312-50 Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

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

Vulnerabilities are all weaknesses that can be exploited.

QUESTION 2

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. Fraggle

C. SYN Flood

D. Ping of Death

Correct Answer: D

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.

QUESTION 3

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

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.

QUESTION 4

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

With Port Security the switch will keep track of which ports are allowed to send traffic on a port.

QUESTION 5

Ethereal works best on ____________.

A. Switched networks

B. Linux platforms

C. Networks using hubs

D. Windows platforms

E. LAN\\'s

Correct Answer: C

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

QUESTION 6

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

Wget is a utility used for mirroring websites, get* doesn\\'t work, as for the actual FTP command to 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 7

Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

A. Polymorphic

B. Boot Sector infector

C. System

D. Macro

Correct Answer: D

The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment.

QUESTION 8

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

C. Netcat -sU -p 1-1024

D. Netcat -u -v -w2 1-1024

E. Netcat -sS -O target/1024

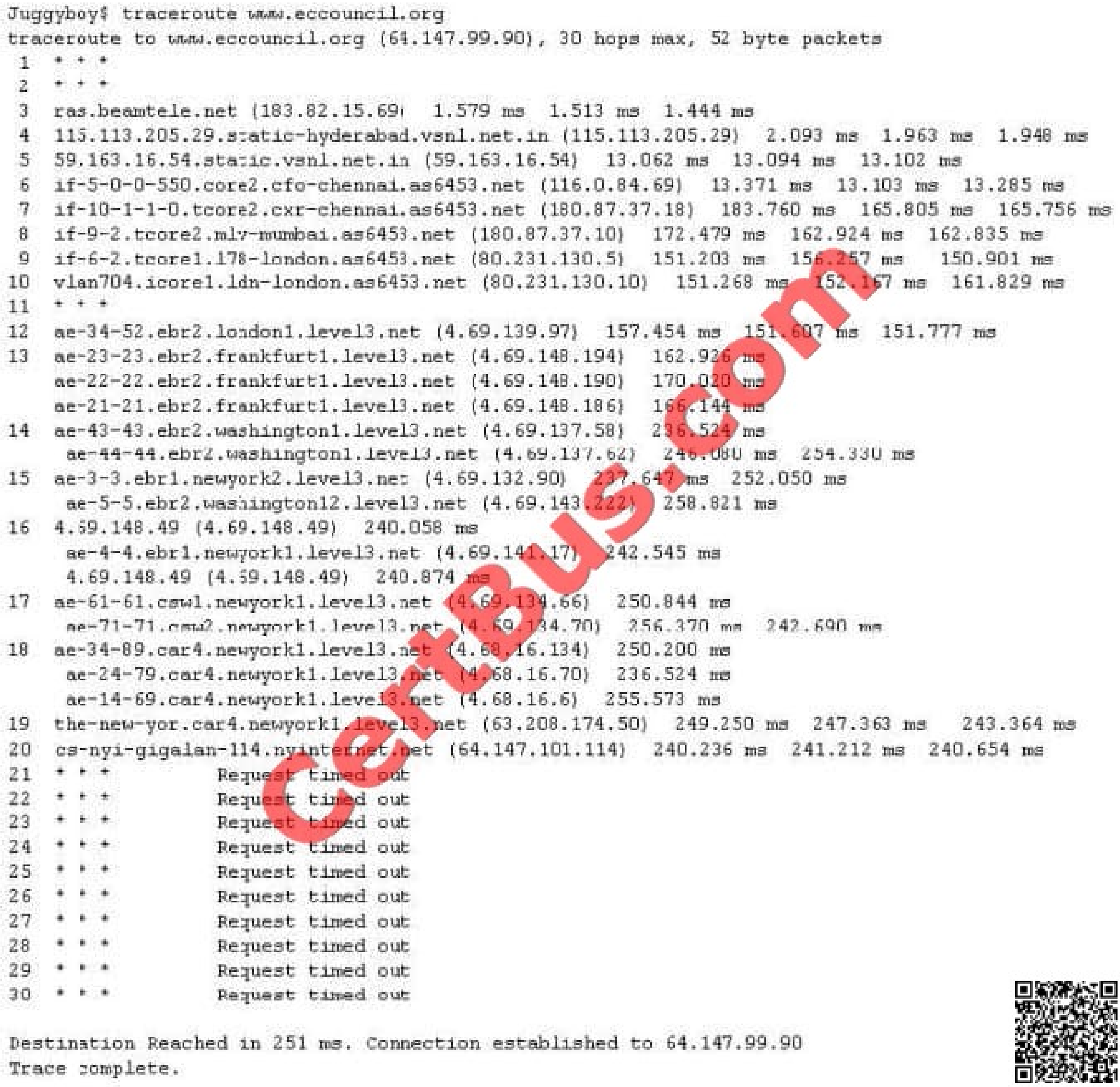
Correct Answer: D

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

QUESTION 9

The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.

