Exam : MK0-201

Title : Certified Penetration Testing Specialist (CPTS)

Ver : 08-21-2008

QUESTION 1:

You have just attempted to perform DNS poisoning on the local network DNS server and did not succeed;you decide to launch an attack against routing tables instead.
Which of the following would NOT be an effective way of attempting to manipulate the routing table on the local network or through its gateway?

A. By using a source route attack
B. By using ICMP redirect messages
C. By adverstising bogus OSDF routes
D. By advertising bogus RIP routes

Answer: C

QUESTION 2:

Why is it so challenging to block packets from Remote Access Troans that use port 80 for network communications?Choose three.

A. To a firewall,the traffic appears simply to be from an internal user making an innoccous HTTP GET request.
B. Port 80 outbound is normally open on corporate firewalls
C. Stateful inspection firewalls will block unsolicited inbound HTTP GET requests
D. Not all firewalls are capable of inspecing data in the HTTP data fields for evidence of tunneling

Answer: A,B,D

QUESTION 3:

Which of the following statements would best describe the act of signing a message with a Digital Signature?

A. The sender creates a hash value of the message he wishes to send
He uses his private key to encrypt the hash value.
The message and the encrypted hash value are sent to the receiver.
B. The sender creates a hash value of the message he wishes to send.
He uses his public key to encrypt the hash value.
The message and the encrypted has value are sent to the receiver.
C. The sender creates a hash value of the message he wihes to send.
The message and the hash value are sent to the receiver.
D. The sender uses his public key to create a digital signature.
The digital signature is sent along with the text message.
The receiver will use the sender private key to validate the signature.

Answer: A

QUESTION 4:

One of the last steps taken by an attacker will be to configure permanent access to a compromised system.
However, the installation of a backdoor, installation of new processes,and changes to key files could be very quickly detected by an administrator.
What tool would assist the attacker in preventing the administrator from detecting changes to files,new processes that are running,or other signs that the system might have been compromised?

A. A Trojan horse
B. A Rootkit
C. A Backdoor
D. A privilege escalation tool

Answer: B

QUESTION 5:

Which of the following tools can detect hidden Alternative Data Streams on an NTFS file or folder?Choose all that apply.

A. Lns.exe
B. Lads.exe
C. FileAlyzer
D. ADSCheker

Answer: A,B,C

QUESTION 6:

In order to idnetify a unique record within a database what would you use?

A. A foreign key
B. A primary key
C. A view
D. A unique key

Answer: B

QUESTION 7:

Why is it important to the security of a network to create a complex password for the SA account on a MSSQL server installation?

A. The SA account is a pseudo-account and does not have any privileges.
B. The SA account can add/delete or change Domain User accounts.
C. The SA account can have privileges of the local adminstrators group on the host OS.
D. The SA account is the most powerful account on the domain controller.

Answer: C

QUESTION 8:

Bryce, who is a great security professional with a perfect track record,has just been called into his supervisor's office.
His supervisor has the sad task of letting him know that hes the next position being cut in their downsizing effort.Bryce has been known to be a mellow type of person but the version of being unemployed after working for 25 years at the same company is just a bit too much for him.He cannot understand why newer employees with only a few years of experience have not been fired before him and why he is the one that must leave.Bryce tells himself that is employer is going to pay dearly for this and hes planning to use his skills to cause disruption within the company infrastructure.
Which of the following term would best describe the reaction of Bryce?

A. Cracker
B. Disgruntied Employee
C. Ethical Hacker
D. Revenge Master

Answer: B

QUESTION 9:

Using Netcat what would be the syntax to setup a listening back door from a compromised Windows Server that will spawn a shell when connecting to the remote server on port 777?

A. nc |p 777 e cmd.exe
B. nc sh p 777 e cmd.exe
C. nc |p 777 sh cmd.exe
D. nc |p 777 exec cmd.exe

Answer: A

QUESTION 10:

Duane is a clever attacker,he has penertrated a system and wishes to hide some files within other files on the file system.Which of the following could be used by Duane to attempt hiding files within the file system?

A. Attrib
B. HideNSeek
C. Chgrp
D. Alternate Data Stream

Answer: D

QUESTION 11:

Which of the following penetration framework is Open Source and offers features that are similar to some of its rival commercial tools?

A. CANVAS
B. CORE IMPACT
C. METASPLOIT
D. DEEP HOLE

Answer: C

QUESTION 12:

Software Restriction Policies,if implemented correctly,can help protect against what kinds of threats? Choose two.

A. Trojans
B. Malware
C. Spam
D. Smurf Attacks

Answer: A,B

QUESTION 13:

If the DS Client software has been installed on Windows 95,Windows 98,and NT 4 comptuers,what setting of the LanMan Authentication level should be applied to counteract LanMan hash sniffing and offline cracking? Choose the best answer.

A. Send NTLM v2/Refuse LM & NTML
B. Send NTLM only
C. Send LM & NTLM responses
D. Send NTLM v2/Refuse LM

Answer: A

QUESTION 14:

Ping utilities can be used for basic network connectivity test; the ping command sends out an ICMP Echo Request packets and the destination host will reply with an ICMP Echo Reply packets if the host is alive.
However,in some cases the host might be alive and responses are not received.What is the most likely cause of such behavior?

A. The packet suffers from time exceeded in transit
B. The packet did not reach the destination gateway
C. A filtering device is dropping the packets
D. The remote device OS does not support the ping command.

Answer: C

QUESTION 15:

When doing a Half-Open Scan what packet type would be expected as a response if the port being probed is closed?

A. FIN
B. ACK
C. RST
D. RST/ACK

Answer: D

QUESTION 16:

Mae i a keen system administration; she constantly monitors the mailing list for best practices that are being used out in the field.On the servers that she maintains,Mae has renamed the administrator account to another name to avoid abuse from crackers.However,she found out that it was possible using the sid2user tool to find the new name she used for the administrator account.Mae does not understand; she has NOT shared this name with anyone.How can this be?What is the most likely reason?

A. Her system have been compromised
B. Renaming the administrator account does not change the SID
C. She has not applied all of the patches
D. Someone social engineered her

Answer: B

QUESTION 17:

What built-in Windows command can be used to help find remote access trojans?Choose the best answer.

A. Netstat a
B. Ipconfig/displaydns
C. Nbtstat c
D. Netdiag

Answer: A

QUESTION 18:

Under the Windows platform,there is something refered to as Null Session.
Which of the following statements would best describe what a null session consists of?

A. It is a session where zero bytes of traffic have been transferred
B. It is a session where erroneous commands are being used showing the a lack of knowledge of the user connected.
C. It is a remote session that is established anonymously to a window machine
D. It is a anonymous FTP session under the Windows platform

Answer: C

QUESTION 19:

Why is tunneling-based trojan software so useful for hackers if it is installed inside a corporate network?Choose the best answer.

A. Tunneling software uses ports that are not well knwon,eg.12345
B. Stateful inspection firewalls can only filter Server ports of 1-1023
C. It makes network penetration trivial the tunneling occurs using Whatever port(s) the firewall is configured to allow
D. Anti-trojan software do not have signatures for tunneling trojans,therefore it is easy to have end-users install tunneling trojans.

Answer: C

QUESTION 20:

On a Linux system,which of the following files would contain the list of user accounts,their shell,and their home directories?

A. useradd
B. shadow
C. passwd
D. group

Answer: C

QUESTION 21:

Looking at the Window presented below,what type of mail server is running on the remote host?

A. Exchange 8.13.4
B. Hotmail 8.13.4
C. Sendmail 8.13.4
D. Exim Mail 8.13.4

Answer: C

QUESTION 22:

Which of the following capabilities do rootkits have?Choose all that apply.

A. Hide any file
B. Hide any process
C. Hide any listening port
D. Cause a blue screen of death on Windows computers.

Answer: A,B,C,D

QUESTION 23:

This document, which is a part of good practices within an organization,describes step by step how to accomplish a specific task.What is the name of this document?

A. Procedures
B. Guidelines
C. Policies
D. Recommendations

Answer: A

Explanation:
Reference: http://en.wikipedia.org/wiki/Procedures

QUESTION 24:

Which of the following password and encryption cracking methods is guaranteed to successfully crack any password or encryption algorithm?

A. Dictionary
B. Hybrid
C. Brute Force
D. RainbowCrack

Answer: B

QUESTION 25:

Which of the following countermeasures could be taken to implement security through obscurity and thus limit reconnaissance if an attacker issues this command against a web server? Choose the best answer.

```
nc www.domain.com 80
GET HEAD HTTP/1.1
[return]
[return]
```

A. Change the default error messages
B. Change the webservers banner
C. Enable SYN flood protection on a capable firewall
D. Change the default homepage

Answer: B

QUESTION 26:

Which of the following SQL scripts will discover the usernames and hashed passwords from a MSSQL server?

A. SELECT *FROM*
B. SELECT name,password FROM master..login UNION ALL SELECT *FROM database.log
C. SELECT name,password FROM master..sysxlogins
D. SELECT uname AND passwd FROM master

Answer: C

QUESTION 27:

What technology has made trojans easy to distribute?Choose the best answer.

A. Digitally Signed Software
B. Assembly language
C. EXE wrappers
D. Personal firewall software

Answer: C

QUESTION 28:

What is traceroute used for?

A. To find gateways that are vulnerable to ICMP based attacks
B. To find the best path to a destination address
C. To find the path a packet traveled to get to the destination address
D. To find the initial TTL (Time to live) value used within a packet

Answer: C

QUESTION 29:

When a digital certificate has been revoked before its expiry date,how will the Certification Authority (CA) that issued the certificate inform other CAs that the specific certificate is no longer valid.

A. By posting it on the CA web site
B. By sending on email message to the other CAs
C. By posting it on the certificate revocation list
D. By posting it on the certificate expiry list

Answer: C

QUESTION 30:

What hashed authentication credentials can be sniffed and possibly cracked offline (assuming time is not an issue)?Choose all that apply.

A. LanMan
B. NTLM
C. Kerberos
D. SHA1

Answer: A,B,C,D

QUESTION 31:

While doing a penetration test you were able to extract a copy of the password database from a Windows server using a vulnerable SQL server that had a blank password.
You now have a copy of the password file in LAN Manager Format,you notice two accounts that could be very interesting to get into.
The first account is the administrator account and there is a terminal user account as well.

It is very likely that the same password might be reused on all hosts for one of these two accounts or both.
Which of the following tools would you to crack the password the fastest?

