CEHv12

(Correction from main pdf)
&
(Extra questions)

By:- Nisarg Shroff

CEHv12

9 - (Exam Topic 1)
The “Gray-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 in only partly accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is completely known to the tester.

Answer: B

26 - (Exam Topic 1)
Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds
B. USER2SID
C. Cheops
D. SID2USER
E. DumpSec

Answer: B D E

77 - (Exam Topic 1)
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk
B. Introduce more controls to bring risk to 0%
C. Mitigate the risk
D. Avoid the risk

Answer: C

18. - (Exam Topic 1)
What is the proper response for a NULL scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: E

106. - (Exam Topic 1)
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: F

Explanation:

A NULL scan is a port scanning technique in which the scanner sends a TCP packet with no flags set (NULL) to the target port. The expected behaviour of the target system in response to a NULL scan depends on whether the port is open or closed.

If the port is open:

The correct response is usually **No response** (F). An open port typically does not respond to a NULL scan, meaning that the absence of a response suggests the port is open.

If the port is closed:

The target system may respond with a **TCP RST (reset)** packet (E) to indicate that the port is closed.
Therefore, in the context of a NULL scan, if there is no response, it generally implies that the port is open.

64. - (Exam Topic 1)
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.
Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil
B. SNScan
C. SNMPScan
D. Solarwinds IP Network Browser
E. Nmap

Answer: A B D

81. - (Exam Topic 1)
Which of the following tools can be used to perform a zone transfer?

A. NSLookup
B. Finger
C. Dig
D. Sam Spade
E. Host

F. Netcat
G. Neotrace

Answer: A C D E

85. - (Exam Topic 1)
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Answer: A C E

108. - (Exam Topic 1)
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110
B. 135
C. 139
D. 161
E. 445
F. 1024

Answer: B C E

115. - (Exam Topic 1)
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Answer: (most common answer is A) A,B,C,D

125. - (Exam Topic 1)
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

A. 200303028
B. 3600
C. 604800
D. 2400

E. 60
F. 4800

Answer: D

Explanation:

The information in the SOA (Start of Authority) record is typically structured as follows:

"(primary nameserver) (responsible party) (serial number) (refresh interval) (retry interval) (expire time) (default TTL)"

In the provided SOA record:

Serial number: 200302028
Refresh interval: 3600 seconds
Retry interval: 3600 seconds
Expire time: 604800 seconds
Default TTL: 2400 seconds

34. - (Exam Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file
B. Run a network sniffer and capture the returned traffic with the configuration file from the router
C. Run Generic Routing Encapsulation (GRE) tunnelling protocol from your computer to the router masking your IP address
D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

Answer: B D

45. - (Exam Topic 2)
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Nikto
B. Nmap
C. Metasploit
D. Armitage

Answer: A

53. - (Exam Topic 2)

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

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Answer: C

83. - (Exam Topic 2)
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

A. Medium
B. Low
C. Critical
D. High

Answer: A

Explanation:

- **0.0 - 3.9:** Low
- **4.0 - 6.9:** Medium
- **7.0 - 8.9:** High
- **9.0 - 10.0:** Critical

105. - (Exam Topic 2)
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

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

Answer: B

107. - (Exam Topic 2)
Which command can be used to show the current TCP/IP connections?

A. Netsh
B. Netstat
C. Net use connection
D. Net use

Answer: B

117. - (Exam Topic 3)
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

A. DroidSheep
B. Androrat
C. Zscaler
D. Trident

Answer: D

150. - (Exam Topic 2)
Which of the following are well known password-cracking programs?

A. L0phtcrack
B. NetCat
C. Jack the Ripper
D. Netbus
E. John the Ripper

Answer: A E

175. - (Exam Topic 2)
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64
B. 128
C. 255
D. 138

Answer: B

Explanation:

- Windows TTL 128,
- Linux TTL 64,
- OpenBSD 255

176. - (Exam Topic 2)
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

A. FTP
B. HTTPS
C. FTPS
D. IP

Answer: C

21. - (Exam Topic 3)
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

A. Platform as a service
B. Software as a service
C. Functions as a service
D. Infrastructure as a service

Answer: C

56. - (Exam Topic 3)
Which Nmap switch helps evade IDS or firewalls?

