Vendor: ECCouncil

Exam Code: 312-50

Exam Name: Certified Ethical Hacker 8

Version: Demo

QUESTION 1

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Configure Port Security on the switch
B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch

Correct Answer: A

QUESTION 2

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

A. Jimmy can submit user input that executes an operating system command to compromise a target system.
B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access.
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database.
D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system.

Correct Answer: D

QUESTION 3

This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly

Correct Answer: C

QUESTION 4

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization. How would you prevent such type of attacks?

A. It is impossible to block these attacks.
B. Hire the people through third-party job agencies who will vet them for you.
C. Conduct thorough background checks before you engage them.
D. Investigate their social networking profiles.

Correct Answer: C

QUESTION 5

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning

Correct Answer: B

QUESTION 6

Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping

Correct Answer: A

QUESTION 7

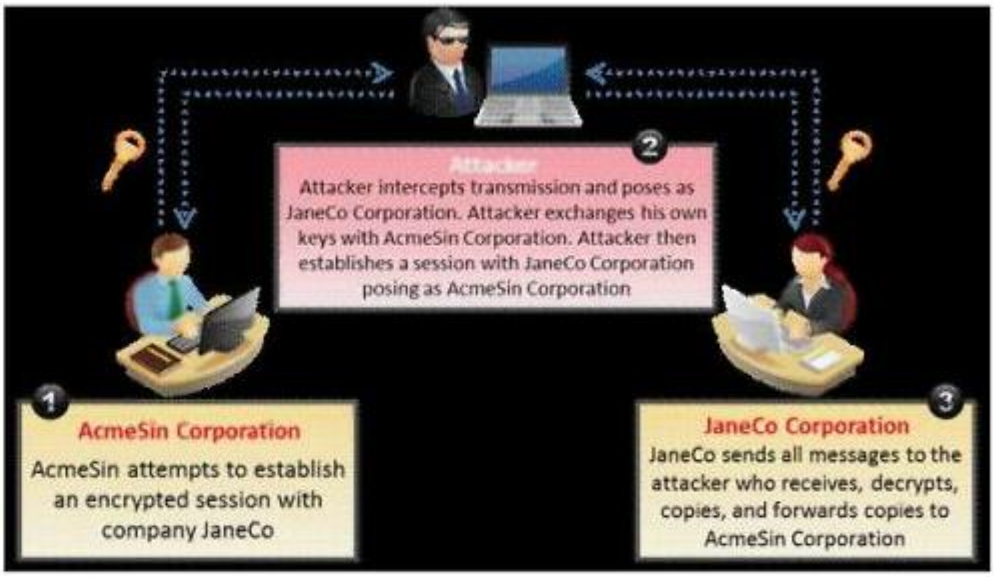
Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit. You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address. These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information. In which situations would you want to use anonymizer? (Select 3 answers)

A. Increase your Web browsing bandwidth speed by using Anonymizer.
B. To protect your privacy and Identity on the Internet.
C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.
D. Post negative entries in blogs without revealing your IP identity.

Correct Answer: BCD

QUESTION 8

What type of attack is shown in the following diagram?


2
Attacker
Attacker intercepts transmission and poses as JaneCo Corporation. Attacker exchanges his own keys with AcmeSin Corporation. Attacker then establishes a session with JaneCo Corporation posing as AcmeSin Corporation
1
AcmeSin Corporation
AcmeSin attempts to establish an encrypted session with company JaneCo
3
JaneCo Corporation
JaneCo sends all messages to the attacker who receives, decrypts, copies, and forwards copies to AcmeSin Corporation

A. Man-in-the-Middle (MiTM) Attack
B. Session Hijacking Attack
C. SSL Spoofing Attack
D. Identity Stealing Attack

Correct Answer: A

QUESTION 9

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him ''just to double check our records.'' Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

A. Reverse Psychology
B. Reverse Engineering
C. Social Engineering
D. Spoofing Identity
E. Faking Identity

Correct Answer: C

QUESTION 10

How do you defend against ARP Spoofing? Select three.

A. Use ARPWALL system and block ARP spoofing attacks.
B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets.
C. Use private VLANS.
D. Place static ARP entries on servers, workstation and routers.

Correct Answer: ACD

QUESTION 11

TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called ___________________.