A. L0pthcrack
B. John the ripper
C. Rainbowcrack
D. Cain&Abel buit in cracker

Answer: C

QUESTION 32:

Billsleigh has been learning about sniffer programs and found out that they can be used to collect information on networks.Billsleigh would definitively like to gather a series of administrative passwords.
Which of the following would be the easiest for Billsleigh to acquire information from using a sniffer?

A. Shared Ethernet
B. Fiber Optic
C. Switch Ethernet
D. ATM Networks

Answer: A

QUESTION 33:

Clement is someone who greatly enjoys fishing.
Clement recently visited a web site that is very proactive in its attempt to save marine life.
While on the site he downloaded a disobedience kit where his free CPU cycle can help contribute to the noble cause of saving the rainbow trout from extinction.
Which of the following terms best describes Clements activity?

A. Compulsive Fishing
B. Hacktivism
C. Green Peace
D. Crackering

Answer: B

QUESTION 34:

Johnny has just installed a small utility to calculate subnet masks.
After installing this utility he was pormpted by his firewall to accept a connection

outbound to a server he was not familiar with.
Further exploration has revealed that there was a new port listening forincoming connection on his computer.
It seems that unwanted software was installed when Johnny installed his great subnet calculator.
What type of malware was he a victim of?

A. Spyware
B. Adware
C. Trojan Horse
D. Virus

Answer: C

QUESTION 35:

Henry and Paul are debating the purchase of a $1500-00 automated vulnerability software package.What is the main disadavantage regarding the automated compared to manual assessments:

A. The network manager gets personal commission when purchasing the software package.
B. False Positive negative results
C. Greater degree of accuracy
D. Reducing Workforce costs

Answer: B

QUESTION 36:

Bob has just produced a very detailed penetration testing report for his client.Bob wishes to ensure that the report will not be chnaged in storage or in transit.What would be the best tool that Bob can use to aasure the integrity of the information and detect any changes that could have happened to the report while being transmitted or stored?

A. A Symmetric Encryption Algorithm
B. An Asymmetric Encryption Algorithm
C. An Hashing Algorithm
D. The ModDetect Algorithm

Answer: C

QUESTION 37:

What Windows techonology should prevent SMB Relay from sniffing user credentials in a man in the middle attack?Choose the best answer.

A. Windows Update
B. SMB Signing
C. NetBIOS over TCP
D. SYSKEY

Answer: B

QUESTION 38:

Bob is using a new sniffer called Ethereal.
However,it seems that Bob can only see packets that are sent from and to his own network interface card (NIC).He cannot see any traffic from the other station.
What could be the cause of Bobs problem?(Select two)

A. The NIC is not in promiscuous mode
B. The network is using UDP traffic
C. Bob is connected to a switched network
D. The sniffer does not support Bobs TCP/IP network stack

Answer: A,B

QUESTION 39:

Name Servers are the Penetration Testers best friend.The Domain Name Registration database contains information about who registered a particular domain.What common command line as well as web based tool could be used to extract this information from the public database of Domain Name registration.

A. Whois
B. traceroute
C. SOA Query tool
D. Resolv

Answer: A

QUESTION 40:

Keystroke loggers can be found in which of the following forms?Choose all that apply.

A. Trojans
B. Spyware
C. Text files
D. A dynamic link library file which replaces the standard GINA.dII

Answer: A,B,D

QUESTION 41:

Nmap is the leading port scanner for security testing and penetration testing.
As a tester it is a must have within your toolbox and you MUST be familiar with its basic syntax.
Which of the following command lines would represent a Ping Sweep being performed using Nmap.

A. nmap sP 10.1.1.0/24
B. nmap sT 10.1.1.0/24
C. nmap sS 10.1.1.0/24
D. nmap sU 10.1.1.0/24

Answer: A

QUESTION 42:

How does a system administrator prevent Idp.exe and user2sid.exe tools from retrieving domain usernames,SIDs,and other information from a Windows 2000 Domain Controller if no username and password are supplied?Choose two.

A. Add the Everyone group to the Pre-Windows 2000 Compatible Access group
B. Remove the Everyone group from the Pre-Windows 2000 Compatible Access group
C. set RestrictAnonymous registry key to two
D. Set RestrictAnonymous registry key to zero

Answer: B,C

QUESTION 43:

Session Hijacking is possible due to which weakness within the TCPIP stack implementation?

A. Initial Sequence Number prediction
B. Flags are not validated properly,it is possible to set all flags to 1 or 0.
C. Validation of the size of a packet after reassembly is not implemented properly.
D. Initial Sequence Number are too low

Answer: A

QUESTION 44:

Why are SYN port scans not as stealthy as what they originally were several years ago?Choose two.

A. Many firewall rulesets detect and block SYN scans
B. IDS systems look for SYN flag packets due to the proliferation of SYN flood-based denial of service attacks
C. RFC 3502 has redefined the TCP three-way handshake thus changing how SYN flags are used
D. The Internet-backbone routers all block SYN flag packets according to new RFC 3705

Answer: A,B

QUESTION 45:

Which tools are capable of capturing Kerberos domain authentication credentials and then running either dictionary or brute force offline password cracking?Choose two.

A. LC5
B. Cain and Abel
C. Ettercap
D. Kerbsniff & kerbcrack

Answer: B,D

QUESTION 46:

Which of the following items is the least likely to be found while doing Scanning?Choose the best answer.

A. IP addresses
B. Operating System
C. System Owner
D. Services

Answer: C

QUESTION 47:

Nathalie,an employee of Corporation XYZ, has notice that Bob,one of her coworkers,has been abusing company assets and resources for his own personal gain.
According to good ethics values,what should Nathalie do in this case?

A. Immediately install a network sniffer and keystroke recorder to monitor Bobs activities.
B. Retaliate by abusing Bobs resources; he does it to the company,hence why not do it against Bob himself.
C. Report Bob to upper management where a decision about a course of action can be made along with the HR and Legal department.
D. Nathalie should not get involved;this is none of her business.

she should simply continue her work day and wait unit he gets caught.

Answer: C

QUESTION 48:

MS SQL server makes use of Stored Procedures.There is an extended stored procedure called sp_makewebtask that can be used with data being returned from executed queries.What would you use this stored procedure for?

A. It is used to start a new web server instance
B. It is used to create and HTML page
C. It is used to perform an entry within a database
D. It is used to schedule a job task

Answer: B

QUESTION 49:

You are concerned about other people sniffing your data while it is travelling over your local network and the internet.
Which of the following would be the most effective countermeauser to protect your data against sniffing while it is in transit?Choose the best answer.

A. Encryption
B. AntiSniff
C. PromiScan
D. Usage of a switch

Answer: A

QUESTION 50:

Which Vulnerability Assessment tools perform dangerous/destructive scans.Choose two.

A. MS Baseline Analyzer
B. Nessus
C. Snort
D. X-Scan

Answer: B,D

QUESTION 51:

Which of the following would represent a technique to embed data within another file whereby it would be near impossible for anyone using or looking at the file to claim that there might be a message hidden within the media or the existence of some from of message?

A. Cryptography
B. Encryption
C. Steganography
D. MimiCry

Answer: C

QUESTION 52:

You have collected a series of messages that are all encrypted.
You do not have access to the matching plaintext nor do you have any idea of the key and algorithm that were used to encrypt those messages.You will attempt a crypto attack in order to find the key.
How would you call such an attack?

A. chosen Plaintext Attack
B. Known ciphertext attack
C. Chosen Key Attack
D. Cliphertext only attack

Answer: D

QUESTION 53:

Which programs might an attacker use to facililate sniffing in a switched network?Choose all that apply.

A. Ettercap
B. Cain and Abel
C. MACof
D. Etherflood

Answer: A,B,C,D

QUESTION 54:

Noah,a penetration tester,has been asked by Certkiller .com to perform a security test against the company network from an internal location.
The owner of Certkiller .com has provided Noah with a network diagram,documentations,and assistance.
Which of the following would best describe the type of test that Noah is about to perform?

A. Black Box
B. Zero Knowledge
C. White Box
D. Gray Box

Answer: C

Explanation:
Also known as glass box, structural, clear box and open box testing. A software testing technique whereby explicit knowledge of the internal workings of the item being tested are used to select the test data. Unlike black box testing, white box testing uses specific knowledge of programming code to examine outputs. The test is accurate only if the tester knows what the program is supposed to do. He or she can then see if the program diverges from its intended goal. White box testing does not account for errors caused by omission, and all visible code must also be readable.
http://www.faqs.org/faqs/software-eng/testing-faq/section-13.html

---

QUESTION 55:

The SNMP protocol makes use of community sring to control access.There are two community strings being used; each of these strings allow you to perform only specific functions within the system being managed by SNMP.which of the following would represent the functions allowed by the two strings?Choose two)

A. Public Gives public access to anyone to reconfigure the device
B. Secret Gives read only access to the remote device being managed
C. Public Gives read only access to the remote device being managed
D. Private Gives read and write access to the remote device being managed

Answer: C,D

QUESTION 56:

Why is it often recommended to rename the built-in Administrator account on a Windows 2000 domain? Choose the best answer.

A. Renaming the Guest account is of little value.
B. If you dont rename the Administrator account you will have NetBIOS name conflicts with the Administrator account from other domains in the forest.
C. Account lockout will not stop password guessing attacks via SMB filesharing or BASIC web authentication against the built-in Administrator account .
D. The default domain policy actually requires the Administrator account to be renamed.

Answer: C

QUESTION 57:

What technology can be deployed at the network layer to protect against snififng?Choose the best answer.

A. SSL
B. Certificates
C. IPSec
D. DAI

Answer: C

QUESTION 58:

When referring to the prevalence of online computer crimes,which of the following would NOT be a factor that contributes to the proliferation or computer crimes?

A. Widespread availability of computers
B. Widespread availability of hacking tools
C. The media and press coverage of incidents glamorizing hackers
D. The laws and penalties associated with online crimes

Answer: D

QUESTION 59:

This technique consists of using social to trick someone into revealing information they should not usually release to unathorized users.
What do we call this technique or type of attack?

A. Shoulder Surfing
B. Eavesdropping
C. Social Engineering
D. Social Coining

Answer: C

QUESTION 60:

A null session allows users to connect remotely to other Windows computers on the network.According to the implementation of NULL sessions of Windows platforms,how long would the password be in order to establish a NULL Session?

