1. **Which of the following information security elements guarantees that the sender of a message cannot later deny having sent the message and the recipient cannot deny having received the message?**

   A Confidentiality
   B Non-repudiation
   C Availability
   D Integrity

   B

2. **A phase of the cyber kill chain methodology triggers the adversary's malicious code, which utilizes a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration.**

   Which is this phase of the cyber kill chain methodology?

   A Reconnaissance
   B Weaponization
   C Exploitation
   D Installation

   C

3. **Which of the following is a category of hackers who are also known as crackers, use their extraordinary computing skills for illegal or malicious purposes, and are often involved in criminal activities?**

   A Black hats
   B White hats
   C Suicide hackers
   D Script kiddies

   A

4. **John, a professional hacker, has launched an attack on a target organization to extract sensitive information. He was successful in launching the attack**

   C

	and gathering the required information. He is now attempting to hide the malicious acts by overwriting the server, system, and application logs to avoid suspicion. **Which of the following phases of hacking is John currently in?** **A Maintaining access** **B Scanning** **C Clearing tracks** **D Gaining access**	
5.	**Which of the following risk management phases involves selecting and implementing appropriate controls for the identified risks to modify them?** **A Risk tracking and review** **B Risk identification** **C Risk treatment** **D Risk assessment**	C
6.	**In which of the following incident handling and response phases are the identified security incidents analyzed, validated, categorized, and prioritized?** **A Incident recording and assignment** **B Incident triage** **C Containment** **D Eradication**	B
7.	**Which of the following phases of risk management is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans to help determine the quantitative and qualitative value of risk?** **A Risk identification** **B Risk treatment**	D

C Risk tracking and review
D Risk assessment

8. **Jack, a security professional, was instructed to introduce a security standard to handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards. In the process, Jack has employed a standard that offers robust and comprehensive standards as well as supporting materials to enhance payment-card data security.**

What is the security standard that Jack has employed?

A HIPAA
B SOX
C DMCA
D PCI DSS

D

9. **Morris, an attacker, has targeted an organization's network. To know the structure of the target network, he combined footprinting techniques with a network utility that helped him create diagrammatic representations of the target network.**

What is the network utility employed by Morris in the above scenario?

A Netcraft
B Tracert
C Shodan
D BuzzSumo

B

10. **Which of the following Google advanced search operators displays similar websites to the specified URL?**

A [site:]
B [info:]

D

C [inurl:]
D [related:]

11. **Which of the following techniques is used by an attacker to perform automated searches on the target website and collect specified information, such as employee names and email addresses?**

A Web spidering
B Website mirroring
C Monitoring of web updates
D Website link extraction

A

12. **Jude, an attacker, has targeted an organization's communication network. While conducting initial footprinting, he used a Google dork to find the VoIP login portals of the organization.**

What is the Google dork that helped Jude find the VoIP login portals?

A inurl:8080 intitle:"login" intext:"UserLogin" "English"
B inurl:/voice/advanced/ intitle:Linksys SPA configuration
C inurl:/remote/login?lang=en
D !Host=*.* intext:enc_UserPassword=* ext:pcf

A

13. **Stokes, an attacker, decided to find vulnerable IoT devices installed in the target organization. In this process, he used an online tool that helped him gather information such as a device's manufacturer details, its IP address, and the location where it is installed.**

What is the online tool that Stokes used in the above scenario?

A DuckDuckGo

C

B Baidu
C Shodan
D Bing

14. **CenSys Solutions hired Clark, a security professional, to enhance the Internet security of the organization. To achieve the goal, Clark employed a tool that provides various Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning.**

What is the tool used by Clark to perform the above activities?

A Blisqy
B OmniPeek
C Netcraft
D BTCrawler

C

15. **Clark is a professional hacker. He targeted an organization for financial benefit and used various footprinting techniques to gather information about the target network. In this process, he employed a protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system.**

What is the protocol employed by Clark in the above scenario?

