Ethical Hacking and Countermeasures

Mock Questions

(Version 13)

1. Which of the following is the warfare category in which viruses, worms, Trojan horses, or sniffers are used to make systems shut down automatically, corrupt data, steal information or services, send fraudulent messages, and access unauthorized data?

   A. Psychological warfare

   B. Hacker warfare

   C. C2 warfare

   D. Electronic warfare

2. Which of the following types of hackers compromise systems by running scripts, tools, and software developed by real hackers and usually focus on the quantity rather than the quality of the attacks they initiate?

   A. Suicide hackers

   B. Cyber terrorists

   C. State-sponsored hackers

   D. Script kiddies

3. James, a professional hacker, is performing an attack on a target organization. He gathered information about the target and identified vulnerabilities in the target network. He is now exploiting the vulnerabilities to enter the target's network and escalate privileges to have complete access to the target system.

   Which of the following phases of hacking is James currently in?

   A. Reconnaissance

   B. Gaining access

   C. Scanning

   D. Maintaining access

4. Nick, a security professional, was tasked with performing intrusion analysis on an organization's compromised network. For this purpose, Nick employed the diamond model of intrusion analysis. As part of the analysis, Nick determined the event's periodicity and documented the event's occurrence details. These details helped him correlate similar events and trace the duration of the attack on the target network.

   Identify the event meta-feature of the diamond model implemented by Nick in the above scenario.

   A. Phase

   B. Direction

   C. Resource

   D. Timestamp

5. The four key steps of the risk management phase are given below.

   1) Risk treatment

   2) Risk tracking and review

   3) Risk assessment

   4) Risk identification

   What is the correct sequence of steps involved in the risk management phase?

   A. 1 → 2 → 3 → 4

   B. 2 → 1 → 3 → 4

   C. 4 → 3 → 1 → 2

   D. 3 → 4 → 2 → 1

6. Which security strategy requires using several diverse methods to protect IT systems against attacks?

   A. Defense in depth

   B. Three-way handshake

   C. Covert channels

   D. Exponential backoff algorithm

7. Which of the following titles of SOX consists of four sections: defines practices to restore investor confidence in securities analysts; defines the SEC's authority to censure or bar securities professionals from practice; and defines the conditions to bar a person from practicing as a broker, advisor, or dealer?

   A. Title V: Analyst Conflicts of Interest

   B. Title VI: Commission Resources and Authority

   C. Title VII: Studies and Reports

   D. Title III: Corporate Responsibility

8. In which of the following footprinting threats does an attacker collect information directly and indirectly through persuasion without using any intrusion methods?

   A. Social engineering

   B. Corporate espionage

   C. Business loss

   D. System and network attacks

9. Smith, a professional hacker, has targeted an organization. He employed footprinting tools to scan through all the domains, subdomains, reachable IP addresses, DNS records, and Whois records to perform further attacks.

   What is the type of information Smith has extracted through the footprinting attempt?

   A. Physical security information

   B. Policy information

   C. Network information

   D. Company's product information

10. Which of the following search engine tools helps an attacker use an image as a search query and track the original source and details of images, such as photographs, profile pictures, and memes?

    A. Intelius

    B. Sublist3r

    C. TinEye

    D. Mention

11. Which of the following tools is a command-line search tool for Exploit-DB that allows taking a copy of the Exploit database for remote use?

    A. SearchSploit

    B. Spyse

    C. Spokeo

    D. DroidSniff

12. Given below is the command generated by ShellGPT to gather email accounts associated with the target organization:

    theHarvester -d microsoft.com -l 200 -b Baidu -f Microsoft_emails.xml

    Which of the following parameters from the above command is used to specify the data source for gathering email accounts?

    A. theHarvester

    B. -d microsoft.com

C. -b baidu

D. -l 200

13. Which of the following utilities is used by Recon-Dog to detect technologies existing in the target system?

    A. Whois lookup

    B. findsubdomains.com

    C. shodan.io

    D. wappalyzer.com

14. Which of the following should NOT be followed when securing an organization from footprinting attacks?

    A. Opting for privacy services on the Whois lookup database

    B. Educating employees to use pseudonyms on blogs, groups, and forums

    C. Ensuring that critical information is not revealed in press releases, annual reports, product catalogs, and so on.

    D. Enabling the geo-tagging functionality on cameras

15. 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

16. Jane, an attacker, is leveraging AI-powered technologies to enhance and automate her network scanning tasks. She uses ShellGPT to perform various Hping3 scans to acquire valuable insights about her target. Jane wants to perform a specific type of scan that sends echo requests to the target IP address and stops after a fixed number of iterations.

    Which of the following commands should Jane use to achieve her goal?