A. At least 8 Characters
B. A passphrase is used not a password
C. There is no password involved

D. Windows makes use of Digital Signature in such case,not passwords

Answer: C

QUESTION 61:

A Windows computer that has not been hardened properly might allow NULL connection from a remote host.
Which of the following commands would be used by a remote attacker to attempt connecting using NULL session?

A. net use \\servername\ipc$NULL/u
B. net use \\servername\ipc$u:
C. net share \\servername\ipc$/u:
D. net use \\servername\ipc$/u:NULL

Answer: B

QUESTION 62:

What sniffer program is capable of reconstructing associated TCP packets into a sessions showing application layer data from the client to the server and vice-versa?Choose the best 2 answers.

A. Packetyzer
B. Etherape
C. Ethereal
D. ARPwatch

Answer: A, C

QUESTION 63:

Which of the following commands would capture all packets going to and from IP address 192.168.1.2 using tcpdump?

A. tcpdump host 192.168.1.2
B. tcpdump dest 192.168.1.2
C. tcpdump any 192.168.1.2/32
D. tcpdump all 192.168.1.2/24

Answer: A

QUESTION 64:

Why is passive sniffing much harder to detect,if not impossible,compared to active sniffing?Choose the best answer.

A. Passive sniffing injects fewer packets into the switch
B. Passive sniffing can be done only via software and not hardware
C. A device that only receives packets and never transmits packets is truly undetectable.
D. It is difficult to obtain software that passively sniffs

Answer: C

QUESTION 65:

What is one way an attacker can use to determine if a database front-end application is vulnerable to SQL injection?

A. By entering a single star (*)in the username field.
B. By entering all outgoing TCP connections after browsing the web application.
C. There is no way to check,they just have to attempt on attack.
D. By entering a single quota ( ) in the password field.

Answer: D

QUESTION 66:

An attacker is sending packets with no flag set.This is also known as doing a NULL scan.Usually,operating system networking stacks will respond with a RST packe,however,some operating systems do not conform to this behavior and respond in appropriately. Such behavior could allow for the identification of the remote OS being used.Which of the following would be one of the Operating systems that responds differently?

A. Solaris
B. Linux
C. Windows
D. HP-UX

Answer: C

QUESTION 67:

Which of the following protocols usually make use of the UDP protocol while querying querying information and the TCP protocol for some other functions?

A. SMTP
B. HTTP
C. DNS
D. TELNET

Answer: C

QUESTION 68:

What are some of the weaknesses that make LAN Manager Hashes much easier to crak by an attacker? (Select all that apply.)

A. The 14 character paasword is split in two
B. The password is converted to Uppercase
C. The hash value is encrypted using MD5
D. The hash value is encrypted with AES

Answer: A,B

QUESTION 69:

What might be good countermeasures to protect the built-in administrator account from automated Terminal Server password guessing programs like tsgrinder?Choose tw.

A. Enable account lockout.
B. Set a complex password that is at least 8 characters or more in length.
C. Using TSVER Resource Kit tool to customize which 4-digit version numbers of the Remote Desktop Client 5.1 software are allowed to connect.
D. Run Terminal Server on a computer located in the DMZ

Answer: B,C

QUESTION 70:

Looking at the graphic presented below,what version of Internet Protocol was used on the network where this packet was sent?Extract the information from the Hex dump below.

A. IP Version 4
B. IP Version 6
C. IP Version 4.5
D. IP Version 45

Answer: A

QUESTION 71:

Automated tools are not always adept at identifying remote applications.By inspecting banners presented when connecting to a specific port,it is possible to gather more information.Considering the graphic below,what type of web server is running on the remot server that you attempted to connect to?

A. IIS 4.0
B. IIS 5.0
C. Netscape Enterprise
D. Apache

Answer: D

QUESTION 72:

A direct attack on a database system is one that attacks what?

A. The application code of the database system.
B. The data residing on the database tables.
C. The web front-end to the database
D. The first user account created on the database server.

Answer: A

QUESTION 73:

To uniquely identify an active session,TCPIP protocol will make use of the client IP address and port as well as the destination IP address and port.
How are these four elements matched together called?

A. Client-Server Pair
B. Socket
C. Session Identifier
D. Server-Client pair

Answer: B

QUESTION 74:

What technology can be deployed at the network layer to protect against sniffing?Choose the best answer.

A. SSL
B. Certificates
C. IPSec
D. DAI

Answer: C

QUESTION 75:

When conducting a TCP scan for SQL servers on a given network address range,what port is being interrogated?

A. 1453
B. 1334
C. 1433
D. 1434

Answer: C

QUESTION 76:

You have been hired by company WXY to perform a Penetration Test,in this first phase of your test you have been challenged to remain totally stealthy. Which of the following reconnaissance types would best be used in such a scenario?

A. Active
B. Passive
C. Intrusive
D. Allusive

Answer: B

QUESTION 77:

A normal TCP connection is always established by using what is called a TCP Three Way Handshake. Which of the packet sequences below would represent a normal TCP connection establishment?

A. SYN,SYN/ACK,ACK
B. SYN,PSH,ACK
C. ACK,SYY,SYN/ACK
D. FIN,ACK,SYN

Answer: A

QUESTION 78:

Footprinting is one of the first steps performed by a Penetration Tester.
Many security testers neglect to perform this phase whereby you have the opportunity to easily information that can later be matched with technical discovery to give you a greater assurance in your finding.
Which of the following would NOT be doen in the footprinting phase?

A. Collecting DNS registration information
B. Finding network IP addresses range in public DB

C. Maintaining Access
D. Visiting and querying the Security Exchange Commission database.

Answer: C

QUESTION 79:

Which of the following scan types would be the least accurate scan considering that may other network conditions could indicate that the port is open even though it might not be open?

A. Vanilla TCP Port Scan
B. UDP Port Scan
C. Half-Open Scan
D. Inverse TCP Scan

Answer: B

QUESTION 80:

When would a secondary name server perform a zone transfer to update its entries and synchronize its database with the primary name server?

A. At random intervals
B. When instructed to do so
C. When its serial number is lower than the primary DNS server
D. When its Time To Live value is lower than the primary DNS server

Answer: C

QUESTION 81:

Bob is doing a penetration test.
He was able to get system level access on one of the servers exploiting one of the known weaknesses of the web server.
Bob attempted to copy the SAM database but it was locked and his operation was not allowed.
How could Bob succeed in getting a copy of the SAM database if it locked while the system is up and running?

A. By bringing the system to single user mode
B. By running samdumpt to create a backup of the SAM
C. By running rdisk /s to create an unlocked backup copy of the SAM
D. By changing the permissions on the file using his System privileges

Answer: C

QUESTION 82:

Wireless Local Area Networks (WLAN) are becoming increasingly popular.
In order to link a wireless network to a wired network what type of device would be used?

A. SSID
B. Access Point
C. Switch
D. Hub

Answer: B

QUESTION 83:

Which of the following resource records would you inspect to find out how long a cache poisoning attack might be effective against a remote DNS server?

A. MX
B. NS
C. SOA
D. PTR

Answer: C

QUESTION 84:

Nathalie has just received a message from her boyfriend,Clement,who is telling her about this severe Popoute virus that none of the virus companies have been able to stop.
In the same message Clement is asking her to pass the message along to anyone she can in order to ensure they will protect themselves before infection.After validating with her IT department it becomes obvious that there was no virus named Popoute that ever existed and that resources have been wasted by the large amount of emails that were sent and time wasted.
What would you call such activities?

A. A joke
B. A hoax
C. A Worm
D. A Troan

Answer: B

QUESTION 85:

When dealing with Wireless Local Area Networks a client will associate with the closest access point.What does the closest access point mean in such a case?

A. The access point that is geographically located the closest to the client
B. The access point that has the strongest signal received by the client
C. The access point that has a frequency that is the closest to the frequency used by the client
D. The access point that has the least number of client connected at the specific time.

Answer: B

QUESTION 86:

On Wireless networks, what is the Service Set Identify used for?

A. It is the network password
B. It is used on the primary key for WEP
C. It is used to distinguish one network from another
D. It is used to authenticate clients.

Answer: C

QUESTION 87:

Which are methods that attackers use to find buffer overflows?Choose all that apply.

A. Trial and error
B. Decompile the executable binary of the application
C. Decompile the executable binary of a software patch
D. Analyze source code,if available

Answer: A,B,C,D

QUESTION 88:

Traditional firewalls have serious limitations where the data payload is not being inspected.These firewalls usually tend to work within the lower layer of the OSI model. What layer does traditional firewall monitor?

A. Layers 2 to 4
B. Layers 2 to 5
C. Layers 2 to 6
D. Layers 1 to 4

Answer: A

QUESTION 89:

While exploiting remote targets using exploits,there are a few stages that have to take place.
Which of the following stages is the payload which is executed after exploitation?

A. Shellcode
B. Injection Vector
C. Request Builder
D. Handler routine

Answer: A

QUESTION 90:

The nbstat tool is used to query the NetBIOS name table from a remote Windows system.The table below shows a sample output of the tool.
The second column is a two digit hexadecimal number that identiifies what the services and entities on the specific machine are.
If you look at line number 3 (in bold below),what does the 20 indiate?

A. The server service is running.
B. The RAS Client service is running.
C. The messenger service is running.
D. The workstation service is running

Answer: A

QUESTION 91:

SSL can be used to protect information sent over a public network while surfing the web.
During the establishment of a secure SSL session,on which side of the communication link is the session key created?

A. It is generated by the server
B. It is generated by the client
C. It is preconfigured on the web server
D. There is no session key used,only public and private keys are being used

Answer: B

QUESTION 92:

Which of the following methods would allow an attacker to get access to the local SAM file if the attacker had physical access? Choose three.

A. Reboot with a Linu-based floppy or CD that can read NTFS filesystems
B. Reboot with NTFSDOS floppy and copy the SAM file
C. Physically remove the hard drive and install it as a second drive in another Windows computer
D. Rebooting into Windows using Safe Mode.

Answer: A,B,C

QUESTION 93:

To prevent the storage of hashes in LANMAN format in either the local SAM file or in Active Dierctory for computers running Windows 2000 SP2 or later,which of the following registry settings should be applied?Choose the best answer.

A. NoLMSam=1
B. NoLMSam=0
C. NoLMHash=1
D. NoLMHash=0

Answer: C

QUESTION 94:

There is a method which allows you to find information on hosts located behind a firewall by using packets similar to the packets used by Traceroute.
This method attempts to find out what are the rules in place on the gateway.
What is the name of this method?