A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"

Correct Answer: B

QUESTION 12

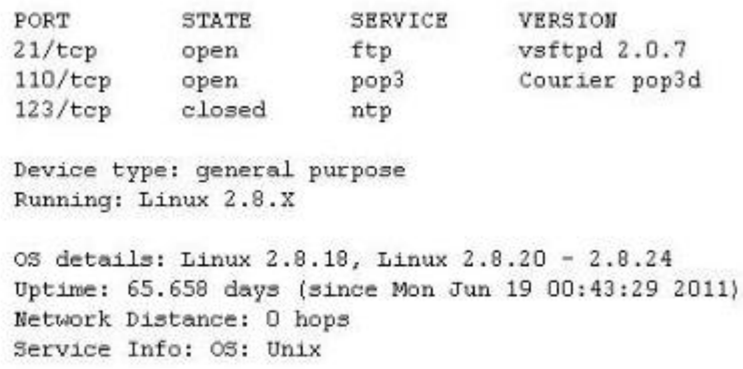
Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company. She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture. What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

A. The Kiley Innovators employee used cryptography to hide the information in the emails sent.
B. The method used by the employee to hide the information was logical watermarking.
C. The employee used steganography to hide information in the picture attachments.
D. By using the pictures to hide information, the employee utilized picture fuzzing.

Correct Answer: C

QUESTION 13

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123. Here is the output of your scan results:



```
PORT        STATE       SERVICE     VERSION
21/tcp      open        ftp         vsftpd 2.0.7
110/tcp     open        pop3        Courier pop3d
123/tcp     closed      ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?

A. nmap -A -sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5

Correct Answer: C

QUESTION 14

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data.
B. Restrict the interactive logon privileges.
C. Run services as unprivileged accounts.
D. Allow security settings of IE to zero or Low.
E. Run users and applications on the least privileges.

Correct Answer: ABCE

QUESTION 15

What does ICMP (type 11, code 0) denote?

A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type

Correct Answer: C

QUESTION 16

You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer. You are confident that this security implementation will protect the customer from password abuse. Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts. Your decision of password policy implementation has cost the bank with USD 925, 000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution. What effective security solution will you recommend in this case?

A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database.
B. Configure your firewall to block logon attempts of more than three wrong tries.
C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories.
D. Implement RSA SecureID based authentication system.

Correct Answer: D

QUESTION 17

More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers. It basically hides the true nature of the shellcode in different disguises. How does a polymorphic shellcode work?

A. They encrypt the shellcode by XORing values over the shellcode,using loader code to decrypt the shellcode,and then executing the decrypted shellcode.
B. They convert the shellcode into Unicode,using loader to convert back to machine code then executing them.
C. They reverse the working instructions into opposite order by masking the IDS signatures.
D. They compress shellcode into normal instructions,uncompress the shellcode using loader code and then executing the shellcode.

Correct Answer: A

QUESTION 18

SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

A. The source and destination address having the same value.
B. A large number of SYN packets appearing on a network without the corresponding reply packets.
C. The source and destination port numbers having the same value.
D. A large number of SYN packets appearing on a network with the corresponding reply packets.

Correct Answer: B

QUESTION 19

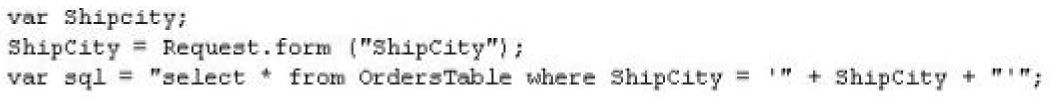
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Port Scanning
B. Single Scanning
C. External Scanning
D. Vulnerability Scanning

Correct Answer: D

QUESTION 20

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:



```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'

How will you delete the OrdersTable from the database using SQL Injection?

A. Chicago'; drop table OrdersTable --

B. Delete table'blah'; OrdersTable --

C. EXEC; SELECT * OrdersTable > DROP --

D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

Correct Answer: A

QUESTION 21

What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilities than more esoteric ones.

B. The scanning speed of their scanners are extremely high.

C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner.

D. The more vulnerabilities detected, the more tests required.

E. They are highly expensive and require per host scan license.

Correct Answer: AC

QUESTION 22

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.

Where can Stephanie go to see past versions and pages of a website?

A. She should go to the web page Samspade.org to see web pages that might no longer be on the website.
B. If Stephanie navigates to Search.com; she will see old versions of the company website.
C. Stephanie can go to Archive.org to see past versions of the company website.
D. AddressPast.com would have any web pages that are no longer hosted on the company's website.

Correct Answer: C

QUESTION 23

Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network.
B. The scenario is incorrect as Dan can spoof his IP and get responses.
C. The server will send replies back to the spoofed IP address.
D. Dan can establish an interactive session only if he uses a NAT.

Correct Answer: C

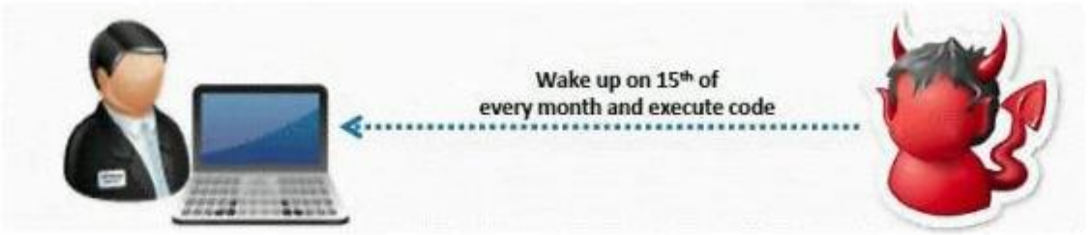
QUESTION 24

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor. Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on. Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them. What technique has Jason most likely used?