    A. hping3 --icmp --count 10 10.10.1.11

    B. hping3 -S 10.10.1.11 -p 80 --tcp-timestamp

    C. hping3 -1 10.0.1.11 --rand-dest –I eth0

    D. hping3 --ack -p 80 10.10.1.11

17. A security engineer is attempting to scan a company's internal network to verify the security policies of their networks. The engineer uses the NMAP command: nmap –n –sS –P0 –p 80 ***.***.**.**. What type of scan is this?

    A. Quick scan

    B. Intense scan

    C. Stealth scan

    D. Comprehensive scan

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

    A. IP address decoy

    B. Sending bad checksums

    C. Source port manipulation

    D. Anonymizers

19. Which of the following Nmap commands helps attackers perform OS discovery on the target IP addresses listed in a file?

    A. nmap -iL scan1.txt -O --script=default --script-args=newtargets -oN os_discovery_results.txt

    B. nmap -p80 --script http-waf-detect --script-args="http-wafdetect.uri=/testphp.vulnweb.com/artists.php,http wafdetect.detectBodyChanges" www.modsecurity.org

    C. nmap --script http-passwd --script-args http-passwd.root =/target IP address

    D. nmap -p 23 –script telnet-brute.nse –script-args userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target IP>

20. Which of the following countermeasures are used to avoid banner grabbing attacks?

    A. Never display false banners to mislead or deceive attackers

    B. Turn on unnecessary services on the network host to limit information disclosure

    C. Use ServerMask tools to disable or change banner information

    D. Enable the details of the vendor and version in the banners

21. Which of the following tools provides complete visibility, real-time detection, and intelligent response to malicious network scanning attempts?

    A. Orbot

    B. CyberGhost VPN

    C. ExtraHop

    D. WinHex

22. Which of the following protocols uses TCP port 179 to enable routers to establish sessions between them?

    A. LDAP

    B. BGP

    C. SIP

    D. SNMP

23. Which of the following NetBIOS service codes is used to obtain information related to the master browser name for the subnet?

    A. <03>

    B. <1E>

    C. <1D>

    D. <20>

24. Robert, a professional hacker, was tasked with retrieving critical information from a target network. For this purpose, Robert employed a command-line tool to fetch information from all the network sub-nodes, such as routers and switches, in the form of an object identifier (OID), which is part of the management information base (MIB).

    Identify the tool employed by Robert in the above scenario.

    A. Spokeo

    B. Tor Browser

    C. Factiva

    D. SnmpWalk

25. Which of the following ntpdate parameters is used by an attacker to perform a function that can force the time to always be slewed?

    A. -b

    B. -B

    C. -d

    D. –q

26. Which of the following commands allows an attacker to list all the SMTP commands available in the nmap directory?

    A. nmap -T4 -p 53 --script dns-brute <Target Domain>

    B. nmap -p 25 -script=smtp-open-relay <Target IP Address>

    C. nmap -p 25 –script=smtp-enum-users <Target IP Address>

    D. nmap -p 25, 365, 587 -script=smtp-commands <Target IP Address >

27. Which of the following Nmap commands is used by an attacker to enumerate the SMB service running on the target IP address?

    A. # nmap -sR <target IP/network>

    B. # nmap -p 445 -A <target IP>

    C. # nmap -p 23 --script telnet-ntlm-info <target IP>

    D. # nmap -sV -v --script nbstat.nse <target IP address>

28. Which of the following practices allows attackers to execute external SNMP enumeration attempts on the target network?

    A. Regularly audit the network traffic.

    B. Encrypt credentials using the "AuthNoPriv" mode.

    C. Never change the default or current passwords.

    D. Avoid using the "NoAuthNoPriv" mode.

29. Which of the following online resources helps an attacker in performing vulnerability research?

    A. AOL

    B. MITRE CVE

    C. EZGif

    D. GNUnet

30. Which of the following types of software vulnerability occurs due to coding errors and allows attackers to gain access to the target system?

    A. Open services

    B. Unpatched servers

    C. Buffer overflow

    D. Misconfiguration

31. John, a security analyst, was tasked with providing a comprehensive assessment report on a newly discovered vulnerability. He used the CVSS scoring system and paid attention to specific metrics that provide additional context and extrinsic attributes of the vulnerability.

    Identify the CVSS metrics discussed in the above scenario.

    A. Base metric

    B. Threat metric

    C. Environmental metric

    D. Supplemental metric

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

    A. Netcraft

    B. DNSdumpster

    C. Nessus

    D. Tor Browser

33. Mary, a security professional, was tasked with enhancing the organization's website security. For this purpose, she deployed an AI-powered automated vulnerability detection tool that utilizes machine learning to constantly analyze the website for vulnerabilities and threats.

    Identify the tool Mary deployed in the above scenario.

