CEH Exam Prep

1. This kind of malware is installed by criminals on your computer so they can lock it from a remote location. This malware generates a popup window, webpage, or email warning from what looks like an official authority such as the FBI. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?
a. Riskware
b. Adware
c. Ransomware
d. Spyware

2. In Risk Management, how is the term "likelihood" related to the concept of "threat?"
a. Likelihood is a possible threat-source that may exploit a vulnerability.
b. Likelihood is the likely source of a threat that could exploit a vulnerability.
c. Likelihood is the probability that the threat-source will exploit a vulnerability.
d. Likelihood is the probability that a vulnerability is a threat source.

3. You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from the command line. Which command would you use?
a. c:\compmgmt.msc
b. c:\ncpa.cpl
c. c:\gpedit
d. c:\services.exe

4. An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web sites's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem/issue?
a. Insufficient exception handling
b. Insufficient security management
c. Insufficient input validation
d. Insufficient database hardening

5. To determine if a 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. This is commonly referred to as what type of testing?
a. Randomizing
b. Fuzzing
c. Mutating
d. Ballin, like a Big Baller

6. You have successfully gained access to your client's internal network and successfully compromised 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. 1433
b. 3389
c. 161
d. 445

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

< iframesrc=http://www.vulnweb.com/updateif.php style=“display:none” > </iframe>

The attacker uses this string to update the victim's profile to a text file and then submit the data to the attackers database.
What is this type of attack (that can use either HTTP GET or HTTP POST) called?
a. Browser Hacking
b. Cross-Site Scripting
c. Cross-Site Request Forgery
d. SQL Injection

8. You want to perform a technical assessment on your network. What is the best approach for discovering vulnerabilities on a Windows based computer?
a. Use the built-in Windows Update tools
b. Create a disk image of a clean installation
c. Use a scan tool like Nessus
d. Check mitre.org for the latest list of CVE findings.

9. Keatron calls you and tells you that his wireless router increases in temperature noticeably after 7 PM every night. What tool could you use to view network traffic being sent and received by Keatron's wireless router?
a. Netcat
b. Wireshark
c. Netstat
d. Nessus

10. 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 organizations interest and your liabilities as a tester?
a. Service Level Agreement
b. Project Scope
c. Non-Disclosure Agreement
d. Terms of engagement

11. Which of the following describes the characteristics of a Boot Sector Virus?
a. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
b. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
c. Overwrites the original MBR and only executes the new virus code.
d. It is related to the Arkanis sector from Star Wars.

12. Which of the following parameters describe LM hashes?
a. It's a simple algorithm so 10,000,000 hashes can be generated per second.
b. Maximum password length is 14 characters
c. There is no distinctions between upper and lower case.
d. All choices are correct

13. You are doing a pentest against an organization that has just recovered from a major cyber attack. The CISO and CIO want to completely and totally eliminate risk. What is one of the first things you should explain to these individuals?
a. Explain to them that they need to buy more services.
b. Start the wireshark application to sniff traffic
c. Explain that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
d. Tell him everything is going to A ok and collect that check!

14. What is the best way to defend against network sniffing?
a. Using encryption protocols to secure network communications.
b. Use Static IP's
c. Register all machines MAC address in a Centralized Database
d. Restrict physical access to server rooms host critical servers.

15. An organization has just experienced a breach. The investigator/incident handler attempts to correlate the information in all of the logs, the sequence of many of the logged events don't match up or line up properly. What is likely the cause?
a. The attacker altered or erased events from the logs.
b. Proper chain of custody was not observed while collecting the logs
c. The breach didn't really happened. The dreamed it.
d. The network devices are not all synchronized

16. You send a receptionist an email that has pdf attached. The pdf has a malicious link in it. When the receptionist opens the email, he clicks on the link and is infected with malware that gives you access to his network. What type of testing method did you use for this attack?
a. Tailgating
b. Eavesdropping
c. Piggybacking
d. Social engineering

17. Which of the following is a component of a risk assessment?
a. Administrative safeguards
b. Logical interfaces and controls
c. Physical security
d. DMZ

18. What is the best description of SQL Injection?
a. It is a MiTM attack
b. It is an attack used to modify the code in an application
c. It is an attack used to gain unauthorized access to a database
d. It is a Denial of Service Attack (DoS)

19. Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?
a. Iris
b. Voice
c. Fingerprints
d. Height and Weight

20. Heartbleed bug leaves which type of key exposed?
a. Shared
b. Public
c. Florida
d. Private

21. You have compromised a server. You want to communicate and pivot traffic from one place to the next over the network securely and evade detection by IDS, etc. What is the best approach?
a. Install and us telnet which is by default encrypted.
b. Use ADS
c. Install cryptcat and encrypt all outgoing packets from this server.
d. Use Http

22. What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?
a. Inherent Risk
b. Residual Risk
c. Impact Risk
d. Deferred Risk

23. A penetration tester just scanned a device and found that ports 21, 23, 80, 139, 515, 631, and 9100 open. What is likely to be installed based on these ports being open?
a. The host is likely a Windows machine
b. The host is likely a printer.
c. The host is likely a router
d. The host is likely a Linux machine

24. Your IDS admin gets an alert for the IDS. The associated packets are saved as a pcap file. What type of network tool can be used to determine if these packets are generally malicious or simply a false positive?
a. Intrusion Prevention System
b. Network Sniffer
c. Vulnerability Scanner
d. Protocol Analyzer

25. A hacker has successfully infected an internet facing server which he will then use to send junk mail, take part in the coordinated attacks, or host junk email content. Which sort of trojan infects this server?
a. Ransomware Trojans
b. Botnet Trojan
c. Banking Trojans
d. Turtle Trojans

26. While doing some online banking Keatron receives an email that contains a link to an interesting web site. When he clicks on the link another browser session opens and shows a video of dogs playing a bass guitar. The next day Keatron's bank contacts him indicating that his bank account has been accessed from a foreign country. What browser based security vulnerability was exploited?
a. Cross Site Scripting
b. Web Form input validation
c. Cross Site Request forgery
d. Clickjacking

27. Which of the following is most secure for storing backup tapes?
a. Inside the data center for faster retrieval in a fireproof safe.
b. On a different floor in the same building
c. In a climate controlled facility offsite
d. In a cool dry environment

28. The white box testing methodology enforces what kind of restriction?
a. Only the external operation of a system is accessible to the tester.
b. The internal operation of a system is completely known to the tester.
c. Only the internal operation of a system is known to the tester
d. The internal operation of a system is only partly accessible to the tester.

29. Which of the following is a protocol specifically designed for transporting event messages?
a. SYSLOG
b. SMS
c. ICMP
d. SNMP

30. Which of the following is a low tech way of gaining unauthorized access to systems?
a. Sniffing
b. Scanning
c. Social engineering
d. Eavesdropping

31. Which of the following is most effective ways to prevent Cross Site Scripting flaws in software applications?
a. Verify access right before allowing access to protected information and UI controls.
b. Use security policies and procedures to define and implement proper security settings.
c. Use digital certificates to authenticate a server prior to sending data.
d. Validate and escape all information sent to a server

32. What does a firewall check to prevent particular ports and applications from getting packets into an organization?
a. Application layer port numbers and transport layer headers.
b. Transport layer port numbers and application layer headers
c. Presentation layer headers and session layer port numbers
d. Network layer headers and the session layer port numbers.

33. During a routine assessment you discover information that suggests the customer is involved in human trafficking.
a. Confront the client in a respectful manner and ask about the data
b. Ignore the data, complete the job, collect a check. Keep it moving!
c. Immediately stop work and contact the proper legal authorities
d. Copy the data to a thumb drive and keep it as leverage.

34. It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosures, denial of service or modification of data. Which term best matches this definition?
a. Risk
b. Threat
c. Attack
d. Vulnerability

35. While using your banks online services you notice the following string in the URL bar; http://www.mypersonalmoney.com/account?id=8949339&Damount=10980&Camount=21" You notice that if you modify the Damount and Camount values and submit the request, the data on the web page reflect the changes. Which type of vulnerability is present on this site?
a. Web Parameter Tampering
b. Cookie Tampering
c. XSS Reflection
d. SQL Injection

36. Nmap -sn 192.168.153.200-215.

The above nmap command performs which of the following?
a. A port scan
b. A trace sweep
c. A ping scan
d. An operating system detect scan

37. Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
a. Wireshark
b. Metasploit
c. Cain & Abel
d. Maltego

38. Which Google command will help you search files using Google as a search engine?
a. domain: target.com archive:xls username password email
b. site: target.com filetype:xls username password email
c. site: target.com file:xls username password email
d. inurl: target.com filename:xls username password email

39. You have several firewall and router logs that are in plain-text. You must review these to evaluate traffic. You know that in order to do this fast and efficiently, you must user regular expressions. Which command-line utility are you most likely to use?
a. Relational Database
b. Grep
c. MS Excel
d. Notepad

40. What is the most important phase in ethical hacking in which you need to spend a considerable amount of time?
a. Gaining access
b. Footprinting
c. Escalating privileges.
d. Network mapping

41. Which of the following is a command line packet analyzer similar to the GUI-based Wireshark
a. Jack the ripper
b. Nessus
c. ethereal
d. tcpdump

42. Which of the following is an extremely common IDS evasion technique in the web world?
a. Using Unicode characters
b. subnetting
c. port knocking
d. spyware

43. 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 one is a binary file named nc (netcat). The logs show the user logged in anonymously, uploaded the files, extracted the contents 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 had to have existed to make this remote attack possible?
a. Privilege Escalation
b. Directory Traversal
c. File system permissions
d. Brute Force Login

44. The Open Web Application Security Project is the worldwide non-profit organization focused on improving the security of software. What item is the primary concern on OWASP's Top 10 Project list of most critical web application security risks?
a. Path Disclosure
b. Cross Site Request Forgery
c. Injection
d. Cross Site Scripting

45. Which tool performs comprehensive tests against web servers, including dangerous files and CGI's?
a. Nikto
b. Snort
c. John the Ripper
d. Dsniff

46. Which of the following types of firewalls ensures that the packets are part of an established session?
a. Stateful Inspection firewall
b. Switch-level firewall
c. Application-level firewall
d. Circuit-level firewall

47. It is important to enumerate which HTTP methods (GET POST HEAD PUT DELETE TRACE) a web server has available. Which nmap script will help you discover the methods?
a. http enum
b. http-git
c. http-methods
d. http-headers

48. You are using nmap to resolve domain names to ip addresses for a ping sweep later. Which of the following commands (Linux command) looks for host IP addresses?
a. host -t AXFR hackedme.com
b. host -t soa hackedme.com
c. host -t a hackedme.com
d. host -t ns hackedme.com

49. An attacker has installed a RAT trojan on a host. The attacker now has control of the machine through the RAT (remote access trojan). The attacker wants to now ensure that if the user attempts to go to www.mybank.com that the user is directed to a phishing site. Which file does the attacker need to modify to make this happen?
a. Sudoers
b. Boot.ini
c. Hosts
d. Networks

50. This attack is based on attackers running exploits on well-known and likely visited trusted sites. They exploit the sites and plant malware on the site, knowing that eventually their targets will visit the site and become infected. What type of attack is this?
a. Spear Phishing
b. Watering Hole Attack
c. Heartbleed
d. Shellshock

51. In 2014 there was a vulnerability in GNU's bash shell. It gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch a denial of service attack, or disrupt websites. What is this vulnerability known as?
a. Rootshock
b. Rootshell
c. Shellbash
d. Shellshock

52. Which wireless hacking tool attacks WEP and WPA-PSK?
a. Airguard
b. WLAN-crack
c. wificracker
d. Aircrack-ng

53. Which regulation defines security and privacy controls for Federal information systems and organizations?
a. NIST-800-53
b. EU Safe Harbor
c. HIPAA
d. PCI-DSS

54. You need to monitor all traffic on your local network for suspicious activity and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?
a. Host based IDS
b. Network based IDS
c. Firewall
d. Proxy

55. This asymmetric cipher is based on factoring the product of two large prime numbers. What cipher is being described?
a. RSA
b. MD5
c. SHA
d. RC5

56. What is a collision attack in cryptography?
a. Collision attacks try to get the public key
b. Collision attacks try to find two inputs that produce the same hash
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 break the hash into three parts.