A. NULL Scan
B. Firewalking
C. Tracert
D. FWpenetrate

Answer: B

QUESTION 95:

Which of the following ports could be associated with a trojan on a Windows computer? Choose two.

A. 135
B. 3268
C. 12345
D. 27374

Answer: C,D

QUESTION 96:

Looking at the SOA records presented below,how long will the secondary server wait before it reattempts to synchronize with the primary server if it was not able to do so when it reached its refresh time of 2 days as presented in the SOA below?

A. 15 minutes
B. 10 minutes
C. It will never retry and will wait another two days
D. 900 minutes

Answer: A

QUESTION 97:

From the items listed below,which would be expected from a cracker or hacker but NOT from an Ethical Hacker or Certified Penetration tester?

A. Code of ethics
B. Signed Authorization
C. Disregard for potential losses
D. Presentation of a detailed report

Answer: C

QUESTION 98:

Which of the following scanning methods would be the most stealthy and best at hiding the source of a scan?

A. TCP Connect()
B. Syn-Ack
C. Fin-Ack
D. Idlescan

Answer: D

QUESTION 99:

Certkiller .com has been getting numerous complaints that one of their employees has been actively probing remote DNS servers and attempting to extact information from them.
After investigation it was detected that jack had used the nslookup command entensively and he also issued commands within nslookup such as server [remoteip]where[remoteip]is the IP address of the target he was probing.

Further investigation also revealed that he used the command is d targetdomain.com where targetdomain.com was the ddomain name he was attempting to get more info about,what was jack really attempting to achieve in this case?

A. See the UNIX permission of files
B. Perform a zone transfer
C. Perform a lookup on user and group permissions of files
D. Perform a zone incremental query

Answer: B

QUESTION 100:

Looking at the graphic below,determine what web site was visited by the user located at IP address 192.168.1.104?

A. Netcraft.com
B. Instacontent.net
C. Geogle.com
D. This sniffer capture is not from a web page request

Answer: C

QUESTION 101:

SQL injection is defined as?

A. The gaining of access to an operating system by injecting code into a system process.
B. The destruction of databases by mailicious code.
C. The destruction of databases by malicious code.
D. Altering data on a victims database server to that of a hackers choice.

Answer: B

QUESTION 102:

Select the best method of securing the underlying data tables on a database system.

A. Create service accounts with the correct privileges for the action the user is carrying out, i.e.read only or full control.
B. Allow only users to connect as the SA account.
C. Create a service account with full access privilege over the underlying data tables.
D. Allow only applications to interrogate a mirror of the database.

Answer: A

QUESTION 103:

When a network switch receives a very large quantity of random MAC addresses which would overfill the Content Addressable Memory (CAM) table,how will the switch react?

A. It will drop packets until the tables are cleard and then will resume normal processing.
B. It will drop the oldest entries in the CAM table to make room for the new packets and will continue working normally
C. It will revert to being a HUB and will broadcast all traffic on each of the ports
D. It is impossible to flood the MAC tables because of their very large size.

Answer: C

QUESTION 104:

Having just downloaded a new version of Cain & Abel,you wish to monitor your network for clear text passwords being sent.
Knowing you are currently connected to a switch you will attempt to perform an ARP poisoning attack that will let you look at all the packets and not only packets sent to your own machine.
What would you call this type of sniffing?

A. Passing Sniffing
B. Active Sniffing
C. ARP Sniffing
D. All stations sniffing

Answer: B

QUESTION 105:

Types of potential vulnerabilities that are commonly scanned for include:(Choose All that Apply)

A. Password vulnerabilities
B. Weak operating system and application default settings
C. Common configuration and coding mistakes
D. Protocol vulnerabilities (such as the TCP/IP stack vulnerabilities)
E. Physical observation of the target building

Answer: A,B,C,D

QUESTION 106:

If IPSec cannot be implemented to secure network communication from sniffing,what program would be an alternative choice for secure terminal logins and file transfers on

Windows computers?Choose the best answer.

A. Hyperterm
B. puTTY
C. Sterm
D. WinPCap

Answer: B

QUESTION 107:

Given the following diagram,what ports shouldbe blocked on the perimeter and internal firewall to best protect the Microsoft SQL databae server from unauthorized inbound connections?

A. 1433, 1434
B. 443, 434
C. 1443,1444
D. 80,139

Answer: A

QUESTION 108:

Which of the following wouldbest match the following description.A program that looks useful at first sight but attempt to break your security policy by installling unwatned software or remote access software without your knowledge?

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

Answer: C

QUESTION 109:

Which of the following password and encyption cracking methods is guaranteed to successfully crack any password or encryption algorithm?

A. Dictionary
B. Hybrid
C. Brute Force
D. RainbowCrack

Answer: B

QUESTION 110:

After completing your reconnaissance and scanning,which of the following would be the next logical step performed bye the Pen Tester?

A. Vulnerability Assessment
B. Enumeration
C. Privilege Escalation
D. Clean up

Answer: B

QUESTION 111:

Clement is someone who greatly enjoys fishing.
Clement recently visited a web site that is very proactive in its attempt to save marine life.
While on the site he downloaded a disobedience kit where his free CPU cycle can help contribute to the noble cause of saving the rainbow trout from extinction.
Which of the following terms best describes Clementss activity?

A. Compulsive Fishing
B. Hacktivism
C. Green Peace
D. Crackering

Answer: B

QUESTION 112:

Which of the following are reasons why fragment-based port scans are often used by attackers?Choose two.

A. Simple non-stateful packet filtering devices can sometimes be bypassed
B. Reassembling fragmented packets is not time or processor intensive
C. RFC 1121 requires that all routers pass fragmented packets
D. Firewalls may be configured for high throughput and thus dont reassemble and inspect fragmented packets

Answer: A,D

QUESTION 113:

What technologies could a company deploy to protect all data passing from an employees home computer to the corporate intranet?Choose two.

A. L2TP/IPsec
B. PPTP/MPPE
C. WEP
D. IKE

Answer: A,B

QUESTION 114:

While doing your testing you discover an MS SQL server within the target range.You attempt to connect to the SA account using the default password which is usually blank.You quickly find out it is not working and the password was changed.Which of the following tools could be used to attempt finding what the new password could be?

A. sqlexec
B. sql2.exe
C. sqlbf
D. Buildsql

Answer: C

QUESTION 115:

Which of the following is the most effective way to reduce the threat of social engineering?Choose the best answer.

A. Require employees to sign a computer usage policy
B. Prevent employees from going to happy hour
C. Require employees to communicate only face-to-face
D. Extensive user education on the nature of social engineering

Answer: D

QUESTION 116:

Looking at the results of hping2 below,what does the flag=RA portion of the response most likely indicate in this case?

A. The ports is open and waiting for connections
B. The port is closed
C. The port is filtered
D. There are no ports open on the remote host

Answer: B

QUESTION 117:

A TCP connect Scan which is also called a Vanilla TCP port scan will send a SYN packet to ports sequentially to see which are open.
Using the Vanilla TCP Port Scan, what would be expected as a response from a port that is open?

A. FIN
B. SYN/ACK
C. RST/ACT
D. ACK

Answer: B

Explanation:
During the Vanilla TCP Connect scan, a hacker sends the first packet of the handshake sequence with the Synchronize flag (SYN) set to the intended target device. If the target port is closed, the target device sends a TCP reply with the Reset (RST) flag set. If the target port is open, the target device sends a TCP reply with the SYN and Acknowledgment (ACK) flag set. Finally, the hacker sends an ACK response to complete the three-way TCP handshake.

QUESTION 118:

A malicious hacker has been trying to penetrate Certkiller .com from an external network location.He has tried every trick in his bag but still did not succeed.
From the choice presented below,what type of logical attempt is he most likely to attempt next?

A. Elevation of privileges
B. Pilfering of data
C. Denial of service
D. Installation of a back door

Answer: C

QUESTION 119:

As you have learned in your Penetration Testing training or field experience,WEP is the encryption that was used with early WLAN implementation.it uses a stream cipher called RC4 to produce a string of bith that will be exclusive OR or XOR with the plain text to form the cliphertext.Which of the following statements represents the rules associated with XOR binary mathematics or comparison?Choose the best answer.

A. If both bits are different the result will be one,if both bits are the same the result will be a zero.
B. If both bits are different the result will be zero,if both bits are the same the result will

be a one.
C. Only when both bits have a value of one,will the result be one.
D. Only when both bits have a value of zero,will the result be one.

Answer: A

QUESTION 120:

Which of these methods would be considered examples of active reconnaissance? (Choose three.)

A. Ware dialing
B. Firewalking
C. Whois lookup
D. FTP banner retrieval

Answer: A,B,D

QUESTION 121:

Which tool speeds up offline password cracking by precomputing tables of password hashes?Choose the best answer.

A. John the Ripper
B. Xcrack
C. Rainbow Crack
D. Cisilia

Answer: C

QUESTION 122:

Dozens of methodologies exist on the market today.Most of them follow the very high level steps.
Which of the following would represent the most common and logical approach to penetration testing from the first step being accomplished on the left to the last step being done on the right side of the statement below?

A. Scanning,Footprinting,Enumeration,Penetration
B. Footprinting,Enumeration,Scanning,Penetration
C. Footprinting,Scanning,Enumeration,Penetration
D. Penetration,Enumeration,Scanning,Footprinting

Answer: C

QUESTION 123:

What are the possible countermeasures to buffer overflow exploits?Choose all that apply.

A. Apply patches as soon as patches testing is completed
B. Learn 0-day exploits from hacker websites
C. Close the port of service at the firewall if there is no patch yet avilable
D. Run application and services with the least privilege necessary

Answer: A,B,C,D

QUESTION 124:

When a company wishes to have some asurance that a product is working as per the vendor claim they usually seek certification.One of the most commonly used certification schemes today is called Common Criteria (CC).Which of the following terms describe a product that is to be evaluated under the Common Criteria to see how well the product meets the claims made by the vendor?

A. Security Target
B. Target of evaluation
C. Protection Profile
D. EAL4

Answer: B

QUESTION 125:

Which of the following password implementation is found only in Windows 2000 and newer Windows versions?

A. LM
B. NTLM
C. NTLMv2
D. Kerberos

Answer: D

QUESTION 126:

Which of the following enumeration techniques can reveal the true built-in Administrator account even if has been renamed?Choose two.

