Pass4sure Exam

Success Guaranteed

ECCouncil

Exam 312-50v9

Certified Ethical Hacker Exam V9

Version: 7.0

[Total Questions: 125]

Question No : 1

Which of the following is component of a risk assessment?

A. Logical interface
B. DMZ
C. Administrative safeguards
D. Physical security

Answer: C

Question No : 2

The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Access Point
B. Wireless Analyzer
C. Wireless Access Control list
D. Wireless Intrusion Prevention System

Answer: D

Question No : 3

An attacker gains access to a Web server’s database and display the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient security management
B. Insufficient database hardening
C. Insufficient exception handling
D. Insufficient input validation

Answer: D

Question No : 4

You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping but you didn't get any response back.

What is happening?

A. TCP/IP doesn't support ICMP.
B. ICMP could be disabled on the target server.
C. The ARP is disabled on the target server.
D. You need to run the ping command with root privileges.

Answer: A

Question No : 5

It is a short-range wireless communication technology intended to replace the cables connecting portables of fixed deviceswhile maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.

Which of the following terms best matches the definition?

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Answer: A

Question No : 6

The Open Web Application Security Project (OWASP) isthe worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project most Critical Web application Security Rules?

A. Injection
B. Cross site Scripting
C. Cross site Request Forgery
D. Path Disclosure

Answer: A

Question No : 7

Session splicing is an IDS evasiontechnique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can used to perform session splicing attacks?

A. Hydra
B. Burp
C. Whisker
D. Tcpsplice

Answer: C

Question No : 8

Which of the following isthe greatest threat posed by backups?

A. An un-encrypted backup can be misplaced or stolen
B. A back is incomplete because no verification was performed.
C. A backup is the source of Malware or illicit information.
D. A backup is unavailable duringdisaster recovery.

Answer: A

Question No : 9

A new wireless client is configured to join a 802.11 network. Thisclient uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

A. The client cannot see the SSID of the wireless network
B. The wireless client is not configured to use DHCP
C. The WAP does not recognize the client's MAC address
D. Client isconfigured for the wrong channel

Answer: C

Question No : 10

What does a firewall check to prevent particularports and applications from getting packets into an organizations?

A. Transport layer port numbers and application layer headers
B. Network layer headers and the session layer port numbers
C. Application layer port numbers and the transport layer headers
D. Presentation layer headers and the session layer port numbers

Answer: A

Question No : 11

An Intrusion Detection System(IDS) has alerted the network administrator to a possibly malicious sequence of packets went to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Intrusion Prevention System (IPS)
C. Vulnerability scanner
D. Network sniffer

Answer: B

Question No : 12

PGP, SSL, and IKE are all examples of which type of cryptography?

A. Hash Algorithm
B. Secret Key
C. Public Key
D. Digest

Answer: C

Question No : 13

A company’s security states that all web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
B. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
D. Attempts by attacks to access the user and password information stores in the company's SQL database.

Answer: C

Question No : 14

Ricardo wants to send secret messages to acompetitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, the technique provides 'security through obscurity'. What technique is Ricardo using?

A. RSA algorithm
B. Steganography
C. Encryption
D. Public-key cryptography

Answer: B

Question No : 15

Which regulationdefines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53

Answer: D

Question No : 16

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. Jack the ripper
B. nessus
C. tcpdump
D. ethereal

Answer: C

Question No : 17

What is the most common method to exploit the “Bash Bug” or ShellShock” vulnerability?

A. SSH
B. SYN Flood
C. Manipulate format strings in text fields
D. Through Web servers utilizing CGI (CommonGateway Interface) to send a malformed environment variable to a vulnerable Web server

Answer: D

Question No : 18

It is a vulnerability in GNU’s bash shell, discovered in September of 2004, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

Which of the following vulnerabilities is being described?

