Ec-council.312-50.878q

Number: 312-50
Passing Score: 800
Time Limit: 120 min
File Version: 14.5

Exam Code: 312-50

Exam Name: Certified Ethical Hacker (CEHv6)

Exam A

QUESTION 1
What is the goal of a Denial of Service Attack?

A. Capture files from a remote computer.
B. Render a network or computer incapable of providing normal service.
C. Exploit a weakness in the TCP stack.
D. Execute service at PS 1009.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: In computer security,a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers,and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

Topic 8, Volume H

QUESTION 2
What is the term 8 to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

A. Fraggle Attack
B. Man in the Middle Attack
C. Trojan Horse Attack
D. Smurf Attack
E. Back Orifice Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Trojan and Back orifice are Trojan horse attacks.Man in the middle spoofs the Ip and redirects the victems packets to the cracker The infamous Smurf attack. preys on ICMP's capability to send traffic to the broadcast address. Many hosts can listen and respond to a single ICMP echo request sent to a broadcast address. Network Intrusion Detection third Edition by Stephen Northcutt and Judy Novak pg 70 The "smurf" attack's cousin is called "fraggle",which uses UDP echo packets in the same fashion as the ICMP echo packets; it was a simple re-write of "smurf".

QUESTION 3
What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
B. A TCP SYN packet,which is a connection initiation,is sent to a target machine,giving the target host's address as both source and destination,and is using the same port on the target host as both source and destination.
C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
To a server that requires an exchange of a sequence of messages. The clientsystem begins by sending a SYN message to the server. The server thenacknowledges the SYN message by sending a SYN-ACK message to the client. Theclient then finishes establishing the connection by responding with an ACKmessage and then data can be exchanged. At the point where the server systemhas sent an acknowledgment (SYN-ACK) back to client but has not yet receivedthe ACK message,there is a half-open connection. A data structuredescribing all pending connections is in memory of the server that can bemade to overflow by intentionally creating too many partially openconnections. Another common attack is the SYN flood,in which a target machine isflooded with TCP connection requests. The source addresses and source TCP ports of the connection request packets are randomized; the purpose is to force the target host to maintain state information for many connections that will never be completed. SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow,crashes,or hangs. It's also possible for the traffic returned from the target host to cause trouble on routers; because this return traffic goes to the randomized source addresses of the original packets,it lacks the locality properties of "real" IP traffic,and may overflow route caches. On Cisco routers,this problem often manifests itself in the router running out of memory.

QUESTION 4
A denial of Service (DoS) attack works on the following principle:

A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
C. Overloaded buffer systems can easily address error conditions and respond appropriately.
D. Host systems cannot respond to real traffic,if they have an overwhelming number of incomplete connections (SYN/RCVD State).
E. A server stops accepting connections from certain networks one those network become flooded.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service,such as a web site.This can be done by exercising a software bug that causes the software running the service to fail (such as the "Ping of Death" attack against Windows NT systems),sending enough data to consume all available network bandwidth (as in the May,2001 attacks against Gibson Research),or sending data in such a way as to consume a particular resource needed by the

service.

QUESTION 5
A Buffer Overflow attack involves:

A. Using a trojan program to direct data traffic to the target host's memory stack
B. Flooding the target network buffers with data traffic to reduce the bandwidth available to legitimate users
C. Using a dictionary to crack password buffers by guessing user names and passwords
D. Poorly written software that allows an attacker to execute arbitrary code on a target system

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
B is a denial of service. By flooding the data buffer in an application with trash you could get access to write in the code segment in the application and that way insert your own code.

QUESTION 6
What would best be defined as a security test on services against a known vulnerability database using an automated tool?

A. A penetration test
B. A privacy review
C. A server audit
D. A vulnerability assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like a nuclear power plant,a computer system,or a larger system (for example the communications infrastructure or water infrastructure of a region).

QUESTION 7
Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.