A. Banner grabbing
B. NetBIOS null session
C. DNS zone transfers

D. SNMP with default community name

Answer: B,D

QUESTION 127:

Which of the following might be used to give false positives when a UDP scan is being performed against a DMZ server running DNS? Choose the best answer.

A. On the firewall,block ICMP TTL Exceeded
B. On the firewall,block all incoming UDP
C. On the firewall,block all TCP SYN packets
D. On the firewall,block all ICMP Port Unreachable messages

Answer: D

QUESTION 128:

Looking at the graphic presented below,what destination port is highlighted in the Hex dump presented?
Extract the information from the Hex dump packet captured below.

A. 53
B. 69
C. 50
D. 80

Answer: D

QUESTION 129:

There are different types of access control that can be used within a company.Logical security will be directly affected depending on the type that you select.
Which of the following access control tyeps would be best to assign permissions according to the job an employee has within a company?

A. Rule Based Access Control
B. Discretionary Access Control
C. Role Base Access Control
D. Task Based Access Control

Answer: C

QUESTION 130:

Which of the following statements would be TRUE when referring to Stream cliphers?

A. Stream Ciphers encrypt one digit at a time
B. Stream Ciphers divide the plaintext message into fixed group of bit and then encrpt these group of bits
C. Stream Ciphers are NOT very commonly used
D. Stream Ciphers can be implemented only in software

Answer: A

QUESTION 131:

At times a tester will be challenged to craft a packet that needs a special quantity of payload data, a specific starting TTL value,a specific speed at which the packet can be sent,and specific number of outgoing packets,and/or very specific IP protocol. Which of the following tools would be best for use for that specific purpose?

A. Hping
B. Hydra
C. Nmap
D. Queso

Answer: A

QUESTION 132:

Which of the following is the best security risk that has been experienced within applications over the past few years?

A. Buffer Overflow
B. Heap Overflow
C. String Overflow
D. Format Bug Overflow

Answer: A

QUESTION 133:

Under the SNMP protocol,what does a trap consist of?Choose the best answer.

A. It is an early implementation of an Honeypot
B. It is a backdoor left the developer for quick access
C. It is an alarm sent by the agent to the manager
D. Older mechanism that is no longer used by SNMP

Answer: C

QUESTION 134:

What does the union operation perform when attempting to execute an SQL Injection through a web form?

A. Union Operation permits combining two results
B. Union Operation permits changing the DB password
C. Union operation is used to combine two accounts
D. Union operation is used to combine two tables

Answer: A

QUESTION 135:

How does a system administrator prevent Idp.exe and user2sid.exe tools from retrieving domain usernames,SIDs,and other information from a Windows 2000 Domain Controller if no username and password are supplied?Choose two.

A. Add the Everyone group to the Pre-Windows 2000 Compatible Access group
B. Remove the Everyone group from the Pre-Windows 2000 Compatible Access group
C. Set RestrictAnonymous registry key to two
D. Set RestrictAnonymous registry key to zero

Answer: B,C

QUESTION 136:

Under the Windows platform,there is something refered to as Null Session.
Which of the following statements would best describe what a null session consists of?

A. It is a session where zero bytes of traffic have been transferred
B. It is a session where erroneous commands are being used showing the lack of knowledge of the user connected.
C. It is a remote session that is established anonymously to a Windows machine.
D. It is a anonymous FTP session under the Windows platform

Answer: C

QUESTION 137:

Nathalie is exclusively making use of a public key crypto system to communicate with her peers.
She would like to send information to Bob while protecting the confidentiality of the content being sent over the public network.
She will ask Bob to send one of his keys that she will use to encrypt the message content before sending it.

Which key will Bob send to Nathalie?

A. His private key
B. His secret key
C. His public key
D. His symmetric key

Answer: C

QUESTION 138:

Why is it more difficult to santilize information about a company that has publicly-traded stock?Choose the best answer.

A. The company wants to promote itself as much as possible
B. The company must regularyly submit financial information to the Securities and Exchange Commission which is then made public
C. It is impossible to remove information from search engines databases
D. The company must hire a security consultant with the expertise to santize the information.

Answer: B

QUESTION 139:

What program can locate computers running sniffers by sending out special ARP packets that only network cards in promiscuous mode will reply to?Choose the best answer.

A. ARPwatch
B. Cain and Abel
C. Macof
D. Microsoft Network Monitor

Answer: D

QUESTION 140:

When you create a hash value of the message you wish to send,then you encrypt the hash value using your private key before sending it to the receiver in order to prove the authenticity of the message.What would this be called within the cryptography world?

A. Hashing
B. Digital Signature
C. Encryption
D. Diffie-Hillman

Answer: B

QUESTION 141:

To block tunneling remote access trojans like 007Shell,what should you do on your firewall?Choose the best answer.

A. Block all IGMP
B. Block UDP port 1900
C. Block all ICMP
D. Block TCP port 27374

Answer: C

QUESTION 142:

Intrusion Detection Systems have multiple ways to decode the information. Which of the following definitions would best describe Protocol Anomaly Detection within an Intrusion Detection System (IDS) engine?

A. Interprets the attack as the victim would for greater accuracy
B. Identifies attacks that are based on condition,not patterns
C. Compares traffic to RFC standards and reports deviations
D. Identifies traffic that breaks policy or is not normal for network

Answer: C

QUESTION 143:

Mary has learned about the different ways authentication can be implemented on a web site. Which of the following forms of authentication would consist of the most basic form and also the less secure?

A. Digest Authentication
B. Basic Authentication
C. LDAP Authentication
D. Token Base Authentication

Answer: A

QUESTION 144:

Which of the following exploits/abuse would all be located at the network layer of the OSI model?(Choose all that applies)

A. Route Spoofing
B. IP Source routing
C. IP Source Address Spoofing
D. ARP Spoofing

Answer: A,B,C

QUESTION 145:

How would you call a malware that is set to trigger at a specific date,or sometime in the future?

A. Virus
B. Worm
C. Time Bomb
D. Clocking

Answer: C

QUESTION 146:

Looking at the SOA records presented below,for how long will the secondary DNS servers attempt to contact the primary DNS server before a zone be considered dead.

A. One week
B. Two weeks
C. 5 days
D. 8 days

Answer: B

QUESTION 147:

Which of the following is NOT a tool that could be used to perform a zone transfer?

A. DIG
B. Host
C. Nslookup
D. WHOIS

Answer: D

QUESTION 148:

When a piece of malware executes on a computer,what privilege level or account will it execute under?Choose the best answer.

A. System
B. Administrator
C. Same privilege as the user who isntalled it
D. Always runs as System or above

Answer: C

QUESTION 149:

Why are SYN port scans not as stealthy as what they originally were several years ago?Choose two.

A. Many firewall rulesets detect and block SYN scans
B. IDS systems look for SYN flag packets due to the proliferation of SYN flood-based denial of service attacks
C. RFC 3502 has redefined the TCP three-way handshake thus changing how SYN flags are used
D. The Internet backtone routers all block SYN flag packets according to new RFC 3705

Answer: A,B

QUESTION 150:

Which of the following actions can often be used as countermeasures to port scans?Choose all that apply.

A. Block unassigned port traffic
B. Monitor transport-layer connections (control of TCP,SYN,RST,ACK)
C. Block ICMP type 3 and 8
D. Use active network monitoring

Answer: A,B,C,D

QUESTION 151:

Spyware is either hardware or software installed on a computer which gather information about the user for later retrieval by whoever controls the Spyware.
It is installed without the users knowledge
What are the two ctegories of Spyware that exist? (Choose two from the list below)

A. Surveillance
B. Screen capture
C. Key loggers
D. Advertising

Answer: A,D

QUESTION 152:

MS SQL server makes use of Stored Procedures.There is an extended stored procedure called sp_makewebtask that can be used with data being returned from executed queries.What would you use this stored procedure for?

A. It is used to start a new web server instance
B. It is used to create and HTML page
C. It is used to perform an entry within a database
D. It is used to schedule a job task

Answer: B

QUESTION 153:

Which of the following statements explain why hardware-based keystroke loggers are so dangerous?Choose three.

A. They are expensive.
B. They can be installed or removed in seconds.
C. They are totally transparent to both the operating system and the user applications
D. Neither system administrator nor users routinely inspect the back of their PCs for suspicious devices

Answer: B,C,D

QUESTION 154:

Wayne,who has a twisted mind,has been watching security mailing lists very closely.Today he has seen a new vulnerability announcement that affects multiple mail servers.Jack wishes to scan the internet for servers that are running one of those vulnerable mail servers.His intent is to do this passively at first by doing DNS queries using the nslookup command.
What type of resource record is Wayne looking for within the DNS query results?

A. Only A resource record
B. Only PTR records
C. Only MX records
D. Only CNAME records

Answer: C

QUESTION 155:

Which of the following is a MS Access database SQL injection script?

A. OR a=a
B. AND 1=1
C. OR 1=1-
D. SELECT *FROM*

Answer: A

QUESTION 156:

Pieces of malware code are getting smarter all the time.
It seems it always finds a way of reinstalling itself on a system after it has been removed.
If you wish to look for malicious registry entries that could be used to restart such malware on a Windows XP computer,which of the following entries would you be looking for? (Choose two from the list below)

A. HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
B. HKLM\Software\Microsoft\windows\CurrentVersion\XP\Startup
C. HKLM\Software\Microsoft\Windows\CurrentVersion\Run
D. HKLM\Software\Microsoft\Windows\CurrentVersion\XP\Run

Answer: A,C

QUESTION 157:

What technologies could a company deploy to protect all data passing from an employees home computer to the corporate intranet?Choose two.

A. L2TP/Ipsec
B. PPTP/MPPE
C. WEP
D. IKE

Answer: A,B

QUESTION 158:

Bob has heard about weaknesses related to phone systems from one of his phreaker friends.His friend warns him about the potential danger of listening devices that are sometimes badly configured.Bob is interested in being proactive and he would like to perform a validation of his company phone number range to see if there are any listening devices that might be used by a malicious attacker to get access to the internal network.What category of tool would Bob use for this purpose?

A. Worm Software
B. War Driving Software
C. War Dialing Software
D. A dialup connection software

Answer: C

QUESTION 159:

System administrators need to be aware of what tool that adds white-bytes of executable code to an existing malicious binary with the goal of evading anti-trojan software using MD5 and CRC checksums?Choose the best answer.