A. -n/-R
B. -0N/-0X/-0G
C. -T
D. -D

Answer: D

57. - (Exam Topic 3)
Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?
<!DOCTYPE blah [< IENTITY trustme SYSTEM "file:///etc/passwd" >] >

A. XXE
B. SQLi
C. IDOR
D. XXS

Answer: A

62. - (Exam Topic 3)
The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WEP
B. WPA
C. WPA2
D. WPA3

Answer: D

130. - (Exam Topic 3)
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

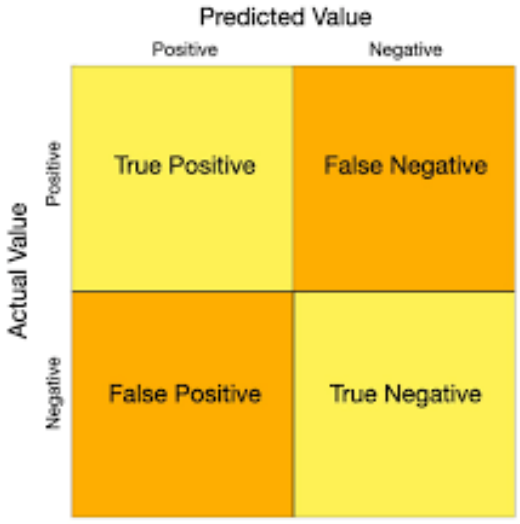
A. Side-channel attack
B. Denial-of-service attack
C. HMI-based attack
D. Buffer overflow attack

Answer: A

136. - (Exam Topic 3)
Richard, an attacker, targets an MNC In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

A. VPN footprinting
B. Email footprinting
C. VoIP footprinting
D. Whois footprinting

Answer: D



EXTRA QUESTIONS
(Just Check Out Once's)

NEW QUESTION 1
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Clickjacking
B. Cross-Site Scripting
C. Cross-Site Request Forgery
D. Web form input validation

Answer: C

NEW QUESTION 2
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Service Level Agreement
B. Project Scope
C. Rules of Engagement
D. Non-Disclosure Agreement

Answer: C

NEW QUESTION 3
Which of the following is an extremely common IDS evasion technique in the web world?

A. Spyware
B. Subnetting
C. Unicode Characters
D. Port Knocking

Answer: C

NEW QUESTION 4
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. The WAP does not recognize the client's MAC address

B. The client cannot see the SSID of the wireless network
C. Client is configured for the wrong channel
D. The wireless client is not configured to use DHCP

Answer: A

NEW QUESTION 5
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){char buffer[8];
strcpy(buffer, ""11111111111111111111111111111111"");} Output: Segmentation fault

A. C#
B. Python
C. Java
D. C++

Answer: D

NEW QUESTION 6
Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

A. Protect the payload and the headers
B. Encrypt
C. Work at the Data Link Layer
D. Authenticate

Answer: D

NEW QUESTION 7
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn
B. nmap -sP -p-65535 -T5
C. nmap -sT -O -T0
D. nmap -A --host-timeout 99 -T1

Answer: C

NEW QUESTION 8
Which of the following footprinting techniques allows an attacker to gather information passively about the target without direct interaction?

A. Extracting information using Internet archives
B. Extracting DNS information
C. Performing traceroute analysis
D. Performing social engineering

Answer: A

NEW QUESTION 9
Passive reconnaissance involves collecting information through which of the following?

A. Email tracking
B. Publicly accessible sources
C. Social engineering
D. Traceroute analysis

Answer: B

NEW QUESTION 10
Which of the following footprinting techniques allows an attacker to gather information about a target with direct interaction?

A. Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
B. Gathering website information using web spidering and mirroring tools
C. Gathering financial information about the target through financial services
D. Gathering infrastructure details of the target organization through job sites

Answer: B

NEW QUESTION 11
A pen tester was hired to perform penetration testing on an organization. The tester was asked to perform passive footprinting on the target organization.

Which of the following techniques comes under passive footprinting?

A. Performing traceroute analysis
B. Querying published name servers of the target
C. Performing social engineering
D. Finding the top-level domains (TLDs) and sub-domains of a target through web services

Answer: D

NEW QUESTION 12
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching the bank employees time in and out, searching the bank's job postings (paying special attention to IT-related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Vulnerability assessment
B. Active information gathering
C. Passive information gathering
D. Information reporting

Answer: C

NEW QUESTION 13
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. Eavesdropping
B. Spoofing
C. Session hijacking
D. Privilege escalation

Answer: A

NEW QUESTION 14
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

Answer: A

NEW QUESTION 15
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

Answer: C

NEW QUESTION 16
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

Answer: D

NEW QUESTION 17

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

Answer: B

NEW QUESTION 18
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
B. Baidu
C. Shodan
D. Bing

Answer: C

NEW QUESTION 19
An attacker runs a virtual machine on the same physical host as the victim's virtual machine and takes advantage of shared physical resources (processor cache) to steal data (cryptographic key) from the victim. Which of the following attacks he is performing?

A. XSS attack
B. MITC attack
C. Side-channel attack
D. Cryptanalysis attack

Answer: C

NEW QUESTION 20
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

Answer: B

NEW QUESTION 21
Given below are the different phases of the APT lifecycle.

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

Answer: C

NEW QUESTION 22
Given below are the steps involved in automated patch management.

1. Test
2. Assess
3. Detect
4. Acquire
5. Maintain
6. Deploy

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

A. 3 -> 2 -> 1 -> 4 -> 6 -> 5
B. 2 -> 3 -> 4 -> 1 -> 6-> 5
C. 3 -> 2 -> 4 -> 1 -> 6 -> 5
D. 1 -> 3 -> 2 -> 5 -> 6 -> 4

Answer: C

NEW QUESTION 23

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

Answer: B

NEW QUESTION 24
Williams, a professional hacker, gained initial access to a remote system via a compromised user. To gain root-level access, he copied the file sethc.exe from %systemroot%\system32 and the file cmd.exe to another location. Now, he restarted the system and pressed the Shift key 5 times to launch Command Prompt with system-level access.

Which of the following privilege escalation techniques did Williams employ in the above scenario?

A. Privilege escalation by abusing boot or logon initialization scripts
B. Privilege escalation using Dylib hijacking
C. Privilege escalation by modifying domain policy
D. Privilege escalation using Windows Sticky Keys

Answer: D

NEW QUESTION 25
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

Answer: D

NEW QUESTION 26
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
C. Risk tracking and review
D. Risk assessment

Answer: D

NEW QUESTION 27
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

Answer: C

NEW QUESTION 28
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

Answer: D

NEW QUESTION 29
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 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

Answer: D

NEW QUESTION 30
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?

A. MAC spoofing attack
B. Evil twin attack
C. Fragmentation attack
D. De-authentication attack

Answer: C

NEW QUESTION 31
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

Answer: C

NEW QUESTION 32
Which of the following tools in OSRFramework is used by attackers to check for a user profile on up to 290 different platforms?

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

Answer: A

NEW QUESTION 33
Mark, a professional hacker, wanted to evade conventional defense mechanisms on a target ICS network. For this purpose, he installed malicious software that hides the presence of malicious services, processes, and other activities.

Which of the following techniques did Mark employ for evasion?

A. Parameter tampering
B. HPP technique
C. Rootkits
D. WS-address spoofing

Answer: C

NEW QUESTION 34
Which of the following is a wireless security layer where per frame/packet authentication provides protection against MITM attacks and prevents an attacker from sniffing data when two genuine users communicate with each other?