What could be the most likely cause?

A. Someone has spoofed Clive's IP address while doing a smurf attack.
B. Someone has spoofed Clive's IP address while doing a land attack.
C. Someone has spoofed Clive's IP address while doing a fraggle attack.
D. Someone has spoofed Clive's IP address while doing a DoS attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: The smurf attack,named after its exploit program,is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack,a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses,all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function,most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply,multiplying the traffic by the number of hosts responding. On a multi-access broadcast network,hundreds of machines might reply to each packet.

QUESTION 8
What do you call a system where users need to remember only one username and password, and be authenticated for multiple services?

A. Simple Sign-on
B. Unique Sign-on
C. Single Sign-on

D. Digital Certificate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Single sign-on (SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems.

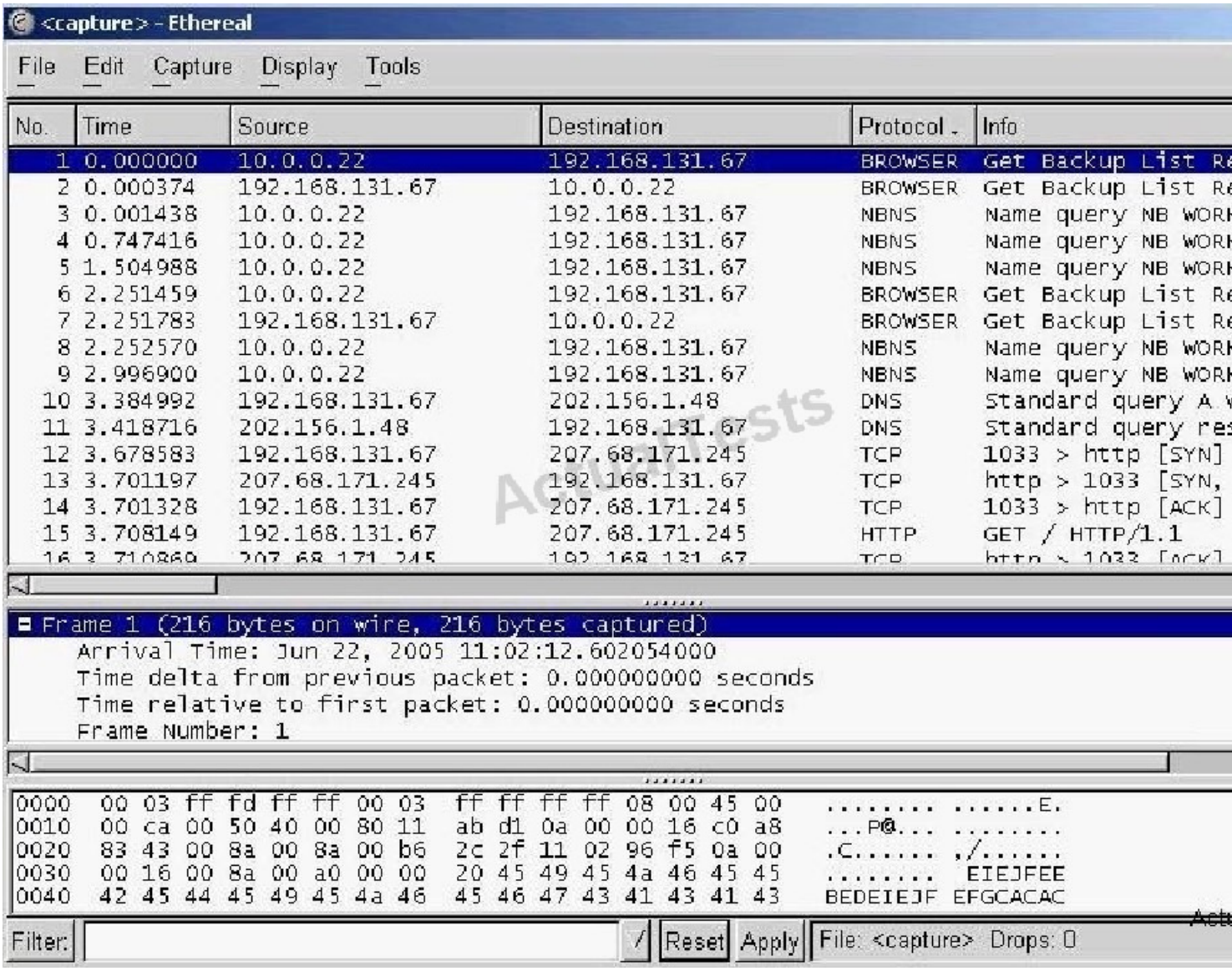
QUESTION 9
Tess King, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65, 536 bytes. From the information given, what type of attack is Tess King attempting to perform?