A. ProDetect
B. RegMon
C. ADMutate
D. Stealth Tools v.2.0

Answer: D

QUESTION 160:

What software can alert an administrator to modified files (system or otherwise) by comparing new the hash to the hash on the original trusted file?Choose all that apply.NOTE:The term Choose all that apply in this and additional questions does not necessarily mean that there is more than one answer.

A. Process Viewer
B. Paketto Keiretsu
C. VOMIT
D. Tripwire

Answer: D

QUESTION 161:

Which of the following ports are used by the Simple Network Management Protocol? (Choose two)

A. 161 UDP
B. 161 TCP
C. 161 TCP
D. 162 UDP

Answer: A,D

QUESTION 162:

When referring to databases,what would you call the number of rows within a table?

A. Cardinality
B. Degree
C. Domain
D. Candidate

Answer: A

QUESTION 163:

Why is it more difficult to sanitize information about a company that has publicly-traded stock?Choose the best answer.

A. The company wants to promote itself as much as possible
B. The company must regularly submit financial information to the Securities and Exchange Commission which is then made public
C. It is impossible to remove information from search engines databases
D. The company must hire a security consultant with the expertise to santize the information.

Answer: B

QUESTION 164:

Which scripting language do most open source vulnerability scanners use?

A. ASNL (Automated Security Nessus Language)
B. NASL (Nessus Attack Scripting Language)
C. SANL (Security Attack Nessus Language)
D. NASA (Nessus Automated Security Attack)

Answer: B

QUESTION 165:

Which of the following is NOT a tool that could be perform a zone transfer?

A. DIG
B. Host
C. Nslookup
D. WHOIS

Answer: D

QUESTION 166:

Yannick who is a very smart security tester has mentioned to one of his friends that he has found a way of appending data to an existing file using the built in Windows tools and no third party utility.
This text appended does not affect the functionality,size,or display within traditional file browsing utilities such as dir or Internet Explorer.What is Yannick making reference to in this case?

A. Steganography
B. Hybrid Encryption
C. Alternate Data Streams
D. Append.exe

Answer: C

QUESTION 167:

Why are Trojans such as Beast a lot harder to detect?Choose the best answer.

A. They use a well known name to hide themselves
B. They inject themselves into another process
C. They have a polymorphic payload
D. They are self garbling and cannot be detected

Answer: B

QUESTION 168:

Doing Operating System identification remotely is an art that requires analysis of responses from packets being sent.In order to do so efficiently,a methodology called fuzzy logic is often used. Which of the following would best describe what fuzzy logic is?

A. A problem solving control system
B. A special type of port scan
C. An operating system feature
D. A hardware device for OS identification

Answer: A

QUESTION 169:

Which of the following is NOT a tool that could be used to perform a zone transfer?

A. DIG
B. Host
C. Nslookup
D. WHOIS

Answer: D

QUESTION 170:

Why are Trojans such as Beast a lot harder to detect? Choose the best answer.

A. They use a well known name to hide themselves
B. They inject themselves into another process
C. They have a polymorphic payload
D. They are self garbling and cannot be detected

Answer: B

QUESTION 171:

This document is a high level document that describes management intentions towards security.What is the name of the document?

A. Procedures
B. Guidelines
C. Policies
D. Baselines

Answer: C

QUESTION 172:

DNS Spoofing can allow an attacker to sniff traffic that is meant to go to particular web sites.Which of the following tools can perform DNS Spoofing?Choose two.

A. Cain and Abel
B. LC5
C. WinDNSSpoof
D. URLSnarf

Answer: A,C

QUESTION 173:

On 802.11x Wireless Local Area Network,what is the effective length of the keys being used?

A. 64 bit and 128 bits
B. 128 bit
C. 56 and 104 bits
D. 104 and 128 bits

Answer: D

QUESTION 174:

Spyware is either hardware or software installed on a computer which gather information about the user for later retrieval by whoever controls the Spyware.
It is installed without the users knowledge.
What are the two categories of Spyware that exist?(Choose two from the list below)

A. Surveillance
B. Screen capture
C. key loggers
D. Advertising

Answer: A,D

QUESTION 175:

System administrators need to be aware of what tool that adds while-bytes of executable code to an existing malicious binary with the goal of evading anti-trojan software using MD5 and CRC checksums?Choose the best answer.

A. ProDetect
B. RegMon
C. ADMutate
D. Stealth Tools v.2.0

Answer: D

QUESTION 176:

Which of the following would best describe the meaning of steganography?

A. The art and science of hiding information by embedding messages within other,seemingly harmless messages
B. The art and science of hiding information by encrypting it with a symmetric cipher where the key will be used only once
C. The art and science of hiding information by encrypting it using a public key

encryption system where the key pair will be used only once
D. The art and science of hiding information by embedding redundant data within the primary data and then using XOR against the stream

Answer: A

QUESTION 177:

In symmetric cryptosystem,how many keys are needed to communicate securely between 10 different people who all wish to have a key pair to talk to each other?

A. 2
B. 1
C. 45
D. 90

Answer: C

QUESTION 178:

What technology has made trojans easy to distribute?Choose the best answer.

A. Digitally Signed Software
B. Assembly language
C. EXE wrappers
D. Personal firewall software

Answer: C

QUESTION 179:

It is common knowledge that a Penetration Test relies on a testers ability to collect information from different sources.
Only about 35% to 40% of the information collected will be from technical sources.
Which of the following would NOT be one of the common ways for a security tester to collect information?

A. Physical Access
B. Authorized Access
C. Social Access
D. Digital Access

Answer: B

QUESTION 180:

One of your clients has been the victim of a brute force attack against their SSH server. They ask you what could be done to protect their Linux servers.You propose the use of IP Tables (the built in kernel firewall) to limit connection attempts to protect their servers.You agree with your client to limit connections to the SSH port to a maximum of only three trials per minutes consideirng there is only one administrator who has a valid need to connect remotely onto this port.
If the threshold of three connectors is exceeded,the attacker will have to wait for another 60 seconds before it will resume allowing connections again.
Which of the following IP Tables entry would meet your clients needs?

A. iptables-A INPUT -p tcp -dport 23 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl -name SSH -j DROP
B. iptables-A INPUT -p tcp -dport 22 -m state -state NEW -m recent -update -second 60 -hit count3 -rttl -name SSH -j DROP
C. iptables-A INPUT -p tcp -dport 22 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl -name SSH -j DROP
D. iptables-A OUTPUT -p tcp -dport 23 -m state -state NEW -m recent -update -second 60 -hitcount4 -rttl -name SdSH -j DROP

Answer: C

QUESTION 181:

Which of the following best describes a Script Kiddie?

A. A programmer who is less than 18 years old but already creating exploits that take advantage of vulnerabilities in software
B. A programmer who reverses engineer application in order to find weaknesses
C. A person who uses already written software or tools in order to compromise systems
D. A person who mastered scripting language since a very early age

Answer: C

QUESTION 182:

Assuming SNMP Agent devices are IPSec-capable,why would implementing IPSec help protect SNMP Agents?Choose three.

A. SNMP is installed by default on Windows computers
B. SNMP v.2 sends the community name in cleartext
C. SNMP v.2 does not encrypt any data
D. IPSec would protect against an attacker spoofing the IP address of the SNMP Management station

Answer: B,C,D

QUESTION 183:

Which tools and or techniques can be used to remove an Alternative Data Stream on an NTFS file? Choose two.

A. Ads_cat
B. ADSChecker
C. ADS_Del
D. Copy the NTFS file containing the stream to a FAT partition,delete the original TFS file,copy the FAT file back to NTFS

Answer: D

QUESTION 184:

Which of the following might be used to give false positives when a UDP scan is being performed against a DMZ server running DNS?Choose the best answer.

A. On the firewall,block ICMP TTL Exceeded
B. On the firewall,block all incoming UDP
C. On the firewall,block all TCP SYN packets
D. On the firewall,block all ICMP Port Unreachable messages

Answer: D

QUESTION 185:

Bob is working as an Instrusion Detection System administrator for a company called CCCure.
Being a keen analyst he has noted a very large amount of SYN packet being sent to some of his external IP addresses.
At first it looked like normal daily traffic but somehow it seems that after his internet facing hosts sends a SYN/ACK reply back to the connection request,the final ACK packet is never received from the remote host.
What type of scan does this pattern indicate?

A. A FIN Scan
B. A Vanilla port scan
C. A Half-Open Scan
D. A NULL scan

Answer: C

QUESTION 186:

An administrator has just completed the installation of Nessus on a Linux System that will only have physical space for the server and no monitor.The administrator was told that Nessus has to be run when performing assessments from the system front end you installed Nessus on.

A. True
B. False

Answer: B

QUESTION 187:

When doing an ACK flag scanning the target host is sent TCP packets with the ACK flag set and the reply is then analyzed.
Which of the following items within the response packets would be used to determine if the port was open on the remote host?(Choose two)

A. The Time To Live field
B. The source port
C. The destination port
D. The Window field

Answer: A,D

QUESTION 188:

There are multiples ways that passwords could be cracked.
Which of the following is not a password cracking method?

A. Salami
B. Brute Force
C. Dictionary
D. Hybrid
E. Pre-Computed Hashes

Answer: A

QUESTION 189:

When referring to database,what would you call the number of rows within a table?

A. Cardinality
B. Degree
C. Domain
D. Candidate

Answer: A

QUESTION 190:

If an attacker gets Adminsitrative-level access, why cant the entries in the Event log be trusted with certainty?Choose two.

A. Entries in the event log are not digitally signed
B. The attacker may have been able to simply clear the event log,thus erasing evidence of the methods of break-in
C. Tools like Winzapper allow the attacker to selectively delete log entries associated with the initial break-in and subsequent malicious activity
D. Event logs have NTFS permissions of Everyone Full Control and thus can be easily edited.

Answer: B,C

QUESTION 191:

Jhezza has just arrived at her office and she is checking her stock portfolio as she does every day.
She connects to her broker web site and decides to buy some stocks that are highly recommended. She makes use of her special Portfolio Credit Card because she wishes to collect travel points.
A few weeks later, Jhezza realized that someone has compromissed her credit Card number and has been doing fraudulent trasactions online,the first of which is on the same day she used it to buy stocks from her office.
How did the Card number get compromised?

A. By a Man in the middle attack
B. By someone who read her emails
C. By someone who was able to perform a FTP server spoofing
D. By a Meet in the middle attack,which comprosmises encryption

Answer: A

QUESTION 192:

Which scripting language do most open source vulnerability scanners use?