A SMB
B Whois
C SNMP
D FTP

B

16. **Which of the following tools in OSRFramework is used by attackers to check for a user profile on up to 290 different platforms?**

A

A usufy.py
B phonefy.py
C entify.py
D searchfy.py

17. **What is the feature in FOCA that checks each domain to ascertain the host names configured in NS, MX, and SPF servers to discover the new host and domain names?**

A Common names
B DNS search
C Web search
D Bing IP

B

18. **Which of the following countermeasures should be followed to safeguard the privacy, data, and reputation of an organization and to prevent information disclosure?**

A Keeping the domain name profile public
B Enabling directory listings in the web servers
C Avoiding domain-level cross-linking for critical assets
D Turning on geolocation access on all mobile devices

C

19. **Which of the following TCP communication flags notifies the transmission of a new sequence number and represents the establishment of a connection between two hosts?**

A FIN flag
B SYN flag
C PSH flag
D RST flag

B

20. **Which of the following hping commands is used by an attacker to scan the entire subnet to detect live**

C

hosts in a target network?

A hping3 -8 50-60 -S 10.0.0.25 -V
B hping3 -F -P -U 10.0.0.25 -p 80
C hping3 -1 10.0.1.x --rand-dest -I eth0
D hping3 -9 HTTP -I eth0

21. **Which of the following commands is used by an attacker to perform an ICMP ECHO ping sweep that can determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts?**

A nmap -sn -PR 10.10.10.10
B nmap -sn -PU 10.10.10.10
C nmap -sn -PE 10.10.10.10
D nmap -sn -PE 10.10.10.5-15

D

22. **Which of the following scanning techniques is used by an attacker to send a TCP frame to a remote device with the FIN, URG, and PUSH flags set?**

A Xmas scan
B TCP Maimon scan
C ACK flag probe scan
D IDLE/IPID header scan

A

23. **A certain scanning technique has no three-way handshake, and the system does not respond when the port is open; when the port is closed, the system responds with an ICMP port unreachable message.**

Which of the following is this scanning technique?

A List scanning
B SCTP COOKIE ECHO scanning
C IPv6 scanning
D UDP scanning

D

24. **A certain type of port scanning technique is similar to the TCP SYN scan and can be performed quickly**

D

by scanning thousands of ports per second on a fast network that is not obstructed by a firewall, offering a strong sense of security.

Which of the following is this type of port scanning technique?

A IDLE/IPID header scanning
B SCTP COOKIE ECHO scanning
C SSDP scanning
D SCTP INIT scanning

25. **An attacker performed OS banner grabbing on a target host. They analyzed the packets received from the target system and identified that the values of time to live (TTL) and TCP window size as 255 and 4128, respectively.**

What is the operating system of the target host on which the attacker performed banner grabbing?

A Linux (Kernel 2.4 and 2.6)
B Google Linux
C Windows 98, Vista, and 7 (Server 2008)
D iOS 12.4 (Cisco Routers)

D

26. **Which of the following OS discovery techniques is used by an attacker to identify a target machine's OS by observing the TTL values in the acquired scan result?**

A OS discovery using Nmap
B OS discovery using Unicornscan
C OS discovery using Nmap Script Engine
D OS discovery using IPv6 fingerprinting

B

27. **Which of the following IDS/firewall evasion techniques is used by an attacker to bypass Internet censors and evade certain IDS and firewall rules?**

D

A IP address decoy
B Sending bad checksums
C Source port manipulation
D Anonymizers

28. **Through which of the following techniques can an attacker obtain a computer's IP address, alter the packet headers, and send request packets to a target machine while pretending to be a legitimate host?**

A IP address decoy
B Source port manipulation
C Packet fragmentation
D IP address spoofing

D

29. **Larry, a professional hacker, was hired to launch a few attacks on an organization. In the process, he identified that FTP server ports are open and performed enumeration on FTP to find the software version and state of existing vulnerabilities for performing further exploitations.**

What is the FTP port number that Larry has targeted?

A TCP 25
B TCP 20/21
C TCP/UDP 5060, 5061
D TCP 179

B

30. **Which of the following Net View commands is used by an attacker to view all the available shares in a domain?**

A net view \<computername> /ALL
B net view /domain:<domain name>
C net view /domain
D net view \<computername>

C

31.

B

Which of the following commands is used by the SNMP manager continuously to retrieve all the data stored in an array or table?

A GetResponse
B GetNextRequest
C GetRequest
D SetRequest

32. **George hired an attacker named Joan to perform a few attacks on a competitor organization and gather sensitive information. In this process, Joan performed enumeration activities on the target organization's systems to access the directory listings within Active Directory.**

What is the type of enumeration that Joan has performed in the above scenario?