57. Which IPSEC mode should you use to assure security and confidentiality of data within the same LAN?
a. ESP transport mode
b. ESP confidential
c. AH permiscuous mode
d. AH Tunnel Mode

58. Which command will allow you to enumerate all machines on the network quickly?
a. nmap -T4 -O 10.10.1.0/24
b. nmap -T4 -r 10.10.1.0/24
c. nmap -T4 -q 10.10.1.0/24
d. nmap -T4 -F 10.10.1.0/24

59. An ISP needs to authenticate users connecting using analog modems, DSL, wireless data services, and Virtual Private Networks (VPN) over frame relay networks. Which AAA protocol is most likely able to handle this requirement?
a. RADIUS
b. TACACS+
c. Kerberos
d. DIAMETER

60. You are doing a penetration test and gathering information. You have found pdfs, docs, and images. You decide to extract metadata from these files and analyze it. What tool will help you with the task?
a. cdpsnarf
b. Dimitry
c. Metagoofil
d. Armitage

61. You have gained access to a Windows 2008 Server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux Live CD. Which Linux based tool has the ability to change any user's password or activate disabled Windows accounts?
a. John the Ripper
b. SET
c. CHNTPW
d. Cain & Abel

62. You have two machines. The first machine (192.168.153.99) has snort installed, and the second machine (192.168.153.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice the kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check and see if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to the kiwi syslog machine?
a. ipaddress=192.168.153.150 -- port=514
b. Summon "The Force" and make it happen with your mind.
c. tcp.srcport==514 && ip.src==192.168.153.99
d. tcp.dstport==514 && ip.dst==192.168.153.150

63. Which of the following tools can be used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
a. tcptrace
b. OpenVAS
c. Nessus
d. tcptraceroute

64. Which of the of the following security operations is used for determining the attack surface of an organization?
a. Training employees on the security policy regarding social engineering.
b. Using configuration management to determine when and where to apply security patches.
c. Running a network scan to detect network services in the corporate DMZ.
d. Reviewing the need for a security clearance for each employee.

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

What is the Shellshock bash vulnerability attempting to do on this vulnerable Linux host?
a. Removes the passwd file.
b. Add new user to the passwd file
c. Display passwd contents to prompt
d. Changes all password in passwd

66. During a security audit of IT processes the auditor finds that there were no documented security procedures. What should the IS auditor do?

Choose all of the correct answers (multiple possibilities).
a. Terminate the audit.
b. Identify and evaluate existing practices.
c. Conduct compliance testing
d. Create a procedures document

67. You try to run the command nmap -T4 -O 10.10.10.0/24 from your command shell in Linux. You are not root (your prompt is a $ instead of #). You get an error message that says "Quitting". What is mostly like the cause?
a. This is common behavior for a corrupted application.
b. The nmap syntax is wrong.
c. An OS scan requires root privileges.
d. Blocked.

68. What is the most common method to exploit the shellshock vulnerability?
a. SSH
b. String manipulation
c. Syn flood
d. CGI

69. During a blackbox pentest 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. Stateful
b. Circuit
c. Packet Filtering
d. Application

70. Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?
a. zero-sum
b. zero-hour
c. zero-day
d. no-day

71. TJ Max breach happened in part because this type of weak wireless security was implemented.
a. WPA2
b. TKIP
c. Wired Equivalent Privacy (WEP)
d. WiFi protected access (WPA)

72. What is the process of logging, recording and resolving events that take place in an organization?
a. Internal Procedure
b. Security Policy
c. Incident Management Process
d. Metrics

73. PGP, SSL, IKE are all examples of which type of cryptography?
a. Hash Algorithm
b. Secret Key
c. Private Key
d. Public Key

74. This configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?
a. Promiscuous Mode
b. WEM
c. Port forwarding
d. Multicast

75. How does the Address Resolution Protocol (ARP) work? a. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
b. It sends a request packet to all the network elements, asking for the domain name from a specific IP.
c. It sends a reply packet for a specific IP, asking for the MAC address.
d. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

76. Which of the following is the greatest threat passed by backup?
a. A backup is unavailable during disaster recovery
b. A backup is the source of Malware or illicit information
c. A backup is incomplete because no verification was performed
d. An un-encrypted backup can be misplaced or stolen

77. The "black box testing" methodology enforces which 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. Only the external operation of a system is accessible to the tester.
d. The internal operation of a system is only partly accessible to the tester.

