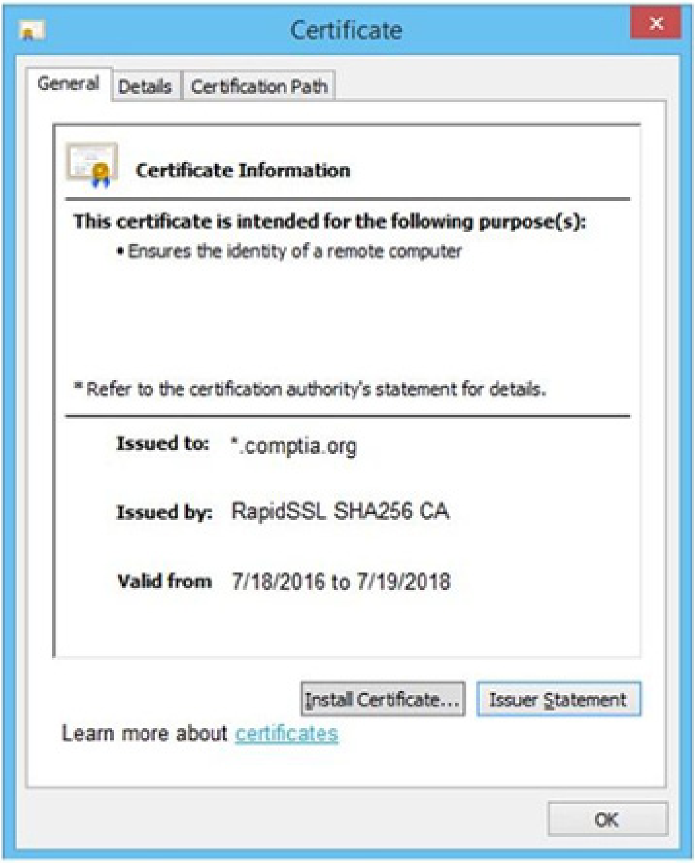
Step 3

?

Step 4

?

Correct Answer:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

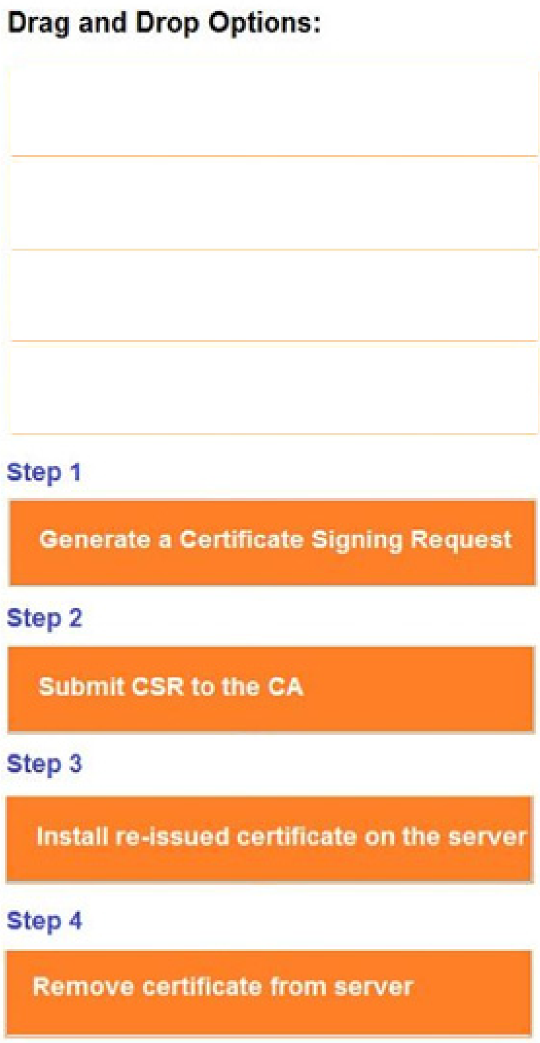
* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

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

Learn more about certificates



Drag and Drop Options:

Step 1

Generate a Certificate Signing Request

Step 2

Submit CSR to the CA

Step 3

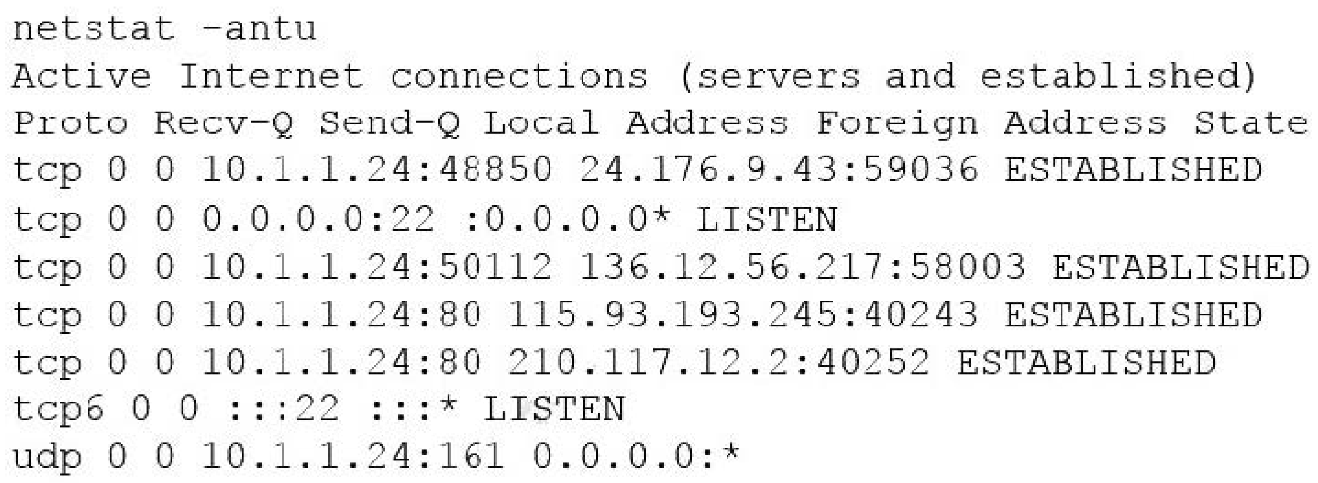
Install re-issued certificate on the server