A. Shellshock
B. Rootshock
C. Shellbash
D. Rootshell

Answer: A

Question No : 19

During a security audit of IT processes, an IS auditor found that there was no documented security procedures. What should the IS auditor do?

A. Terminate the audit.
B. Identify and evaluate existing practices.
C. Create a procedures document
D. Conduct compliance testing

Answer: B

Question No : 20

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.

Which file does the attacker needto modify?

A. Hosts
B. Networks
C. Boot.ini
D. Sudoers

Answer: A

Question No : 21

An incident investigator asks to receive a copy of the event from all firewalls, prosy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs the sequence of many of the logged events do not match up.

What is the most likely cause?

A. The network devices are not all synchronized
B. The securitybreach was a false positive.
C. The attack altered or erased events from the logs.
D. Proper chain of custody was not observed while collecting the logs.

Answer: C

Question No : 22

You are performing a penetration test. You achieved access via a bufferoverflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.

What should you do?

A. Do not transfer the money but steal the bitcoins.
B. Report immediately to the administrator.
C. Transfer money from the administrator's account to another account.
D. Do not report it and continue the penetration test.

Answer: B

Question No : 23

Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening port on the targeted system.

If a scanned port is open, what happens?

A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.

Answer: A

Question No : 24

You've just been hired to perform a pentest on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.

What is one of the first thing you should to when the job?

A. Start the wireshark application to start sniffing network traffic.
B. Establish attribution to suspected attackers.
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Interview all employees in the company to rule out possible insider threats.

Answer: C

Question No : 25

Which of the following describes the characteristics of a Boot Sector Virus?

A. Overwrites the original MBR and only executes the new virus code
B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

Answer: C

Question No : 26

The phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the“landscape” looks like.

What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. Network Mapping
B. Gaining access
C. Footprinting
D. Escalating privileges

Answer: C

Question No : 27

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGI's?

A. Snort
B. Dsniff

C. Nikto
D. John the Ripper

Answer: C

Question No : 28

In Risk Management, how is the term “likelihood” related to the concept of “threat?”

A. Likelihood is the probability that a vulnerability is a threat-source.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a threat-source will exploit a vulnerability.

Answer: D

Question No : 29

You have successfully gained access to your client’s internal network and successfully comprised a linux server which is part of the internal IP network. You want to know which Microsoft Windows workstation have the sharing enabled.

Which port would you see listeningon these Windows machines in the network?

A. 1443
B. 3389
C. 161
D. 445

Answer: D

Question No : 30

The heartland bug was discovered in 2014 and is widely referred to under MITRE’s Common Vulnerabilities and Exposures (CVE) as CVE-2004-1060. Thisbug affects the OpenSSL implementation of the transport Layer security (TLS) protocols defined in RFC6520.

What types of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Root
B. Private
C. Shared
D. Public

Answer: A

Question No : 31

You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host-based IDS
B. Firewall
C. Network-Based IDS
D. Proxy

Answer: C

Question No : 32

You just set up a security system in your network. In what kind of system would you find thefollowing string of characters used as a rule within its configuration?

alert tcp any any ->192.168.100.0/24 21 (msg: "FTP on the network!";)

A. A firewall IPTable
B. A Router IPTable
C. An Intrusion Detection System
D. FTP Server rule

Answer: C

Question No : 33

Jimmy is standing outside a secure entrance to a facility. He is pretending to having a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it beginsto close.

What just happened?

A. Masquading
B. Phishing
C. Whaling
D. Piggybacking

Answer: D

Question No : 34

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

A. Bounding
B. Mutating
C. Puzzing
D. Randomizing

Answer: C

Question No : 35

During a blackbox pen test you attempt to pass IRC traffic over post 80/TCP from a compromised web enabled host. The traffic gets blocked; however outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

A. Circuit
B. Packet Filtering
C. Application
D. Stateful

Answer: C

Question No : 36

The configuration allows a wired or wireless network interface controller to pass all trafice it receives to thecentral processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. WEM
B. Multi-cast mode
C. Promiscuous mode
D. Port forwarding

Answer: B

Question No : 37

Which of the following is considered the best way to prevent Personally Identifiable Information (PII) from web application vulnerabilities?