78. 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. Maskgen
b. Burpsuite
c. Proxychains
d. Dimitry

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

80. The security concept of "separation of duties" is most similar to the operation of which type of security device?
a. Firewall
b. Bastion host
c. Honeypot
d. Intrusion Detection System

81. The "gray box testing" methodology enforces what kind of restriction?
a. The internal operation of a system is completely known to the tester.
b. Only the internal operation of a system is known to the tester.
c. Only the external operation of a system is accessible to the tester.
d. The internal operation of a system is only partly accessible to the tester.

82. Which of the following is assured by the use of a hash?
a. Authentication
b. Confidentially
c. Availability
d. Integrity

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

Which of the following regulations best matches the description?
a. HIPAA
b. ISO/IEC 27002
c. FISMA
d. COBIT

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

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

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

a. An Intrusion Detection System
b. A Router IPTable
c. A firewall IPTable
d. FTP Server rule

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

Which of the following organizations is being described?
a. Institute of Electrical and Electronics Engineers (IEEE)
b. Center for Disease Control (CDC)
c. International Security Industry Organization (ISIO)
d. Payment Card Industry (PCI)

87. Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
a. Netstumbler
b. Kismet
c. Nessus
d. Abel

88. A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?
a. Client is configured for the wrong channel
b. The wireless client is not configured to use DHCP
c. The client cannot see the SSID of the wireless network
d. The WAP does not recognize the client's MAC address

89. After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?
a. Download and Install Netcat
b. Disable Key Services
c. Disable IPTables
d. Create User Account

90. Jimmy is standing outside a secure entrance to a facility. He is pretending to be having a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close. What just happened?
a. Phishing
b. Masquerading
c. Piggybacking
d. Whaling

91. 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. Intrusion Prevention System (IPS)
b. Protocol analyzer
c. Vulnerability scanner
d. Network sniffer

92. The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate 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. $100
b. $146
c. $1320
d. $440

93. What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?
a. SYN Flood
b. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
c. SSH
d. Manipulate format strings in text fields

94. Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?
a. Agile Process
b. Lean Coding
c. Object Oriented Architecture
d. Service Oriented Architecture

95. Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, The technique provides 'security through obscurity'. What technique is Ricardo using?
a. Steganography
b. Public-key cryptography
c. Encryption
d. RSA algorithm

96. Which of the following is the successor of SSL?
a. TLS
b. GRE
c. RSA
d. IPSec

97. 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. Port scanner
b. Intrusion Detection System
c. Protocol analyzer
d. Vulnerability scanner

98. The purpose of a _______ is to deny network access to local area networks and other information assets by unauthorized wireless devices.
a. Wireless Access Point
b. Wireless Analyzer
c. Wireless Access Control List
d. Wireless Intrusion Prevention System

99. Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?
a. Use encrypted communications protocols to transmit PII
b. Use full disk encryption on all hard drives to protect PII
c. Use a security token to log into all Web applications that use PII
d. Use cryptographic storage to store all PII

100. Sid is a judge for a programing contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is the middle step called?
a. String validating the code
b. Sandboxing the code
c. Third party running the code
d. Fuzzy-testing the code

101. In order to have an anonymous Internet surf, which of the following is best choice?
a. Use Tor network with multi-node
b. Use shared WiFi
c. Use SSL sites when entering personal information
d. Use public VPN

102. 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 corporate network. What tool should the analyst use to perform a Blackjacking attack?
a. BBCrack
b. Blooover
c. BBProxy
d. Paros Proxy

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

```
$nmap -sV host.domain.com -p 80
```

He gets the following output.

```
Starting Nmap 6.47 (http://nmap.org) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
```

What did the hacker accomplish?
a. The hacker should've used nmap -O host.domain.com
b. nmap can't retrieve the version number of any running remote service.
c. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server
d. The hacker successfully completed the banner grabbing.