The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.



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

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

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

A. Firewalls will permit inbound TCP packets to specific ports that hosts sitting behind the firewall are listening for 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

QUESTION 10

What is the IV key size used in WPA2?

A. 32

B. 24

C. 16

D. 48

E. 128

Correct Answer: D

QUESTION 11

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

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

QUESTION 12

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

lsof 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 13

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

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

QUESTION 14

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

If you manage to get the system to start a shell for you, that shell will be running as LOCAL_SYSTEM.

QUESTION 15

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

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 16

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

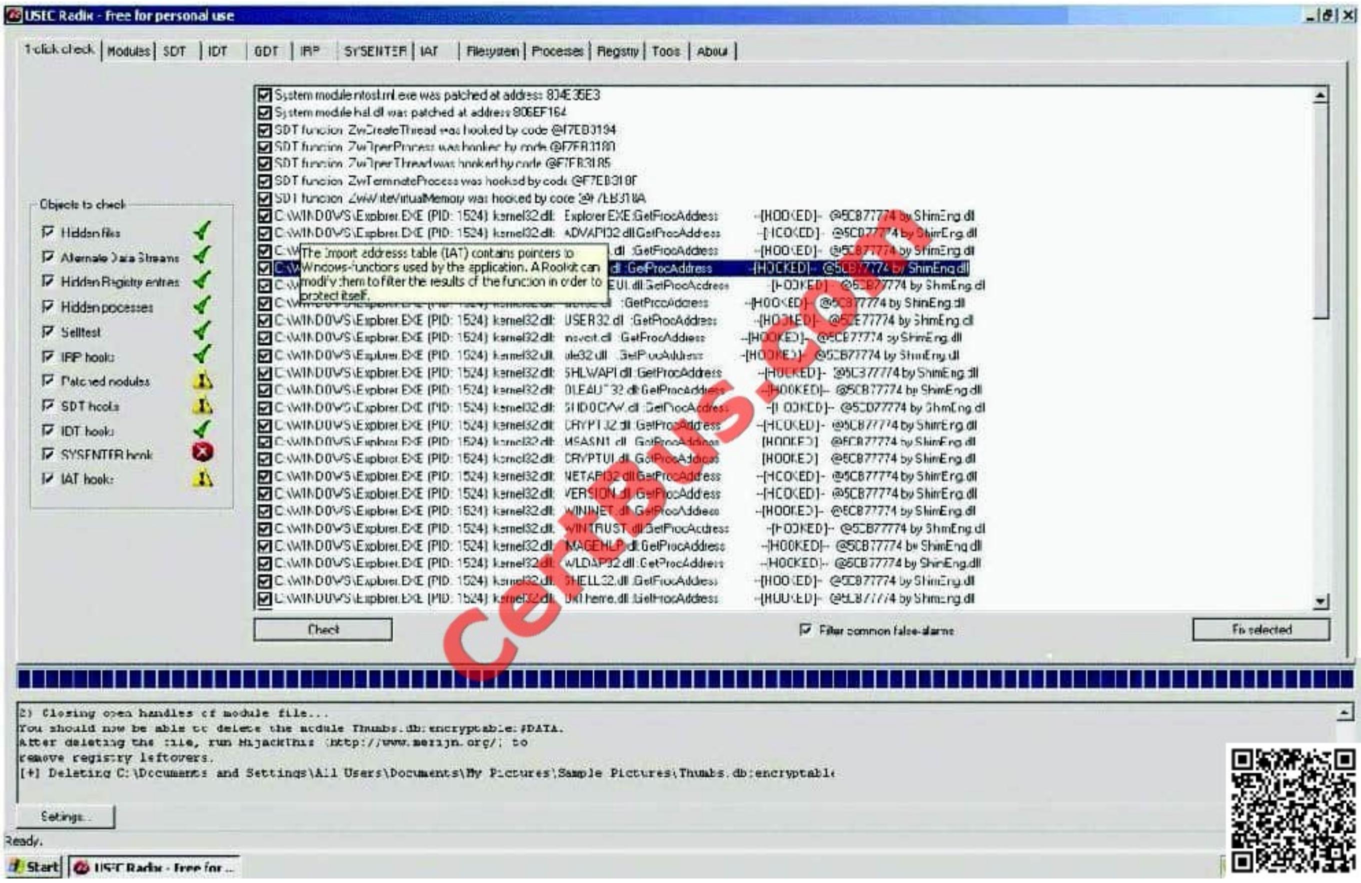
E. A portion of the hash will be all 0\\'s