A. Use encrypted communications protocols to transmit PII
B. Use full disk encryption on all hard drives to protect PII
C. Use cryptographic storage to store all PII
D. Use a security token to log onto into all Web application that use PII

Answer: A

Question No : 38

It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage,or email warning from what looks like an officialauthority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again.

Which term best matches this definition?

A. Spyware
B. Adware
C. Ransomware
D. Riskware

Answer: C

Question No : 39

Your team has won a contract to infiltrate an organization. The company wants to have the attack be a realistic as possible; therefore, they did not provide any information besides the company name.

What should be thefirst step in security testing the client?

A. Scanning
B. Escalation
C. Enumeration
D. Reconnaissance

Answer: D

Question No : 40

It is a regulation that has a set if guideline,which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

A. HIPAA
B. COBIT
C. ISO/IEC 27002
D. FISMA

Answer: A

Question No : 41

Which of the following is a design pattern based on distinct pieces ofsoftware providing application functionality as services to other applications?

A. Lean Coding
B. Service Oriented Architecture
C. Object Oriented Architecture
D. Agile Process

Answer: B

Question No : 42

Which of the following tools can be used for passiveOS fingerprinting?

A. tcpdump
B. ping
C. nmap
D. Tracert

Answer: C

Question No : 43

When you are getting informationabout a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

What nmap script will help you with this task?

A. http enum
B. http-git
C. http-headers
D. http-methods

Answer: B

Question No : 44

Which of the following statements regarding ethical hacking is incorrect?

A. Testing should be remotely performed offsite.
B. Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the
organizations IT system.
C. Ethical hacking should not involve writing to or modifying the target systems.
D. An organization should use ethical hackers who do not sell hardware/software or other

consulting services.

Answer: B

Question No : 45

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such as audit?

A. Port scanner
B. Protocol analyzer
C. Vulnerability scanner
D. Intrusion Detection System

Answer: C

Question No : 46

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.

What is the best approach?

A. Install and use Telnet to encrypt all outgoing traffic from this server.
B. Install Cryptcat and encrypt outgoing packets from this server
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Answer: A

Question No : 47

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing inconcluding the Operating System (OS) version installed. Considering the NMAP result below, which of the follow is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report

for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80 /tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tec open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

A. The host is likely a printer.
B. The host is likely a router.
C. The host is likely a Linux machine.
D. The host is likely a Windows machine.

Answer: A

Question No : 48

Which of the following is designed to indentify malicious attempts to penetrate systems?

A. Proxy
B. Router
C. Firewall
D. Intrusion Detection System

Answer: D

Question No : 49

Risk = Threats x Vulnerabilities is referred to as the:

A. Threat assessment
B. Disaster recovery formula
C. BIA equation
D. Risk equation

Answer: D

Question No : 50

You have compromised a server on a network and successfully open a shell. You aimed to identify all operating systems running on the network. However, as you attemptto fingerprint all machines in the machines in the network using the nmap syntax below, it is not going through.

invictus@victim_server:~$nmap –T4 –O 10.10.0.0/24

TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxxx.

QUITTING!

What seems to be wrong?

A. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
B. This is a common behavior for a corrupted nmap application.
C. OS Scan requires root privileged.
D. The nmap syntax is wrong.

Answer: D

Question No : 51

You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. ICMP
B. TCP
C. UDP
D. UPX

Answer: B

Question No : 52

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best nmap command you will use?

A. Nmap –T4 –F 10.10.0.0/24
B. Nmap –T4 –q 10.10.0.0/24
C. Nmap –T4 –O 10.10.0.0/24
D. Nmap –T4 –r 10.10.0.0/24

Answer: A

Question No : 53

This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

Which of the following tools is being described?

