Exam : 312-50v10

Title : Certified Ethical Hacker v10 Exam

Version : V11.02

1.An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush.

What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

Answer: B

2.Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares

B. Keep some generation of off-line backup

C. Analyze the ransomware to get decryption key of encrypted data

D. Pay a ransom

Answer: B

3.If an attacker uses the command SELECT*FROM user WHERE name = ‘x’ AND userid IS NULL; --‘; which type of SQL injection attack is the attacker performing?

A. End of Line Comment

B. UNION SQL Injection

C. Illegal/Logically Incorrect Query

D. Tautology

Answer: D

4.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. Full Disk encryption

B. BIOS password

C. Hidden folders

D. Password protected files

Answer: A

5.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. Boot.ini

B. Sudoers

C. Networks

D. Hosts

Answer: D

6.Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Produces less false positives

B. Can identify unknown attacks
C. Requires vendor updates for a new threat
D. Cannot deal with encrypted network traffic
Answer: B

7.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:\gpedit
B. c:\compmgmt.msc
C. c:\ncpa.cp
D. c:\services.msc
Answer: B

8.Which of the following act requires employer’s standard national numbers to identify them on standard transactions?
A. SOX
B. HIPAA
C. DMCA
D. PCI-DSS
Answer: B

9.In Wireshark, the packet bytes panes show the data of the current packet in which format?
A. Decimal
B. ASCII only
C. Binary
D. Hexadecimal
Answer: D

10._________ is a set of extensions to DNS that provide to DNS clients (resolvers) the origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.
A. DNSSEC
B. Resource records
C. Resource transfer
D. Zone transfer
Answer: A

11.PGP, SSL, and IKE are all examples of which type of cryptography?
A. Hash Algorithm
B. Digest
C. Secret Key
D. Public Key
Answer: D

12.Which of the following is considered as one of the most reliable forms of TCP scanning?
A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL Scan
D. Xmas Scan
Answer: A

13.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?
A. ICMP Echo scanning
B. SYN/FIN scanning using IP fragments
C. ACK flag probe scanning
D. IPID scanning
Answer: B

14.Which of the following is the BEST way to defend against network sniffing?
A. Restrict Physical Access to Server Rooms hosting Critical Servers
B. Use Static IP Address
C. Using encryption protocols to secure network communications
D. Register all machines MAC Address in a Centralized Database
Answer: C

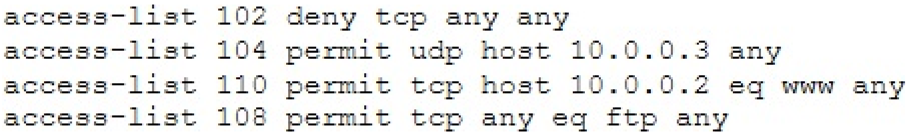
15.You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?
A. Out of band signaling
B. Protocol Isolation
C. Encryption
D. Alternate Data Streams
Answer: C

16.What is the purpose of a demilitarized zone on a network?
A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect
Answer: B

17.You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet.
What is the recommended architecture in terms of server placement?
A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network