A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique
D. Image Steganography Technique

Correct Answer: D

QUESTION 25
What type of Virus is shown here?



A. Cavity Virus
B. Macro Virus
C. Boot Sector Virus
D. Metamorphic Virus
E. Sparse Infector Virus

Correct Answer: E

QUESTION 26
An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming. Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company. What is this deadly attack called?

A. Spear phishing attack

B. Trojan server attack

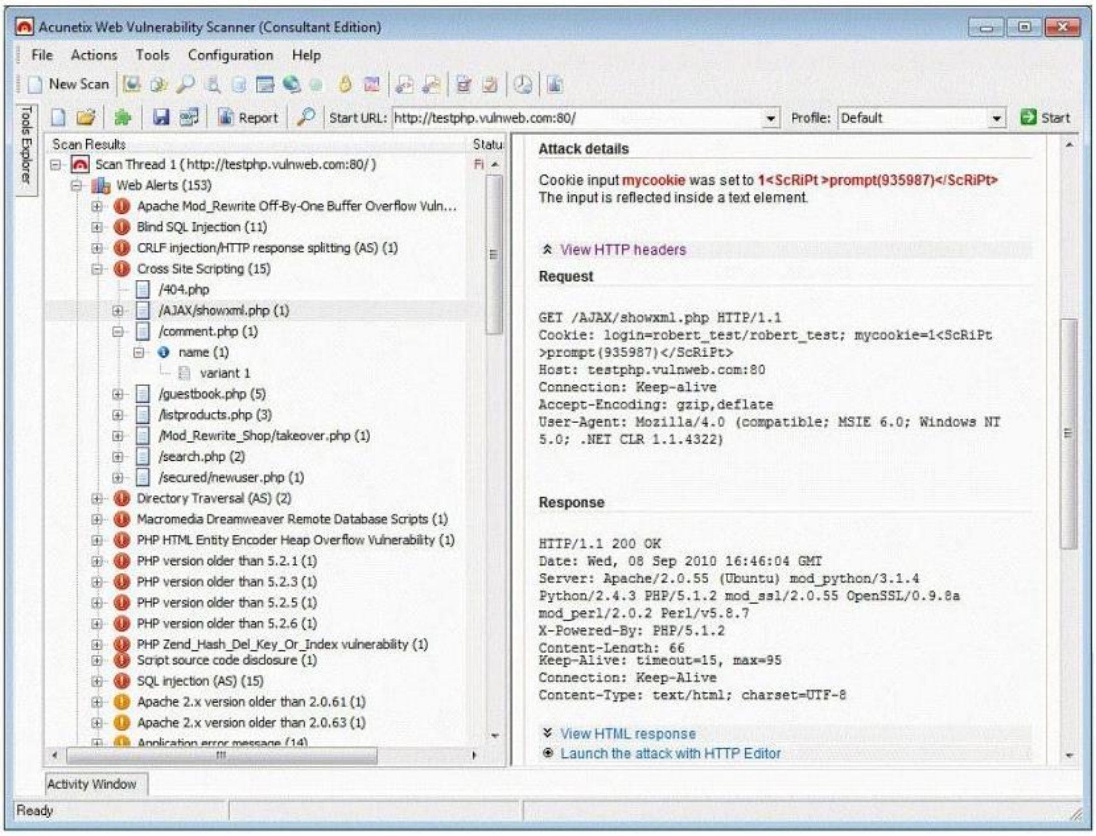
C. Javelin attack

D. Social networking attack

Correct Answer: A

QUESTION 27

Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.



Start URL: http://testphp.vulnweb.com:80/

Profile: Default

```
Scan Results
Scan Thread 1 ( http://testphp.vulnweb.com:80/ )
  Web Alerts (153)
    Apache Mod_Rewrite Off-By-One Buffer Overflow Vuln...
    Blind SQL Injection (11)
    CRLF injection/HTTP response splitting (AS) (1)
    Cross Site Scripting (15)
      /404.php
      /AJAX/showxml.php (1)
      /comment.php (1)
        name (1)
          variant 1
      /guestbook.php (5)
      /listproducts.php (3)
      /Mod_Rewrite_Shop/takeover.php (1)
      /search.php (2)
      /secured/newuser.php (1)
    Directory Traversal (AS) (2)
    Macromedia Dreamweaver Remote Database Scripts (1)
    PHP HTML Entity Encoder Heap Overflow Vulnerability (1)
    PHP version older than 5.2.1 (1)
    PHP version older than 5.2.3 (1)
    PHP version older than 5.2.5 (1)
    PHP version older than 5.2.6 (1)
    PHP Zend_Hash_Del_Key_Or_Index vulnerability (1)
    Script source code disclosure (1)
    SQL injection (AS) (15)
    Apache 2.x version older than 2.0.61 (1)
    Apache 2.x version older than 2.0.63 (1)
    Application error message (14)
```

Attack details

Cookie input mycookie was set to 1<ScRiPt >prompt(935987)</ScRiPt>
The input is reflected inside a text element.