A. Wificracker
B. WLAN-crack
C. Airguard
D. Aircrack-ng

Answer: D

Question No : 54

Which of these options is the most secure procedure for strong backup tapes?

A. In a climate controlled facility offsite
B. Inside the data center for faster retrieval in afireproof safe
C. In a cool dry environment
D. On a different floor in the same building

Answer: A

Question No : 55

Which tool allows analysis and pen testers to examine links between data using graphs and link analysis?

A. Metasploit
B. Maltego
C. Wireshark
D. Cain &Abel

Answer: B

Question No : 56

You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from the server will not be caught by a Network Based Intrusion Detection System (NIDS).

Which is the best way to evade the NIDS?

A. Out of band signaling
B. Encryption
C. Alternate Data Streams
D. Protocol Isolation

Answer: B

Question No : 57

The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and received by the wireless router?

A. Netcat
B. Wireshark
C. Nessus
D. Netstat

Answer: B

Question No : 58

Which of the following is not a Bluetooth attack?

A. Bluejacking
B. Bluedriving
C. Bluesnarfing
D. Bluesmaking

Answer: B

Question No : 59

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.

What wireshark filter will show the connections from the snort machineto kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.dstport==514 &&ip.dst==192.168.0.99
C. tcp.srcport==514 && ip.src==192.168.0.99
D. tcp.srcport==514 && ip.src==192.168.150

Answer: A

Question No : 60

Which of the followingis the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns
B. Voice
C. Fingerprints
D. Height and Weight

Answer: D

Question No : 61

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Inherent Risk
B. ResidualRisk
C. Deferred Risk
D. Impact Risk

Answer: B

Question No : 62

This international organizationregulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

A. Payment Card Industry (PCI)
B. International Security Industry Organization (ISIO)
C. Institute of Electrical and Electronics Engineers (IEEE)
D. Center for Disease Control (CDC)

Answer: B

Question No : 63

Which method of password cracking takes the most time and effect?

A. Rainbow Tables
B. Shoulder surfing
C. Bruce force
D. Directory attack

Answer: C

Question No : 64

Which of the following is an extremelycommon IDS evasion technique in the web world?

A. post knocking
B. subnetting
C. unicode characters
D. spyware

Answer: C

Question No : 65

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.

Which algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)
B. Temporal Key Integrity Protocol (TRIP)
C. Wi-Fi Protected Access (WPA)
D. Wi-Fi Protected Access 2(WPA2)
E.

Answer: A

Question No : 66

Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Sniffing
B. Social engineering
C. Scanning
D. Eavesdropping

Answer: B

Question No : 67

When you return to your desk after a lunch break, you notice a strange email in your inbox. The senders is someone you did business with recently but the subject line has strange characters in it.

What should you do?

A. Forward the message to your company’s security response team and permanently delete the message from your computer.
B. Delete the email and pretend nothing happened.
C. Forward the message to your supervisor andask for her opinion on how to handle the situation.
D. Reply to the sender and ask them for more information about the message contents.

Answer: A

Question No : 68

As a Certified Ethical hacker, you were contracted by aprivate firm to conduct an external security assessment through penetration testing.

What document describes the specified of the testing, the associated violations, and essentially protects both the organization's interest and your li abilities as a tester?

A. Term of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement

Answer: B

Question No : 69

A Regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?

A. Move the financial data to another server on the same IP subnet
B. Place a front-end web server in a demilitarized zone that only handles external web traffic
C. Issue new certificates to the web servers from the root certificate authority
D. Require all employees to change their passwords immediately

Answer: A

Question No : 70

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

A. Copy the data to removable media and keep it in case you need it.
B. Ignore the data and continue the assessment until completed as agreed.
C. Confront theclient on a respectful manner and ask her about the data.
D. Immediately stop work and contact the proper legal authorities.