C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves
Answer: B

18.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
```

A. The ACL 104 needs to be first because is UDP
B. The ACL 110 needs to be changed to port 80
C. The ACL for FTP must be before the ACL 110
D. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
Answer: D

19.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?
A. Identifying operating systems, services, protocols and devices
B. Modifying and replaying captured network traffic
C. Collecting unencrypted information about usernames and passwords
D. Capturing a network traffic for further analysis
Answer: B

20.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. Web site defacement vulnerability
C. SQL injection vulnerability
D. Cross-site Request Forgery vulnerability
Answer: A

21.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?

A. “GET/restricted/goldtransfer?to=Rob&from=1 or 1=1’ HTTP/1.1Host: westbank.com”
B. “GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com”
C. “GET/restricted/bank.getaccount(‘Ned’) HTTP/1.1 Host: westbank.com”
D. “GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com”
Answer: B

22.Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
A. Metasploit
B. Cain & Abel
C. Maltego
D. Wireshark
Answer: C

23.Which of these is capable of searching for and locating rogue access points?
A. HIDS
B. NIDS
C. WISS
D. WIPS
Answer: D

24.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?
A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat
Answer: C

25.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?
A. Based on XML
B. Only compatible with the application protocol HTTP
C. Exchanges data between web services
D. Provides a structured model for messaging
Answer: B

26.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?

A. John the Ripper

B. SET

C. CHNTPW

D. Cain & Abel

Answer: C

27.What type of vulnerability/attack is it when the malicious person forces the user’s browser to send an authenticated request to a server?

A. Cross-site request forgery

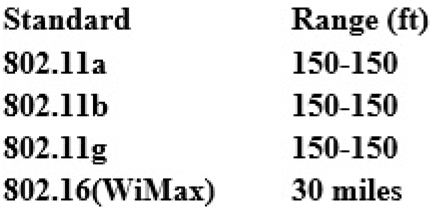
B. Cross-site scripting

C. Session hijacking

D. Server side request forgery

Answer: A

28.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

A. 802.11b

B. 802.11g

C. 802.16(WiMax)

D. 802.11a

Answer: D

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

A. nmap -sU

B. nmap -sS

C. nmap -sM

D. nmap -sT

Answer: B

30.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?

A. Scan servers with Nmap

B. Scan servers with MBSA

C. Telnet to every port on each server

D. Physically go to each server

Answer: A

31.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:
A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people
Answer: B

32.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?
A. Honeypots
B. Firewalls
C. Network-based intrusion detection system (NIDS)
D. Host-based intrusion detection system (HIDS)
Answer: C

33.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. SSL/TLS Renegotiation Vulnerability
B. Shellshock
C. Heartbleed Bug
D. POODLE
Answer: C

34.Which protocol is used for setting up secure channels between two devices, typically in VPNs?
A. PPP
B. IPSEC
C. PEM
D. SET
Answer: B

35.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?
A. SHA-2
B. SHA-3
C. SHA-1
D. SHA-0
Answer: C

36.When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?
A. At least twice a year or after any significant upgrade or modification

B. At least once a year and after any significant upgrade or modification
C. At least once every two years and after any significant upgrade or modification
D. At least once every three years or after any significant upgrade or modification
Answer: B

37.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. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping
Answer: B

38.Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?
A. Bootrom Exploit
B. iBoot Exploit
C. Sandbox Exploit
D. Userland Exploit
Answer: D

39.What is not a PCI compliance recommendation?
A. Use a firewall between the public network and the payment card data.
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. Limit access to card holder data to as few individuals as possible.
Answer: C

40.The "white box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. Only the external operation of a system is accessible to the tester.
Answer: B

41.Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.
A. SQL injection attack
B. Cross-Site Scripting (XSS)
C. LDAP Injection attack
D. Cross-Site Request Forgery (CSRF)
Answer: B

42.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. wificracker

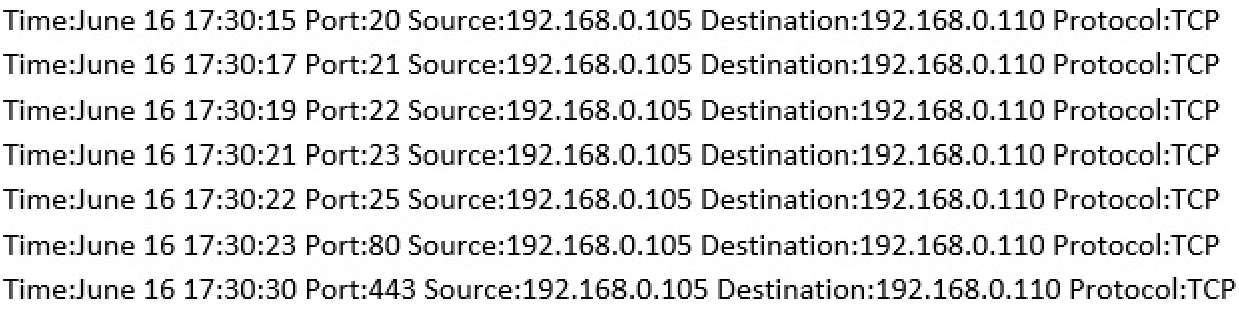
B. Airguard

C. WLAN-crack

D. Aircrack-ng

Answer: D

43.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?

A. Teardrop attack targeting 192.168.0.110

B. Denial of service attack targeting 192.168.0.105

C. Port scan targeting 192.168.0.110

D. Port scan targeting 192.168.0.105

Answer: C

44.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?

A. nmap –A - Pn

B. nmap –sP –p-65535-T5

C. nmap –sT –O –T0

D. nmap –A --host-timeout 99-T1

Answer: C

45.Bob, your senior colleague, has sent you a mail regarding aa 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 send a mail?

A. Confidentiality

B. Integrity

C. Non-Repudiation

D. Authentication

Answer: C

46.What is attempting an injection attack on a web server based on responses to True/False questions called?
A. DMS-specific SQLi
B. Compound SQLi
C. Blind SQLi
D. Classic SQLi
Answer: C

47.The establishment of a TCP connection involves a negotiation called three-way handshake.
What type of message does the client send to the server in order to begin this negotiation?
A. ACK
B. SYN
C. RST
D. SYN-ACK
Answer: B

48.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?
A. Snort
B. Nmap
C. Cain & Abel
D. Nessus
Answer: A

49.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 192.168.1.254
D. nmap -sV 192.168.1.254
Answer: C

50.Code injection is a form of attack in which a malicious user:
A. Inserts text into a data field that gets interpreted as code
B. Gets the server to execute arbitrary code using a buffer overflow
C. Inserts additional code into the JavaScript running in the browser
D. Gains access to the codebase on the server and inserts new code
Answer: A

51.The collection of potentially actionable, overt, and publicly available information is known as
A. Open-source intelligence
B. Human intelligence

C. Social intelligence
D. Real intelligence
Answer: A

52.Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?
A. [cache:]
B. [site:]
C. [inurl:]
D. [link:]
Answer: B

53.This asymmetry cipher is based on factoring the product of two large prime numbers.
What cipher is described above?
A. SHA
B. RSA
C. MD5
D. RC5
Answer: B

54.Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?
A. Data-driven firewall
B. Stateful firewall
C. Packet firewall
D. Web application firewall
Answer: D

55.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. DynDNS
B. DNS Scheme
C. DNSSEC
D. Split DNS
Answer: D

56.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?
A. Chosen-plaintext attack
B. Ciphertext-only attack
C. Adaptive chosen-plaintext attack
D. Known-plaintext attack

Answer: A

57.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?
A. Command Injection Attacks
B. File Injection Attack
C. Cross-Site Request Forgery (CSRF)
D. Hidden Field Manipulation Attack
Answer: C

58.Which is the first step followed by Vulnerability Scanners for scanning a network?
A. TCP/UDP Port scanning
B. Firewall detection
C. OS Detection
D. Checking if the remote host is alive
Answer: D

59.Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?
A. Linux
B. Unix
C. OS X
D. Windows
Answer: D

60.Alice encrypts her data using her public key PK and stores the encrypted data in the cloud.
Which of the following attack scenarios will compromise the privacy of her data?
A. None of these scenarios compromise the privacy of Alice’s data
B. Agent Andrew subpoenas Alice, forcing her to reveal her private key.
However, the cloud server successfully resists Andrew’s attempt to access the stored data
C. Hacker Harry breaks into the cloud server and steals the encrypted data
D. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before
Answer: D

61.A hacker named Jack is trying to compromise a bank’s computer system. He needs to know the operating system of that computer to launch further attacks.
What process would help him?
A. Banner Grabbing
B. IDLE/IPID Scanning
C. SSDP Scanning
D. UDP Scanning
Answer: A

62.What two conditions must a digital signature meet?

A. Has to be legible and neat.
B. Has to be unforgeable, and has to be authentic.
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.
Answer: B

63.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?
A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network
Answer: C

64.Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?
A. Bluesmacking
B. Bluesniffing
C. Bluesnarfing
D. Bluejacking
Answer: D

65.Which method of password cracking takes the most time and effort?
A. Shoulder surfing
B. Brute force
C. Dictionary attack
D. Rainbow tables
Answer: B

66.Which of the following program infects the system boot sector and the executable files at the same time?
A. Stealth virus
B. Polymorphic virus
C. Macro virus
D. Multipartite Virus
Answer: D

67.You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?

A. ACK flag scanning
B. TCP Scanning
C. IP Fragment Scanning
D. Inverse TCP flag scanning
Answer: C