A SNMP enumeration
B LDAP enumeration
C NTP enumeration
D NetBIOS enumeration

B

33. **Sam, an ethical hacker, is launching an attack on a target company. He performed various enumeration activities to detect any existing vulnerabilities on the target network and systems. In this process, he performed NTP enumeration and executed some commands to acquire the list of hosts connected to the NTP server.**

Which of the following NTP enumeration commands helps Sam in collecting system information such as the number of time samples from several time sources?

A ntptrace
B ntpdc

C

C ntpdate
D ntpq

34. **Jim, a professional hacker, was hired to perform an attack on an organization. In the attack process, Jim targeted the SMTP server of the target organization and performed SMTP enumeration using the smtp-user-enum tool. He used some options in the tool to gather the usernames of the target organization's employees.**

Which of the following options did Jim use in the SMTP command for guessing the username from among EXPN, VRFY, and RCPT TO?

A -m n
B -u user
C -M mode
D -p port

C

35. **Given below are the different phases of the vulnerability management lifecycle.**

1) Monitor
2) Vulnerability scan
3) Identify assets and create a baseline
4) Risk assessment
5) Verification
6) Remediation

What is the correct sequence of phases involved in the vulnerability management lifecycle?

A 1 ’ 2 ’ 3 ’ 4 ’ 5 ’ 6
B 2 ’ 1 ’ 5 ’ 3 ’ 6 ’ 4
C 3 ’ 2 ’ 4 ’ 6 ’ 5 ’ 1
D 3 ’ 1 ’ 4 ’ 5 ’ 6 ’ 2

C

36.

B

Jaden, a security professional in an organization, introduced new tools and services into the organization. Before introducing the tools, he had to evaluate whether the tools are effective and appropriate for the organization. He used a publicly available and free-to-use list of standardized identifiers for software vulnerabilities and exposures to evaluate the tools.

Which of the following databases did Jaden use to evaluate the tools and services?

A LACNIC
B CVE
C Whois
D ARIN

37. **Edward, a security professional in an organization, was instructed by higher officials to calculate the severity of the organization' s systems.In the process, he used CVSS, a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. He used three metrics provided by CVSS for measuring vulnerabilities.**

Which of the following CVSS metrics represents the features that continue to change during the lifetime of the vulnerability?

A Base metric
B Environmental metric
C Temporal metric
D Overall score

C

38. **Which of the following types of vulnerability assessment sniffs the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities?**

B

A Active assessment
B Passive assessment
C Credentialed assessment
D Distributed assessment

39. **Ben, an ethical hacker, was hired by an organization to check its security levels. In the process, Ben examined the network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers.**

Which of the following types of vulnerability assessment did Ben perform on the organization?

A Active assessment
B Passive assessment
C External assessment
D Internal assessment

C

40. **Clark, an ethical hacker, is performing vulnerability assessment on an organization's network. Instead of performing footprinting and network scanning, he used tools such as Nessus and Qualys for the assessment.**

Which of the following types of vulnerability assessment did Clark perform on the organization?

A Manual assessment
B Credentialed assessment
C Distributed assessment
D Automated assessment

D

41. **Ray, a security professional in an organization, was instructed to identify all potential security weaknesses in the organization and fix them before an attacker can exploit them. In the process, he consulted a**

B

third-party consulting firm to run a security audit of the organization's network.

Which of the following types of solutions did Ray implement in the above scenario?

A Product-based solution
B Service-based solution
C Tree-based assessment
D Inference-based assessment

---

42. **Karen, a security professional in an organization, performed a vulnerability assessment on the organization's network to check for vulnerabilities. In this process, she used a type of location data examination scanner that resides on a single machine but can scan several machines on the same network.**

Which of the following types of location and data examination tools did Karen use?

A Network-based scanner
B Agent-based scanner
C Proxy scanner
D Cluster scanner

B

---

43. **Rick, an ethical hacker, is performing a vulnerability assessment on an organization and a security audit on the organization's network. In this process, he used a tool for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks.**

Which of the following tools did Rick use to perform vulnerability assessment?

A Metagoofil
B Infoga

D

C Immunity Debugger
D Nessus

44. **Which of the following types of password attacks does not require any technical knowledge about hacking or system exploitation and includes techniques such as shoulder surfing, social engineering, and dumpster diving?**

A Active online attacks
B Passive online attacks
C Non-electronic attacks
D Offline attacks

C

45. **Given below are the different steps involved in exploiting vulnerabilities.**

1) Develop the exploit.
2) Determine the risk associated with the vulnerability.
3) Determine the capability of the vulnerability.
4) Identify the vulnerability.
5) Gain remote access.
6) Select the method for delivering: local or remote.
7) Generate and deliver the payload.