Answer: D

Question No : 71

The security concept of “separation of duties” is most similar to the operation ofwhich type of security device?

A. Bastion host
B. Honeypot
C. Firewall
D. Intrusion Detection System

Answer: C

Question No : 72

> NMAP –sn 192.168.11.200-215

The NMAP command above performs which of the following?

A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

Answer: A

Question No : 73

Which of the following is the successor of SSL?

A. RSA
B. GRE
C. TLS
D. IPSec

Answer: C

Question No : 74

An attacker changes the profile information of a particular user on a target website (the victim). The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<frame src=http://www/vulnweb.com/updataif.php Style="display:none"></iframe>

What is this type of attack (that can use either HTTP GET or HRRP POST) called?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. SQL Injection
D. Browser Hacking

Answer: A

Question No : 75

You've gained physical access to a Windows 2008 R2 server which has as accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD.Which Linux tool has the ability to change any user's password or to activate disabled Windows Accounts?

A. John the Ripper
B. CHNTPW
C. Cain & Abel
D. SET

Answer: A

Question No : 76

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shallscript files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in the server, uploaded the files, and extracted the contents of the tarball and ran

the script using a function providedby the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.

Which kind of vulnerability must be present to make this remote attack possible?

A. Filesystem permissions
B. Brute Force Login
C. Privilege Escalation
D. Directory Traversal

Answer: D

Question No : 77

What is the best description of SQL Injection?

A. It is a Denial of Service Attack.
B. It is an attack used to modify code in an application.
C. It is and attack used to gain unauthorized access to a database.
D. It isa Man-in-the-Middle attack between your SQL Server and Web App Server.

Answer: D

Question No : 78

A company's Web development team has become aware ofa certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of web application vulnerability likely exists in their software?

A. Web site defacement vulnerability
B. SQL injection vulnerability
C. Cross-site Scripting vulnerability
D. Cross-site Request Forgery vulnerability

Answer: C

Question No : 79

Which of the following incident handling process phases is responsible for defining rules, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase
B. Recovery phase
C. Identification phase
D. Containment phase

Answer: A

Question No : 80

The “Gray box testing” methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is completely known to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: D

Question No : 81

This asymmetry cipther is based on factoring the product of two large prime numbers.

What cipher is described above?

A. SHA
B. RC5
C. RSA
D. MD5

Answer: C

Question No : 82

Using Windows CMD, how would an attacker list all the shares to which the current user context hasaccess?

A. NET CONFIG

B. NET USE
C. NET FILE
D. NET VIEW

Answer: D

Question No : 83

env x= '(){ :;};echo exploit ' bash –c 'cat/etc/passwd

What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A. Add new user to the passwd file
B. Display passwd contents to prompt
C. Change all password in passwd
D. Remove the passwd file.

Answer: B

Question No : 84

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP confidential
B. AH Tunnel mode
C. ESP transport mode
D. AH permiscuous

Answer: C

Question No : 85

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

A. c:\services.msc
B. c:\ncpa.cp

C. c:\compmgmt.msc
D. c:\gpedit

Answer: C

Question No : 86

Which of the following parameters describe LM Hash:

I – The maximum password length is 14 characters.

II – There are no distinctions between uppercase and lowercase.

III – It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I and II
C. II
D. I, II and III

Answer: D

Question No : 87

What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of thetarget network.
B. The tester could not provide an honest analysis.
C. Network security would be in a "best state" posture.
D. It is best to catch critical infrastructure unpatched.

Answer: A

Question No : 88

You are usingNMAP to resolve domain names into IP addresses for a ping sweep later.

Which of the following commands looks for IP addresses?

A. >host –t ns hackeddomain.com

B. >host –t AXFR hackeddomain.com
C. >host –t soa hackeddomain.com
D. >host –t a hackeddomain.com

Answer: D

Question No : 89

Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website byinserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known toincorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.

What type of attack is outlined in the scenario?