    A. SCEMU

    B. Akamai DDoS Protection

    C. Colasoft Packet Builder

    D. SmartScanner

34. Below is the command ShellGPT generated to perform automated vulnerability scanning tasks.

    nmap -sV –script=vuln www.moviescope.com -oN output.txt

    Which part of the above command is used to specify the filename where the scan results will be saved?

    A. nmap

    B. --script=vuln

    C. -oN output.txt

    D. www.moviescope.com

35. Which of the following types of stack memory register stores the address of the next instruction to be executed?

    A. ESP

    B. EDI

    C. EIP

    D. ESI

36. Given below are the various steps involved in performing a GPU-based attack.

    1. When the victim installs the malware-loaded application, the malware starts accessing the browser's OpenGL API.
    2. When the victim accesses any website via the browser, attackers can copy every character entered by the victim on the password field of the website.
    3. The malware on OpenGL API sets up a spy on the device to track activities on the browser.
    4. The attacker lures or forces the victim into visiting an insecure site or downloading a malware-loaded application on their system.

    Identify the correct sequence of steps.

    A. 1 → 3 → 2 → 4

    B. 3 → 2 → 4 → 1

    C. 4 → 1 → 3 → 2

    D. 2 → 1 → 3 → 4

37. Identify the command that helps an attacker generate a customized dictionary of passwords while performing a dictionary attack.

    A. nc -nv <Target IP> <Target Port>

    B. **john --wordlist=</path_to/rockyou.txt> --rules --stdout > <path_to/output_wordlist.txt>**

    C. john --show /path/to/ntlm_hashes.txt

    D. hashcat -a 3 -m 0 md5_hasheshashcat -a 3 -m 0 md5_hashes.txt -1 ?l?u ?1?l?l?l19?d?ds-1 ?l?u

38. Which of the following techniques is the best defensive measure against privilege escalation?

    A. Run users and applications with the highest privileges

    B. Run services as privileged accounts

    C. Restrict interactive logon privileges

    D. Increase the privileges of users and groups

39. In which of the following steganography attacks does an attacker perform probability analysis to test whether a given stego-object and original data are the same?

    A. Chosen-message

    B. Chi-square

    C. Known-cover

    D. Distinguishing statistical

40. Which of the following commands allows an attacker with administrator privileges to hide any file or folder in a Windows system?

    A. attrib +h +s +r <FolderName>

    B. net user <UserName> /add

    C. net user <UserName> /active:no

    D. mkdir .HiddenMaliciousFiles

41. Which of the following malware components is a piece of software that can conceal the existence of malware and be used to elude antivirus detection?

    A. Dropper

    B. Crypter

    C. Injector

    D. Packer

42. Which of the following techniques involves leveraging features of regularly used applications such as PDFs or Windows shortcut files (.lnk) to execute malicious commands?

    A. Memory code injection

    B. Exploiting non-malicious files

    C. Malicious websites

    D. Native applications

43. Which of the following indicators helps the security analysts identify AI-based malware presence in the organization's systems?

    A. Optimal CPU or memory usage patterns

    B. Stable rate of false positives or negatives in security tools

    C. Use of uncommon ports or protocols

    D. Security solutions maintaining their effectiveness

44. Which of the following Windows Service Manager (SrvMan) commands is used to install and start a legacy driver with a single call?

    A. srvman.exe add <file.exe/file.sys> [service name] [display name] [/type:<service type>] [/start:<start mode>] [/interactive:no] [/overwrite:yes]

    B. srvman.exe delete <service name>

    C. srvman.exe restart <service name> [/delay:<delay in msec>]

    D. srvman.exe run <driver.sys> [service name] [/copy:yes] [/overwrite:no] [/stopafter:<msec>]

45. Asher, a security analyst, was tasked with analyzing a recent malware incident at an organization. For this purpose, Asher employed a malware analysis platform that scans files, URLs, end points, and memory dumps. It helped Asher extract strings from the malware samples and identify whether those strings were used in other files.

    Identify the tool employed by Asher in the above scenario.

    A. xHelper

    B. cSploit

    C. Intezer

    D. Network Spoofer

46. Which of the following file dependencies is a networking DLL that helps connect to a network or perform network-related tasks?

    A. Kernel32.dll

    B. Advapi32.dll

    C. WSock32.dll

    D. Ntdll.dll

47. Which of the following practices helps security analysts defend an organizational network against Trojan attacks?

    A. Do not check the SSL authenticity before accessing any e-commerce website.

    B. Avoid clicking on unsolicited pop-ups and banners.

    C. Download and execute applications from untrusted sources.

    D. Enable the autorun option for external devices such as USB drives and hard drives.

48. Which of the following protocols allows a user's workstation to access mail from a mailbox server and send mail from the workstation to the mailbox server via SMTP?

