



Reference Solution for 312- 50v10.examcollection.premium.exam.29 4q 312-50v10

312-50v10

Certified Ethical Hacker v10 Exam

Version 3.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (160 questions)

Question 1

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of what the engineer performed?

- ☐ Cross-site scripting
- ☒ Banner grabbing
- ☐ SQL injection
- ☐ Who is database query

Question 2

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

- ☒ Incident Management Process
- ☐ Security Policy
- ☐ Internal Procedure
- ☐ Metrics

Question 3

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- ☒ 123
- ☐ 161
- ☐ 69
- ☐ 113

Question 4

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

- ☒ Administrative safeguards
- ☐ Physical security
- ☐ Logical interface
- ☐ DMZ

Question 5

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

- ☐ Set a BIOS password
- ☒ Encrypt the data on the hard drive.
- ☐ Use a strong logon password to the operating system.
- ☐ Back up everything on the laptop and store the backup in a safe place.

Question 6

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

- ☐ ICMP
- ☒ TCP
- ☐ UPX
- ☐ UPD

Question 7

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

- ☐ SSH communications are encrypted it's impossible to know who is the client or the server
- ☐ Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
- ☒ Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
- ☐ Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Question 8

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?

- ☒ Single sign-on
- ☐ Windows authentication
- ☐ Role Based Access Control (RBAC)
- ☐ Discretionary Access Control (DAC)

Question 9

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

- ☒ Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK
- ☐ Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
- ☐ Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
- ☐ Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN

Question 10

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 biometric system that bases authentication decisions on behavioral attributes.
- ☐ A biometric system that bases authentication decisions on physical attributes.
- ☒ An authentication system that creates one-time passwords that are encrypted with secret keys.
- ☐ An authentication system that uses passphrases that are converted into virtual passwords.

Question 11

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

- ☐ list domain=abccorp.local type=zone
- ☒ ls -d accorp.local
- ☐ list server=192.168.10.2 type=all
- ☐ lserver 192.168.10.2 -t all

Question 12

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- ☐ White Hat
- ☐ Suicide Hacker
- ☒ Gray Hat
- ☐ Black Hat

Question 13

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions.

Which of the following tools is he most likely using?

- ☐ Armitage
- ☒ Nikto
- ☐ Metasploit
- ☐ Nmap

Question 14

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?

- ☐ The amount of time and resources that are necessary to maintain a biometric system
- ☐ How long it takes to setup individual user accounts
- ☒ The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
- ☐ The amount of time it takes to convert biometric data into a template on a smart card

Question 15

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

- ☐ 64 bit and CCMP
- ☐ 128 bit and CRC
- ☒ 128 bit and CCMP
- ☐ 128 bi and TKIP

Question 16

An attacker scans a host with the below command. Which three flags are set? (Choose three.)

```
#nmap -sX host.domain.com
```

- ☐ This is ACK scan. ACK flag is set
- ☐ This is Xmas scan. SYN and ACK flags are set
- ☒ This is Xmas scan. URG, PUSH and FIN are set
- ☐ This is SYN scan. SYN flag is set

Question 17

The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:

```
Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
```

What type of activity has been logged?

- ☐ Teardrop attack targeting 192.168.0.110
- ☐ Denial of service attack targeting 192.168.0.105
- ☒ Port scan targeting 192.168.0.110
- ☐ Port scan targeting 192.168.0.105

Question 18

Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.

What is the main security risk associated with this scenario?

- ☒ External script contents could be maliciously modified without the security team knowledge
- ☐ External scripts have direct access to the company servers and can steal the data from there
- ☐ There is no risk at all as the marketing services are trustworthy
- ☐ External scripts increase the outbound company data traffic which leads greater financial losses

Question 19

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?

- ☐ Host 192.168.99.7 is an iPad.
- ☒ He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7
- ☐ Host 192.168.99.1 is the host that he launched the scan from.
- ☐ Host 192.168.99.7 is down.

Question 20

In Wireshark, the packet bytes panes show the data of the current packet in which format?

- ☐ Decimal
- ☐ ASCII only
- ☐ Binary
- ☒ Hexadecimal

Question 21

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

- ☐ Likelihood is the likely source of a threat that could exploit a vulnerability.
- ☒ Likelihood is the probability that a threat-source will exploit a vulnerability.
- ☐ Likelihood is a possible threat-source that may exploit a vulnerability.
- ☐ Likelihood is the probability that a vulnerability is a threat-source.