A. Watering Hole Attack
B. Spear Phising Attack
C. Heartbleed Attack
D. Shellshock Attack

Answer: A

Question No : 90

The “white box testing” methodology enforces what kind of restriction?

A. The internal operation of a system is completely known to the tester.
B. Only the internal operation of a system is known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: A

Question No : 91

After trying multiple exploits, you’ve gained root access to a Centos 6 answer. To ensure you maintain access. What would you do first?

A. Disable IPTables
B. Create User Account
C. Downloadand Install Netcat
D. Disable Key Services

Answer: C

Question No : 92

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate theSLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A. $100
B. $146
C. 440
D. 1320

Answer: B

Question No : 93

Which of the following is a protocol specifically designed for transporting event messages?

A. SMS
B. SNMP
C. SYSLOG
D. ICMP

Answer: C

Question No : 94

Which of the following is assured by the use of a hash?

A. Availability

B. Confidentiality
C. Authentication
D. Integrity

Answer: D

Question No : 95

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. PKI
B. biometrics
C. SOA
D. single sign on

Answer: A

Question No : 96

Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications
B. Restrict Physical Access to Server Rooms hosting Critical Servers
C. Use Static IP Address
D. Register all machines MAC Address in a centralized Database

Answer: A

Question No : 97

Which of the followingtypes of firewalls ensures that the packets are part of the established session?

A. Switch-level firewall
B. Stateful inspection firewall
C. Application-level firewall
D. Circuit-level firewall

Answer: B

Question No : 98

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet
B. Netstumbler
C. Abel
D. Nessus

Answer: A

Question No : 99

You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do this fast and efficiently you must user regular expressions.

Which command-line utility are you most likely to use?

A. Notepad
B. MS Excel
C. Grep
D. Relational Database

Answer: C

Question No : 100

How does the Address Resolution Protocol (ARP) work?

A. It sends a reply packet for a specific IP, asking for the MAC address.
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a request packet to all the network elements, asking for the domainname from a specific IP.
D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.

Answer: D

Question No : 101

You are tasked to perform a penetration test. While you are performinginformation gathering, you find ab employee list in Google. You find receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected.

What testing method did you use?

A. Piggybacking
B. Tailgating
C. Evesdropping
D. Social engineering

Answer: D

Question No : 102

While using your bank's online servicing you notice the following stringin the URL bar: "http://www.MyPersonalBank/Account?

Id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

What type of vulnerability is present on this site?

A. SQL injection
B. XSS Reflection
C. Web Parameter Tampering
D. Cookie Tampering

Answer: C

Question No : 103

What is the process of logging, recording, and resolving events that take place in an organization?

A. Metrics
B. Security Policy
C. Internal Procedure
D. Incident Management Process

Answer: D

Question No : 104

Which of the following statements is TRUE?

A. Sniffers operation on Layer 3 of the OSI model
B. Sniffers operation on Layer 2 of the OSI model
C. Sniffers operation on the Layer 1 of the OSI model
D. Sniffers operation on both Layer 2 & Layer 3 of the OSImodel

Answer: D

Question No : 105

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Create a disk imageof a clean Windows installation
C. Check MITRE.org for the latest list of CVE findings
D. Used a scan tool like Nessus

Answer: D

Question No : 106

It isan entity or event with the potential to adversely impact a system through unauthorized access destruction disclosures denial of service or modification of data.

Which of the following terms best matches this definition?

A. Threat
B. Attack
C. Risk
D. Vulnerability

Answer: A

Question No : 107

A common cryptographically tool is the use of XOR. XOR the following binary value:

10110001

00111010

A. 10001011
B. 10011101
C. 11011000
D. 10111100

Answer: A

Question No : 108

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark,and EtherPeek?

A. Nessus
B. Tcptraceroute
C. Tcptrace
D. OpenVAS

Answer: C

Question No : 109

Nation-state threat actors often discover vulnerabilitiesand hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack

because it used four types of this vulnerability.