    A. POP

    B. HTTP

    C. FTP

    D. SMTP

49. In which of the following ARP poisoning threats does an attacker manipulate a client's connection to take complete control of the network?

    A. Data manipulation

    B. Connection resetting

    C. Man-in-the-middle attack

    D. Connection hijacking

50. Which of the following measures should NOT be followed to prevent DNS spoofing attacks?

    A. Allow outgoing traffic to use UDP port 53 as a default source port

    B. Resolve all DNS queries to a local DNS server

    C. Implement an intrusion detection system (IDS) and deploy it correctly

    D. Maintain a single or specific range of IP addresses to login to the systems

51. Karbon, a professional hacker, targeted an organization to bypass the network traffic. For this purpose, he used a network forensic analysis tool that can monitor and extract information from network traffic as well as capture application data contained in the network traffic.

    Which of the following tools did Karbon utilize in the above scenario?

    A. AnDOSid

    B. Xplico

    C. Akamai

    D. Vindicate

52. Which of the following countermeasure should be followed to defend against sniffing?

    A. Allow physical access to network media

    B. Turn on network identification broadcasts

    C. Retrieve MAC addresses directly from NICs instead of the OS

    D. Use dynamic IP addresses and ARP tables

53. An ethical hacker is performing penetration testing on the target organization. He decided to test the organization's network to identify the systems running in promiscuous mode. Identify the tool that the ethical hacker needs to employ.

    A. FaceNiff

    B. FOCA

    C. Nmap

    D. Recon-ng

54. Below are the different phases of a social engineering attack.

    1) Develop a relationship

    2) Research the target company

    3) Select a target

    4) Exploit the relationship

    Identify the correct sequence of steps involved in a social engineering attack.

A. 1 → 2 → 3 → 4

B. 2 → 1 → 3 → 4

C. 2 → 3 → 1 → 4

D. 2 → 4 → 3 → 1

55. Which of the following techniques does an attacker use to snoop on the communication between users or devices and record private information to launch passive attacks?

A. Session hijacking

B. Privilege escalation

C. Spoofing

D. Eavesdropping

56. Which of the following social engineering techniques involves dynamically changing a webpage's content to mimic a legitimate site while the user is focused on another browser panel?

A. Tabnabbing

B. Spear phishing

C. Clone phishing

D. Piggybacking

57. In which of the following attack techniques does an attacker use sophisticated machine learning algorithms to convincingly mimic an individual's tone, intonation, and speaking style?

A. Clone phishing

B. Voice cloning

C. PRINCE attack

D. Markov-chain attack

58. Which of the following is a generic exploit designed to perform advanced attacks against human elements to compromise a target to offer sensitive information?

A. NetScanTools Pro

B. Wireshark

C. Social-Engineer Toolkit (SET)

D. Cain and Abel

59. Which of the following practices are not effective in preventing or minimizing voice cloning attacks?

    A. Establish policies and procedures for verifying the identity of individuals during voice-based interactions

    B. Use anti-spoofing technologies and techniques to detect and prevent the use of fake or synthetic voices

    C. Use unencrypted communication channels during voice calls

    D. Implement voice biometrics or other advanced authentication technologies to verify the authenticity of voice-based communications

60. Remin, a professional hacker, targeted an organization and attempted to propagate malicious code. In this process, he placed an attack toolkit on his own system, and a copy of the attack toolkit was transferred to a newly discovered vulnerable system in the organization's network.
    Which of the following techniques did Remin employ in the above scenario?

    A. Back-chaining propagation

    B. Autonomous propagation

    C. Central source propagation

    D. Spyware propagation

61. Which of the following scanning methods makes use of the information obtained from an infected machine to find new vulnerable machines in a target network?

    A. Topological scanning

    B. Permutation scanning

    C. Hit-list scanning

    D. Random scanning

62. In which of the following attacks does an attacker use a combination of volumetric, protocol, and application-layer attacks to take down a target system or service?

    A. Slowloris attack

    B. Peer-to-peer attack

    C. Multi-vector attack

    D. HTTP GET/POST attack

63. Fiona, an attacker, targeted an organization to diminish their network bandwidth. In this process, she used an attack technique in which zombies send large volumes of traffic to the victim's systems to exhaust the network, application, or service resources, thereby restricting access to legitimate employees.

Which of the following types of attack did Fiona perform in the above scenario?

A. Smurf attack

B. Flood attack

C. Amplification attack

D. Peer-to-peer attack

64. Sarah is facing one of the biggest challenges in her career—she has to design the early warning DDoS detection techniques for her employer. She starts developing the detection technique which uses signal analysis to detect anomalies. The technique she is employing analyzes network traffic in terms of spectral components where she divides the incoming signals into various frequencies and analyzes different. Which DDoS detection technique is she trying to implement?