Question 22

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.

What may be the problem?

- ☒ Traffic is Blocked on UDP Port 53
- ☐ Traffic is Blocked on UDP Port 80
- ☐ Traffic is Blocked on UDP Port 54
- ☐ Traffic is Blocked on UDP Port 80

Question 23

Cross-site request forgery involves:

- ☐ A request sent by a malicious user from a browser to a server
- ☐ Modification of a request by a proxy between client and server
- ☒ A browser making a request to a server without the user's knowledge
- ☐ A server making a request to another server without the user's knowledge

Question 24

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?

- ☒ The port will ignore the packets.
- ☐ The port will send an RST.
- ☐ The port will send an ACK.
- ☐ The port will send a SYN.

Question 25

You are doing an internal security audit and intend to find out what ports are open on all the servers. What is the best way to find out?

- ☒ Scan servers with Nmap
- ☐ Scan servers with MBSA
- ☐ Telnet to every port on each server
- ☐ Physically go to each server

Question 26

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

- ☐ Port scan targeting 192.168.1.103
- ☐ Teardrop attack targeting 192.168.1.106
- ☐ Denial of service attack targeting 192.168.1.103
- ☒ Port scan targeting 192.168.1.106

Question 27

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- ☐ Event logs on the PC
- ☒ Internet Firewall/Proxy log
- ☐ IDS log
- ☐ Event logs on domain controller

Question 28

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- ☐ nslookup -fullrecursive update.antivirus.com
- ☐ dnsnoping -rt update.antivirus.com
- ☒ nslookup -norecursive update.antivirus.com
- ☐ dns --snoop update.antivirus.com

Question 29

Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

- ☐ Command Injection Attacks
- ☐ File Injection Attack
- ☒ Cross-Site Request Forgery (CSRF)
- ☐ Hidden Field Manipulation Attack

Question 30

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 organization is being described?

- ☐ Institute of Electrical and Electronics Engineers(IEEE)
- ☐ International Security Industry Organization (ISIO)
- ☐ Center for Disease Control (CDC)
- ☒ Payment Card Industry (PCI)

Question 31

Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

- ☐ Function Testing
- ☐ Dynamic Testing
- ☐ Static Testing
- ☒ Fuzzing Testing

Question 32

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- ☐ Omnidirectional antenna
- ☐ Dipole antenna
- ☒ Yagi antenna
- ☐ Parabolic grid antenna

Question 33

Which type of security feature stops vehicles from crashing through the doors of a building?

- ☐ Turnstile
- ☒ Bollards
- ☐ Mantrap
- ☐ Receptionist

Question 34

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?

- ☐ The computer is not using a private IP address.
- ☒ The gateway is not routing to a public IP address.
- ☐ The gateway and the computer are not on the same network.
- ☐ The computer is using an invalid IP address.

Question 35

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?

- ☐ Accept
- ☒ Delegate
- ☐ Mitigate
- ☐ Avoid

Question 36

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- ☐ openssl s_client -site www.website.com:443
- ☐ openssl_client -site www.website.com:443
- ☐ openssl_client -connect www.website.com:443
- ☒ openssl s_client -connect www.website.com:443

Question 37

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?

- ☐ DynDNS
- ☐ DNS Scheme
- ☐ DNSSEC
- ☒ Split DNS

Question 38

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- ☐ IANA
- ☐ CAPTCHA
- ☐ IETF
- ☒ WHOIS

Question 39

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

- ☐ HIPAA
- ☐ EU Safe Harbor
- ☐ PCI-DSS
- ☒ NIST-800-53

Question 40

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?

- ☒ Cross-Site Request Forgery
- ☐ SQL Injection
- ☐ Browser Hacking
- ☐ Cross-Site Scripting

Question 41

.....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.

- ☒ Evil Twin Attack
- ☐ Sinkhole Attack
- ☐ Collision Attack
- ☐ Signal Jamming Attack

Question 42

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

- ☒ In a climate controlled facility offsite
- ☐ In a cool dry environment
- ☐ On a different floor in the same building
- ☐ Inside the data center for faster retrieval in a fireproof safe

Question 43

What is the purpose of DNS AAAA record?

- ☐ Address prefix record
- ☐ Address database record
- ☐ Authorization, Authentication and Auditing record
- ☒ IPv6 address resolution record

Question 44

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?