Request

```
GET /AJAX/showxml.php HTTP/1.1
Cookie: login=robert_test/robert_test; mycookie=1<ScRiPt
>prompt(935987)</ScRiPt>
Host: testphp.vulnweb.com:80
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.0; .NET CLR 1.1.4322)
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 08 Sep 2010 16:46:04 GMT
Server: Apache/2.0.55 (Ubuntu) mod_python/3.1.4
Python/2.4.3 PHP/5.1.2 mod_ssl/2.0.55 OpenSSL/0.9.8a
mod_perl/2.0.2 Perl/v5.8.7
X-Powered-By: PHP/5.1.2
Content-Length: 66
Keep-Alive: timeout=15, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Which of the following statements is incorrect?

A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades.
C. They can validate compliance with or deviations from the organization's security policy.
D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention.

Correct Answer: D

QUESTION 28

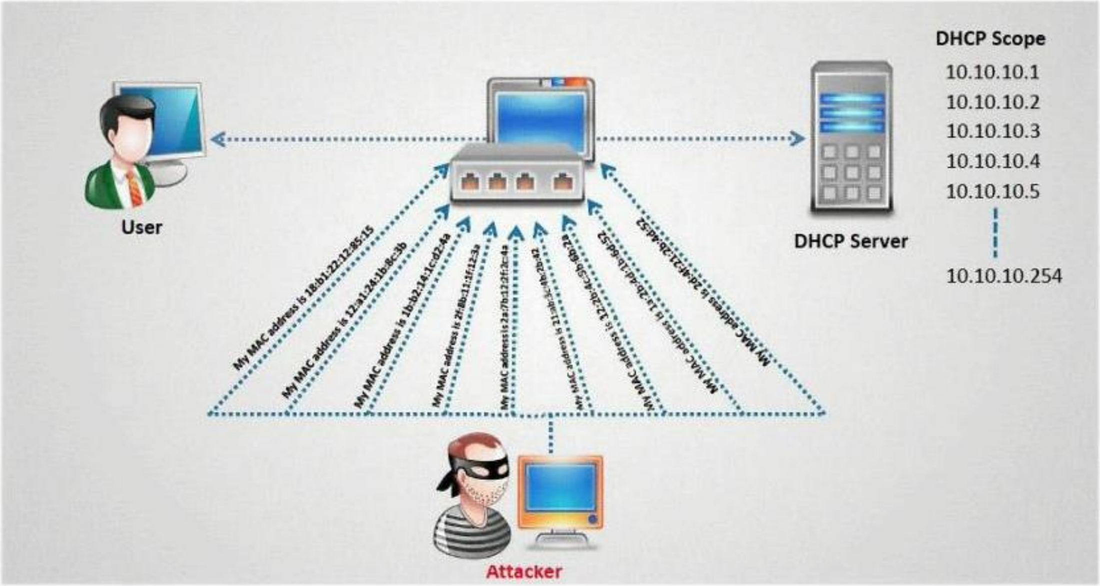
How does traceroute map the route a packet travels from point A to point B?

A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message.
B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message.
C. Uses a protocol that will be rejected by gateways on its way to the destination.
D. Manipulates the flags within packets to force gateways into generating error messages.

Correct Answer: B

QUESTION 29

How do you defend against DHCP Starvation attack?


DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.5
10.10.10.254
User
DHCP Server
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:2c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
My MAC address is 1a:2b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
Attacker

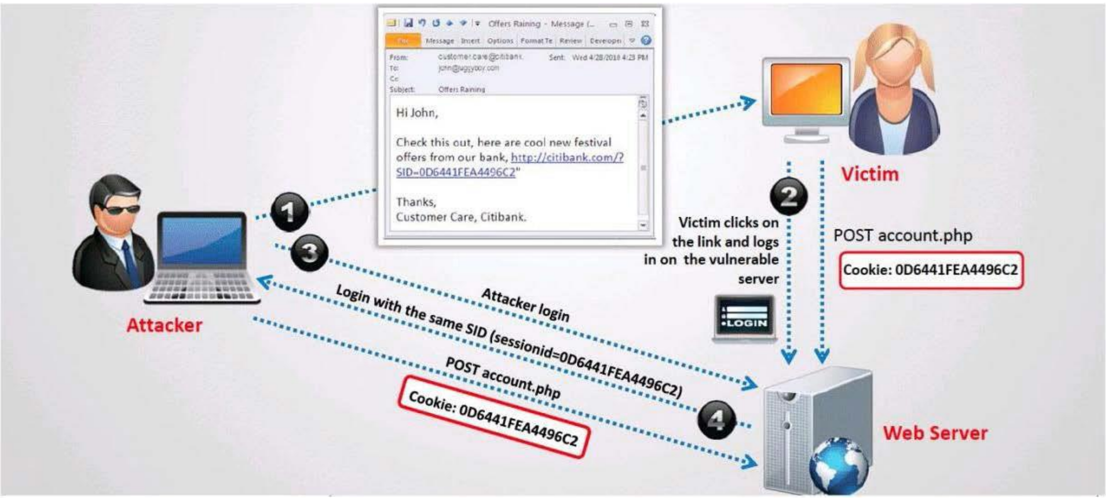
A. Enable ARP-Block on the switch.

B. Enable DHCP snooping on the switch.
C. Configure DHCP-BLOCK to 1 on the switch.
D. Install DHCP filters on the switch to block this attack.

Correct Answer: B

QUESTION 30

What type of session hijacking attack is shown in the exhibit?



From: customer.care@citibank. Sent: Wed 4/28/2010 4:23 PM
To: john@uggyboy.com
Cc:
Subject: Offers Raining

Hi John,

Check this out, here are cool new festival offers from our bank, http://citibank.com/?SID=0D6441FEA4496C2"

Thanks,
Customer Care, Citibank.

A. Cross-site scripting Attack
B. SQL Injection Attack
C. Token sniffing Attack
D. Session Fixation Attack

Correct Answer: D

QUESTION 31

The SYN flood attack sends TCP connections requests faster than a machine can process them. Attacker creates a random source address for each packet SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes) Victim's connection table fills up waiting for replies and ignores new connections Legitimate users are ignored and will not be able to access the server How do you protect your network against SYN Flood attacks?

A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory on the third packet of the handshake, not the first.

B. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.

C. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall.

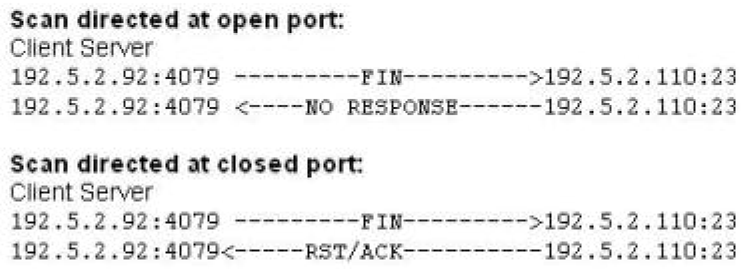
D. Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection.

E. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object.

Correct Answer: ABDE

QUESTION 32

What type of port scan is shown below?