A. Wavelet-based signal analysis

B. Activity profiling

C. Change-point detection

D. NetFlow detection

65. Scarlet, a security professional at Imperial Tech, received intermittent complaints from her colleagues about service unavailability, diminishing network bandwidth, and suspended network services. She recognized that these issues were due to DoS/DDoS attacks. To curb the occurrence of such issues in the future, she used a service that enabled high-end protection from these severe DoS/DDoS attacks.

Which of the following DoS/DDoS protection services did Scarlet use in the above scenario?

A. Fritzing

B. Stormwall PRO

C. Suphacap

D. KillerBee

66. In which of the following session hijacking phases does an attacker break the connection to a victim's machine with knowledge of the next sequence number (NSN)?

A. Monitor

B. Session desynchronization

C. Session ID prediction

D. Command injection

67. In which of the following levels of the OSI model does an attacker gain control over the HTTP user session and create new unauthorized sessions by using the stolen data?

    A. Application level

    B. Network level

    C. Presentation level

    D. Physical level

68. In one of the following attacks, an attacker exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS, and hijacks the session by decrypting secret session cookies. Which is this attack?

    A. CRIME attack

    B. Proxy servers

    C. Session donation attack

    D. Forbidden attack

69. Below are the various steps involved in the PetitPotam hijacking attack.

    1. Now, the attacker initiates an NTLM replay attack to gain remote access to the target AD CS.
    2. The attacker uses the EfsRpcOpenFileRaw command from MS-EFSRPC API to coerce the target server to perform NTLM authentication of another system.
    3. The attacker uses the already captured NTLM credentials to authenticate with the target server.
    4. Finally, the attacker creates an AD certificate to gain administrator privileges to the target AD server.

    Identify the correct sequence of steps involved in the PetitPotam hijacking.

    A. 1 → 2 → 3 → 4

    B. 3 → 1 → 2 → 4

    C. 3 → 2 → 1 → 4

    D. 2 → 3 → 1 → 4

70. Julie, a cybercriminal, intercepts communication between a client and a server using a connectionless protocol. She sends spoofed UDP packets that appear to be from a legitimate client, followed by forged packets with malicious data. This data introduces false information into the stream, changing the application's behavior.

    Identify the type of attack discussed in the above scenario.

    A. UDP hijacking

    B. UDP flooding

C. Shoulder surfing

D. Dumpster diving

71. Which of the following guidelines should be implemented to protect connections against session hijacking?

A. Use the same usernames and passwords for different accounts

B. Pass authentication cookies over HTTP connections

C. Include the session ID in the URL or query string

D. Use strings or long random numbers as session keys

72. Which of the following attributes in a packet can be used to check whether the packet originated from an unreliable zone?

A. Direction

B. Interface

C. TCP flag bits

D. Source IP address

73. Which of the following is a malware research tool that allows security analysts to detect and classify malware or other malicious codes through a rule-based approach?

A. Nmap

B. YARA

C. Hping3

D. Fing

74. An organization's web application firewall (WAF) allows specific queries and syntaxes that originate from their internal addresses. Jack, a professional hacker, exploited this functionality to send spoofed requests to trick the target WAF and server into believing that the request originated from their internal network. Jack also appended various extensions such as X-Originating-IP, X-Forwarded-For, X-Remote-IP, and X-Remote-Addr to the spoofed requests to bypass the target WAF.

Identify the technique employed by Jack to bypass the target WAF.

A. ARP spoofing

B. MAC spoofing

C. VLAN hopping

D. HTTP header spoofing

75. Given below are the various steps involved in creating malicious CPL files using CPLResourceRunner:

    1. Run the following command to encode the contents of shellcode.txt into Base64 format and prepare it for inclusion in a resource file:

       cat shellcode.txt |sed 's/[,]//g; s/0x//g;' |tr -d '\n' |xxd -p -r |gzip -c |base64 > b64shellcode.txt

    2. Use Cobalt Strike to generate a fully staged payload in x86 format, saving it as a beacon bin.
    3. Copy the encoded content from b64shellcode.txt to the Resources.txt file in the same folder.
    4. Collect the resources in x86 format and copy the CPLResourceRunner.dll into a new file named maliciousnew.cpl
    5. Execute ConvertShellcode.py on beacon.bin to convert it into useful shellcode saved as shellcode.txt.

    Identify the correct sequence of steps involved in creating malicious CPL files.

    A. 1 → 3 → 4 → 2 → 5

    B. 3 → 5 → 1 → 2 → 4

    C. 2 → 5 → 1 → 3 → 4

    D. 2 → 1 → 3 → 5 → 4

76. Which of the following techniques manipulates the TCP/IP stack and is effectively employed to slow down the spread of worms and backdoors?