A. Device security
B. Wireless signal security
C. End-user protection
D. Connection security

Answer: D

NEW QUESTION 34
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

Answer: C

NEW QUESTION 34
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
B. DNS server hijacking
C. DNS amplification attack
D. Directory traversal attack

Answer: C

NEW QUESTION 35
An organization named Cybersol.org hired a third-party team to run its business operations. The company provided full access to the team for hosting their services. A team member with malicious intentions misused the access permissions and installed a backdoor on a host system.

Identify the third-party risk demonstrated in the above scenario.

A. Improper input handling
B. Data storage
C. System integration
D. Design flaws

Answer: C

NEW QUESTION 36

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

Answer: C

NEW QUESTION 37

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
C. Multi-vector attack
D. Smurf attack

Answer: A

NEW QUESTION 38

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?

A. Heavy query
B. Error-based SQL injection
C. No error message returned
D. Boolean exploitation

Answer: D

NEW QUESTION 39

Which of the following is a bidirectional antenna used to support client connections, rather than site-to-site applications?

A. Yagi antenna
B. Reflector antenna
C. Dipole antenna
D. Directional antenna

Answer: C

NEW QUESTION 40
Jacob, a security analyst, was hired to perform malware analysis on a compromised machine. As part of the analysis, Jacob used a sophisticated tool to analyze all MS Office documents and review all the components that are suspected to be malicious.

Identify the tool used by Jacob in the above scenario.

A. Runscope
B. oleid
C. IDA Pro
D. Power Spy

Answer: B

NEW QUESTION 41
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
C. Immunity Debugger
D. Nessus

Answer: D

NEW QUESTION 42
An attacker is sending spoofed router advertisement messages so that all the data packets travel through his system. Then the attacker is trying to sniff the traffic to collect valuable information from the data packets to launch further attacks such as man-in-the-middle, denial-of-service, and passive sniffing attacks on the target network.

Which of the following technique is the attacker using in the above scenario?

A. IRDP spoofing
B. DHCP starvation attack
C. MAC flooding
D. ARP spoofing

Answer: D

NEW QUESTION 43
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

Answer: D

NEW QUESTION 44
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
B. Exploit kits
C. Network pivoting
D. BlueBorne attack

Answer: A

NEW QUESTION 45
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

Answer: C

NEW QUESTION 46
Which of the following hping commands is used by an attacker to scan the entire subnet to detect live 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

Answer: C

NEW QUESTION 47
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>

Answer: C

NEW QUESTION 48
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

Answer: B

NEW QUESTION 49
Which of the following practices is known to be an active footprinting method involving direct interaction with a target?

A. Finding information through search engines
B. Performing traceroute analysis
C. Collecting competitive intelligence
D. Performing people search using social networking sites

Answer: B

NEW QUESTION 50
Which of the following practices is known to be an active footprinting method involving direct interaction with a target?

A. Finding information through search engines
B. Performing traceroute analysis
C. Collecting competitive intelligence
D. Performing people search using social networking sites

Answer: B

NEW QUESTION 51
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

Answer: C

NEW QUESTION 52
Identify the type of cluster computing in which work is distributed among nodes to avoid overstressing a single node and periodic health checks are performed on each node to identify node failures and reroute the incoming traffic to another node.

A. Fail-over
B. Load balancing
C. Highly available
D. High-performance computing

Answer: B

NEW QUESTION 53
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

Answer: C

NEW QUESTION 54
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

Answer: C

NEW QUESTION 55
David, a content writer, was searching online for a specific topic. He visited a web page that appears legitimate 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

Answer: C

NEW QUESTION 56
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

Answer: C

NEW QUESTION 57
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

Answer: C

NEW QUESTION 58

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

Answer: B

NEW QUESTION 59
Cooper, a certified hacker, targeted multiple user accounts of an organization's work group to crack their passwords. In this process, he used a single commonly used password on multiple accounts simultaneously and waited for responses before initiating another password on the same accounts. This technique allowed Cooper to attempt more passwords without being affected by automatic lockout mechanisms.