A. Syn flood
B. Smurf
C. Ping of death
D. Fraggle

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://insecure.org/sploits/ping-o-death.html

QUESTION 10
Exhibit:



You have captured some packets in Ethereal. You want to view only packets sent from 10.0.0.22.
What filter will you apply?

A. ip = 10.0.0.22
B. ip.src == 10.0.0.22
C. ip.equals 10.0.0.22
D. ip.address = 10.0.0.22

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: ip.src tells the filter to only show packets with 10.0.0.22 as the source.

QUESTION 11
How would you describe a simple yet very effective mechanism for sending and receiving unauthorized information or data between machines without alerting any firewalls and IDS's on a network?

A. Covert Channel
B. Crafted Channel
C. Bounce Channel
D. Deceptive Channel

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially,it is a method of communication that is not part of an actual computer system design,but can be used to transfer information to users or system processes that normally would not be allowed access to the information.

QUESTION 12
ARP poisoning is achieved in _____ steps

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: The hacker begins by sending a malicious ARP "reply" (for which there was no previous request) to your router,associating his computer's MAC address with your IP Address. Now your router thinks the hacker's computer is your computer. Next,the hacker sends a malicious ARP reply to your computer,associating his MAC Address with the routers IP Address. Now your machine thinks the hacker's computer is your router. The hacker has now used ARP poisoning to accomplish a MitM attack.

QUESTION 13
Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. Smurf
C. Ping of Death
D. SYN flood
E. SNMP Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The teardrop attack uses overlapping packet fragments to confuse a target system and cause the system to reboot or crash.

QUESTION 14
What happens when one experiences a ping of death?

A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP),the Last Fragment bit is set,and (IP offset ` 8) + (IP data length) >65535.
In other words,the IP offset (which represents the starting position of this fragment in the original packet,and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
D. This is when an the IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A hacker can send an IP packet to a vulnerable machine such that the lastfragment contains an offest where (IP offset *8) + (IP data length)>65535.This means that when the packet is reassembled,its total length is largerthan the legal limit,causing buffer overruns in the machine's OS (becousethe buffer sizes are defined only to accomodate the maximum allowed size ofthe packet based on RFC 791)...IDS can generally recongize such attacks bylooking for packet fragments that have the IP header's protocol field set to1 (ICMP),the last bit set,and (IP offset *8) +(IP data length)>65535" CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 414 "Ping of Death" attacks cause systems to react in an unpredictable fashion when receiving oversized IP packets. TCP/IP allows for a maximum packet size of up to 65536 octets (1 octet = 8 bits of data),containing aminimum of 20 octets of IP header information and zero or more octets ofoptional information,with the rest of the packet being data. Ping of Deathattacks can cause crashing,freezing,and rebooting.

QUESTION 15
Global deployment of RFC 2827 would help mitigate what classification of attack?

A. Sniffing attack
B. Denial of service attack
C. Spoofing attack
D. Reconnaissance attack
E. Prot Scan attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

QUESTION 16
Which one of the following instigates a SYN flood attack?