    A. Layer 4 tar pits

    B. Layer 2 tar pits

    C. Layer 7 tar pits

    D. Honeyd honeypot

77. Which of the following practices helps security professionals defend their organizational network against IDS evasion attempts?

    A. Never use a traffic normalizer to remove potential ambiguity from the packet stream

    B. Do not store the attack information for future analysis

    C. Look for 0x90 other than nop opcode to defend against the polymorphic shellcode problem

    D. Ensure that the packets are arriving from a path secured with IDS

78. Lisa, a senior developer, was tasked with setting up a mechanism in Nginx to reduce the load on the backend servers and speed up response time. She wants to store copies of requested content and serve frequently accessed content directly from temporary storage.

    Which of the following Nginx components should Lisa configure to achieve this?

    A. Master Process

    B. Worker Processes

    C. Proxy Cache

    D. Application Server

79. In which of the following attack types does an attacker flood an application with an excess amount of data so that the application may crash or exhibit vulnerable behavior?

    A. Directory traversal

    B. Parameter/form tampering

    C. Denial-of-service attack

    D. Buffer overflow attack

80. Given below is the command generated by ShellGPT to perform a brute-force attack on an FTP server:

    hydra -L/usr/share/wordlists/ftp-usernames.txt -p /usr/share/wordlists/ftp-passwords.txt ftp://10.10.1.11

    Which of the following elements from the above command is used to specify the file containing the collection of usernames for the brute-force attack?

    A. -P

    B. Hydra

    C. -L

    D. ftp://10.10.1.11

81. An attacker wants to perform a session hijacking attack. What tool should he use to achieve his objective?

    A. Nessus

    B. Hydra

    C. Burp Suite

    D. Netcraft

82. Identify the fingerprinting tool that not only runs simple commands such as ping, traceroute, and nslookup, but also conducts static, dynamic, and stress checks on web servers.

    A. BuzzSumo

    B. Sherlock

    C. Uniscan

    D. BCTextEncoder

83. Which of the following techniques is NOT a countermeasure to defend against web server attacks?

    A. Install IIS server on a domain controller

    B. Secure the SAM

    C. Relocate sites and virtual directories to non-system partitions

    D. Use a dedicated machine as a web server

84. Which of the following components of the web service architecture is an extension of SOAP and can be used to maintain the integrity and confidentiality of SOAP messages?

    A. UDDI

    B. WSDL

    C. WS-Security

    D. WS-Policy

85. One of the following is a clickjacking technique in which an attacker creates an iframe of 1 × 1 pixels containing malicious content placed secretly under the mouse cursor. When the user clicks on this cursor, it will be registered on a malicious page. Which is this clickjacking technique?

    A. Complete transparent overlay

    B. Hidden overlay

    C. Click event dropping

    D. Rapid content replacement

86. Fred, a cybercriminal, targets an e-commerce website with outdated software to steal customer data. He exploits vulnerabilities in third-party plugins to gain illegitimate access and embeds malicious JavaScript on the checkout page, capturing customers' credit card details during checkout and transmitting them to his server.

    Identify the attack executed by Fred in the above scenario.

    A. Birthday attack

    B. Rainbow table attack

C. Magecart attack

D. Padding oracle attack

87. Dennis, a security analyst, was analyzing unauthorized transactions on an e-commerce application's customer accounts. He noticed several logins into these accounts from different geographic locations within a short timeframe, indicating that the application's user verification mechanism had been evaded.

    Identify the security evasion technique employed by Dennis in the above scenario.

    A. Bypass client-side controls

    B. Signature bypass

    C. Bypassing IDOR via parameter pollution

    D. Bypass multifactor authentication

88. Which of the following protocols provides transport-level security for API messages to ensure confidentiality through encryption and integrity through signature?

    A. NTP

    B. IMAP

    C. FTP

    D. SSL

89. Identify the API security risk that enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.

    A. Unrestricted resource consumption

    B. Server-side request forgery

    C. Broken authentication

    D. Unsafe consumption of APIs

90. In which of the following SQL injection attacks does an attacker deface a web page, insert malicious content into web pages, or alter the contents of a database?

    A. Authorization bypass

    B. Compromised data integrity

    C. Remote code execution

    D. Compromised availability of data

91. In which of the following attacks does an attacker inject an additional malicious query into an original query to make the DBMS execute multiple SQL queries?

    A. Piggybacked query

    B. Illegal/logically incorrect query

    C. System stored procedure

    D. Tautology

92. Which of the following tools can allow an attacker to intercept and edit HTTP/HTTPS requests sent by the browser, as well as the responses from server?