- ☐ request smtp 25
- ☒ tcp.port eq 25
- ☐ smtp port
- ☐ tcp.contains port 25

Question 45

Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

- ☒ Work at the Data Link Layer
- ☐ Protect the payload and the headers
- ☐ Encrypt
- ☐ Authenticate

Question 46

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?

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

Question 47

How does the Address Resolution Protocol (ARP) work?

- ☐ It sends a request packet to all the network elements, asking for the domain name from a specific IP.
- ☒ It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
- ☐ It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
- ☐ It sends a reply packet for a specific IP, asking for the MAC address.

Question 48

What is not a PCI compliance recommendation?

- ☐ Use a firewall between the public network and the payment card data.
- ☐ Use encryption to protect all transmission of card holder data over any public network.
- ☒ Rotate employees handling credit card transactions on a yearly basis to different departments.
- ☐ Limit access to card holder data to as few individuals as possible.

Question 49

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

- ☐ Passive
- ☒ Active
- ☐ Reflective
- ☐ Distributive

Question 50

In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

- ☐ Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
- ☒ Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
- ☐ Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addressed.
- ☐ Vulnerabilities in the application layer are greatly different from IPv4.

Question 51

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

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

Question 52

What is the difference between the AES and RSA algorithms?

- ☐ Both are symmetric algorithms, but AES uses 256-bit keys
- ☐ AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data
- ☐ Both are asymmetric algorithms, but RSA uses 1024-bit keys
- ☒ RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data

Question 53

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?

- ☐ Session Fixation
- ☐ HTML Injection
- ☐ HTTP Parameter Pollution
- ☒ Clickjacking Attack

Question 54

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 that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 20011-03-15 11:06 NMAP scan report for 172.16.40.65 Host ip 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:8

- ☐ The host is likely a Linux machine.
- ☒ The host is likely a printer.
- ☐ The host is likely a router.
- ☐ The host is likely a Windows machine.

Question 55

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?

- ☐ Attack
- ☐ Vulnerability
- ☒ Threat
- ☐ Risk

Question 56

Which of the following provides a security professional with most information about the system's security posture?

- ☐ Wardriving, warchalking, social engineering
- ☐ Social engineering, company site browsing, tailgating
- ☐ Phishing, spamming, sending trojans
- ☒ Port scanning, banner grabbing, service identification

Question 57

Which of the following is not a Bluetooth attack?

- ☐ Bluesnarfing
- ☒ Bluedriving
- ☐ Bluesmacking
- ☐ Bluejacking

Question 58

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 is the following options can be useful to ensure the integrity of the data?

- ☒ The CFO can use a hash algorithm in the document once he approved the financial statements
- ☐ The CFO can use an excel file with a password
- ☐ 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 is the same document
- ☐ The document can be sent to the accountant using an exclusive USB for that document

Question 59

It is a short-range wireless communication technology intended to replace the cables connecting portable or 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?

- ☒ Bluetooth
- ☐ WLAN
- ☐ InfraRed
- ☐ Radio-Frequency identification

Question 60

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 tool could the tester use to get a response from a host using TCP?

- ☐ Traceroute
- ☒ Hping
- ☐ TCP ping
- ☐ Broadcast ping

Question 61

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?

- ☒ Snort
- ☐ Nmap
- ☐ Cain & Abel
- ☐ Nessus

Question 62

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

- ☐ Availability, Non-repudiation, Confidentiality
- ☐ Authenticity, Integrity, Non-repudiation
- ☒ Confidentiality, Integrity, Availability
- ☐ Authenticity, Confidentiality, Integrity

Question 63

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server? The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- ☐ Stacheldraht
- ☐ LOIC
- ☒ R-U-Dead-Yet? (RUDY)
- ☐ MyDoom

Question 64

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?

- ☐ Use fences in the entrance doors.
- ☒ Install a CCTV with cameras pointing to the entrance doors and the street.
- ☐ Use an IDS in the entrance doors and install some of them near the corners.
- ☐ Use lights in all the entrance doors and along the company's perimeter.

Question 65

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?

- ☒ The network devices are not all synchronized.
- ☐ Proper chain of custody was not observed while collecting the logs.
- ☐ The attacker altered or erased events from the logs.
- ☐ The security breach was a false positive.

Question 66

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

- ☐ "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
- ☒ "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
- ☐ "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"
- ☐ "GET/restricted/\r\n%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

Question 67

Code injection is a form of attack in which a malicious user:

- ☒ Inserts text into a data field that gets interpreted as code
- ☐ Gets the server to execute arbitrary code using a buffer overflow
- ☐ Inserts additional code into the JavaScript running in the browser
- ☐ Gains access to the codebase on the server and inserts new code

Question 68

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 reflects the changes.