Identify the type of password cracking attack performed by Cooper in the above scenario.

A. Password guessing
B. Password spraying attack
C. Pass-the-ticket attack
D. GPU-based attack

Answer: A

NEW QUESTION 60
Ethan, an Internet user, accessed a web application of a healthcare institution through his registered account. As security controls were not properly implemented during the development of that web application, Ethan's credentials were compromised during an active session with the application.

Identify the application security flaw exploited in the above scenario.

A. Insecure design
B. Vulnerable and outdated components
C. Injection
D. Broken access control

Answer: A

NEW QUESTION 61
Which of the following components of public key infrastructure acts as a verifier for the certificate authority?

A. Authentication authority
B. Registration authority
C. Certificate management system
D. Validation authority

Answer: B

NEW QUESTION 62
Joe, a security analyst, was tasked with developing a threat model for a private company. For this purpose, Joe implemented a popular global knowledge base that comprises adversary tactics and techniques based on real-world observations, which can help the company identify threats in advance.

Identify the framework implemented by Joe in the above scenario.

A. MITRE ATT&CK Framework
B. HIPAA Framework
C. Advanced Forensic Framework 4 (AFF4)
D. Advanced Forensics Format (AFF)

Answer: A

NEW QUESTION 63
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

Answer: A

NEW QUESTION 64
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

Answer: B

NEW QUESTION 65

Which of the following practices makes an organization's network vulnerable to SMB enumeration attacks?

A. Implement a proper authentication mechanism with a strong password policy.
B. Implement secure VPNs to secure the organizational data during remote access.
C. Enable TCP ports 88, 139, and 445 and UDP ports 88, 137, and 138.
D. Implement digitally signed data transmission and communication for accessing SMB resources.

Answer: C

NEW QUESTION 66
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

Answer: D

NEW QUESTION 67
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

Answer: D

NEW QUESTION 68
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?

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

Answer: B

NEW QUESTION 69

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

Answer: B

NEW QUESTION 70
Ronnie disguised himself as a salesperson, entered a target company, and managed to access phone bills, contact information, and financial information secretly from printer trash bins and user desks to perform further exploitation.

What is the attack performed by Ronnie in the above scenario?

A. Eavesdropping
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Answer: C

NEW QUESTION 71
Smith works as a professional Ethical Hacker with a large MNC. He is a CEH certified professional and was following the CEH methodology to perform the penetration testing. He is assigned a project for information gathering on a client's network. He started penetration testing and was trying to find out the company's internal URLs, (mostly by trial and error), looking for any information about the different departments and business units. Smith was unable to find any information.

What should Smith do to get the information he needs?

A. Smith should use online services such as netcraft.com to find the company's internal URLs
B. Smith should use WayBackMachine in Archive.org to find the company's internal URLs
C. Smith should use website mirroring tools such as HTTrack Website Copier to find the company's internal URLs
D. Smith should use email tracking tools such as eMailTrackerPro to find the company's internal URLs

Answer: B

NEW QUESTION 72
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

Answer: C

NEW QUESTION 73
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
B. WPA3
C. WPA2
D. WPA

Answer: C

NEW QUESTION 74
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

Answer: D

NEW QUESTION 75
In which of the following phases of social engineering attacks does an attacker collect sensitive information about the organization's accounts, finance, technologies in use, and upcoming plans?

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

Answer: D

NEW QUESTION 76
Lenin, a professional hacker, was attempting to bypass the WAF connected to the target network. To achieve his goal, Lenin started fingerprinting the target WAF to identify the list of restricted or abandoned keywords. Using this information, he created a suitable regex and payloads to evade the WAF detection.

Which of the following techniques did Lenin abuse in the above scenario?

A. Blacklist detection
B. Activity profiling
C. Deterrence controls
D. Fast flux DNS method

Answer: A

NEW QUESTION 77
TechSoft Inc. recently experienced many cyberattacks. The management of the organization instructed David, a security engineer, to strengthen the security of the organization. In this process, David employed a tool for detecting session hijacking attempts and performed asset discovery, intrusion detection, threat intelligence, and vulnerability assessment using that tool.