    A. Hoverwatch

    B. Tamper Dev

    C. Elcomsoft Distributed Password Recovery

    D. KeyGrabber

93. Which of the following is a Snort rule that is used to detect and block an SQL injection attack?

    A. ' OR 5 BETWEEN 1 AND 7

    B. UNION Select Password

    C. SqlDataAdapter myCommand = new SqlDataAdapter("LoginStoredProcedure '" + Login.Text +"'", conn);

    D. /(\%27)|(\')|(\-\-)|(\%23)|(#)/ix

94. In one of the following methods, an attacker attempts to replicate error-free navigation by injecting simple inputs such as **' and '1' = '1 Or ' and '1' = '2** and forces an application to generate application errors that reveal information such as table names, column names, and data types. Which is this method?

    A. Determining a SELECT query structure

    B. Determining the database engine type

    C. Parameter tampering

    D. Type mismatch

95. In which of the following evasion techniques does an attacker use a WHERE statement that is always evaluated as “true” so that any mathematical or string comparison can be used, such as “' or '1'='1'”?

    A. Variations

    B. Declare variables

    C. Case variation

    D. Null byte

96. Which of the following is a communication standard that is also known as WiMAX and is designed to provide multiple physical layer (PHY) and MAC options?

    A. 802.15.1

    B. 802.16

    C. 802.11n

    D. 802.11g

97. Which of the following Wi-Fi security protocols uses GCMP-256 for encryption and HMAC-SHA-384 for authentication?

    A. PEAP

    B. WEP

    C. CCMP

    D. WPA3

98. Which of the following is a type of access-control attack in which an attacker uses any USB adapter or wireless card and connects a host to an unsecured client to attack a specific client or to avoid AP security?

    A. Ad hoc association

    B. Promiscuous client

    C. Client mis-association

    D. Unauthorized association

99. Which of the following attack techniques is used by an attacker to send forged control, management, or data frames over a wireless network to misdirect wireless devices and perform other types of attacks such as DoS?

    A. Confidentiality attack

    B. Availability attack

    C. Authentication attack

    D. Integrity attack

100. Which of the following tools is used by an attacker to create rogue APs and perform sniffing and MITM attacks?

    A. Halberd

    B. Gobuster

    C. Skyhook

    D. MANA Toolkit

101. Which of the following techniques is used by network management software to detect rogue APs?

    A. RF scanning

    B. Wired side inputs

    C. AP scanning

    D. Virtual-private network

102. In which of the following techniques can an attacker use the **"netstat -p | grep <pid>"** command to get information about network activity?

    A. Disassemble the targeted app package

    B. Monitoring logs

    C. List out the open connections

    D. Signing and installing malicious APK

103. Chris, a professional hacker, was tasked with obtaining credentials and certificates from a target iOS device. For this purpose, Chris employed a tool to extract secrets such as passwords, certificates, and encryption keys from the target iOS device's storage system.

    Identify the tool Chris used in the above scenario.

    A. N-Stalker X

    B. ScanMyServer

    C. Keychain Dumper

    D. CORE Impact

104. Which of the following is the correct BYOD security guideline that an employee should follow to secure sensitive personal or corporate information stored on a mobile device?

    A. Provide offline access to the organization's sensitive information

    B. Disable session authentication and the timeout policy on the access gateway

    C. Do not allow jailbroken and rooted devices

    D. Never control access based on a need-to-know basis

105. Which of the following risks can be addressed using secure coding practices and validated third-party libraries?

    A. Insecure authentication/authorization usage

    B. Inadequate supply chain security

    C. Inadequate privacy controls

    D. Insufficient input/output validation

106. 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

107. Which of the following commands helps attackers list all the currently installed applications on an iOS device using a specific tool?

    A. r2 frida://usb//iGoat-Swift

    B. frida-ps -Uai

    C. \e~search

    D. rvictl -s <UDID of the iOS device>

108. Which of the following protocols is a type of LAN that consists of a wired connection between computers in a small building, office, or campus?

    A. MQTT

    B. LTE-Advanced

    C. Li-Fi

    D. Ethernet

109. If an attacker wants to gather information such as IP address, hostname, ISP, device's location, and the banner of the target IoT device, which of the following tools should he use to do so?

    A. Nmap

    B. Shodan

    C. RIoT vulnerability scanner

    D. Foren6

110. Encrypted communications, strong authentication credentials, secure web interface, encrypted storage, and automatic updates are the security considerations for which of the following components?

    A. Mobile

    B. Cloud platform

    C. Edge

    D. Gateway

111. Smith, a professional hacker, was attempting to gain access to a target ICS network. To achieve his goal, he initiated reconnaissance to gather information about the devices in the network, their IP addresses, hostnames, and other details.

    Which of the following techniques did Smith employ in the above scenario?