104. What is the correct process for the TCP three-way handshake connection establishment and connection termination?
a. Connection Establishment: FIN, ACK-FIN, ACK
Connection Termination: SYN, SYN-ACK, ACK

b. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: ACK, ACK-SYN, SYN

c. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: FIN, ACK-FIN, ACK

d. Connection Establishment: ACK, ACK-SYN, SYN
Connection Termination: FIN, ACK-FIN, ACK

105. The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28

Why he cannot see the servers?
a. The network must be down and the nmap command and IP address are ok
b. He needs to change the address to 192.168.1.0 with the same mask
c. He needs to add the command ""ip address"" just before the IP address
d. 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

106. A hacker has managed to gain access to a Linux host and stolen the password file from /etc/password How can he use it?
a. The password file does not contain the passwords themselves.
b. The file reveals the passwords to the root user only.
c. He cannot read it because it is encrypted
d. He can open it and read the user ids and corresponding passwords.

107. 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. Exclamation mark
b. Single quote
c. Semicolon
d. Double quote

108. Scenario:

Victim opens the attacker's web site.
Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?"
Victim clicks to the interesting and attractive content url.
Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?
a. ClickJacking Attack
b. HTTP Parameter Pollution
c. HTML Injection
d. Session Fixation

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

SECURE (plain text)
+1 (+1 next letter. for example, the letter ""T"" is used for ""S"" to encrypt.)
TFDVSF (encrypted text)
+ = logic => Algorithm
1= Factor => Key
Which of the following choices are true about cryptography?
a. 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.
b. Algorithm is not the secret, key is the secret.
c. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
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

110. You want to analyze packets on your wireless network. Which program would you use?
a. Airsnort with Airpcap
b. Ethereal with Winpcap
c. Wireshark with Airpcap
d. Wireshark with Winpcap

111. 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 a SYN
c. The port will send an ACK
d. The port will send an RST

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

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

113. How can rainbow tables be defeated?
a. Passwords salting
b. All uppercase character passwords
c. Lockout accounts under brute force password cracking attempts
d. Use of non-dictionary words

114. 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. Acceptable-use policy
b. Remote- access policy
c. Firewall-management policy
d. Permissive policy

115. You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?
a. Physically go to each server
b. Scan servers with Nmap
c. Scan servers with MBSA
d. Telnet to every port on each server

116. Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?
a. OS X
b. Unix
c. Linux
d. Windows

117. Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?
a. Information protection policy
b. Remote access policy
c. Network security policy
d. Access control policy

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

119. Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
a. msfencode
b. msfcli
c. msfd
d. msfpayload

120. A newly discovered flaw in a software application would be considered which kind of security vulnerability?
a. Time-to-check to time-to-use flaw
b. HTTP header injection vulnerability
c. 0-day vulnerability
d. Input validation flaw

121. Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA/local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?
a. Macro Virus
b. Worm
c. Trojan
d. Key-Logger

122. 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. Dictionary attack
b. Session hijacking
c. Brute-force attack
d. Man-in-the-middle attack

123. In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?
a. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
b. Vulnerabilities in the application layer are greatly different from IPv4
c. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addressed
d. Implementing IPv4 security in a dual-stack network offers protection form IPv6 attacks too.

124. 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. Redirection of the traffic cannot happen unless the admin allow it explicitly
d. Only using OSPFv3 will mitigate this risk.

125. 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. Gaining Access
b. Maintaining Access
c. Reconnaissance
d. Scanning and Enumeration

126. 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 transfer the money but steal the bitcoins.
b. Transfer money from the administrator's account to another account
c. Do not report it and continue the penetration test
d. Report immediately to the administrator

127. What is not a PCI compliance recommendation?
a. Limit access to card holder data to as few individuals as possible.
b. Use encryption to protect all transmission of card holder data over any public network.
c. Use a firewall between the public network and the payment card data
d. Rotate employees handling credit card transactions on a yearly basis to different departments.

128. 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 account was not modified once he approved it. What of 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 document can be sent to the accountant using an exclusive USB for that document
d. 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

129. Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting
a. Results matching all words in the query
b. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
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

130. Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?
a. Compound SQLi
b. Blind SQLi
c. DMS-specific SQLi
d. Classic SQLi

131. Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?
a. Nothing, but suggest to him to change the network's SSID and password
b. Log onto his network, after all it is his fault that you can get it.
c. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
d. Only use his network when you have large downloads so you don't tax your own network

132. 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. Port Scanning
c. Shoulder-Surfing
d. Hacking Active Directory