```
Scan directed at open port:
Client Server
192.5.2.92:4079 ---------FIN--------->192.5.2.110:23
192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23

Scan directed at closed port:
Client Server
192.5.2.92:4079 ---------FIN--------->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23
```

A. Idle Scan

B. FIN Scan

C. XMAS Scan

D. Windows Scan

Correct Answer: B

QUESTION 33

Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored. Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it. What should Stephanie use so that she does not get in trouble for surfing the Internet?

A. Stealth IE
B. Stealth Anonymizer
C. Stealth Firefox
D. Cookie Disabler

Correct Answer: B

QUESTION 34

Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

A. Neil will have to configure a Bridged port that will copy all packets to the protocol analyzer.
B. Neil will need to setup SPAN port that will copy all network traffic to the protocol analyzer.
C. He will have to setup an Ether channel port to get a copy of all network traffic to the analyzer.
D. He should setup a MODS port which will copy all network traffic.

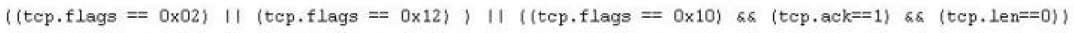
Correct Answer: B

QUESTION 35

In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:

- FIN = 1
- SYN = 2
- RST = 4
- PSH = 8
- ACK = 16
- URG = 32
- ECE = 64
- CWR = 128

Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.