What is the correct sequence of steps involved in exploiting vulnerabilities?

A 1 ’ 2 ’ 3 ’ 4 ’ 5 ’ 6 ’ 7
B 3 ’ 6 ’ 7 ’ 4 ’ 2 ’ 1 ’ 5
C 2 ’ 3 ’ 6 ’ 4 ’ 5 ’ 1 ’ 7
D 4 ’ 2 ’ 3 ’ 1 ’ 6 ’ 7 ’ 5

D

46. **Which of the following is a shim that runs in the user mode and is used by attackers to bypass UAC and perform different attacks including the disabling of Windows Defender and backdoor installation?**

A

	A RedirectEXE **B Schtasks** **C launchd** **D WinRM**	
47.	**Joan, a professional hacker, was hired to retrieve sensitive information from a target organization. In this process, she used a post-exploitation tool to check common misconfigurations and find a way to escalate privileges.** **Which of the following tools helps Joan in escalating privileges?** **A ShellPhish** **B GFI LanGuard** **C Netcraft** **D BeRoot**	D
48.	**Which of the following steganography techniques is used by attackers for hiding the message with a large amount of useless data and mixing the original data with the unused data in any order?** **A Null ciphers** **B Grille ciphers** **C Jargon codes** **D Semagrams**	A
49.	**Which of the following commands is used by an attacker to delete only the history of the current shell and retain the command history of other shells?** **A cat /dev/null> ~.bash_history && history -c && exit** **B history -w** **C export HISTSIZE=0** **D history -c**	B
50.	**David, a content writer, was searching online for a specific topic. He visited a web page that appears le-**	C

gitimate and downloaded a file. As soon as he downloaded the file, his laptop started to behave in a weird manner. Out of suspicion, he scanned the laptop for viruses but found nothing.

Which of the following programs conceals the malicious code of malware via various techniques, making it difficult for security mechanisms to detect or remove it?

A Exploit
B Downloader
C Obfuscator
D Payload

51. **Given below are the different phases of the APT lifecycle.** B

1) Initial intrusion
2) Persistence
3) Preparation
4) Cleanup
5) Expansion
6) Search and exfiltration

What is the correct sequence of phases in the APT lifecycle?

A 1 ’ 2 ’ 3 ’ 4 ’ 5 ’ 6
B 3 ’ 1 ’ 5 ’ 2 ’ 6 ’ 4
C 5 ’ 3 ’ 2 ’ 6 ’ 4 ’ 1
D 2 ’ 4 ’ 6 ’ 1 ’ 5 ’ 3

52. **Which of the following types of malware remains dormant until the user performs an online financial transaction, replicates itself on the computer, and edits the registry entries each time the computer starts?** B

A TAN grabber

B Covert credential grabber
C HTML injection
D Form grabber

53. **Which of the following types of viruses infects Microsoft Word or similar applications by automatically performing a sequence of actions after triggering an application?**

A Multipartite viruses
B Macro viruses
C Encryption viruses
D Sparse infector viruses

B

54. **Identify the fileless malware obfuscation technique in which an attacker uses the below command to bypass antivirus software.**

```
cmd.exe /c ((echo command1)&&(echo command2))
```

A Inserting characters
B Inserting parentheses
C Inserting double quotes
D Custom environment variables

B

55. **Victor, an employee in an organization, received an executable file as an email attachment. Out of suspicion, he reached out to the organization's IT team. The team used a tool to dismantle the executable file into a binary program to find harmful or malicious processes.**

Which of the following tools did the IT team employ to analyze the application?

A Splunk
B Spam Mimic
C IDA Pro
D CCleaner

C

56. **John, an attacker, performed sniffing on a target organization's network and found that one of the protocols used by the target organization is vulnerable as it allows a client to access and manipulate the emails on a server. John exploited that protocol to obtain the data and employee credentials that are transmitted in cleartext.**

Which of the following protocols was exploited by John in the above scenario?