A. ASNL (Automated Security Nessus Language)
B. NASL (Nessus Attack Scripting Language)
C. SANL (Security Attack Nessus Language)
D. NASA (Nessus Automated Security Attack)

Answer: B

QUESTION 193:

Which of the following SQL injection scripts would attempt to discover all usernames on the table users beginning with Ad?

A. SELECT *FROM* WHERE username =AD*
B. OR 1=1; SELECT username FROM users WHERE username LIKE ad%:-
C. SELECT name FROM Master..sysxlogins
D. OR 1=2 WHERE name is like AD%-

Answer: B

QUESTION 194:

Why wouldn't it be surprising to find netcat on a trojaned-computer?Choose three.

A. Netcat can listen on any port and send data to any port
B. Netcat can be used to send or receive files over any port
C. Netcat can be used to perform port scanning
D. Netcat encrypts all communications

Answer: A,B,C

QUESTION 195:

Which of the following techniques would be effective to get around some of the blocking rules on certain firewalls?
The same technique could be used to avoid detection by intrusion Detection Systems (IDS) in some cases.

A. Injection
B. Spoofing
C. Fragmentation
D. Diffusion

Answer: C

QUESTION 196:

When a digital certificate has been revoked before its expiry date,how will the Certification Authority (CA) that issued the certificate inform other CAs that the specific certificate is no longer valid.

A. By posting it on the CA web site
B. By sending an email message to the other CAs
C. By posting it on the certificate revocation list

D. By posting it on the certificate expiry list

Answer: C

QUESTION 197:

Examining all web pages from a site might be a tedious task.
In order to facilitate such as task you can make use of a web crawler.
Which of the choices presented below would best describe what a web crawler is used for?

A. To test the performance of a web server
B. To perform a load test bringing the remote server to a crawl
C. To created a mirror copy of a website for later inspection
D. To attempt escalating your privilege on a compromised web server

Answer: C

QUESTION 198:

While performing a penetration test you discover that the system being tested is already compromised by an intruder.Further examination shows the intruder being currently on the system and doing his deeds.As a Certified Penetration Testing Specialist What should you do?

A. Retaliate immediately and attempt to break into the attacker system before you loose track of where he is doing the attack from.
B. Suspend your test immediately and advise your client.Once the client gives you authorization you would resume your testing.
C. Immediately attempt to gather as much information as possible about the intruder,monitor his moves very closely but never attempt to break into this system or retaliate.
D. Call 911 immediately and then call management to notify them of your promptaction.Once management gives you authorization you can resume your testing.

Answer: B

QUESTION 199:

Why is it often recommended to rename the built-in Administrator account on a Windows 2000 domain?Choose the best answer.

A. Renaming the Guest account is of little value
B. If you dont rename the Administrator account you will have NetBIOS name conflicts with the Administrator account from other domains in the forest
C. Account lockout will not stop password guessing attacks via SMB filesharing or

BASIC web authentication against the built-in Administrator account
D. The default domain policy actually requires the Administrator account to be renamed

Answer: C

QUESTION 200:

Which of the following pieces of information can be obtained from a Whois query?Choose all that apply.

A. Technical point of contact
B. Authoritative DNS servers
C. Private IP Address block
D. Public IP address block

Answer: A,B,D

QUESTION 201:

A Denial of Service (DoS) attack can have severe effect on a company network or systems.What is the main purpose of a DoS attack?Choose the best response.

A. To compromise a remote system
B. To disallow access from legitimate users
C. To disallow access from illegitimate users
D. To create a lot of log entries

Answer: B

QUESTION 202:

John is attempting to reduce the likelihood that his Linux server could be compromised through exploitation of ports and services that are not necessary or through the use of packets that might be out of state,modified,or malicious.His first step will be to configure the built in firewall that exists on the recent Linux version.
What is the name of the user space program used to configure this firewall?

A. IPChains
B. IPwall
C. IPTables
D. IPFW

Answer: C

QUESTION 203:

Password attack fall within two main categories:Social Attacks and Digital Attacks.
Which of the following would not be considered a Social Attack on passwords?

A. Social Engineering
B. Shoulder Surfing
C. Dumpster Diving
D. Dictionary Attack

Answer: D

QUESTION 204:

Julius has been hired to perform a test on Certkiller .com networks.
Julius knows that Certkiller .com has a large team of security administrators who are very proactive in their security approach.
Most likely there are some Intrusion Detection Systems (IDS) in place that would quickly identify Julius IP address and he would then be blocked from accessing the network he is supposed to test.
How can Julius avoid having his IP address identified and then blocked?
Which of the following would be the most practical solution and the easiest to implement?

A. By using public key encryption;it is well known that IDS cannot make any sense of encrypted traffic and they would not be able to determine the source of the probes
B. By using Secure Socket Layer (SSL) Which will shield the intruder from the IDS and they wont be able to determine the source of the probes
C. By using only computers within the local internet caf.All traffic will be traced to the internet caf instead of being traced to the security tester
D. By using an internet anonymizer instead of connecting directly to the target.The anonymizer will shield the real source of the probes.

Answer: D

QUESTION 205:

Bob has accessed a nice site that sells high end wireless network equipment.
However,after looking around for a while it was obvious that most items were too expensive for his low income salary.
After fidding around for a while,he identified that modifying some of the page variables would allow him to modify the price easily and then he could save the page locally and resubmit the page in order to get a significant rebate.What weakness within the page code did he use to perform his attack?

A. HTML code
B. Hidden From Field code
C. Java Code

D. ActiveX

Answer: B

QUESTION 206:

BASIC authentication for HTTP authentication is universally understood but has the disadvantage of passing username and password in BASE64 encoding.What technology could be used to encrypt the BASE64 encoding and thus secure BASIC authentication for all web browsers and all Internet users?Choose the best answer.

A. SSH
B. IPsec
C. SSL
D. IKE

Answer: C

QUESTION 207:

Joshua, a specialist in Penetration Testing,has been hired by Certkiller .com to perform a security test on some of their servers.Joshua has been challenged to remain undetected by Certkiller .com internal security team.
Over the past few days Joshua has been collecting tons of information about his target.He did so by accessing public database and never sending any packets to his target.How would you call this type of information gathering?

A. Active Information Gathering
B. Passive Information Gathering
C. Stealth Information Gathering
D. Secret Information Gathering

Answer: B

QUESTION 208:

The process of flooding a local segment with thousands of random MAC addresses can result in some switches behaving like a hub.The goal of the hacker is to accomplish what?Choose the best answer.

A. Denial of service
B. ARP cache poisoning
C. Sniffing in a switched network
D. SYN flood

Answer: C

QUESTION 209:

What is one possible method that hackers can use to sniff SSL connections?Choose the best answer.

A. Use dsniff
B. Act as a man in the middle between the client and the webserver and send the client a fake certificate that the user will accept as legitimate
C. Use SSLSniff to sniff the session key exchange
D. Use SSL Relay

Answer: B

QUESTION 210:

You are the security administrator of Certkiller .com Inc.
You have noticed that one of your users has installed a tool named KerbCrack as well as another tool named KerbSniff on his machine withou your authroization.
The company is making use of active directory to store its users database.
What would these two tools be used for?

A. To attempt sniffing passwords off the network and then crack them
B. To capture Kerberos packets and then attempt a brute force attack
C. To connect to encrypted peer to peer networks
D. To administer the Kerberos portion of Active Directory

Answer: B

QUESTION 211:

The Advanced Encryption Standard (AES) was released to protect sensitive data used by U.S.Government organizations.
Up to what classification level was AES built for?

A. Up to Top Secret
B. Up to Secret
C. Up to Confidential
D. Unclassified Information Only

Answer: D

QUESTION 212:

Which of the following SQL script will cause the SQL server to cease operations?

A. NET STOP SQLSERVER -
B. OR 1=1; CLOSE WITHNOWAIT;
C. NET STOP SQLSERVERAGENT -
D. SHUTDOWN WITH NOWAIT;-

Answer: D

QUESTION 213:

What techniques are often used to perform an active-stack fingerprint of an operating system?Choose all that apply.

A. TCP Window and ACK sampling
B. TCP sequence number sampling
C. ICMP Echo integrity
D. IP Type of Service sampling

Answer: A,B,C,D

QUESTION 214:

Johny has been trying to defeat a crypto system for some time.
He has in his possession a whole collection of ciphertext documents that were captured from the network.
However,he does not know what algorithm or plain text was used to create this ciphertext.
Through statistical analysis he is attempting to decipher the encrypted text.
What would you call such an attack?

A. Known Plaintext attack
B. Ciphertext Only Attack
C. Chosen Ciphertext Attack
D. Chosen Plaintext Attack

Answer: B

QUESTION 215:

What are some of the weaknesses that make LAN Manager Hashes much easier to crack by an attacker? (Select all that apply)

A. The 14 character password is split in two
B. The password is converted to Uppercase
C. The hash value is encrypted using MD5
D. The hash value is encrypted with AES

Answer: A,B

QUESTION 216:

Billybastard.c and pipeupadmin are examples of what type of attack?Choose the best answer.

A. Denial of service
B. Privilege escalation
C. FTP bounce
D. SQL Injection

Answer: B

QUESTION 217:

Most search engine support Advanced Search Operators; as a Penetrtion Tester you must be familiar with some of the larger search engines such as Geogle.There is a wealth of information to be gathered from these public databases.Which of the following operators would you use if you attempt to find an older copy of a website that might have information which is no longer available on the target website?

A. Link:
B. InCache:
C. Cache:
D. Related:

Answer: C

QUESTION 218:

Detailed logging is the enemy of all cracers.
After getting unauthorized access to a computer,a cracker will attempt to disable logging on the remote hosts that he compromises.
In order to do so there are a few tools that could be used.
Which of the following command lines would disable auditing on a Windows platform?

A. auditpol/disable
B. auditlog/disable
C. auditpol/off
D. auditlog/off

Answer: A

QUESTION 219:

You have been asked to assist an investigation team in collecting data and evidence related to an internal hacking case.
The investigator in charge of the case would like to capture all keystrokes from the suspect but is afraid the employee under investigation who possesses great technical skills might have installed integrity tools on his system that would detect any new software installed.
What solution would be best to use to reach the investigator requirement?

A. Disable the integrity tools in place
B. Install a software key logger that does not show in the process list
C. Install a hardware based key logger
D. Sniff all traffic and keystrokes from the network

Answer: C

QUESTION 220:

Pen testing is another area of security where acronyms and expressions abound.
What does the term rooting refers to?