Which type of vulnerability is present on this site?

- ☐ Cookie Tampering
- ☐ SQL Injection
- ☒ Web Parameter Tampering
- ☐ XSS Reflection

Question 69

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

- ☐ Only the internal operation of a system is known to the tester.
- ☒ The internal operation of a system is completely known to the tester.
- ☐ The internal operation of a system is only partly accessible to the tester.
- ☐ Only the external operation of a system is accessible to the tester.

Question 70

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- ☐ nmap -A -Pn
- ☐ nmap -sP -p-65535-T5
- ☒ nmap -sT -O -T0
- ☐ nmap -A --host-timeout 99-T1

Question 71

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

- ☐ Increase his technical skills
- ☐ Read the incident manual every time it occurs
- ☐ Select someone else to check the procedures
- ☒ Create an incident checklist

Question 72

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

- ☐ HIDS
- ☐ NIDS
- ☐ WISS
- ☒ WIPS

Question 73

Which service in a PKI will vouch for the identity of an individual or company?

- ☐ CBC
- ☐ KDC
- ☒ CA
- ☐ CR

Question 74

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

- ☐ Restrict Physical Access to Server Rooms hosting Critical Servers
- ☐ Use Static IP Address
- ☒ Using encryption protocols to secure network communications
- ☐ Register all machines MAC Address in a Centralized Database

Question 75

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

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

Question 76

You want to analyze packets on your wireless network. Which program would you use?

- ☒ Wireshark with Airpcap
- ☐ Aircrack-ng with Airpcap
- ☐ Wireshark with Winpcap
- ☐ Ethereal with Winpcap

Question 77

Which is the first step followed by Vulnerability Scanners for scanning a network?

- ☐ TCP/UDP Port scanning
- ☐ Firewall detection
- ☐ OS Detection
- ☒ Checking if the remote host is alive

Question 78

By using a smart card and pin, you are using a two-factor authentication that satisfies

- ☐ Something you know and something you are
- ☒ Something you have and something you know
- ☐ Something you have and something you are
- ☐ Something you are and something you remember

Question 79

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 of the protocol?

- ☐ Based on XML
- ☒ Only compatible with the application protocol HTTP
- ☐ Exchanges data between web services
- ☐ Provides a structured model for messaging

Question 80

If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

- ☐ -sP
- ☒ -P
- ☐ -r
- ☐ -F

Question 81

On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service. What is the name of the process by which you can determine those critical business?

- ☐ Risk Mitigation
- ☐ Emergency Plan Response (EPR)
- ☐ Disaster Recovery Planning (DRP)
- ☒ Business Impact Analysis (BIA)

Question 82

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 value is?

- ☐ Polymorphism
- ☐ Escrow
- ☐ Collusion
- ☒ Collision

Question 83

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

- ☐ AH permiscuous
- ☐ ESP confidential
- ☐ AH Tunnel mode
- ☒ ESP transport mode

Question 84

From the following table, identify the wrong answer in terms of Range (ft).

Standard	Range (ft)
802.11a	150-150
802.11b	150-150
802.11g	150-150
802.16(WiMax)	30 miles

- ☐ 802.11b
- ☐ 802.11g
- ☐ 802.16(WiMax)
- ☒ 802.11a

Question 85

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

- ☐ Linux
- ☐ Unix
- ☐ OS X
- ☒ Windows

Question 86

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?

- ☐ The sequence does not matter. Both steps have to be performed against all hosts.
- ☐ First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
- ☒ First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
- ☐ The port scan alone is adequate. This way he saves time.

Question 87

What is the role of test automation in security testing?

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

Question 88

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.

What should Bob recommend to deal with such a threat?

- ☐ The use of security agents in clients' computers
- ☒ The use of DNSSEC
- ☐ The use of double-factor authentication
- ☐ Client awareness

Question 89

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: `nmap -Pn -p -sl kiosk.adobe.com www.riaa.com kiosk.adobe.com` is the host with incremental IP ID sequence. What is the purpose of using “-sl” with Nmap?