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

69.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?
A. Telnet
B. POP3
C. Network Time Protocol
D. DNS
Answer: C

70.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
A. SSH communications are encrypted it’s impossible to know who is the client or the server
B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server
Answer: C

71.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 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24
Answer: B

72.........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. Evil Twin Attack
B. Sinkhole Attack
C. Collision Attack
D. Signal Jamming Attack
Answer: A

73.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?
A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com
Answer: C

74.You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.
While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.
After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?
A. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Rootkit Attack
Answer: A

75.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?
A. Function Testing
B. Dynamic Testing
C. Static Testing
D. Fuzzing Testing
Answer: D

76.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?
A. The use of security agents in clients’ computers
B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness
Answer: B

77.In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing
Answer: C

78.Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
A. –T0
B. –T5
C. -O
D. -A
Answer: B

79.Which of the following provides a security professional with most information about the system’s security posture?
A. Wardriving, warchalking, social engineering
B. Social engineering, company site browsing, tailgating
C. Phishing, spamming, sending trojans
D. Port scanning, banner grabbing, service identification
Answer: D

80.What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?
A. Manipulate format strings in text fields
B. SSH
C. SYN Flood
D. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
Answer: D

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

B. Impact risk
C. Inherent risk
D. Residual risk
Answer: D

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

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

84.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?
A. Heuristic Analysis
B. Code Emulation
C. Integrity checking
D. Scanning
Answer: B

85.An attacker scans a host with the below command.
Which three flags are set? (Choose three.)
#nmap –sX host.domain.com
A. This is ACK scan. ACK flag is set
B. This is Xmas scan. SYN and ACK flags are set
C. This is Xmas scan. URG, PUSH and FIN are set
D. This is SYN scan. SYN flag is set
Answer: C

86.Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic

for all of the employees.
From a legal standpoint, 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.
Answer: C

87.Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?
A. Internet Key Exchange (IKE)
B. Oakley
C. IPsec Policy Agent
D. IPsec driver
Answer: A

88.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?
A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump
Answer: B

89.You are monitoring the network of your organizations. You notice that:
There are huge outbound connections from your Internal Network to External IPs
On further investigation, you see that the external IPs are blacklisted
Some connections are accepted, and some are dropped
You find that it is a CnC communication
Which of the following solution will you suggest?
A. Block the Blacklist IP's @ Firewall
B. Update the Latest Signatures on your IDS/IPS
C. Clean the Malware which are trying to Communicate with the External Blacklist IP's
D. Both B and C
Answer: D

90.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?
A. Availability, Non-repudiation, Confidentiality

B. Authenticity, Integrity, Non-repudiation
C. Confidentiality, Integrity, Availability
D. Authenticity, Confidentiality, Integrity
Answer: C

91.Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?
A. Omnidirectional antenna
B. Dipole antenna
C. Yagi antenna
D. Parabolic grid antenna
Answer: C

92.Why should the security analyst disable/remove unnecessary ISAPI filters?
A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks
Answer: B

93.Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?
A. Network security policy
B. Information protection policy
C. Access control policy
D. Remote access policy
Answer: D

94.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. Randomizing
B. Bounding
C. Mutating
D. Fuzzing
Answer: D

95.If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
A. -sP
B. -P
C. -r
D. -F
Answer: D

96.In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the likely source of a threat that could exploit a vulnerability.
B. Likelihood is the probability that a threat-source will exploit a vulnerability.
C. Likelihood is a possible threat-source that may exploit a vulnerability.
D. Likelihood is the probability that a vulnerability is a threat-source.
Answer: B

97.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.
Answer: A

98.What is the least important information when you analyze a public IP address in a security alert?
A. ARP
B. Whois
C. DNS
D. Geolocation
Answer: A

99.You are the Network Admin, and you get a compliant 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?
A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on UDP Port 80
C. Traffic is Blocked on UDP Port 54
D. Traffic is Blocked on UDP Port 80
Answer: A

100.Internet Protocol Security IPsec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.
A. Work at the Data Link Layer
B. Protect the payload and the headers
C. Encrypt
D. Authenticate
Answer: A

101.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?

A. Risk Mitigation
B. Emergency Plan Response (EPR)
C. Disaster Recovery Planning (DRP)
D. Business Impact Analysis (BIA)
Answer: D

102.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?
A. External script contents could be maliciously modified without the security team knowledge
B. External scripts have direct access to the company servers and can steal the data from there
C. There is no risk at all as the marketing services are trustworthy
D. External scripts increase the outbound company data traffic which leads greater financial losses
Answer: A

103.What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
A. Black-box
B. Announced
C. White-box
D. Grey-box
Answer: D

104.Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends “many” IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:
A. Just a network monitoring tool
B. A signature-based IDS
C. A hybrid IDS
D. A behavior-based IDS
Answer: A

105.Which of the following is a low-tech way of gaining unauthorized access to systems?
A. Scanning
B. Sniffing
C. Social Engineering
D. Enumeration
Answer: C

106.When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives
B. Rise False positives Rise False Negatives
C. Decrease the false positives
D. Decrease False negatives
Answer: A

107.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. Privilege Escalation
B. Shoulder-Surfing
C. Hacking Active Directory
D. Port Scanning
Answer: A

108.Which regulation defines security and privacy controls for Federal information systems and organizations?
A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53
Answer: D

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

110.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 staring an investigation to roughly analyze the severity of the situation.
Which of the following is appropriate to analyze?
A. Event logs on the PC
B. Internet Firewall/Proxy log
C. IDS log
D. Event logs on domain controller
Answer: B

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

A. 123

B. 161

C. 69

D. 113

Answer: A

112.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. Discovery

B. Recovery

C. Containment

D. Eradication

Answer: C

113.Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by a coercion or torture?

A. Chosen-Cipher text Attack

B. Ciphertext-only Attack

C. Timing Attack

D. Rubber Hose Attack

Answer: D

114.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 whose credentials are known. It was written by sysinternals and has been integrated within the framework. The 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 used in the psexec module's 'smbpass' option?

A. LM:NT

B. NTLM:LM

C. NT:LM

D. LM:NTLM

Answer: A

115.You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

A. Double quotation

B. Backslash
C. Semicolon
D. Single quotation
Answer: D

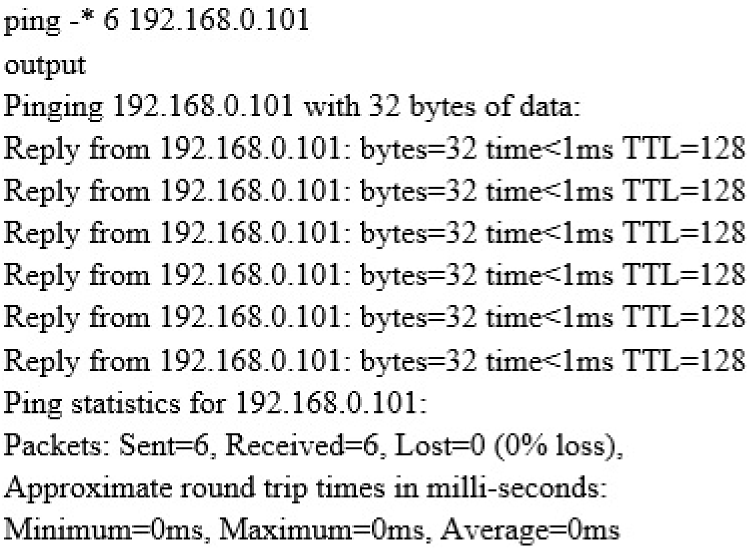
116.A virus that attempts to install itself inside the file it is infecting is called?
A. Tunneling virus
B. Cavity virus
C. Polymorphic virus
D. Stealth virus
Answer: B

117.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?
A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
D. Bob is partially right. DMZ does not make sense when a stateless firewall is available
Answer: C

118.Sam is working as s 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?
A. Denial-of-Service
B. False Positive Generation
C. Insertion Attack
D. Obfuscating
Answer: B

119.Cross-site request forgery involves:
A. A request sent by a malicious user from a browser to a server
B. Modification of a request by a proxy between client and server
C. A browser making a request to a server without the user’s knowledge
D. A server making a request to another server without the user’s knowledge
Answer: C

120.What does the option * indicate?