A IMAP
B HTTPS
C IPsec
D DTLS

A

57. **Which of the following DNS poisoning techniques is used by an attacker to infect a victim's machine with a Trojan and remotely change their DNS IP address to that of the attacker's?**

A DNS cache poisoning
B Proxy server DNS poisoning
C Internet DNS spoofing
D Intranet DNS spoofing

C

58. **Which of the following filters in Wireshark displays only the traffic in a LAN (192.168.x.x) between workstations and servers with no Internet?**

A ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16
B ip.src!= xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip
C ip.addr==192.168.1.100 && tcp.port=23
D ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5

A

59. **In which of the following phases of social engineering attacks does an attacker collect sensitive information about the organization's accounts, finance, technolo-**

D

gies in use, and upcoming plans?

A Research the target company
B Select a target
C Develop a relationship
D Exploit the relationship

60. **In one of the following social engineering techniques, an attacker assumes the role of a knowledgeable professional so that the organization's employees ask them for information. The attacker then manipulates questions to draw out the required information.**

Which is this technique?

A Baiting
B Quid pro quo
C Reverse social engineering
D Dumpster diving

C

61. **When Jake, a software engineer, was using social media, he abruptly received a friend request from an unknown lady. Out of curiosity, he accepted it. She pretended to be nice and tricked Jake into revealing sensitive information about his organization. Once she obtained the information, she deactivated her account.**

Which of the following types of attack was performed on Jake in the above scenario?

A Shoulder surfing
B Honey trap
C Diversion theft
D Tailgating

B

62. **Kate, a disgruntled ex-employee of an organization, decided to hinder the operations of the organization and gather sensitive information by injecting mal-**

B

ware into the organization's network.

Which of the following categories of insiders does Kate belong to?

A Negligent insider
B Malicious insider
C Compromised insider
D Professional insider

63. **In one of the following types of identity theft, the perpetrator obtains information from different victims to create a new identity by stealing a social security number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity.**

Which is this type of identity theft?

A Social identity theft
B Synthetic identity theft
C Child identity theft
D Medical identity theft

B

64. **Santa, an attacker, targeted an organization's web infrastructure and sent partial HTTP requests to the target web server. When the partial requests were received, the web server opened multiple connections and waited for the requests to complete; however, these requests remained incomplete, causing the target server's maximum concurrent connection pool to be exhausted and additional connection attempts to be denied.**

Which of the following attack techniques was employed by Santa?

A Slowloris attack
B Ping-of-death (PoD) attack

A

C Multi-vector attack
D Smurf attack

65. **Which of the following techniques scans the headers of IP packets leaving a network and ensures that unauthorized or malicious traffic never leaves the internal network?**

A Ingress filtering
B TCP intercept
C Rate limiting
D Egress filtering

D

66. **Which of the following techniques is also called a one-click attack or session riding and is used by an attacker to exploit a victim's active session with a trusted site to perform malicious activities?**

A Cross-site request forgery attack
B Cross-site script attack
C Session replay attacks
D Session fixation

A

67. **An attacker aims to hack an organization and gather sensitive information. In this process, they lure an employee of the organization into clicking on a fake link, which appears legitimate but redirects the user to the attacker's server. The attacker then forwards the request to the legitimate server on behalf of the victim.**

Which of the following types of attack is performed by the attacker in the above scenario?

A Man-in-the-middle attack
B Cross-site script attack
C Session replay attack
D Session hijacking using proxy servers

D

68.

B

In which of the following types of hijacking can an attacker inject malicious data or commands into intercepted communications in a TCP session, even if the victim disables source routing?

A RST hijacking

B Blind hijacking

C UDP hijacking

D Session fixation

69. **Which of the following types of IDS alerts is an alarm raised when no actual attack is in progress?**

A True positive

B False positive

C True negative

D False negative

B

70. **Which of the following firewalls works at the session layer of the OSI model or TCP layer of TCP/IP, forwards data between networks without verification, and blocks incoming packets from the host but allows traffic to pass through?**

A Packet filtering firewall

B Circuit-level gateway firewall

C Application-level firewall

D Application proxy

B

71. **Which of the following is an IDS evasion technique used by attackers to encode an attack packet payload in such a manner that the destination host can decode the packet but not the IDS?**

A Evasion

B Session splicing

C Obfuscating

D Fragmentation

C

72.

C

In which of the following techniques does an attacker use a combination of upper- and lower-case letters in an XSS payload to bypass the WAF?