- ☐ Conduct stealth scan
- ☐ Conduct ICMP scan
- ☒ Conduct IDLE scan
- ☐ Conduct silent scan

Question 90

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 gain access to the DNS server and redirect the direction `www.google.com` to his own IP address. Now when the employees of the office wants to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- ☐ MAC Flooding
- ☐ Smurf Attack
- ☒ DNS spoofing
- ☐ ARP Polsoning

Question 91

What is correct about digital signatures?

- ☒ 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.
- ☐ Digital signatures may be used in different documents of the same type.
- ☐ A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- ☐ Digital signatures are issued once for each user and can be used everywhere until they expire.

Question 92

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.

- ☐ Session hijacking
- ☒ Firewalking
- ☐ Man-in-the middle attack
- ☐ Network sniffing

Question 93

During an Xmas scan, what indicates a port is closed?

- ☒ RST
- ☐ SYN
- ☐ ACK
- ☐ No return response

Question 94

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

- ☐ Hash Algorithm
- ☐ Digest
- ☐ Secret Key
- ☒ Public Key

Question 95

Initiating an attack against targeted business 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?

- ☐ Heartbeat Attack
- ☐ Spear Phishing Attack
- ☐ Shellshock Attack
- ☒ Watering Hole Attack

Question 96

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

- ☐ Only the internal operation of a system is known to the tester.
- ☐ The internal operation of a system is completely known to the tester.
- ☒ The internal operation of a system is only partly accessible to the tester.
- ☐ Only the external operation of a system is accessible to the tester.

Question 97

Why should the security analyst disable/remove unnecessary ISAPI filters?

- ☐ To defend against social engineering attacks
- ☒ To defend against webserver attacks
- ☐ To defend against jailbreaking
- ☐ To defend against wireless attacks

Question 98

What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

- ☐ User Access Control (UAC)
- ☒ Data Execution Prevention (DEP)
- ☐ Address Space Layout Randomization (ASLR)
- ☐ Windows firewall

Question 99

Which of the following will perform an Xmas scan using NMAP?

- ☐ nmap -sA 192.168.1.254
- ☐ nmap -sP 192.168.1.254
- ☒ nmap -sX 192.168.1.254
- ☐ nmap -sV 192.168.1.254

Question 100

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?

- ☐ Randomizing
- ☐ Bounding
- ☐ Mutating
- ☒ Fuzzing

Question 101

Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

- ☐ Network security policy
- ☐ Information protection policy
- ☐ Access control policy
- ☒ Remote access policy

Question 102

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach.

After that, people must approximate their RFID badges. Both the identifications are required to open the door.

In this case, we can say:

- ☐ Although the approach has two phases, it actually implements just one authentication factor
- ☒ The solution implements the two authentication factors: physical object and physical characteristic
- ☐ The solution will have a high level of false positives
- ☐ Biological motion cannot be used to identify people

Question 103

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige.

After 2 days, Bob denies that he had ever sent a mail.

What do you want to "know" to prove yourself that it was Bob who had sent a mail?

- ☐ Confidentiality
- ☐ Integrity
- ☒ Non-Repudiation
- ☐ Authentication

Question 104

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?

- ☒ Privilege Escalation
- ☐ Shoulder-Surfing
- ☐ Hacking Active Directory
- ☐ Port Scanning

Question 105

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?

- ☐ Cross Site Scripting
- ☒ Injection
- ☐ Path disclosure
- ☐ Cross Site Request Forgery

Question 106

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?

- ☐ Do not report it and continue the penetration test.
- ☐ Transfer money from the administrator's account to another account.
- ☐ Do not transfer the money but steal the bitcoins.
- ☒ Report immediately to the administrator.

Question 107

_____ 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.

- ☒ DNSSEC
- ☐ Resource records
- ☐ Resource transfer
- ☐ Zone transfer

Question 108

When tuning security alerts, what is the best approach?

- ☒ Tune to avoid False positives and False Negatives
- ☐ Rise False positives Rise False Negatives
- ☐ Decrease the false positives
- ☐ Decrease False negatives

Question 109

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

- ☐ Maintaining Access
- ☐ Gaining Access
- ☒ Reconnaissance
- ☐ Scanning and Enumeration

Question 110

In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

- ☒ Chosen-plaintext attack
- ☐ Ciphertext-only attack
- ☐ Adaptive chosen-plaintext attack
- ☐ Known-plaintext attack

Question 111

The change 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?

- ☐ \$1320
- ☐ \$440
- ☐ \$100
- ☒ \$146

Question 112

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?