```
ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

A. s

B. t

C. n

D. a

Answer: C

121.An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

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

A. DIAMETER

B. RADIUS

C. TACACS+

D. Kerberos

Answer: B

122.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?

A. Host-Based Intrusion Detection System

B. Security through obscurity

C. Defense in depth

D. Network-Based Intrusion Detection System

Answer: C

123.During the process of encryption and decryption, what keys are shared?

A. Private keys

B. User passwords

C. Public keys

D. Public and private keys

Answer: C

124.How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

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

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

D. It sends a reply packet for a specific IP, asking for the MAC address.

Answer: B

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

A. AH promiscuous

B. ESP confidential

C. AH Tunnel mode

D. ESP transport mode

Answer: D

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

A. Black-box

B. Announced

C. White-box

D. Grey-box

Answer: D

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

A. HIPAA

B. EU Safe Harbor

C. PCI-DSS

D. NIST-800-53

Answer: D

128.You want to do an ICMP scan on a remote computer using hping2.

What is the proper syntax?

A. hping2 -1 host.domain.com

B. hping2-i host.domain.com

C. hping2 –set-ICMP host.domain.com

D. hping2 host.domain.com

Answer: A

129.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. Common

B. Criminal
C. Civil
D. International
Answer: C

130.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?
A. The CFO can use a hash algorithm in the document once he approved the financial statements
B. The CFO can use an excel file with a password
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 is the same document
D. The document can be sent to the accountant using an exclusive USB for that document
Answer: A

131.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. Session hijacking
B. Firewalking
C. Man-in-the middle attack
D. Network sniffing
Answer: B

132.What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?
A. Passive
B. Active
C. Reflective
D. Distributive
Answer: B

133.Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below.
What conclusions can be drown based on these scan results?
TCP port 21 – no response
TCP port 22 – no response
TCP port 23 – Time-to-live exceeded
A. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server

C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: C

134.A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?
A. Man-in-the-middle attack
B. Session hijacking
C. Brute-force attack
D. Dictionary-attack
Answer: D

135.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 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:8
A. The host is likely a Linux machine.
B. The host is likely a printer.
C. The host is likely a router.
D. The host is likely a Windows machine.
Answer: B

136.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 scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
B. This is scam because Bob does not know Scott.
C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
D. This is probably a legitimate message as it comes from a respectable organization.
Answer: A

137.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?
A. The amount of time and resources that are necessary to maintain a biometric system
B. How long it takes to setup individual user accounts
C. The amount of time it takes to be either accepted or rejected from when an individual provides

identification and authentication information
D. The amount of time it takes to convert biometric data into a template on a smart card
Answer: C

138.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. SQL Injection
C. Browser Hacking
D. Cross-Site Scripting
Answer: A

139.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 this action so that is escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.
Answer: A

140.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. Single sign-on
B. Windows authentication
C. Role Based Access Control (RBAC)
D. Discretionary Access Control (DAC)
Answer: A

141.Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?
A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Polymorphic virus
Answer: A

142.If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?
A. Spoof Scan
B. TCP SYN

C. TCP Connect scan
D. Idle scan
Answer: B

143.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?
A. Polymorphism
B. Escrow
C. Collusion
D. Collision
Answer: D

144.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?
A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Who is database query
Answer: B

145.A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network.
What tool should the analyst use to perform a Blackjacking attack?
A. Paros Proxy
B. BBProxy
C. Bloover
D. BBCrack
Answer: B

146.What attack is used to crack passwords by using a precomputed table of hashed passwords?
A. Brute Force Attack
B. Rainbow Table Attack
C. Dictionary Attack
D. Hybrid Attack
Answer: B

147.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. Multi-cast mode
B. Promiscuous mode
C. WEM
D. Port forwarding
Answer: B

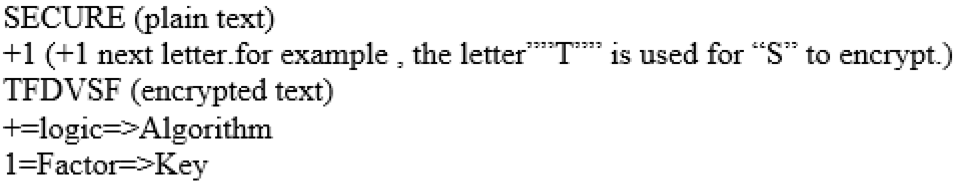
148.A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server,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

149.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
Answer: A

150.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
Answer: B

151.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 confidentially, 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 true about cryptography?
A. Algorithm is not the secret; key is the secret.
B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
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. 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.
Answer: C

152.What is the difference between the AES and RSA algorithms?
A. Both are symmetric algorithms, but AES uses 256-bit keys
B. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data
C. Both are asymmetric algorithms, but RSA uses 1024-bit keys
D. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data
Answer: D

153.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)

Answer: A

154.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.

Answer: D

155.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.

Answer: A

156.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.

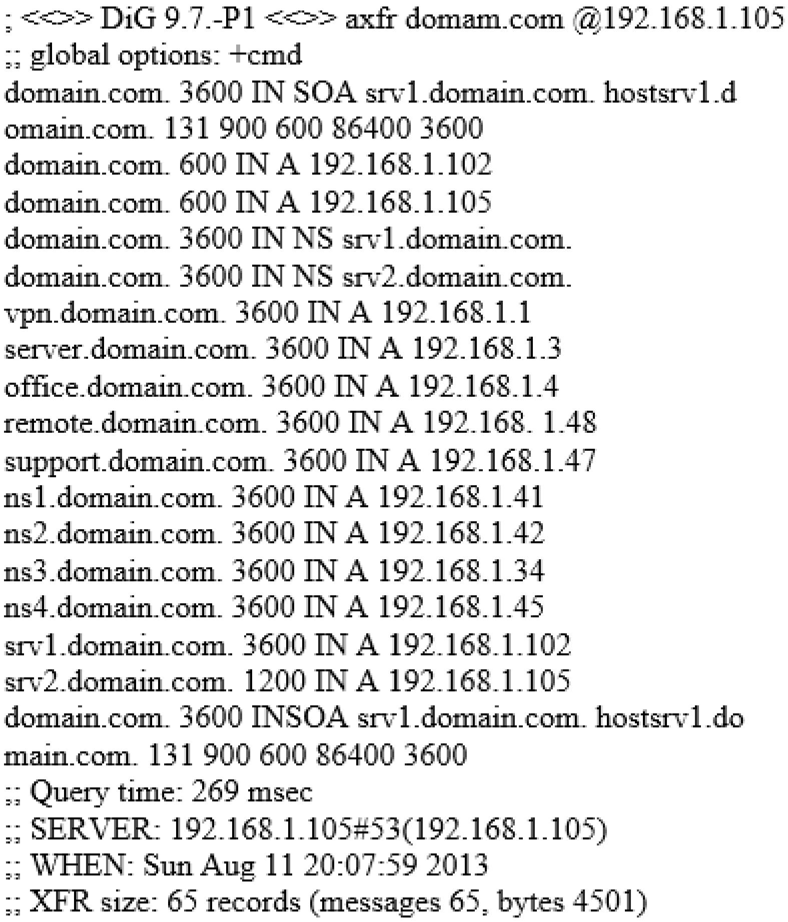
B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.

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.

Answer: C

157.Look at the following output.



```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.d
omain.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 INSOA srv1.domain.com. hostsrv1.do
main.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)
```

What did the hacker accomplish?

A. The hacker used who is 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 transferred the zone and enumerated the hosts.

Answer: D

158.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

Answer: D

159.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.

Answer: B

160.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 fingerprint scanner and his username and password

B. His username and a stronger password

C. A new username and password

D. Disable his username and use just a fingerprint scanner

Answer: A

161.A bank stores and processes sensitive privacy information related to home loans.
However, auditing has never been enabled on the system.
What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

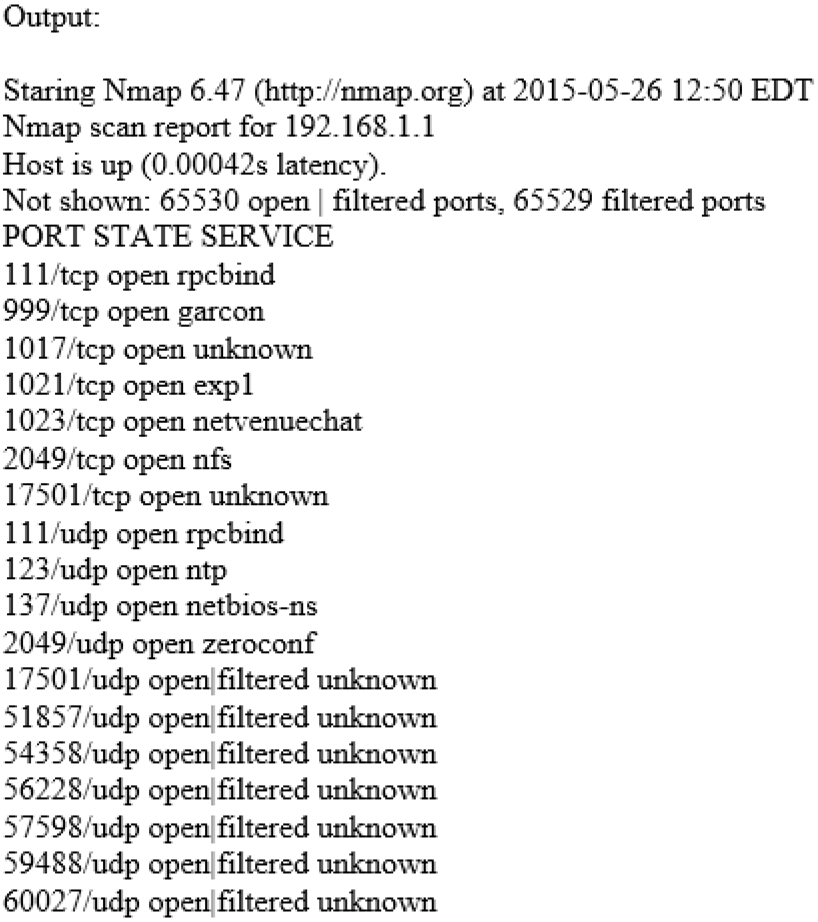
B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