Step 4

Remove certificate from server

QUESTION 8

A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:



```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```

Which of the following should the penetration tester do NEXT?

A. Close the reverse shell the tester is using.

B. Note this finding for inclusion in the final report.

C. Investigate the high numbered port connections.

D. Contact the client immediately.

Correct Answer: C

The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

QUESTION 9

During a client engagement, a penetration tester runs the following Nmap command and obtains the following output:

nmap -sV -- script ssl-enum-ciphers -p 443 remotehost

| TLS_ECDHE_ECDSA_WITH_RC4_128_SHA

| TLS_ECDHE_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_RC4_128_SHA (rsa 2048)

TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)

Which of the following should the penetration tester include in the report?

A. Old, insecure ciphers are in use.

B. The 3DES algorithm should be deprecated.

C. 2,048-bit symmetric keys are incompatible with MD5.

D. This server should be upgraded to TLS 1.2.

Correct Answer: A

The output of the Nmap command shows that the remote host supports RC4 ciphers, which are considered weak and vulnerable to several attacks, such as the BEAST and the RC4 NOMORE attacks. RC4 ciphers should not be used in modern TLS implementations, and they are not supported by TLS 1.3. Therefore, the penetration tester should include this finding in the report and recommend disabling RC4 ciphers on the server.

QUESTION 10

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

A. Spawned shells

B. Created user accounts

C. Server logs

D. Administrator accounts

E. Reboot system

F. ARP cache

Correct Answer: AB

Removing shells: Remove any shell programs installed when performing the pentest.

Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts. Removing tools: Remove any software tools that were installed on the customer\\'s systems that were

used to aid in the exploitation of systems.

QUESTION 11

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 system 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

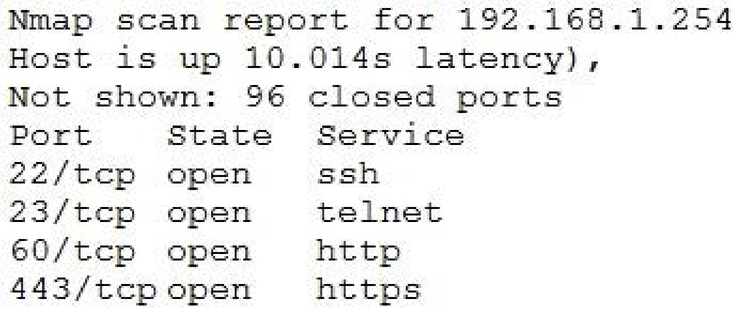
Correct Answer: A

https://hosakacorp.net/p/systemd-user.html

Creating a one-shot system service to establish a reverse shell is a technique that would best support maintaining persistence after reboot on a Linux-based file server. A system service is a program that runs in the background and performs various tasks without user interaction. A one-shot system service is a type of service that runs only once and then exits. A reverse shell is a type of shell that connects back to an attacker-controlled machine and allows remote command execution. By creating a one-shot system service that runs a reverse shell script at boot time, the penetration tester can ensure persistent access to the file server even after reboot.

QUESTION 12

An Nmap scan of a network switch reveals the following:



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

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

A. Encrypted passwords

B. System-hardening techniques

C. Multifactor authentication

D. Network segmentation

Correct Answer: B

QUESTION 13

Which of the following is the activity that is typically required the MOST during the post-engagement cleanup phase?

A. Removing shells

B. Launching new attacks

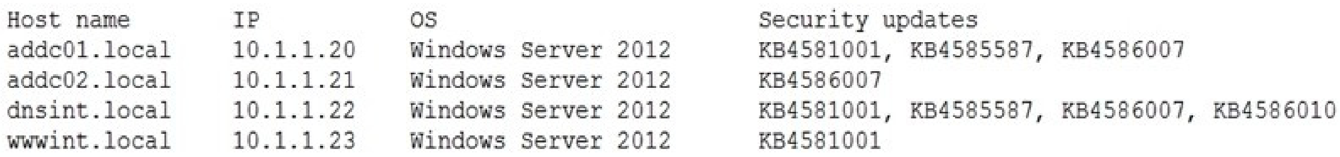
C. Documenting vulnerabilities

D. Requesting payment

Correct Answer: A

QUESTION 14

A penetration tester conducted a vulnerability scan against a client\\'s critical servers and found the following:



```
Host name      IP          OS                     Security updates
addc01.local   10.1.1.20   Windows Server 2012    KB4581001, KB4585587, KB4586007
addc02.local   10.1.1.21   Windows Server 2012    KB4586007
dnsint.local   10.1.1.22   Windows Server 2012    KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local   10.1.1.23   Windows Server 2012    KB4581001
```

Which of the following would be a recommendation for remediation?

A. Deploy a user training program

B. Implement a patch management plan

C. Utilize the secure software development life cycle

D. Configure access controls on each of the servers

Correct Answer: B

QUESTION 15

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

A. A vulnerability scan

B. A WHOIS lookup

C. A packet capture

D. An Nmap scan

Correct Answer: A

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