A. Getting access to the root directory
B. Getting administrator access on a Linux system
C. Getting administrator access on a Windows system
D. Planting a worm that will develop and grow within the system

Answer: B

QUESTION 221:

Vulnerabilities Scanners have large databases of known vulnerabilities and exposures that exist within a very large number of operating systems and applications.
Most scanners are prone to false positive and in some cases false negative.
The results presented by the scanners must be manually validated.
What is one of the biggest disadvantages of automated security scanners when remaining stealthy is an issue?

A. A very large amount of traffic will be sent against the target
B. They can only test UDP based vulnerabilities
C. The database is not regularly updated is most cases
D. The scanner might require a large amount of memory,disk space,and processing power

Answer: A

QUESTION 222:

What technology is often used by employees to get access to web sites that are blocked by their corporate proxy server?Choose the best answer.

A. DNS spoofing
B. ARP poisoning
C. Anonymizers
D. BASIC web authentication

Answer: C

QUESTION 223:

Cracking encryption is often impossible due to time constraints whereby it would take hundreds of years in some cases.
Great advancement has taken place lately regarding the cracking of password based on the time memory trade-off.
Such an attack allows an attacker to crack the password within a very short period of time.
Under the memory trade-off technique,which of the followig would be used to speed the cracking of password?

A. Large dictionaries
B. Large collection of common passwords
C. Pre Computed hashes tables
D. Pre sorted dictionaries will most likely matches tried first

Answer: C

QUESTION 224:

Which of these methods would be considered examples of active reconnaissance?(Choose three.)

A. War dialing
B. Firewalking
C. Whois lookup
D. FTP banner retrieval

Answer: A,B,D

QUESTION 225:

Bob has just produced a very detailed penetration testing report for his client.Bob wishes to ensure that the report will not be changed in storage or in transit.What would be the best tool that Bob can use to assure the integrity of the information and detect any changeds that could have happend to the report while being transmitted or stored?

A. A Symmetric Encryption Algorithm
B. An Asymmetric Encryption Algorithm
C. An Hashing Algorithm
D. The ModDetect Algorithm

Answer: C

QUESTION 226:

Which of the following is the best method to counteract offline password cracking?Choose the best answer.

A. Setting a password policy with a maximum age of 30 days
B. Setting a password policy with a minimum age of 30 days
C. Setting a password policy with a minimum length of 6 characters
D. Use of one time passwords

Answer: D

QUESTION 227:

Which of the following could be countermeasures to scanning?Choose all that apply.

A. Drop all traffic destined directly at the firewall
B. Disable all ICMP packets at exterior gateways
C. Use a firewall ruleset that leads to many false positives and thus security through obscurity
D. Permit UDP port 500 packets at the firewall

Answer: A,B,C

QUESTION 228:

Which of the following are reasons why LAN Manager hashes stored in the SAM file are considered relatively easy to crack?Choose two.

A. All uppercase characters in the password are converted to all lowercase
B. All lowercase characters in the password are converted to all uppercase
C. The password is broken cannot contain special characters
D. Lan Manager password cannot contain special characters

Answer: B,C

QUESTION 229:

A null session allows users to connect remotely to other Windows computers on the network.According to the implementation of NULL Session on Windows platforms,how long would the password be in order to establish a NULL Session?

A. At least 8 Characters
B. A passphrase is used not a password
C. There is no password involved
D. Windows makes use of Digital Signature in such case,not passwords

Answer: C

QUESTION 230:

Todays security infrastructures are composed of firewall,instrusion detection systems,content screening,certificates,tokens,and a lot more.
Howeve,there is still one aspect that is considered to be weak link in all infrastructures.
Which of the following would represent this weak link?

A. Bad hardware
B. Bad software
C. People
D. Process

Answer: C

QUESTION 231:

You have successfully exploited a remote computer.You now have limited privilege on the remote computer.
You tests have revealed that it is possible to download files from the internet but the size of the limited to less than 60K.
You would like to escalate your privilege by scanning the internal network and also setup a permanent backdoor that would allow you to return to the compromised host at will.
Which of the following tools could be used for such purpose?

A. Hijack This
B. Netcat
C. ButtSniff
D. BackOrifice

Answer: B

QUESTION 232:

Keen administrators (the enemy of penetration testers)will take great steps in order to collect logs on different servers.By having a detailed log of activities they may be able to detect abnormal activities.
A skilled intruder will attempt to modify the logging policy in order to prevent the administrator from having access to his detailed log.What command line tool could an attacker use to disable auditing on a Windows server?

A. Syslog
B. Eventlog
C. Auditpol
D. Auditlog

Answer: C

QUESTION 233:

What is the most secure method of implementing Software Restriction Policies to prevent users from running both unauthorized and undesirable software?Choose the best answer.

A. Define a policy to permit software found only in specified paths and disallow all else
B. Define a policy to permit software based only upon specified filenames and disallow all else
C. Define a policy to permit all software except those based upon specified filenames
D. Define a policy to permit software only based upon specified executable hashes and disallow all else

Answer: D

QUESTION 234:

One of the challenges when doing large scale security tests is the time required.
If you have to scan a class B network it might take you a very long time. Scanrand is a tool that has been optimized to scan a large number of hosts in very little time.It was reported that it was used to scan about 8300 web servers in less than 4 seconds.
How does scanrand achieve such an impressive benchmark?

A. It does not maintain any state
B. It makes use of multiple Network Interface Cards (NIC)
C. It has a probabilistic algorithm that can predict if a port is open or not
D. It does not attempt to use UDP due to the overhead involved

Answer: A

QUESTION 235:

When talking about databases search query languages,commands such as

Select,Update,Insert,Grant,and Revoke would all the part of what language?

A. C++
B. SQL
C. Python
D. Perl

Answer: B

QUESTION 236:

Which of the following would best represent the definition of a Penetration Test?

A. Testing of the effectiveness of applied security controls by breaking in and bypassing them.
B. Testing of the policies in place to see how compliant a company is with its own control definition.
C. Testing the effectiveness of applied security controls by evaluating vulnerabilities and reporting them to the client.
D. Testing the effectiveness of access control mechanisms by constant and deep inspection of all log files.Also called Deep Packet Inspection.

Answer: A

QUESTION 237:

Which of the following countermeasures can make it more difficult for an attacker to gain access to the local SAM file if the attacker has physical access to that computer?Choose two.

A. Change the BIOS to always boot first from the hard drive and enable a BIOS password
B. Install a smartcard reader for login
C. Encrypt the SAM file using EFS
D. Physically remove the floppy drive and CD/DVD drives

Answer: A,D

QUESTION 238:

A system administrator deploys a Windows-based server in a publicly-accessible DMZ.The sole purpose of this machine is to run IIS and allow anonymous access.After a few days the security log is full of failed login against the Administrator account.What is the best strategy to totally prevent future password guessing attempts? Choose the best answer.

A. Enable account lockout
B. Change the Administrator password to be even longer
C. Remove File and Print Sharing for Microsoft Networks on the network adapter
D. Configure the security policy to shut down the system when the event log is full

Answer: C

QUESTION 239:

Why is it important to ensure that SRV records are not publicly accessible?Choose the best answer.

A. SRV records indicate how long a machine has been up since reboot and hence could indicate patch levels
B. SRV records reveal Active Directory domain controllers
C. SRV records reveal software Update Services computers
D. SRV records are required on NT 4 domains

Answer: B

QUESTION 240:

Cisco Catalyst Switches have which feature intended to prevent ARP cache poisoning?Choose the best answer.

A. ARP watch
B. Dynamic ARP Inspection
C. VLANs
D. IPSec-ready

Answer: B

QUESTION 241:

Which of the following capabilities do rootkits have?Choose all that apply.

A. Hide any file
B. Hide any process
C. Hide any listening port
D. Cause a blue screen of death on Windows computers

Answer: A,B,C,D

QUESTION 242:

One key skill a penetration Tester must possess is documentation.

There are different documents that will be produced in the course of doing a penetration test,out of the documents listed below which one would be the most important document that a Penetration Tester must have in order to be performing a test?

A. Network Diagram
B. Host and services list
C. Written Authorization
D. Security Policies

Answer: C

QUESTION 243:

Which of these methods would help protect DNS records from unauthorized users?(Choose two.)

A. Removing the default setting on NT 4 and Windows 2000 DNS servers that allows zone transfers to any IP address
B. Using Active Directory Integrated zones on publicly-available DNS servers
C. Blocking incoming UDP port 53 requests to a DMZ hosting a DNS server
D. Using two DNS servers;An internal DNS server with internal resource records and an external DNS server with DMZ-based resource records

Answer: A,D

QUESTION 244:

Which registry key setting will disable the automatic playing of executables on a CD-room when the CD-room is inserted into the computer?Choose the best answer.

A. HKEY_Current_User\System\CurrentControlSet\Control\cdrom\autoplay=0
B. HKEY_Current_Machine\System\CurrentControlSet\Service\cdrom\autorun=0
C. HKEY_Current_Machine\System\CurrentControlSet\Service\cdrom\auto=1
D. HKEY_Current_Machine\System\Services\Windows\cdrom\autoplay=0

Answer: B

QUESTION 245:

A normal connection is usally established using a TCP Three Way handshake where sequences of packets are sent as follows;Syn,Syn-Ack,Ack.A malicious attacker probing a remote target is sending a Syn packet to a target;however,when he gets a Syn-Ack response from the target,he always sends a Reset packet (RST)instead of completing the three way handshake with an Ack packet as per the protocol.
What is the attackers goal when doing this?Choose the best answer.

A. Attacker does not like to follow protocols and agreements
B. Attacker has his own modified protocol stacks
C. Attacker attempts to avoid being logged on remote hosts
D. Attacker attempts to avoid sending too much traffic

Answer: C

QUESTION 246:

Which of the following would best describe a scanning technique that is the most reliable but also the most noticeable on the target is being evaluated?

A. Half-Scan
B. TCP Connect( )
C. Fin Scan
D. NMAP scan

Answer: B

QUESTION 247:

If the DS Client software has been installed on Windows 95,Windows 98, and NT 4 computers,what setting of the LanMan Authentication level should be applied to counteract LanMAn hash sniffing and offline cracking?Choose the best answer.

A. Send NTLM v2/Refuse LM & NTLM
B. Send NTLM only
C. Send LM & NTLM responses
D. Send NTLM v2/Refuse LM

Answer: A