Answer: B

162.Which of the following Nmap commands will produce the following output?



```
Output:

Staring 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 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 –sT –sX –Pn –p 1-65535 192.168.1.1

B. nmap –sN –Ps –T4 192.168.1.1

C. nmap –sS –sU –Pn –p 1-65535 192.168.1.1

D. nmap –sS –Pn 192.168.1.1

Answer: C

163.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

Answer: B

164.Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

Answer: C

165.A new wireless client is configured to join an 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

Answer: A

166.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.

Answer: A

167.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

Answer: A

168.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, ““11111111111111111111111111111””);
}
```

Output:

```
Segmentation fault
```

A. C#

B. Python

C. Java

D. C++

Answer: D

169.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 attempts 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 UPL 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. Session Fixation

B. HTML Injection

C. HTTP Parameter Pollution

D. Clickjacking Attack

Answer: D

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

A. Usernames

B. File permissions

C. Firewall rulesets

D. Passwords

Answer: D

171.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

Answer: B

172.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.

Answer: A

173.A large mobile telephony and data network operator has a data center 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.

Answer: A

174.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

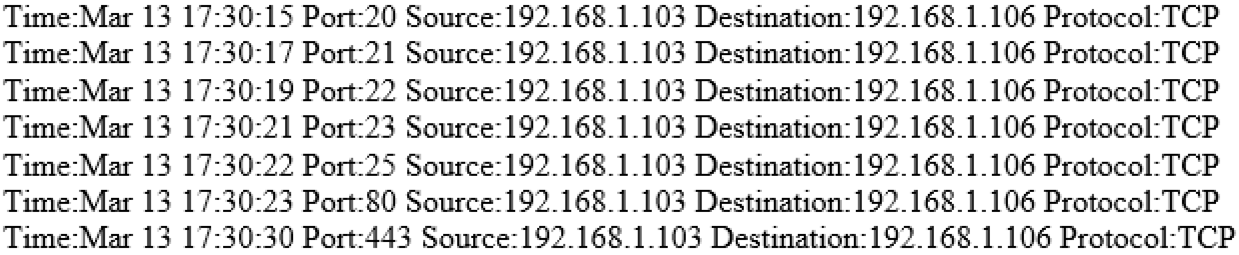
B. Containment phase

C. Identification phase

D. Recovery phase

Answer: A

175.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?

A. Port scan targeting 192.168.1.103

B. Teardrop attack targeting 192.168.1.106

C. Denial of service attack targeting 192.168.1.103

D. Port scan targeting 192.168.1.106

Answer: D

176.A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.

Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy

B. Acceptable-use policy

C. Remote-access policy

D. Permissive policy

Answer: C

177.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

Answer: B

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

A. Turnstile

B. Bollards

C. Mantrap

D. Receptionist

Answer: B

179.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
Answer: A

180.Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?
A. Nessus
B. Metasploit
C. Maltego
D. Wireshark
Answer: B

181.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
Answer: A

182.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. Masquerading
B. Tailgating
C. Phishing
D. Whaling
Answer: B

183.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.
Answer: B

184.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. Both pharming and phishing attacks are identical.
B. 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.
C. 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 phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
Answer: B

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

186.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
Answer: A

187.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
Answer: B

188.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
Answer: C

189.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.

Answer: C

190.How can rainbow tables be defeated?

A. Password salting

B. Use of non-dictionary words

C. All uppercase character passwords

D. Lockout accounts under brute force password cracking attempts

Answer: A

191.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. He needs to change the address to 192.168.1.0 with the same mask

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. The network must be down and the nmap command and IP address are ok

Answer: C

192.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.

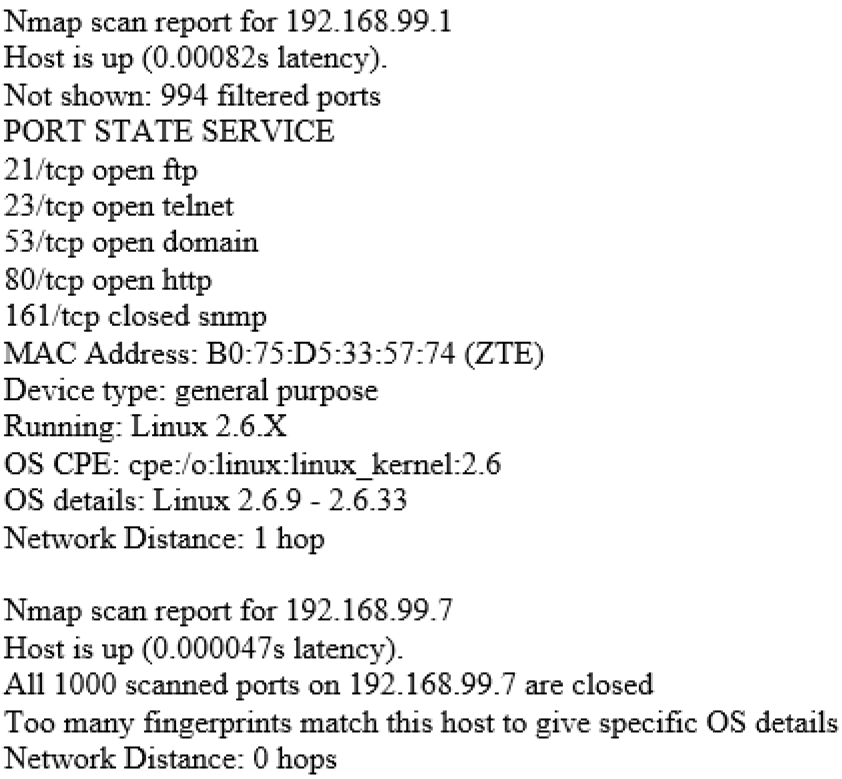
D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

Answer: B

193.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.

Answer: B

194.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.