```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags == 0x10) && (tcp.ack==1) && (tcp.len==0))
```

What is Jason trying to accomplish here?

A. SYN, FIN, URG and PSH
B. SYN, SYN/ACK, ACK

C. RST, PSH/URG, FIN

D. ACK, ACK, SYN, URG

Correct Answer: B

QUESTION 36

Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

A. Jayden can use the command. ip binding set.

B. Jayden can use the command. no ip spoofing.

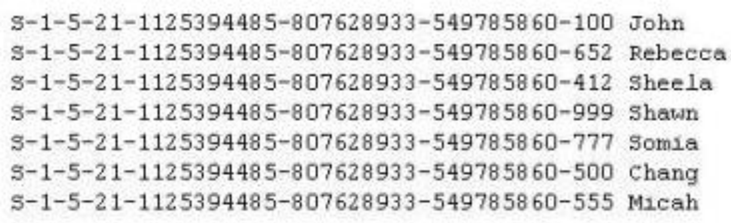
C. She should use the command. no dhcp spoofing.

D. She can use the command. ip dhcp snooping binding.

Correct Answer: D

QUESTION 37

Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output of the SIDs:



```
S-1-5-21-1125394485-807628933-549785860-100 John
S-1-5-21-1125394485-807628933-549785860-652 Rebecca
S-1-5-21-1125394485-807628933-549785860-412 Sheela
S-1-5-21-1125394485-807628933-549785860-999 Shawn
S-1-5-21-1125394485-807628933-549785860-777 Somia
S-1-5-21-1125394485-807628933-549785860-500 Chang
S-1-5-21-1125394485-807628933-549785860-555 Micah
```

From the above list identify the user account with System Administrator privileges?

A. John

B. Rebecca

C. Sheela

D. Shawn

E. Somia

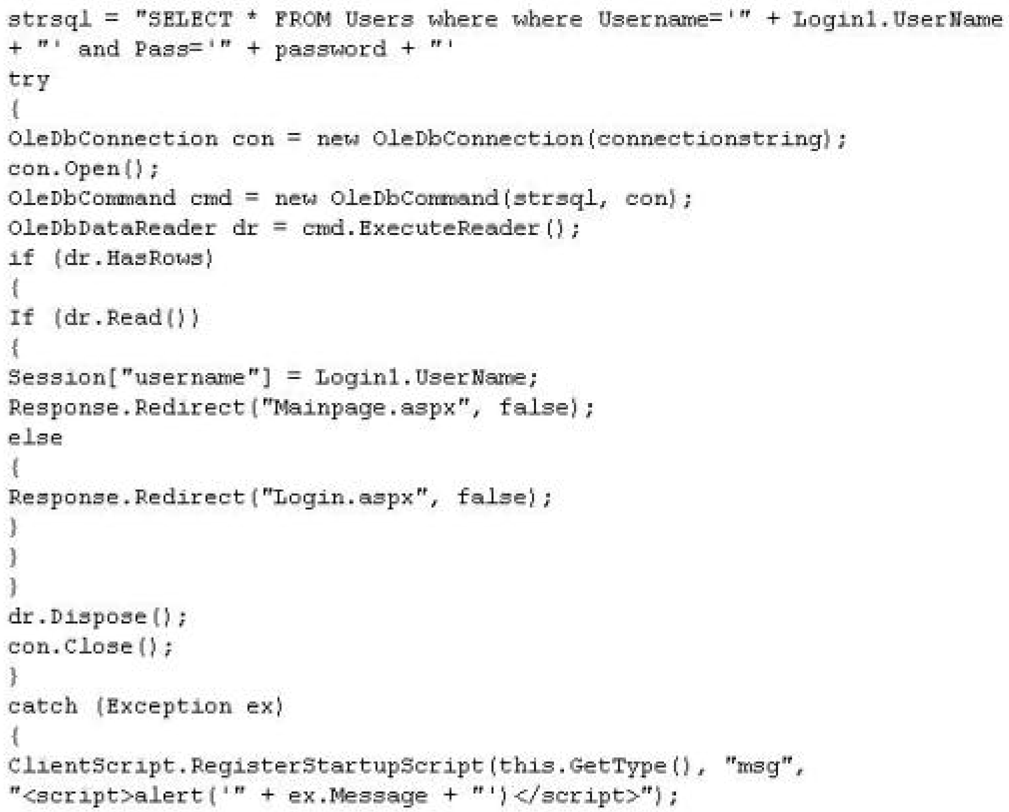
F. Chang

G. Micah

Correct Answer: F

QUESTION 38

What is the problem with this ASP script (login.asp)?