- ☐ Circuit
- ☐ Stateful
- ☒ Application
- ☐ Packet Filtering

Question 113

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

- ☐ ICMP Echo scanning
- ☒ SYN/FIN scanning using IP fragments
- ☐ ACK flag probe scanning
- ☐ IPID scanning

Question 114

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?

- ☒ Forward the message to your company's security response team and permanently delete the message from your computer.
- ☐ Reply to the sender and ask them for more information about the message contents.
- ☐ Delete the email and pretend nothing happened.
- ☐ Forward the message to your supervisor and ask for her opinion on how to handle the situation.

Question 115

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

- ☐ He needs to gain physical access.
- ☒ He must perform privilege escalation.
- ☐ He already has admin privileges, as shown by the "501" at the end of the SID.
- ☐ He needs to disable antivirus protection.

Question 116

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?

- ☒ Cross-site scripting vulnerability
- ☐ Session management vulnerability
- ☐ SQL injection vulnerability
- ☐ Cross-site Request Forgery vulnerability

Question 117

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- ☐ Usernames
- ☐ File permissions
- ☐ Firewall rulesets
- ☒ Passwords

Question 118

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- ☐ Black-box
- ☐ Announced
- ☐ White-box
- ☒ Grey-box

Question 119

Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

- ☐ [cache:]
- ☒ [site:]
- ☐ [inurl:]
- ☐ [link:]

Question 120

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 the “landscape” looks like. What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

- ☐ network mapping
- ☒ footprinting
- ☐ escalating privileges
- ☐ gaining access

Question 121

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?

- ☐ Armitage
- ☐ Dmitry
- ☒ Metagoofil
- ☐ cdpsnarf

Question 122

An LDAP directory can be used to store information similar to a SQL database. LDAP uses a _____ database structure instead of SQL’s _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.

- ☐ Strict, Abstract
- ☐ Simple, Complex
- ☐ Relational, Hierarchical
- ☒ Hierarchical, Relational

Question 123

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?

- ☐ Nessus
- ☒ Metasploit
- ☐ Maltego
- ☐ Wireshark

Question 124

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.

When users accessed any page, the applet ran and exploited many machines.

Which one of the following tools the hacker probably used to inject HTML code?

- ☐ Wireshark
- ☒ Ettercap
- ☐ Aircrack-ng
- ☐ Tcpdump

Question 125

You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

- ☐ Telnet
- ☐ POP3
- ☒ Network Time Protocol
- ☐ DNS

Question 126

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

- ☐ Identifying operating systems, services, protocols and devices
- ☒ Modifying and replaying captured network traffic
- ☐ Collecting unencrypted information about usernames and passwords
- ☐ Capturing a network traffic for further analysis

Question 127

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- ☐ Bob can be right since DMZ does not make sense when combined with stateless firewalls
- ☐ Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
- ☒ Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
- ☐ Bob is partially right. DMZ does not make sense when a stateless firewall is available

Question 128

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?

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

Question 129

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 firewall IPTable
- ☐ FTP Server rule
- ☐ A Router IPTable
- ☒ An Intrusion Detection System

Question 130

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.

He identified this when the IDS alerted for malware activities in the network.

What should Bob do to avoid this problem?

- ☐ Disable unused ports in the switches
- ☐ Separate students in a different VLAN
- ☒ Use the 802.1x protocol
- ☐ Ask students to use the wireless network

Question 131

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?

- ☐ 161
- ☐ 3389
- ☒ 445
- ☐ 1433

Question 132

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

Question 133

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

- ☐ NoSQL injection
- ☒ Blind SQL injection
- ☐ Union-based SQL injection
- ☐ Error-based SQL injection

Question 134

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- ☐ Black-box
- ☐ Announced
- ☐ White-box
- ☒ Grey-box

Question 135

What would you enter, if you wanted to perform a stealth scan using Nmap?

- ☐ nmap -sU
- ☒ nmap -sS
- ☐ nmap -sM
- ☐ nmap -sT

Question 136

How can rainbow tables be defeated?

- ☒ Password salting
- ☐ Use of non-dictionary words
- ☐ All uppercase character passwords
- ☐ Lockout accounts under brute force password cracking attempts

Question 137

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

- ☐ The file reveals the passwords to the root user only.
- ☒ The password file does not contain the passwords themselves.
- ☐ He cannot read it because it is encrypted.
- ☐ He can open it and read the user ids and corresponding passwords.

Question 138

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?