Answer: A

195.Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfencode

B. msfpayload

C. msfcli

D. msfd

Answer: A

196.Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. OpenVAS

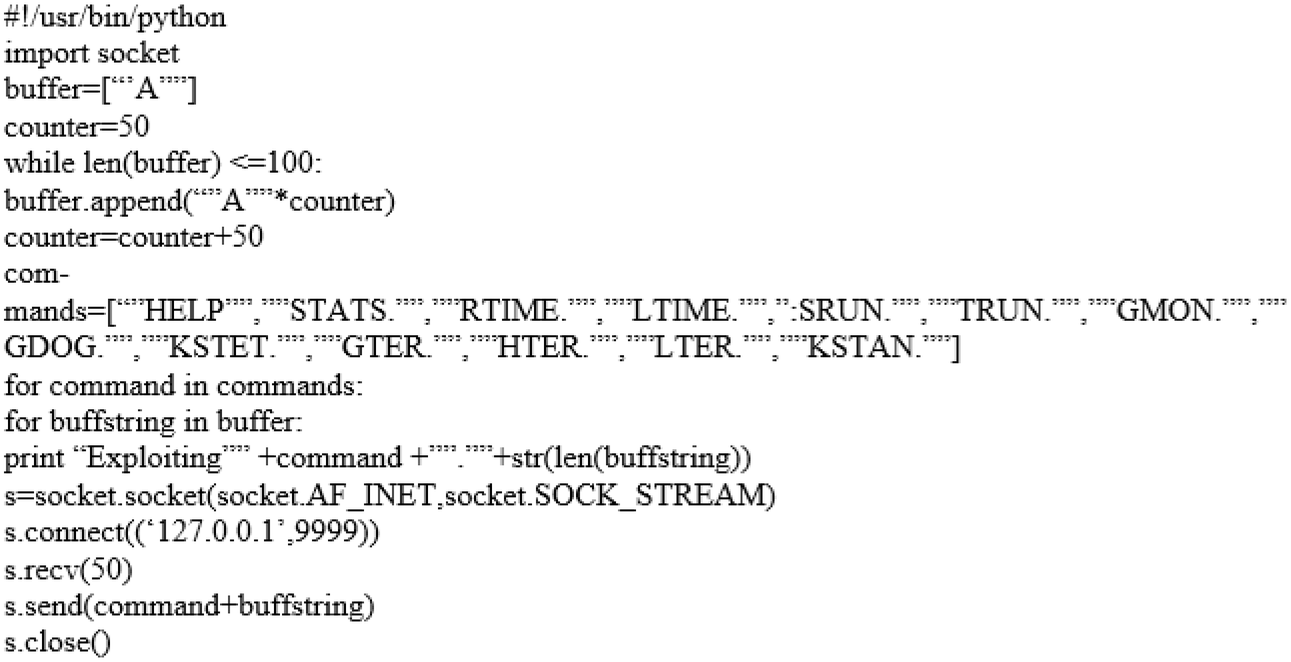
B. Burp Suite
C. tshark
D. Kismet
Answer: D

197.Which service in a PKI will vouch for the identity of an individual or company?
A. CBC
B. KDC
C. CA
D. CR
Answer: C

198.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
Answer: B

199.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, Blackbox
B. External, Blackbox
C. External, Whitebox
D. Internal, Whitebox
Answer: A

200.What is the code written for?



```
#!/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()
```

A. Buffer Overflow

B. Encryption

C. Denial-of-service (DoS)

D. Bruteforce

Answer: A

201.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. Do not report it and continue the penetration test.

B. Transfer money from the administrator’s account to another account.

C. Do not transfer the money but steal the bitcoins.

D. Report immediately to the administrator.

Answer: D

202.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. Make sure that legitimate network routers are configured to run routing protocols with authentication.

B. Disable all routing protocols and only use static routes

C. Only using OSPFv3 will mitigate this risk.

D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Answer: A

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

A. IANA
B. CAPTCHA
C. IETF
D. WHOIS
Answer: D

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

205.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.
Answer: B

206.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. FISMA
B. ISO/IEC 27002
C. HIPAA
D. COBIT
Answer: C

207.Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip 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. Worm
B. Macro Virus
C. Key-Logger
D. Trojan
Answer: D

208.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. Session management vulnerability
C. SQL injection vulnerability
D. Cross-site Request Forgery vulnerability
Answer: A

209.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?
A. MAC Flooding
B. Smurf Attack
C. DNS spoofing
D. ARP Polsoning
Answer: C

210.Which results will be returned with the following Google search query? site:target.com site:Marketing.target.com accounting
A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
B. Results matching all words in the query.
C. Results for matches on target.com and Marketing,target.com that include the word “accounting”
D. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
Answer: C

211.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. Malicious code is attempting to execute instruction a non-executable memory region.
B. A page fault is occuring, which forces the operating system to write data from the hard drive.
C. A race condition is being exploited, and the operating system is containing the malicious process.

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

Answer: A

212.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. Service Level Agreement

B. Project Scope

C. Rules of Engagement

D. Non-Disclosure Agreement

Answer: C

213.When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator’s Computer to update the router configuration.

What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Answer: D

214.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. Public

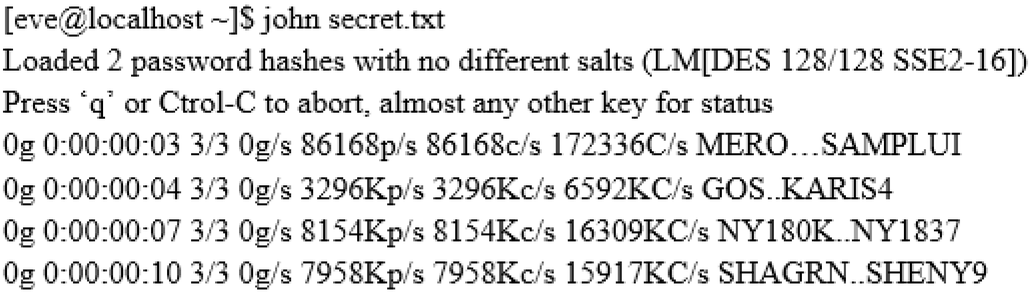
B. Private

C. Shared

D. Root

Answer: B

215.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 Ctrol-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?

A. She is using ftp to transfer the file to another hacker named John.

B. She is using John the Ripper to crack the passwords in the secret.txt file
C. She is encrypting the file.
D. She is using John the Ripper to view the contents of the file.
Answer: B

216.What is the correct process for the TCP three-way handshake connection establishment and connection termination?
A. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK
B. Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
C. Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
D. Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN
Answer: A

217.env x='(){ :;};echo exploit' bash –c 'cat/etc/passwd'
What is the Shellshock bash vulnerability attempting to do a vulnerable Linux host?
A. Removes the passwd file
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Display passwd content to prompt
Answer: D

218.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. Encryption
B. Steganography
C. RSA algorithm
D. Public-key cryptography
Answer: B

219.A well-intentioned researcher discovers a vulnerability on the web site of a major corporation.
What should he do?
A. Try to sell the information to a well-paying party on the dark web.
B. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.
C. Ignore it.
D. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
Answer: D

220.Trinity needs to scan all hosts on a /16 network for TCP port 445 only.
What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.
A. nmap –p 445 –n –T4 –open 10.1.0.0/16
B. nmap –p 445 –max –Pn 10.1.0.0/16

C. nmap –sn –sF 10.1.0.0/16 445

D. nmap –s 445 –sU –T5 10.1.0.0/16

Answer: A

221.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. WLAN

C. InfraRed

D. Radio-Frequency identification

Answer: A

222.Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Read the first 512 bytes of the tape

B. Perform a full restore

C. Read the last 512 bytes of the tape

D. Restore a random file

Answer: B

223.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 the user and password information stored in the company’s SQL database.

B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user’s authentication credentials.

C. Attempts by attackers to access password 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.

Answer: B

224.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. Protocol analyzer

B. Intrusion Detection System

C. Port scanner

D. Vulnerability scanner

Answer: D

225.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. Piggybacking
C. Tailgating
D. Eavesdropping
Answer: A

226.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. Escalation
C. Scanning
D. Enumeration
Answer: A

227.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. Accept
B. Delegate
C. Mitigate
D. Avoid
Answer: B

228.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?
A. openssl s_client –site www.website.com:443
B. openssl_client –site www.website.com:443
C. openssl_client –connect www.website.com:443
D. openssl s_client –connect www.website.com:443
Answer: D

229.Which of the following describes the characteristics of a Boot Sector Virus?
A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

D. Overwrites the original MBR and only executes the new virus code.

Answer: C

230.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?

A. Increase his technical skills

B. Read the incident manual every time it occurs

C. Select someone else to check the procedures

D. Create an incident checklist

Answer: D

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

A. Voice

B. Fingerprints

C. Iris patterns

D. Height and Weight

Answer: D

232.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?