A. Generating excessive broadcast packets.
B. Creating a high number of half-open connections.
C. Inserting repetitive Internet Relay Chat (IRC) messages.
D. A large number of Internet Control Message Protocol (ICMP) traces.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake.The attacker floods the target system's small "in-process" queue with connection requests,but it does not respond when a target system replies to those requests.This causes the target system to time out while waiting for the proper response,which makes the system crash or become unusable.

QUESTION 17
Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

A. RSA,LSA,POP
B. SSID,WEP,Kerberos
C. SMB,SMTP,Smart card
D. Kerberos,Smart card,Stanford SRP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Kerberos,Smart cards and Stanford SRP are techniques where the password never leaves the computer.

QUESTION 18
The follows is an email header. What address is that of the true originator of the message?

```
Return-Path: <bgates@microsoft.com>
Received: from smtp.com (fw.emumail.com [215.52.220.122].
by raq-221-181.ev1.net (8.10.2/8.10.2. with ESMTP id h78NIn404807
for <mikeg@thesolutionfirm.com>; Sat, 9 Aug 2003 18:18:50 -0500
Received: (qmail 12685 invoked from network.; 8 Aug 2003 23:25:25 -
Received: from ([19.25.19.10].
by smtp.com with SMTP
Received: from unknown (HELO CHRISLAPTOP. (168.150.84.123.
by localhost with SMTP; 8 Aug 2003 23:25:01 -0000
From: "Bill Gates" <bgates@microsoft.com>
To: "mikeg" <mikeg@thesolutionfirm.com>
Subject: We need your help!
Date: Fri, 8 Aug 2003 19:12:28 -0400
Message-ID: <51.32.123.21@CHRISLAPTOP>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0052_01C35DE1.03202950"
X-Priority: 3 (Normal.
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.2627
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Importance: Normal
```


A. 19.25.19.10
B. 51.32.123.21
C. 168.150.84.123
D. 215.52.220.122
E. 8.10.2/8.10.2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Spoofing can be easily achieved by manipulating the "from" name field,however,it is much more difficult to hide the true source address. The "received from" IP address 168.150.84.123 is the true source of the

QUESTION 19
Ethereal works best on _____.

A. Switched networks
B. Linux platforms
C. Networks using hubs
D. Windows platforms

E. LAN's

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Ethereal is used for sniffing traffic. It will return the best results when used on an unswitched (i.e. hub. network.

QUESTION 20
Samantha was hired to perform an internal security test of XYZ. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.

Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

A. Ethernet Zapping
B. MAC Flooding
C. Sniffing in promiscuous mode
D. ARP Spoofing

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation: In a typical MAC flooding attack,a switch is flooded with packets,each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.The result of this attack causes the switch to enter a state called failopen mode,in which all incoming packets are broadcast out on all ports (as with a hub),instead of just down the correct port as per normal operation. The principle of ARP spoofing is to send fake,or 'spoofed',ARP messages to an Ethernet LAN. These frames contain false MAC addresses,confusing network devices,such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).

QUESTION 21
Which of the following is not considered to be a part of active sniffing?

A. MAC Flooding
B. ARP Spoofing
C. SMAC Fueling
D. MAC Duplicating

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

A. macof

B. webspy
C. filesnarf
D. nfscopy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Filesnarf - sniff files from NFS traffic
OPTIONS
-i interface
Specify the interface to listen on.

-v "Versus" mode. Invert thesenseofmatching,to
select non-matching files.

Pattern
Specify regular expression for filename matching.

Expression
Specifyatcpdump(8)filter expression to selecttraffic to sniff.

SEE ALSO
Dsniff,nfsd

QUESTION 23
Which of the following display filters will you enable in Ethereal to view the three-way handshake for a connection from host 192.168.0.1?