```
strsql = "SELECT * FROM Users where where Username='" + Login1.UserName
+ "' and Pass='" + password + "'
try
{
OleDbConnection con = new OleDbConnection(connectionstring);
con.Open();
OleDbCommand cmd = new OleDbCommand(strsql, con);
OleDbDataReader dr = cmd.ExecuteReader();
if (dr.HasRows)
{
If (dr.Read())
{
Session["username"] = Login1.UserName;
Response.Redirect("Mainpage.aspx", false);
else
{
Response.Redirect("Login.aspx", false);
}
}
}
dr.Dispose();
con.Close();
}
catch (Exception ex)
{
ClientScript.RegisterStartupScript(this.GetType(), "msg",
"<script>alert('" + ex.Message + "')</script>");
```

A. The ASP script is vulnerable to Cross Site Scripting attack.

B. The ASP script is vulnerable to Session Splice attack.

C. The ASP script is vulnerable to XSS attack.

D. The ASP script is vulnerable to SQL Injection attack.

Correct Answer: D

QUESTION 39

Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes:

- Everything you search for using Google
- Every web page you visit that has Google AdSense ads

How would you prevent Google from storing your search keywords?

A. Block Google Cookie by applying Privacy and Security settings in your web browser.

B. Disable the Google cookie using Google Advanced Search settings on Google Search page.
C. Do not use Google but use another search engine Bing which will not collect and store your search keywords.
D. Use MAC OS X instead of Windows 7. Mac OS has higher level of privacy controls by default.

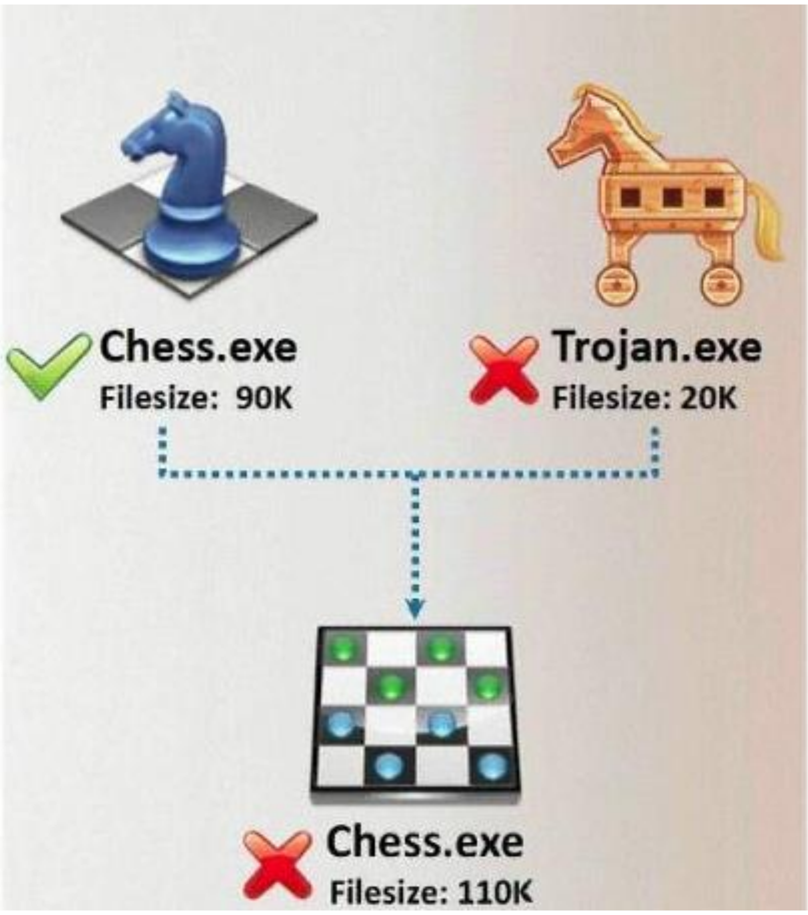
Correct Answer: A

QUESTION 40
How many bits encryption does SHA-1 use?

A. 64 bits
B. 128 bits
C. 256 bits
D. 160 bits

Correct Answer: D

QUESTION 41
In Trojan terminology, what is required to create the executable file chess.exe as shown below?



A. Mixer

B. Converter

C. Wrapper

D. Zipper

Correct Answer: C

QUESTION 42

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to notify administrators of problems or performance. What default port Syslog daemon listens on?

System Messages from the previous week

Thursday, July 20, 2006 12:21:25 PM CDT

Lists all system messages reported during the past 7 days

Number of records reported: 5

▼TimeStamp	ID	Severity	Server	Component	Error Co
Monday, July 17, 2006 2:49:30 PM CDT	870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Monday, July 17, 2006 12:36:59 PM CDT	870ef3dd1c10e5c6:1983ad7:10c7d8ece05:-7ffb	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Thursday, July 20, 2006 12:20:46 PM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fc0	Fatal	dhcp-uaus09-147-110	Logging	ERROR