- ☐ Discovery
- ☐ Recovery
- ☒ Containment
- ☐ Eradication

Question 139

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- ☐ SHA-2
- ☐ SHA-3
- ☒ SHA-1
- ☐ SHA-0

Question 140

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

- ☐ Honeypots
- ☐ Firewalls
- ☒ Network-based intrusion detection system (NIDS)
- ☐ Host-based intrusion detection system (HIDS)

Question 141

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.

Which type of virus detection method did Chandler use in this context?

- ☐ Heuristic Analysis
- ☒ Code Emulation
- ☐ Integrity checking
- ☐ Scanning

Question 142

The "black box testing" methodology enforces what kind of restriction?

- ☐ Only the internal operation of a system is known to the tester.
- ☐ The internal operation of a system is completely known to the tester.
- ☐ The internal operation of a system is only partly accessible to the tester.
- ☒ Only the external operation of a system is accessible to the tester.

Question 143

Sam is working as a pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

- ☐ Denial-of-Service
- ☒ False Positive Generation
- ☐ Insertion Attack
- ☐ Obfuscating

Question 144

Due to a slowdown of normal network operations, the 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?

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

Question 145

Which of the following act requires employer's standard national numbers to identify them on standard transactions?

- ☐ SOX
- ☒ HIPAA
- ☐ DMCA
- ☐ PCI-DSS

Question 146

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 fingerprint scanner and his username and password
- ☐ His username and a stronger password
- ☐ A new username and password
- ☐ Disable his username and use just a fingerprint scanner

Question 147

What does the -oX flag do in an Nmap scan?

- ☐ Perform an Xmas scan
- ☐ Perform an eXpress scan
- ☐ Output the results in truncated format to the screen
- ☒ Output the results in XML format to a file

Question 148

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?

- ☐ Encryption
- ☒ Steganography
- ☐ RSA algorithm
- ☐ Public-key cryptography

Question 149

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 15917KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

- ☐ She is using ftp to transfer the file to another hacker named John.
- ☒ She is using John the Ripper to crack the passwords in the secret.txt file
- ☐ She is encrypting the file.
- ☐ She is using John the Ripper to view the contents of the file.

Question 150

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. He also 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 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
```

- ☐ The ACL 104 needs to be first because is UDP
- ☐ The ACL 110 needs to be changed to port 80
- ☐ The ACL for FTP must be before the ACL 110
- ☒ The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

Question 151

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?

- ☒ Malicious code is attempting to execute instruction a non-executable memory region.
- ☐ A page fault is occurring, which forces the operating system to write data from the hard drive.
- ☐ A race condition is being exploited, and the operating system is containing the malicious process.
- ☐ Malware is executing in either ROM or a cache memory area.

Question 152

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?

- ☐ Protocol analyzer
- ☐ Intrusion Detection System
- ☐ Port scanner
- ☒ Vulnerability scanner

Question 153

A virus that attempts to install itself inside the file it is infecting is called?

- ☐ Tunneling virus
- ☒ Cavity virus
- ☐ Polymorphic virus
- ☐ Stealth virus

Question 154

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?

- ☒ Internal, Blackbox
- ☐ External, Blackbox
- ☐ External, Whitebox
- ☐ Internal, Whitebox

Question 155

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?

- ☐ Boot.ini
- ☐ Sudoers
- ☐ Networks
- ☒ Hosts

Question 156

Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

- ☐ Scalability
- ☒ Speed
- ☐ Key distribution
- ☐ Security

Question 157

What two conditions must a digital signature meet?

- ☐ Has to be legible and neat.
- ☒ Has to be unforgeable, and has to be authentic.
- ☐ Must be unique and have special characters.
- ☐ Has to be the same number of characters as a physical signature and must be unique.

Question 158

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?

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

- ☐ Host-Based Intrusion Detection System
- ☐ Security through obscurity
- ☒ Defense in depth
- ☐ Network-Based Intrusion Detection System

Question 159

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer) <=100:
    buffer.append("A"*counter)
    counter=counter+50
com-
mands=["HELP","STATS","RTIME","LTIME","SRUN","TRUN","GMON","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?

- ☒ Buffer Overflow
- ☐ Encryption
- ☐ Denial-of-service (DoS)
- ☐ Bruteforce

Question 160

You have 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 toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- ☐ John the Ripper
- ☐ SET
- ☒ CHNTPW
- ☐ Cain & Abel