    A. IP address decoy

    B. Password guessing

    C. Hooking

    D. Identifying remote systems

112. Which of the following Nmap commands helps attackers identify the HMI systems in a target OT network?

    A. nmap -Pn -sT -p 46824 <Target IP>

    B. nmap -Pn -sT -p 102 --script s7-info <Target IP>

    C. nmap -Pn -sU -p 44818 --script enip-info <Target IP>

    D. nmap -Pn -sT -p 1911,4911 --script fox-info <Target IP>

113. Which of the following practices helps security professionals defend against attacks on the OT environment?

    A. Install and maintain endpoint protection solutions

    B. Enable unused services and functionalities

    C. Avoid using password hashing

    D. Avoid using DMZ connections between the ICS and corporate networks

114. Through which of the following Kubernetes vulnerabilities can an attacker exploit the kube-apiserver with the disabled debug mode to directly interact with it and perform various malicious activities?

    A. Exposed bearer tokens in logs

    B. Log rotation is not atomic

    C. No back-off process for scheduling

    D. No non-repudiation

115. Alex, a cloud security engineer, wants to list the computing resources running in the company's AWS cloud environment during a security assessment. Alex runs a command to get details about all the active resources.

    Identify the command used by Alex in the above scenario.

    A. aws ec2 describe-volumes

    B. aws ec2 describe-instances

    C. aws ec2 describe-snapshots

    D. aws ec2 describe-hosts

116. Which of the following Azure CLI cmdlets allows attackers to create a folder and store the function's results to be executed?

A. New-Item -Name "microburst_output" -ItemType "directory"

B. Import-Module .\MicrosBurst.psm1

C. Get-AzDomainInfo -Verbose -Folder microburst-output

D. explorer microburst-output

117. Which of the following commands helps an attacker view predefined roles or custom roles in the target Google Cloud environment?

A. gcloud iam roles list [--show-deleted] [--organization=<organization>] [--project=<project_id>]

B. gcloud sql databases list --instance=<instance_name>

C. prowler aws --profile custom-profile --filter-region <region_1> <region_2>

D. kubectl get services

118. lex, a cloud security engineer, is tasked with enhancing the security of his organization's container orchestration system. As part of his job, he uses a tool for vulnerability scanning to identify potential security issues specific to this environment.
Identify the tool used by Alex in the above scenario.

A. pwncat

B. **Kubescape**

C. Dependency Walker

D. Dylib Hijack Scanner

119. Which of the following best practices should be followed for securing a cloud environment?

A. Do not disclose applicable logs and data to customers

B. Allow unauthorized server access using security checkpoints

C. Do not enforce legal contracts in employee behavior policy

D. **Verify one's cloud in public domain blacklists**

120. In one of the following types of cipher, letters in plaintext are rearranged according to a regular system to produce ciphertext. Which is this type of cipher?

A. Substitution cipher

B. Block cipher

C. **Transposition cipher**

D. Stream cipher

121. Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4

B. RC5

C. MD4

D. MD5

122. Given below are the various steps involved in performing multilayer hashing using CyberChef:

1. Click on the "Open file as input" option to upload the sample file.
2. Based on these requirements, select another hashing algorithm using the output of the SHA1 hash as the input and perform hashing recursively, as shown in the screenshot.
3. Search for the desired hashing algorithm in the Operations panel (e.g., MD5), and drag and drop it into the Recipe panel. The output is shown in the Output panel.
4. Create a sample file and open the CyberChef (https://gchq.github.io/CyberChef).
5. Using the MD5 hash value as the input, select another hashing algorithm (e.g., SHA1) and drag and drop it into the Recipe panel.

Identify the correct sequence of steps involved in performing multilayer hashing using CyberChef.

A. 1 → 3 → 5 → 4 → 2

B. 3 → 5 → 1 → 2 → 4

C. 4 → 1 → 3 → 5 → 2

D. 2 → 4 → 1 → 3 → 5

123. Which of the following is an example of a private blockchain where a supervisor or central authority decides who can join and participate in the blockchain network?

A. Ethereum

B. IBM Food Trust

C. Ripple (XRP)

D. Bitcoin

124. Which of the following cryptanalysis methods is also known as a plaintext attack, is based on finding affine approximations to the action of a cipher, and is commonly used on block ciphers?

A. Differential cryptanalysis

B. Linear cryptanalysis

C. Integral cryptanalysis

D. Frequency analysis

125. David, a professional hacker, targets a high-security quantum cryptographic system by embedding malicious quantum components within the network. These components covertly gather and transmit sensitive information to David, allowing him to bypass the system's security without directly attacking the quantum algorithms.

Which of the following attacks did David perform in the above scenario?

A. Quantum bit-flipping attack

B. Quantum Trojan horse attack

C. Quantum supply chain attack

D. Quantum error correction mechanism exploitation