A. Cookie Tampering

B. SQL Injection

C. Web Parameter Tampering

D. XSS Reflection

Answer: C

233.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. Attack

B. Vulnerability

C. Threat

D. Risk

Answer: C

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

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

235.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?
A. Armitage
B. Nikto
C. Metasploit
D. Nmap
Answer: B

236.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?
A. He needs to gain physical access.
B. He must perform privilege escalation.
C. He already has admin privileges, as shown by the “501” at the end of the SID.
D. He needs to disable antivirus protection.
Answer: B

237.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?
A. NoSQL injection
B. Blind SQL injection
C. Union-based SQL injection
D. Error-based SQL injection
Answer: B

238.You have successfully logged on a Linux system. You want to now cover your track. Your login attempt may be logged on several files located in /var/log.
Which file does NOT belong to the list:
A. wtmp
B. user.log
C. btmp
D. auth.log
Answer: B

239.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.
Answer: A

240.The "Gray-box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. Only the external operation of a system is accessible to the tester.
Answer: C

241.Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours.
What protocol used on Linux serves to synchronize the time has stopped working?
A. NTP
B. TimeKeeper
C. OSPF
D. PPP
Answer: A

242.The "black box testing" methodology enforces what kind of restriction?
A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. Only the external operation of a system is accessible to the tester.
Answer: D

243.>NMAP –sn 192.168.11.200-215 The NMAP command above performs which of the following?
A. A port scan
B. A ping scan
C. An operating system detect
D. A trace sweep
Answer: B

244.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.

A. Strict, Abstract
B. Simple, Complex
C. Relational, Hierarchical
D. Hierarchical, Relational
Answer: D

245.What is the purpose of DNS AAAA record?
A. Address prefix record
B. Address database record
C. Authorization, Authentication and Auditing record
D. IPv6 address resolution record
Answer: D

246.Which of the following statements is FALSE with respect to Intrusion Detection Systems?
A. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
B. Intrusion Detection Systems can examine the contents of the data in context of the network protocol
C. Intrusion Detection Systems can be configured to distinguish specific content in network packets
D. Intrusion Detection Systems require constant update of the signature library
Answer: A

247.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?
A. list domain=abccorp.local type=zone
B. Is –d accorp.local
C. list server=192.168.10.2 type=all
D. Iserver 192.168.10.2 –t all
Answer: B

248.Which command can be used to show the current TCP/IP connections?
A. Netsh
B. Net use connection
C. Netstat
D. Net use
Answer: C

249.You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?
A. Armitage
B. Dmitry

C. Metagoofil
D. cdpsnarf
Answer: C

250.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. Relational Database
B. MS Excel
C. Notepad
D. Grep
Answer: D

251.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?
A. network mapping
B. footprinting
C. escalating privileges
D. gaining access
Answer: B

252.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. domain: target.com archieve:xls username password email
C. inurl: target.com filename:xls username password email
D. site: target.com file:xls username password email
Answer: A

253.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. 161
B. 3389
C. 445
D. 1433
Answer: C

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

A. Authentication
B. Confidentially
C. Availability
D. Integrity
Answer: D

255.Risks=Threats x Vulnerabilities is referred to as the:
A. BIA equation
B. Disaster recovery formula
C. Risk equation
D. Threat assessment
Answer: C

256.The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?
A. Network Sniffer
B. Vulnerability Scanner
C. Intrusion Prevention Server
D. Security Incident and Event Monitoring
Answer: D

257.You have 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. Establish attribution to suspected attackers
B. Interview all employees in the company to rule out possible insider threats
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.
Answer: C

258.The purpose of a _______is to deny network access to local area networks and other information assets by unauthorized wireless devices.
A. Wireless Analyzer
B. Wireless Jammer
C. Wireless Access Point
D. Wireless Access Control List
Answer: D

259.What does the –oX flag do in an Nmap scan?
A. Perform an Xmas scan
B. Perform an eXpress scan
C. Output the results in truncated format to the screen

D. Output the results in XML format to a file

Answer: D

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

A. RST

B. SYN

C. ACK

D. No return response

Answer: A

261.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. Clickjacking

B. Cross-Site Scripting

C. Cross-Site Request Forgery

D. Web form input validation

Answer: C

262.Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company.

He is looking for an IDS with the following characteristics:

- Verifies success or failure of an attack
- Monitors system activities
- Detects attacks that a network-based IDS fails to detect.
- Near real-time detection and response
- Does not require additional hardware
- Lower entry cost.

Which type of IDS is best suited for Tremp's requirements?

A. Network-based IDS

B. Open source-based IDS

C. Host-based IDS

D. Gateway-based IDS

Answer: C

263.Which of the following parameters describe LM Hash:

I – The maximum password length is 14 characters

II – There are no distinctions between uppercase and lowercase

III – The password is split into two 7-byte halves

A. II

B. I

C. I, II, and III

D. I and II

Answer: C

264.Which of the following is not a Bluetooth attack?

A. Bluesnarfing

B. Bluedriving

C. Bluesmacking

D. Bluejacking

Answer: B

265.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. Cross Site Scripting

B. Injection

C. Path disclosure

D. Cross Site Request Forgery

Answer: B

266.A pen-tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscous mode?

A. Winprom

B. Libpcap

C. Winpsw

D. Winpcap

Answer: D

267.Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical java script.

What is the name of this technique to hide the code and extend analysis time?

A. Steganography

B. Code encoding

C. Obfuscation

D. Encryption

Answer: C

268.During the security audit of IT processes, an IS auditor found that there were no documented security procedures.

What should the IS auditor do?

A. Create a procedures document

B. Terminate the audit

C. Conduct compliance testing

D. Identify and evaluate existing practices
Answer: D

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

270.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?
A. Conduct stealth scan
B. Conduct ICMP scan
C. Conduct IDLE scan
D. Conduct silent scan
Answer: C

271.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
Answer: A

272.During a black-box 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. Circuit
B. Stateful
C. Application
D. Packet Filtering
Answer: C

273.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?
A. $1320

B. $440
C. $100
D. $146
Answer: D

274.An IT employee got a call from one 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. The employee can not provide any information: but, anyway, he/she will provide the name of the person in charge
B. Since the company’s policy is all about Customer Service. he/she will provide information
C. The employee should not provide any information without previous management authorization
D. Disregarding the call, the employee should hang up
Answer: C

275.You are attempting to man-in-the-middle a session.
Which protocol will allow you to guess a sequence number?
A. ICMP
B. TCP
C. UPX
D. UPD
Answer: B

276.What is a “Collision attack” in cryptography?
A. Collision attacks try to get the public key
B. Collision attacks try to break the hash into three parts to get the plaintext value
C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
D. Collision attacks try to find two inputs producing the same hash
Answer: D

277.Which of the following is the successor of SSL?
A. GRE
B. IPSec
C. RSA
D. TLS
Answer: D

278.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?
A. Institute of Electrical and Electronics Engineers (IEEE)

B. International Security Industry Organization (ISIO)
C. Center for Disease Control (CDC)
D. Payment Card Industry (PCI)
Answer: D

279.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.
A. Stacheldraht
B. LOIC
C. R-U-Dead-Yet? (RUDY)
D. MyDoom
Answer: C

280.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 bi and TKIP
Answer: C

281.You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23.
Which of the following IP addresses could be leased as a result of the new configuration?
A. 10.1.4.254
B. 10.1.255.200
C. 10.1.5.200
D. 10.1.4.156
Answer: C

282.Your company was hired by a small healthcare provider to perform a technician assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?
A. Create a disk image of a clean Windows installation
B. Use the built-in Windows Update tool
C. Use a scan tool like Nessus
D. Check MITRE.org for the latest list of CVE findings
Answer: C

283.You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs. – 192.168.8.0/24.
What command you would use?
A. tshark –net 192.255.255.255 mask 192.168.8.0
B. wireshark –capture –local –masked 192.168.8.0 –range 24

C. sudo tshark –f “net 192.168.8.0/24”

D. wireshark –fetch “192.168.8/*”

Answer: B

284.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?