133. The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
access-list 102 deny tcp any any
```

a. The ACL 104 needs to be first because is UDP
b. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
c. The ACL 110 needs to be changed to port 80
d. The ACL for FTP must be before the ACL 110

134. 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 through a technique known as wardriving. Which Algorithm is this referring to?
a. Wi-Fi Protected Access (WPA)
b. Wired Equivalent Privacy (WEP)
c. Wi-Fi Protected Access 2 (WPA2)
d. Temporal Key Integrity Protocol (TKIP)

135. There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?
a. Polymorphism
b. Escrow
c. Collision
d. Collusion

136. .... 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 user 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. Collision Attack
c. Sinkhole Attack
d. Signal Jamming Attack

137. An attacker changes the profile picture 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. SQL Injection
b. Browser Hacking
c. Cross-Site Scripting
d. Cross-Site Request Forgery

138. Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?
a. Security
b. Scalability
c. Key distribution
d. Speed

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

140. What attack is used to crack passwords by using a precomputed table of hashed passwords?
a. Rainbow Table Attack
b. Brute Force Attack
c. Dictionary Attack
d. Hybrid Attack

141. Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?
a. Not informing the employees that they are going to be monitored could be an invasion of privacy.
b. All of the employees would stop normal work activities
c. The network could still experience traffic slow down.
d. IT department would be telling employees who the boss is

142. 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 though the packet-filtering of the firewall.
a. Session hijacking
b. Network sniffing
c. Firewalking
d. Man-in-the-middle attack

143. Which of the following programming languages is not susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?

Code:

```
#include
int main () {
char buffer[8];
strcpy(buffer,""1111111111111111111111111111111"");
}
```

Output:

```
Segmentation fault
```

a. Python
b. C++
c. Java
d. C#

144. Which of the following programs is usually targeted at Microsoft Office products?
a. Stealth virus
b. Multipart virus
c. Macro virus
d. Polymorphic virus

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

146. Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?
a. Internal, Whitebox
b. Internal, Blackbox
c. External, Whitebox
d. External,Blackbox

147. 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

148. 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 his 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. 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 external gateway
d. Both static routes indicate that the traffic is internal with different gateway

149. What is the role of test automation in security testing?
a. Test automation is not usable in security die to the complexity of the tests
b. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies
c. It is an option but it tends to be very expensive
d. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

150. 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 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. Banner grabbing
b. Whois database query
c. Cross-site scripting
d. SQL injection

151. A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
a. The gateway is not routing to a public IP address
b. The computer is using an invalid IP address
c. The gateway and the computer are not on the same network
d. The computer is not using a private IP address

152. 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. BIOS password
b. Password protected files
c. Hidden folders
d. Full disk encryption

153. Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?
a. A page fault is occurring, which forces the operating system to write data from the hard drive
b. A race condition is being exploited, and the operating system is containing the malicious process
c. Malicious code is attempting to execute instruction in a non-executable memory region
d. Malware is executing in either ROM or a cache memory area

154. 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. Root
b. Shared
c. Private
d. Public

155. Which of these is capable of searching for and locating rogue access points?
a. NIDS
b. HIDS
c. WISS
d. WIPS

156. Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?
a. Wireshark
b. Metasploit
c. Nessus
d. Maltego

157. 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. TCP ping
b. Hping
c. Traceroute
d. Broadcast ping

158. 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. smtp port
b. request smtp 25
c. tcp.contains port 25
d. tcp.port eq 25

159. You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
a. hping2 -i host.domain.com
b. hping2 -1 host.domain.com
c. hping2 --set-ICMP host.domain.com
d. hping2 host.domain.com

160. Which service in a PKI will vouch for the identity of an individual or company?
a. CR
b. KDC
c. CBC
d. CA

161. If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?
a. Spoof Scan
b. TCP Connect scan
c. TCP SYN
d. Idle Scan

162. What two conditions must a digital signature meet?
a. Must be unique and have special characters.
b. Has to be the same number of characters as a physical signature and must be unique.
c. Has to be unforgeable, and has to be authentic.
d. Has to be legit and neat.

163. Which of the following is a series 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. POODLE
c. Heartbleed Bug
d. Shellshock

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

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

Output:

```
Starting Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

a. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
b. nmap -sN -Ps -T4 192.168.1.1
c. nmap -sS -Pn 192.168.1.1
d. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