Correct Answer: B

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.

QUESTION 17

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.


USEC Radix - Free for personal use
1-click check | Modules | SDT | IDT | GDT | IRP | SYSENTER | IAT | Filesystem | Processes | Registry | Tools | About
Check
Fix selected
Settings...
Start
USEC Radix - Free for ...

Objects to check

- ☑ Hidden files ✓
- ☑ Alternate Data Streams ✓
- ☑ Hidden Registry entries ✓
- ☑ Hidden processes ✓
- ☑ Selftest ✓
- ☑ IRP hooks ✓
- ☑ Patched modules ⚠
- ☑ SDT hooks ⚠
- ☑ IDT hooks ✓
- ☑ SYSENTER hook ☒
- ☑ IAT hooks ⚠

```
☑ System module ntoskrnl.exe was patched at address 804E35E3
☑ System module hal.dll was patched at address 806EF164
☑ SDT function ZwCreateThread was hooked by code @F7EB3194
☑ SDT function ZwOpenProcess was hooked by code @F7EB3180
☑ SDT function ZwOpenThread was hooked by code @F7EB3185
☑ SDT function ZwTerminateProcess was hooked by code @F7EB318F
☑ SDT function ZwWriteVirtualMemory was hooked by code @F7EB318A
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: Explorer.EXE:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: ADVAPI32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                .dll :GetProcAddress          --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                .dll :GetProcAddress          --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                EUI.dll:GetProcAddress        --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\W                                                     :GetProcAddress          --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: USER32.dll :GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: msvcrt.dll :GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: ole32.dll :GetProcAddress      --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: SHLWAPI.dll:GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: OLEAUT32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: SHDOCVW.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: CRYPT32.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: MSASN1.dll :GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: CRYPTUI.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: NETAPI32.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: VERSION.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: WININET.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: WINTRUST.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: IMAGEHLP.dll:GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: WLDAP32.dll:GetProcAddress     --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: SHELL32.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524) kernel32.dll: UxTheme.dll :GetProcAddress    --[HOOKED]-- @5CB77774 by ShimEng.dll
```

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

☑ Filter common false-alarms

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

Ready.

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

QUESTION 18

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

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

QUESTION 19

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

QUESTION 20

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

A. script kiddies

B. grey hat hackers

C. black hat hackers

D. disgruntled employees

Correct Answer: D

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.

QUESTION 21

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

Because the traffic is encrypted, an IDS cannot understand it or evaluate the payload.

QUESTION 22

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

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

QUESTION 23

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. Which organization coordinates computer crime investigations throughout the United States?