Which of the following tools did David employ in the above scenario?

A. USM Anywhere
B. Dependency Walker
C. Weevely
D. API Monitor

Answer: A

NEW QUESTION 78
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

Answer: D

NEW QUESTION 79

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

Answer: A

NEW QUESTION 80
Clark, a professional hacker, was attempting to capture packet flow on a target organization's network. After exploiting certain vulnerabilities in the network, Clark placed his Raspberry Pi device between the server and an authorized device to make all the network traffic pass through his device so that he can easily sniff and monitor the packet flow. Using this technique, Clark successfully bypassed NAC controls connected to the target network.

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

A. Using reverse ICMP tunnels
B. Using pre-authenticated device
C. Double tagging
D. Session splicing

Answer: B

NEW QUESTION 81
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

Answer: B

NEW QUESTION 82
Which of the following social engineering techniques can be mitigated by keeping all the trash in secured, monitored areas; shredding important data; and erasing magnetic media?

A. Eavesdropping
B. Dumpster diving

C. Shoulder surfing
D. Piggybacking

Answer: B

NEW QUESTION 83
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?

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

Answer: C

NEW QUESTION 84
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

Answer: D

NEW QUESTION 85
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

Answer: A

NEW QUESTION 86
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?

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

Answer: C

NEW QUESTION 87
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

Answer: B

NEW QUESTION 88
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

Answer: A

NEW QUESTION 89
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

Answer: D

NEW QUESTION 90
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
   modbus write <Target IP> %M100 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

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 91
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

Answer: B

NEW QUESTION 92
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

Answer: B

NEW QUESTION 93
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

Answer: B

NEW QUESTION 94
Smith, a professional hacker, gained unauthorized access to a target system. To access password-protected files, he established a keylogger using Metasploit to sniff users' keystrokes on the target machine. This command displays all the sniffed keystrokes on the Smith's system console.

Identify the Metasploit command that allowed Smith to sniff the user's keystrokes on the target machine.

A. keyscan_stop
B. getsystem
C. keyscan_dump
D. clearev

Answer: C

NEW QUESTION 95
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

Answer: D

NEW QUESTION 96
A hacker is attempting to check for all the systems alive in the network by performing a ping sweep. Which NMAP switch would the hacker use?

A. -sS
B. -sn
C. -sT
D. -sU

Answer: D

NEW QUESTION 97
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

Answer: C

NEW QUESTION 98
Which of the following practices helps security professionals defend the web server against various online attacks?

A. Never remove unnecessary IIS script mappings
B. Use an anti-bot mitigation service such as DataDome
C. Install the IIS server on a domain controller
D. Do not use server-side session ID tracking

Answer: B

NEW QUESTION 99
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

Answer: D

NEW QUESTION 100
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?

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

Answer: B

NEW QUESTION 101
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

Answer: A

NEW QUESTION 102
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. Require EditBuzzSumo

Answer: B

NEW QUESTION 103
Which of the following can pose a risk to mobile platform security?

A. Installing applications from trusted application stores
B. Securely wiping or deleting the data when disposing off the device
C. Disabling wireless access such as Wi-Fi and Bluetooth, if not in use
D. Connecting two separate networks such as Wi-Fi and Bluetooth simultaneously

Answer: D

NEW QUESTION 104
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. 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>

Answer: A

NEW QUESTION 105
Which of the following countermeasure should be used to prevent a ping sweep?