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

167. Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.
a. Authenticate
b. Encrypt
c. Protect the payload and the headers
d. Work at the Data Link Layer

168. 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 the technique; psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump,pwdump, or cachedump and then utilize rainbowtables to crack those hash values. Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'
a. NT:LM
b. NTLM:LM
c. LM:NTLM
d. LM:NT

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

170. 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 12 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:192.168.1.106Protocol:TCP Time:Mar 12 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 192.168.1.106
b. Teardrop attack targeting 192.168.1.106
c. Denial of service attack targeting 192.168.1.103
d. Port scan targeting 192.168.1.103

171. A security team is doing a network scan. While doing reconnaissance on a host, they found several ports opened that were confusing in concluding the Operating System (OS) version installed.
Based on the NMAP result below, which OS is likely to be installed on the target machine?

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

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. ARP is disabled on the target server
C. You need to run ping with root privelege
D. TCP/IP doesn't support ICMP

173.Which of the following Nmap commands will produce an X-mas tree scan?

A. nmap -sX 192.168.1.1
B. nmap -sN -Ps -T4 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

174.Which flags are used in an Nmap X-mas scan?

A. FIN
B. PUSH, URG, FIN
C. SYN, FIN
D. SYN, ACK

175. 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 enterprise?

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

Q176. XOR is a common cryptographic tool. 10110001 XOR 00111010 is?
A.10111100
B.11011000
C.10011101
D.10001011

Q177. First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?
A .Delete the email and pretend nothing happened.
B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.
C. Forward the message to your company's security response team and permanently delete the message from your computer.
D. Reply to the sender and ask them for more information about the message contents.

Q178. Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?
A.Social Engineering
B.Piggybacking
C.Tailgating
D.Eavesdropping

Q179. The following are types of Bluetooth attack EXCEPT_____?
A.Bluejacking
B.Bluesmaking
C.Bluesnarfing
D.Bluedriving

Q180. A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?
A. Insufficient security management
B. Insufficient database hardening
C. Insufficient input validation
D. Insufficient exception handling

Q181. Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?
A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

Q182. Perspective clients want to see sample reports from previous penetration tests.
What should you do next?
A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.

Q183. Which of the following is a tool that will copy details from a USB drive without user knowing it?
A. USBDumper
B. USBShuffle
C. USBCrash
D. dd

Answer Key

1	C	41	D	81	D	121	C	161	B
2	C	42	A	82	D	122	A	162	C
3	A	43	A	83	A	123	A	163	C
4	C	44	C	84	D	124	A	164	D
5	B	45	A	85	A	125	C	165	D
6	D	46	A	86	D	126	D	166	B
7	B	47	C	87	B	127	D	167	D
8	C	48	C	88	D	128	A	168	C
9	B	49	C	89	A	129	D	169	C
10	D	50	B	90	C	130	B	170	A
11	B	51	D	91	B	131	A	171	C
12	D	52	D	92	B	132	A	172	A
13	C	53	A	93	B	133	B	173	A
14	A	54	B	94	D	134	B	174	B
15	A	55	A	95	A	135	C	175	D
16	D	56	B	96	A	136	A	176	D
17	A	57	A	97	D	137	C	177	C
18	C	58	D	98	D	138	D	178	A
19	D	59	A	99	A	139	C	179	D
20	D	60	C	100	B	140	A	180	A
21	C	61	C	101	A	141	A	181	C
22	B	62	D	102	C	142	C	182	A
23	B	63	A	103	C	143	C	183	A
24	D	64	C	104	C	144	C		
25	B	65	C	105	D	145	B		
26	C	66	BC	106	A	146	B		
27	C	67	C	107	B	147	A		
28	B	68	D	108	A	148	C		
29	A	69	D	109	B	149	D		
30	C	70	C	110	D	150	A		
31	D	71	C	111	A	151	A		
32	B	72	C	112	B	152	D		
33	C	73	D	113	A	153	C		
34	B	74	A	114	B	154	C		
35	A	75	A	115	B	155	D		
36	C	76	D	116	D	156	B		
37	D	77	C	117	B	157	B		
38	B	78	B	118	B	158	D		
39	B	79	B	119	A	159	B		
40	B	80	B	120	C	160	D		