A. NDCA

B. NICP

C. CIRP

D. NPC

E. CIA

Correct Answer: D

QUESTION 24

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

A. Network aliasing

B. Domain Name Server (DNS) poisoning

C. Reverse Address Resolution Protocol (ARP)

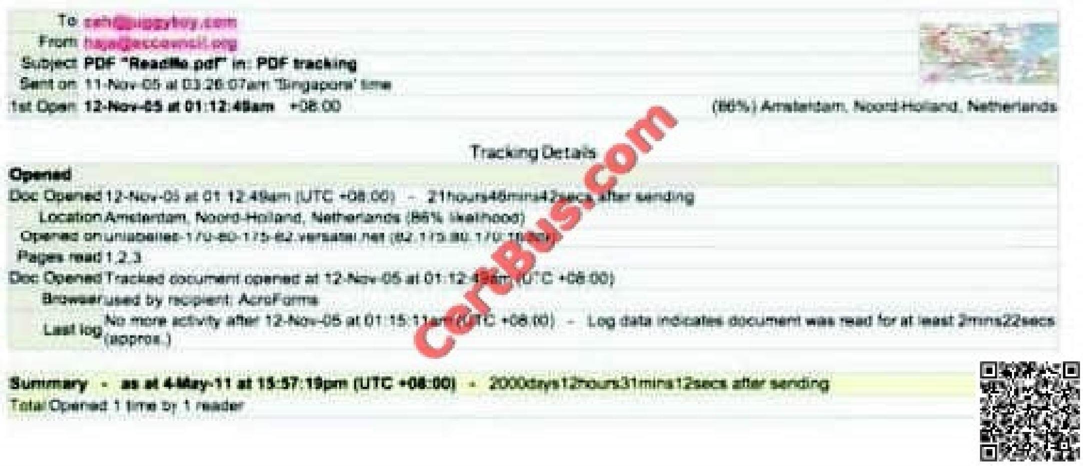
D. Port scanning

Correct Answer: B

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 poisoning.

QUESTION 25

E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient.



To: ceh@piggybuy.com
From: haja@eccouncil.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) - 21hours46mins42secs after sending
Location Amsterdam, Noord-Holland, Netherlands (86% likelihood)
Opened on unlabelled-170-80-175-62.versatel.net (62.175.80.170:16895)
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: AcroForms
Last log No more activity after 12-Nov-05 at 01:15:11am (UTC +08:00) - Log data indicates document was read for at least 2mins22secs (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

QUESTION 26

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

All are DDOS tools.

QUESTION 27

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

If you check the website, cards for all three (A, B, G) are supported. See: http://www.stumbler.net/

QUESTION 28

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and infers that they mist 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

Correct Answer: C

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 29

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: and*#@!(%)

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@andba

H. Passwords that contain Uppercase/Lowercase from a dictionary list Example: OrAnGe

Correct Answer: EH

QUESTION 30

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.

D. A sheepdip computers defers a denial of service attack.

Correct Answer: A

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 31

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

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

QUESTION 32

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

Machine A: netcat -1 p 1234

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

B. Machine A: netcat -1 e magickey p 1234

C. Machine A: netcat -1 p 1234

D. Use cryptcat instead of netcat.

Correct Answer: D

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 33

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 suck 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

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 34

_____ 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

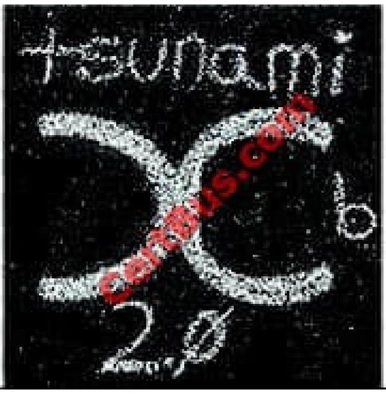
D. Stream Cipher

Correct Answer: C

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 a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext.

QUESTION 35

What does the this symbol mean?



A. Open Access Point

B. WPA Encrypted Access Point

C. WEP Encrypted Access Point

D. Closed Access Point

Correct Answer: A

This symbol is a "warchalking" symbol for a open node (open circle) with the SSID tsunami and the bandwidth 2.0 Mb/s

QUESTION 36

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 fist 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 tires to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill\\'s problem?

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

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 not 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 37

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

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.

QUESTION 38

Jack Hacker wants to break into company\\'s computers and obtain their secret double fudge cookie recipe. Jacks 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

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 39

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

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 40

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?

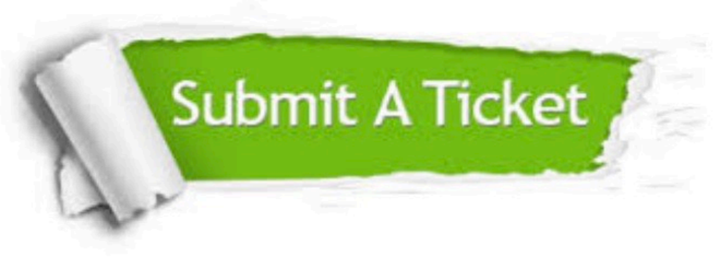
A. Hayden is attempting to find live hosts on her company\\'s network by using an XMAS scan

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


Submit A Ticket