A. Disabling the firewall
B. Allowing connection with any host performing more than 10 ICMP ECHO requests
C. Avoiding the use of DMZ and disallowing commands such as ICMP ECHO_REPLY, HOST UNREACHABLE, and TIME EXCEEDED in DMZ
D. Limiting ICMP traffic with access-control lists (ACLs) to the ISP's specific IP addresses

Answer: D

NEW QUESTION 106
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

Answer: C

NEW QUESTION 107
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)

Answer: B

NEW QUESTION 108
A certain type of port scanning technique is similar to the TCP SYN scan and can be performed quickly 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

Answer: C

NEW QUESTION 109
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

Answer: B

NEW QUESTION 110
In which of the following types of vulnerability assessment does an organization assess the assets situated at multiple locations, such as client and server applications, simultaneously through appropriate synchronization techniques?

A. Internal assessment
B. Network-based assessment
C. Credentialed assessment
D. Distributed assessment

Answer: D

NEW QUESTION 111
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

Answer: B

NEW QUESTION 112
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

Answer: C

NEW QUESTION 113
Which of the following cryptography algorithms can be used in low-complexity applications such as RFID tags, sensor-based applications, and other IoT-based applications for easy processing?

A. Elliptic curve cryptography
B. Lightweight cryptography
C. Hard drive encryption
D. Quantum cryptography

Answer: B

NEW QUESTION 114

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)

Answer: A

NEW QUESTION 115
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

Answer: A

NEW QUESTION 116
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)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/ix

Answer: C

NEW QUESTION 117
Which of the following communication protocols is a variant of the Wi-Fi standard that provides an extended range, making it useful for communications in rural areas, and offers low data rates?

A. HaLow
B. Z-Wave
C. 6LoWPAN
D. QUIC

Answer: A

NEW QUESTION 118
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)

Answer: D

NEW QUESTION 119
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

Answer: C

NEW QUESTION 120
Maira wants to establish a connection with a server using the three-way handshake. As a first step she sends a packet to the server with the SYN flag set. In the second step, as a response for SYN, she receives packet with a flag set.

Which flag does she receive from the server?

A. ACK
B. SYN+ACK
C. RST
D. FIN

Answer: B

NEW QUESTION 121
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

Answer: B

NEW QUESTION 122
In which of the following technique, an attacker draws symbols in public places to advertise open Wi-Fi networks?

A. WarFlying
B. WarWalking
C. WarChalking
D. WarDriving

Answer: A

NEW QUESTION 123
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

Answer: A

NEW QUESTION 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 text?

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

Answer: D

NEW QUESTION 125
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

Answer: B

NEW QUESTION 126
Which of the following parameters enable NMAP's operating system detection feature?

A. NMAP -sV
B. NMAP -oS
C. NMAP -sC
D. NMAP -O

Answer: D

NEW QUESTION 127
Which of the following commands allows an attacker to retrieve all the subdomains associated with the target host?

A. nmap -T4 -p 53 --script dns-brute <Target Domain>
B. nmap --script=broadcast-dns-service-discovery <Target Domain>
C. nmap -p 445 -A <target IP>
D. nmap –sU –p 500 <target IP address>

Answer: B

NEW QUESTION 128
Which of the following scanning techniques is used by an attacker to check whether a machine is vulnerable to UPnP exploits?

A. UDP scanning
B. SCTP INIT scanning
C. SSDP scanning
D. List scanning

Answer: C

NEW QUESTION 129
Cooper, a professional hacker, targeted an organization's network to gain remote access. For this reason, he employed a technique to modify the structure of the malware code and append arbitrary code without affecting its functionality. This technique helped him in bypassing endpoint security agents.

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

A. Windows BITS
B. Password cracking
C. Buffer overflow
D. Ghostwriting

Answer: D

NEW QUESTION 130
Which of the following static malware analysis techniques provides information about the basic functionality of any program and is also used to determine the harmful actions that a program can perform?

A. Identifying packing/obfuscation methods
B. Strings search
C. Finding information on portable executables (PE)
D. Malware disassembly

Answer: D

NEW QUESTION 131
Bob, a professional hacker, gained unauthorized access to a Windows-based system. To escalate privileges, he abused an interface module in Windows that enables a software component to interact with another software component. He manipulated valid object references by replacing them with malicious content in Windows Registry. When the victim executes that object, the malicious code is automatically executed, allowing Bob to escalate privileges.