Thursday, July 20, 2006 9:43:14 AM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fdd	Fatal	dhcp-uaus09-147-110	Logging	ERROR

A. 242

B. 312

C. 416

D. 514

Correct Answer: D

QUESTION 43

This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

A. Wiresharp attack

B. Switch and bait attack

C. Phishing attack

D. Man-in-the-Middle attack

Correct Answer: C

QUESTION 44

Which of the following statements would NOT be a proper definition for a Trojan Horse?

A. An authorized program that has been designed to capture keyboard keystroke while the user is unaware of such activity being performed.

B. An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user.

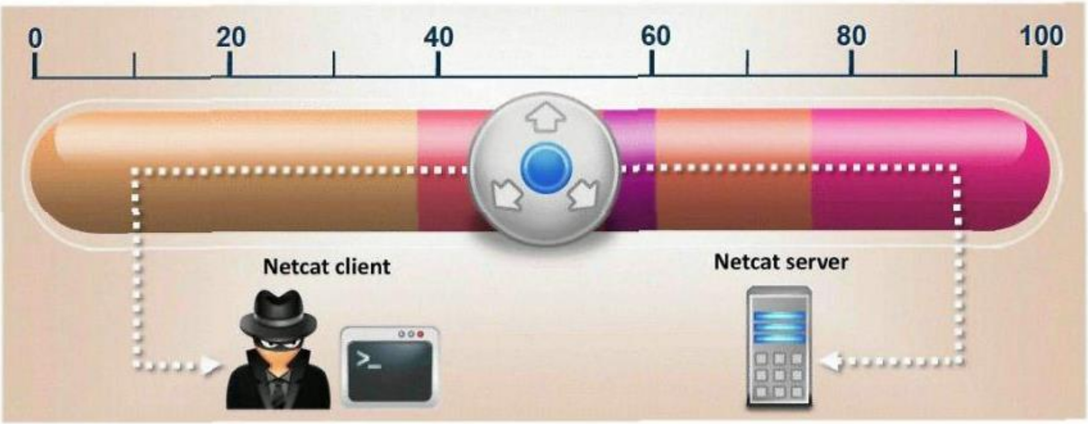
C. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user.

D. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user.

Correct Answer: A

QUESTION 45

What is the correct command to run Netcat on a server using port 56 that spawns command shell when connected?



A. nc -port 56 -s cmd.exe

B. nc -p 56 -p -e shell.exe

C. nc -r 56 -c cmd.exe

D. nc -L 56 -t -e cmd.exe

Correct Answer: D

QUESTION 46

SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true

B. false

Correct Answer: A

QUESTION 47

TCP/IP Session Hijacking is carried out in which OSI layer?

A. Data link layer

B. Transport layer

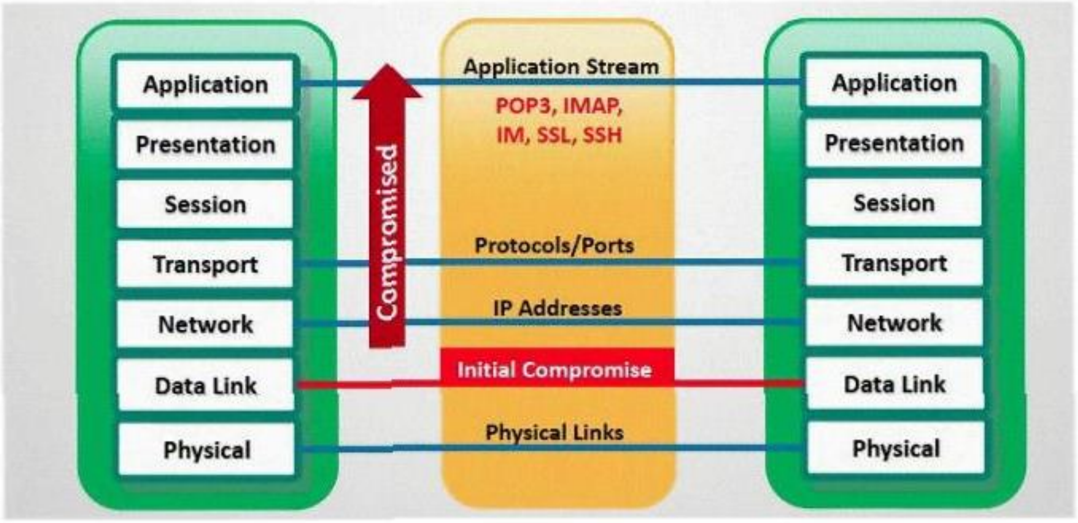
C. Network layer

D. Physical layer

Correct Answer: B

QUESTION 48

In which part of OSI layer, ARP Poisoning occurs?



A. Transport Layer

B. Data link Layer

C. Physical Layer

D. Application layer

Correct Answer: B

QUESTION 49

You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS streams. How will you accomplish this?

A. copy secret.txt c:\windows\system32\tcpip.dll kernel>secret.txt
B. copy secret.txt c:\windows\system32\tcpip.dll:secret.txt
C. copy secret.txt c:\windows\system32\tcpip.dll |secret.txt
D. copy secret.txt >< c:\windows\system32\tcpip.dll kernel secret.txt

Correct Answer: B

QUESTION 50

You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

A. New installation of Windows should be patched by installing the latest service packs and hotfixes.
B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed.
C. Install a personal firewall and lock down unused ports from connecting to your computer.
D. Install the latest signatures for Antivirus software.
E. Configure "Windows Update" to automatic.
F. Create a non-admin user with a complex password and logon to this account.
G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

Correct Answer: ACDEF

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820		