A. Heartbeat Attack

B. Spear Phishing Attack

C. Shellshock Attack

D. Watering Hole Attack

Answer: D

285.What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it’s made on the provider’s environment.

A. Behavioral based

B. Heuristics based

C. Honypot based

D. Cloud based

Answer: D

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

A. In a climate controlled facility offsite

B. In a cool dry environment

C. On a different floor in the same building

D. Inside the data center for faster retrieval in a fireproof safe

Answer: A

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

A. Defense in depth

B. Covert channels

C. Exponential backoff algorithm

D. Three-way handshake

Answer: A

288.Which utility will tell you in real time which ports are listening or in another state?

A. Netsat

B. Loki

C. Nmap

D. TCPView

Answer: D

289.Which of the following statements regarding ethical hacking is incorrect?

A. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services

B. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems

C. Ethical hacking should not involve writing to or modifying the target systems.

D. Testing should be remotely performed offsite.

Answer: B

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

A. 10011101

B. 10001011

C. 10111100

D. 11011000

Answer: B

291.Why containers are less secure that virtual machine?

A. Host OS on containers has a larger surface attack.

B. Containers are attached to the same virtual network.

C. Containers may fulfill disk space of the host.

D. A compromise container may cause a CPU starvation of the host.

Answer: D

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

A. Administrative safeguards

B. Physical security

C. Logical interface

D. DMZ

Answer: A

293.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. SOA

C. biometrics

D. single sign on

Answer: A

294.You are monitoring the network of your organizations. You notice that:

There are huge outbound connections from your Internal Network to External IPs

On further investigation, you see that the external IPs are blacklisted
Some connections are accepted, and some are dropped
You find that it is a CnC communication
Which of the following solution will you suggest?
A. Block the Blacklist IP’s @ Firewall
B. Update the Latest Signatures on your IDS/IPS
C. Clean the Malware which are trying to Communicate with the External Blacklist IP’s
D. Block the Blacklist IP’s @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP’s.
Answer: D

295.Peter is surfing the internet looking for information about DX Company.
Which hacking process is Peter doing?
A. Scanning
B. Footprinting
C. Enumeration
D. System Hacking
Answer: B

296.Jim’s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim’s company keeps the backup tapes in a safe in the office. Jim’s company is audited each year, and the results from this year’s audit show a risk because backup tapes are not stored off-site.
The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
A. Encrypt the backup tapes and transport them in a lock box.
B. Degauss the backup tapes and transport them in a lock box.
C. Hash the backup tapes and transport them in a lock box.
D. Encrypt the backup tapes and use a courier to transport them.
Answer: A

297.A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department.
Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?
A. tcp port = = 21
B. tcp. port = 23
C. tcp.port = = 21 | | tcp.port = =22
D. tcp.port ! = 21
Answer: A

298.What is the known plaintext attack used against DES which gives the result that encrypting plaintext

with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?
A. Man-in-the-middle attack
B. Meet-in-the-middle attack
C. Replay attack
D. Traffic analysis attack
Answer: B

299.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 generates alerts, which enable Sam to hide the real traffic.
What type of method is Sam using to evade IDS?
A. Denial-of-Service
B. Obfuscating
C. Insertion Attack
D. False Positive Generation
Answer: D

300.Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Dsniff
B. John the Ripper
C. Snort
D. Nikto
Answer: D

301.Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized 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. tcpsplice
B. Burp
C. Hydra
D. Whisker
Answer: D

302.DHCP snooping is a great solution to prevent rogue DHCP servers on your network.
Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?
A. Spanning tree
B. Dynamic ARP Inspection (DAI)
C. Port security
D. Layer 2 Attack Prevention Protocol (LAPP)
Answer: B

303.Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted.
What is the name of the command used by SMTP to transmit email over TLS?
A. OPPORTUNISTICTLS
B. UPGRADETLS
C. FORCELTS
D. STARTTLS
Answer: D

304.Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers.
The time a hacker spends performing research to locate this information about a company is known as?
A. Exploration
B. Investigation
C. Reconnaissance
D. Enumeration
Answer: C

305.Your business has decided to add credit card numbers to the data it backs up to tape.
Which of the following represents the best practice your business should observe?
A. Do not back up either the credit card numbers or their hashes.
B. Encrypt backup tapes that are sent off-site.
C. Back up the hashes of the credit card numbers not the actual credit card numbers.
D. Hire a security consultant to provide direction.
Answer: D

306.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, 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
Answer: A

307.Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%.

Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk

B. Introduce more controls to bring risk to 0%

C. Mitigate the risk

D. Avoid the risk

Answer: A

308.Which of the following Linux commands will resolve a domain name into IP address?

A. >host-t a hackeddomain.com

B. >host-t ns hackeddomain.com

C. >host -t soa hackeddomain.com

D. >host -t AXFR hackeddomain.com

Answer: A

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

A. Nessus

B. Jack the ripper

C. Tcpdump

D. Ethereal

Answer: C

310.User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email.

At what layer of the OSI layer does the encryption and decryption of the message take place?

A. Application

B. Transport

C. Session

D. Presentation

Answer: D

311.Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Assigns values to risk probabilities; Impact values

B. Determines risk probability that vulnerability will be exploited (High, Medium, Low)

C. Identifies sources of harm to an IT system (Natural, Human, Environmental)

D. Determines if any flaws exist in systems, policies, or procedures

Answer: D

312.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. Network sniffer
C. Intrusion Prevention System (IPS)
D. Vulnerability scanner
Answer: A

313.CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test.
Your email message looks like this:
From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com
Subject: Test message
Date: 4/3/2017 14:37
The employee of CompanyXYZ receives your email message.
This proves that CompanyXYZ's email gateway doesn't prevent what?
A. Email Masquerading
B. Email Harvesting
C. Email Phishing
D. Email Spoofing
Answer: D

314.Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?
A. IPsec
B. SFTP
C. FTPS
D. SSL
Answer: A

315.What is one of the advantages of using both symmetric and asymmetric cryptogrsphy in SSL/TLS?
A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
C. Symmetric encryption allows the server to security transmit the session keys out-of-band.
D. Asymmetric cryptography is computationally expensive in comparison.
However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
Answer: D

316.In the field of cryptanalysis, what is meant by a "rubber-hose" attack?
A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
B. A backdoor placed into a cryptographic algorithm by its creator.
C. Extraction of cryptographic secrets through coercion or torture.
D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Answer: C

317.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 perfrom 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.srcport= = 514 && ip.src= = 192.168.0.99

B. tcp.srcport= = 514 && ip.src= = 192.168.150

C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Answer: D

318.Which of the following tools can be used for passive OS fingerprinting?

A. tcpdump

B. nmap

C. ping

D. tracert

Answer: A

319.Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.

B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.

C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.

D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Answer: B

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

A. Kismet

B. Netstumbler

C. Nessus

D. Abel

Answer: A

321.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. Nessus

C. OpenVAS

D. tcptraceroute

Answer: A

322.To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https.
Which of the following firewall rules meets this requirement?
A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
D. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit
Answer: A

323.What is the minimum number of network connections in a multihomed firewall?
A. 3
B. 2
C. 5
D. 4
Answer: B

324.Which of the following is an extremely common IDS evasion technique in the web world?
A. Unicode Characters
B. Subnetting
C. Port Knocking
D. Spyware
Answer: A