A Using hex encoding to bypass the WAF
B Using ASCII values to bypass the WAF
C Using obfuscation to bypass the WAF
D Using ICMP tunneling

---

73. **One of the following techniques redirects all malicious network traffic to a honeypot after any intrusion attempt is detected. Attackers can identify such honeypots by examining specific TCP/IP parameters such as the round-trip time (RTT), time to live (TTL), and TCP timestamp.**

Which is this technique?

A Fake AP
B Snort_inline
C User-Mode Linux (UML)
D Bait and switch

D

---

74. **Which of the following web-server components is located between the web client and web server to pass all the requests and is also used to prevent IP blocking and maintain anonymity?**

A Server root
B Web proxy
C Virtual document tree
D Virtual hosting

B

---

75. **In which of the following attack types does an attacker use compromised PCs with spoofed IP addresses to intensify DDoS attacks on the victims' DNS server by exploiting the DNS recursive method?**

A DoS/DDoS attack

C

B DNS server hijacking
C DNS amplification attack
D Directory traversal attack

76. **In which of the following attack types does an attacker exploit vulnerabilities that evolve from the unsafe use of functions in an application in public web servers to send crafted requests to internal or backend servers?**

A SSH brute forcing
B Web-server password cracking
C Server-side request forgery
D Web-server misconfiguration

C

77. **In which of the following attack types does an attacker modify the content of a web page by examining its HTML code and identifying form fields that lack valid constraints?**

A Directory traversal
B Buffer overflow attack
C Command injection attack
D Cross-site scripting (XSS) attack

C

78. **Which of the following is a technique used by an attacker to gather valuable system-level data such as account details, OS, software version, server names, and database schema details?**

A Whois
B Session hijacking
C Web server footprinting
D Vulnerability scanning

C

79. **In which of the following stages of the web server attack methodology does an attacker determine the web server's remote access capabilities, its ports and services, and other aspects of its security?**

B

A Information gathering
B Web server footprinting
C Website mirroring
D Vulnerability scanning

80. **Which of the following modules establishes a communication channel between the Metasploit framework and a victim host?**

A Exploit module
B Auxiliary module
C Payload module
D NOPS module

C

81. **Given below are the steps involved in automated patch management.**

a. Test
b. Assess
c. Detect
d. Acquire
e. Maintain
f. Deploy

What is the correct sequence of steps involved in automatic patch management?

A c ' b ' a ' d ' f ' e
B b ' c ' d ' a ' f ' e
C c ' b ' d ' a ' f ' e
D a ' c ' b ' e ' f ' d

C

82. **Which of the following web services is designed to make services more productive and uses many underlying HTTP concepts to define the services?**

A SOAP
B RESTful

B

C XML-RPC
D JSON-RPC

83. **In which of the following web application threats does an attacker manipulate the variables that reference files with "dot-dot-slash (../)" sequences and its variations?**

A Unvalidated redirects and forwards
B Hidden field manipulation attack
C Directory traversal attack
D Cookie/session poisoning

C

84. **Which of the following is a process that can be used to convert object data into a linear format for transportation to a different system or different network?**

A Deserialization
B Serialization
C Insecure deserialization
D Directory traversal

B

85. **Which of the following attacks runs malicious code inside a browser and causes an infection that persists even after closing or browsing away from the malicious web page that spread the infection?**

A Clickjacking attack
B DNS rebinding attack
C MarioNet attack
D XML poisoning

C

86. **Which of the following information is exploited by an attacker to perform a buffer overflow attack on a target web application?**

A Cleartext communication
B Error message
C Application code
D Email interaction

C

87. **In which of the following attacks does an attacker obtain the user session ID and then reuse it to gain unauthorized access to a target user account?** D

A Session token prediction
B Session token tampering
C Session hijacking
D Session replay

88. **In which of the following security risks does an API accidentally expose internal variables or objects because of improper binding and filtering based on a whitelist, allowing attackers with unauthorized access to modify object properties?** B

A Broken object-level authorization
B Mass assignment
C Improper assets management
D Injection

89. **Which of the following encoding schemes represents any binary data using only printable ASCII characters and is used for encoding email attachments for safe transmission over SMTP?** C

A URL encoding
B Unicode encoding
C Base64 encoding
D Hex encoding

90. **Which of the following attacks is performed by asking the appropriate questions to an application database, with multiple valid statements evaluated as true or false being supplied in the affected parameter in the HTTP request?** D

A Heavy query
B Error-based SQL injection

C No error message returned
D Boolean exploitation

91. **Which of the following elements can be extracted using the query**

http://www.certifiedhacker.com/page.aspx?id=1 or 1=convert (int,(select top 1 name from sysobjects where xtype=char(85)))-- ?