What is this style of attack called?

A. zero-hour
B. no-day
C. zero-day
D. zero-sum

Answer: C

Question No : 110

Under the “Post-attach Phase and Activities,” it is the responsibility of the tester to restore the system to a pre-test state.

Which of the following activities should not be included in this phase?

I.Removing all files uploaded on the system

II.Cleaning all registry entries

III.Mapping of network state

IV.Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Answer: A

Question No : 111

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal Network.

What is this type of DNS configuration commonly called?

A. DNS Scheme
B. DynDNS

C. Split DNS
D. DNSSEC

Answer: C

Question No : 112

Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip file is a file named “Court_Notice_21206.docx.exe” disguised as a word document.Upon execution, a windows appears stating, “This word document is corrupt.” In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?

A. Trojan
B. Worm
C. Key-Logger
D. Micro Virus

Answer: A

Question No : 113

When you are collecting information to perform a dataanalysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

A. site:target.com file:xls username password email
B. domain: target.com archive:xls username password email
C. site: target.com filetype:xls username password email
D. inurl: target.com filename:xls username password email

Answer: C

Question No : 114

A medium-sized healthcare IT business decides to implement a risk management strategy.

Which of the following is NOT one of the five basic responses to risk?

A. Mitigate
B. Avoid
C. Accept
D. Delegate

Answer: D

Question No : 115

What isa “Collision attach” in cryptography?

A. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
B. Collision attacks try to break the hash into three parts to get the plaintext value.
C. Collision attacks try to find two inputs producing the same hash.
D. Collision attacks try to get the public key

Answer: C

Question No : 116

The “Black box testing” methodology enforces which kind of restriction?

A. Only the external operation of a systemis accessible to the tester
B. The internal operation of a system is completely known to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: A

Question No : 117

You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

What tool will help you with the task?

A. Armitage
B. Dimitry
C. cdpsnarf
D. Metagoofil

Answer: D

Question No : 118

When you are testing a web application, it is very useful to employ a prosy tool to save every request and response.Nyou can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

A. Burpsuite
B. Dimitry
C. Proxychains
D. Maskgen

Answer: A

Question No : 119

While performing online banking using a web browser, a user receives an email that contains alink to an interesting Web site. When the user clicks on the link, another web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What web browser-based security vulnerability was exploited to compromise the user?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Web form input validation
D. Clickjacking

Answer: A

Question No : 120

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A. Verity access right before allowing access to protected information and UI controls
B. Use security policies and procedures to define and implement proper security settings
C. Validate and escape all information sent over to a server
D. Use digital certificates to authenticate a server prior to sending data

Answer: A

Question No : 121

An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, digital Subscriber Line (DSL), wireless data services, and virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is most likely able to handle this requirement?

A. DIAMETER
B. Kerberos
C. RADIUS
D. TACACS+

Answer: D

Question No : 122

Perspective clients wantto see sample reports from previous penetration tests.

What should you do next?

A. Share full reports, not redacted.
B. Share full reports, with redacted.
C. Decline but, provide references.
D. Share reports, after NDA is signed.

Answer: B

Question No : 123

A hacker has successfully infected an internet-facing server, which he will then use to send junk mail, take part incoordinated attacks, or host junk email content.

Which sort of trojan infects this server?

A. Botnet Trojan
B. Banking Trojans
C. Ransomware Trojans
D. Turtle Trojans

Answer: A

Question No : 124

You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. False Negative
B. True Negative
C. True Positive
D. False Positive

Answer: A

Question No : 125

Which of the following security operations is used for determining the attack surface of an organization?

A. Reviewing the need for a security clearance for each employee
B. Running a network scan to detect network services in the corporate DMZ
C. Training employees on the security policy regarding social engineering
D. Using configuration management to determine when and where to apply security patches

Answer: B