A. ip == 192.168.0.1 and tcp.syn
B. ip.addr = 192.168.0.1 and syn = 1
C. ip.addr==192.168.0.1 and tcp.flags.syn
D. ip.equals 192.168.0.1 and syn.equals on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Which tool/utility can help you extract the application layer data from each TCP connection from a log file into separate files?

A. Snort
B. argus
C. TCPflow
D. Tcpdump

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Tcpflow is a program that captures data transmitted as part of TCP connections (flows),and stores

the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire,but usually doesn't store the data that's actually being transmitted. In contrast,tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

QUESTION 25
A file integrity program such as Tripwire protects against Trojan horse attacks by:

A. Automatically deleting Trojan horse programs
B. Rejecting packets generated by Trojan horse programs
C. Using programming hooks to inform the kernel of Trojan horse behavior
D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Tripwire generates a database of the most common files and directories on your system. Once it is generated,you can then check the current state of your system against the original database and get a report of all the files that have been modified,deleted or added. This comes in handy if you allow other people access to your machine and even if you don't,if someone else does get access,you'll know if they tried to modify files such as /bin/login etc.

QUESTION 26
Sniffing is considered an active attack.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Sniffing is considered a passive attack.

QUESTION 27
Which of the following Netcat commands would be used to perform a UDP scan of the lower 1024 ports?

A. Netcat -h -U
B. Netcat -hU <host(s.>
C. Netcat -sU -p 1-1024 <host(s.>
D. Netcat -u -v -w2 <host> 1-1024
E. Netcat -sS -O target/1024

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: The proper syntax for a UDP scan using Netcat is "Netcat -u -v -w2 <host> 1-1024". Netcat is considered the Swiss-army knife of hacking tools because it is so versatile.

QUESTION 28
Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the

network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

A. Port 1890 (Net-Devil Trojan)
B. Port 1786 (Net-Devil Trojan)
C. Port 1909 (Net-Devil Trojan)
D. Port 6667 (Net-Devil Trojan)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: From trace,0x1A0B is 6667,IRC Relay Chat,which is one port used. Other ports are in the 900's.

QUESTION 29
A POP3 client contacts the POP3 server:

A. To send mail
B. To receive mail
C. to send and receive mail
D. to get the address to send mail to
326
E. initiate a UDP SMTP connection to read mail

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: POP is used to receive e-mail.
SMTP is used to send e-mail.

QUESTION 30
A remote user tries to login to a secure network using Telnet, but accidently types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

A. Invalid Username
B. Invalid Password
C. Authentication Failure
D. Login Attempt Failed
E. Access Denied

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As little information as possible should be given about a failed login attempt. Invalid username or password is not desirable.

QUESTION 31
Exhibit:

ettercap NCLzs --quiet

What does the command in the exhibit do in "Ettercap"?

A. This command will provide you the entire list of hosts in the LAN
B. This command will check if someone is poisoning you and will report its IP.
C. This command will detach from console and log all the collected passwords from the network to 325 a file.
D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
-N = NON interactive mode (without ncurses)
-C = collect all users and passwords
-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form "YYYYMMDD-collected-pass.log"
-z = start in silent mode (no arp storm on start up)
-s = IP BASED sniffing
--quiet = "demonize" ettercap. Useful if you want to log all data in background.

QUESTION 32
Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally. He enters the following at the command prompt.

$ nc -l -p 1026 -u -v

In response, he sees the following message.

cell(?(c)????STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.

Windows has found 47 Critical Errors.

To fix the errors please do the following:

1. Download Registry Repair from: www.reg-patch.com

2. Install Registry Repair

3. Run Registry Repair

4. Reboot your computer

FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

What would you infer from this alert?

A. The machine is redirecting traffic to www.reg-patch.com using adware
B. It is a genuine fault of windows registry and the registry needs to be backed up
C. An attacker has compromised the machine and backdoored ports 1026 and 1027
D. It is a messenger spam. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities

Correct Answer: D
Section: (none)