A 1st database table
B 1st table column name
C 1st field of the 1st row
D Database name

A

92. **Which of the following is an evasion technique that involves replacing characters with their ASCII codes in hexadecimal form and prefixing each code point with the percent sign (%)?**

A URL encoding
B Sophisticated matches
C Null byte
D Case variation

A

93. **Which of the following regular expressions helps security professionals detect zero or more alphanumeric and underscore characters involved in an attack?**

A /(\')|(\%27)|(\-\-)|(#)|(\%23)/ix
B /exec(\s|\+)+(s|x)p\w+/ix
C /\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix
D /((\%3D)|(=))[^]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/ix

C

94. **Which of the following protocols uses AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption?**

A WEP

C

B WPA3
C WPA2
D WPA

95. **Which of the following is a mode of operation that includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates?**

A WPA3-Personal
B WPA2-Personal
C WPA3-Enterprise
D WPA2-Enterprise

D

96. **In which of the following attacks does an attacker install a fake communication tower between two authentic endpoints with the intention of misleading a user and interrupting the data transmission between the user and real tower to hijack an active session?**

A Rogue AP attack
B Key reinstallation attack
C Wardriving
D aLTEr attack

D

97. **In which of the following types of attack does an attacker exploit the carrier-sense multiple access with collision avoidance (CSMA/CA) clear channel assessment (CCA) mechanism to make a channel appear busy?**

A Beacon flood
B Denial of service
C Access point theft
D EAP failure

B

98. **Which of the following attacks does not directly recover a WEP key and requires at least one data packet from a target AP for initiation?**

C

	A MAC spoofing attack **B Evil twin attack** **C Fragmentation attack** **D De-authentication attack**	
99.	**Which of the following Bluetooth attacks is similar to the ICMP ping-of-death attack, where the attacker sends an oversized ping packet to a victim's device to cause a buffer overflow?** **A Bluesnarfing** **B Bluesniff** **C Bluejacking** **D Bluesmacking**	D
100.	**Which of the following techniques involves sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones and laptops?** **A Bluejacking** **B Bluesmacking** **C Bluebugging** **D BluePrinting**	A
101.	**In which of the following attacks does an attacker dump memory by rebooting a victim's device with a malicious OS and then extract sensitive data from the dumped memory?** **A iOS jailbreaking** **B OS data caching** **C Carrier-loaded software** **D User-initiated code**	B
102.	**Which of the following drozer commands is used by an attacker to find the list of various exported activities, services, broadcast receivers, and content providers in a target mobile device?**	A

A dz> run app.package.attacksurface <package_name>
B dz> run app.activity.start --component <package_name> <activity_name>
C dz> run app.package.list
D dz> run app.package.info -a <package_name>

103. **In one of the following jailbreaking techniques, a user turns their device off and back on, following which the device starts up completely and the kernel is patched without the help of a computer.**

Which is this jailbreaking technique?

A Semi-tethered jailbreaking
B Tethered jailbreaking
C Semi-untethered jailbreaking
D Untethered jailbreaking

D

104. **John, an employee of an organization, always connects to the corporate network using his own mobile device. Which of the following best practices prevents BYOD risk when John connects to the corporate network?**

A Improperly disposing of a device
B Not reporting a lost or stolen device
C Providing support for many different devices
D Separating personal and private data

D

105. **In one of the following IoT attacks, attackers intercept legitimate messages from a valid communication and continuously send the intercepted message to the target device to perform a denial-of-service attack or crash the target device.**

Which is this IoT attack?

A Replay attack

A

B Exploit kits
C Network pivoting
D BlueBorne attack

106. **Which of the following RFCrack commands is used by an attacker to perform an incremental scan on a target IoT device while launching a rolling-code attack?**

A python RFCrack.py -b -v 5000000
B python RFCrack.py -j -F 314000000
C python RFCrack.py -r -M MOD_2FSK -F 314350000
D python RFCrack.py -i

A

107. **Which of the following components of an IoT framework must incorporate strong encryption techniques for secure communications between endpoints and the authentication mechanism for the edge components?**

A Gateway
B Cloud platform
C Mobile
D Edge

A

108. **Through which of the following SCADA vulnerabilities does an attacker exploit code security issues that include out-of-bound read/write vulnerabilities and heap- and stack-based buffer overflow?**

A Credential management
B Code injection
C Lack of authorization
D Memory corruption

D

109. **Which of the following modbus-cli commands is used by attackers to manipulate the register values in a target PLC device?**

A modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1 1

B

	modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1 1 **B modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2** **modbus write <Target IP> 400101 2 2 2 2 2 2 2 2** **C modbus read <Target IP> 101 10** **modbus read <Target IP> %M100 10** **D modbus read <Target IP> %MW100 10** **modbus read <Target IP> 400101 10**	
110.	**Which of the following Purdue levels is commonly referred to as an industrial demilitarized zone (IDMZ)?** **A Level 2** **B Level 3** **C Level 3.5** **D Level 4**	C
111.	**Which of the following cloud services provides data processing services, such as IoT services for connected devices, mobile and web applications, and batch-and-stream processing?** **A Function as a service (FaaS)** **B Container as a service (CaaS)** **C Security as a service (SECaaS)** **D Identity as a service (IDaaS)**	A
112.	**Which of the following cloud deployment models is also known as the internal or corporate cloud and is a cloud infrastructure operated by a single organization and implemented within a corporate firewall?** **A Community cloud** **B Multi cloud** **C Private cloud** **D Public cloud**	C
113.		C

	Which of the following is the component in the docker architecture where images are stored and pulled and can be either private or public? **A Docker daemon** **B Docker client** **C Docker registries** **D Docker objects**	
114.	**Which of the following is a serverless security risk due to the poor design of identity and access controls, paving the way for attackers to identify missing resources, such as open APIs and public cloud storage, and leading to system business logic breakage and execution flow disruption?** **A Injection** **B Broken authentication** **C Sensitive data exposure** **D XML external entities (XXE)**	B
115.	**In which of the following attacks does an attacker exploit the vulnerability residing in a bare-metal cloud server and use it to implant a malicious backdoor in its firmware?** **A Wrapping attack** **B Cloudborne attack** **C Cryptanalysis attack** **D Cross-site scripting attack**	B
116.	**Which of the following information does an attacker enumerate by analyzing the AWS error messages that reveal information regarding the existence of a user?** **A Enumerating AWS account IDs** **B Enumerating S3 buckets** **C Enumerating IAM roles** **D Enumerating bucket permissions**	C

117. **An attacker is using DumpsterDiver, an automated tool, to identify potential secret leaks and hardcoded passwords in target cloud services.**

Which of the following flags is set by the attacker to analyze the files using rules specified in "rules.yaml"?

A -r, --remove
B -a, --advance
C -s, --secret
D -o OUTFILE

B

118. **Which of the following encryption algorithms is a large tweakable symmetric-key block cipher with equal block and key sizes of 256, 512, or 1024 and involves only three operations, that is, addition-rotation-XOR?**

A RC4
B Twofish
C RC5
D Threefish

D

119. **Which of the following symmetric-key block ciphers has either 18 rounds for 128-bit keys or 24 rounds for 256-bit keys and uses four 8 × 8-bit S-boxes that perform affine transformations and logical operations?**

A RSA
B Diffie-Hellman
C Camellia
D YAK

C

120. **Which of the following components of public key infrastructure acts as a verifier for the certificate authority?**

A Authentication authority

B

B Registration authority
C Certificate management system
D Validation authority

121. **Which of the following protocols is often used for data compression, digital signing, encryption and decryption of messages, emails, files, and directories as well as to enhance the privacy of email communications?**

A EAP
B PGP
C CHAP
D HMAC

B

122. **Which of the following is an attack where an attacker intercepts the communication between a client and server, negotiates cryptographic parameters to decrypt the encrypted content, and obtains confidential information such as system passwords?**

A Chosen-key attack
B Man-in-the-middle attack
C Rubber hose attack
D Chosen-ciphertext attack

B

123. **Which of the following cryptography attacks is similar to the chosen plaintext attack, except that the attacker can obtain ciphertexts encrypted under two different keys?**

A Ciphertext-only attack
B Known-plaintext attack
C Chosen-key attack
D Related-key attack

D

124. **Which of the following is an attack technique where the only information available to the attacker is some plaintext blocks along with the corresponding ciphertext and algorithm used to encrypt and decrypt the**

D

text?

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