Which of the following privilege escalation methods did Bob employ in the above scenario?

A. COM hijacking
B. Modifying domain policy
C. Application shimming
D. Kernel exploits

Answer: A

NEW QUESTION 132
Garry, a security professional in an organization, recently noticed that someone was remotely controlling the network devices in the organization. After thorough research, he found that an attacker took advantage of SNMP vulnerabilities to gain access to the systems.

Which of the following countermeasures should Garry follow to secure the organization from SNMP enumeration?

A. Allowing access to TCP/UDP port 161
B. Always keeping the SNMP agent or turning on the SNMP service
C. Upgrading to SNMP3, which encrypts passwords and messages
D. Ensuring that the access to null session pipes is allowed

Answer: C

NEW QUESTION 133

Which of the following attacks helps an attacker bypass a same-origin policy's security constraints, allowing a malicious web page to communicate or make arbitrary requests to local domains?

A. MarioNet attack
B. Watering hole attack
C. Clickjacking attack
D. DNS rebinding attack

Answer: D

NEW QUESTION 134
Jack, a security professional, was hired to secure the organization's web environment from malicious activities. Jack implemented a domain level security protocol that sends a segment of a necessary domain name to fetch the results from a server instead of sending the complete domain name entered by a user. This protocol makes it difficult for attackers to peek at or snoop on the users' web activities.

Which of the following protocols did Jack implement in the above scenario?

A. DNS over HTTPS (DoH)
B. WEP/WPA encryption
C. IPsec protocol
D. VPN

Answer: A

NEW QUESTION 135
Which of the following techniques is used to gather information about the target without direct interaction with the target?

A. Active footprinting
B. Scanning
C. Passive footprinting
D. Enumeration

Answer: C

NEW QUESTION 136
Which of the following is defined as a package that is used to address a critical defect in a live environment, and contains a fix for a single issue?

A. Hotfix
B. Patch
C. Vulnerability
D. Penetration test

Answer: A

NEW QUESTION 137
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. Which cryptanalytic technique can the attacker use now in his attempt to discover the encryption key?

A. Birthday attack
B. Known plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Answer: B

NEW QUESTION 138
Which of the following tools allows attackers to test industrial networks for potential errors and exploitable vulnerabilities?

A. Low Orbit Ion Cannon (LOIC)
B. Fuzzowski
C. DroidSheep
D. NCollector Studio

Answer: B

NEW QUESTION 139
Which of the following UDDI information structures takes the form of keyed metadata and represents unique concepts or constructs in UDDI?

A. businessEntity
B. businessService
C. bindingTemplate
D. technicalModel

Answer: D

NEW QUESTION 140
Which of the following is the root file directory of a web server that stores critical HTML files related to web pages of a domain name that will be sent in response to requests?

A. Server root
B. Document root
C. Virtual hosting
D. Web proxy

Answer: D

NEW QUESTION 141

Which of the following Encryption techniques is used in WEP?

A. RC4
B. TKIP
C. AES
D. DES

Answer: A

NEW QUESTION 142
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Answer: D

NEW QUESTION 143
Which location and data examination tool interacts only with the real machine where it resides and provides a report to the same machine after scanning?

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

Answer: D

NEW QUESTION 144
Ronald, a professional hacker, is launching a few attacks on a target organization. In this process, he exploited a vulnerability found in all Intel and ARM processors deployed by Apple to trick a process into accessing out-of-bounds memory by exploiting CPU optimization mechanisms such as speculative execution.

Which of the following vulnerabilities was exploited by Ronald in the above scenario?

A. Dylib hijacking
B. Meltdown
C. Unattended installs
D. Open services

Answer: B

NEW QUESTION 145
During a penetration test, Marin discovered a session token that had had the content: 20170801135433_Robert. Why is this session token weak, and what is the name used for this type of vulnerability?

A. Unknown Session Token
B. Predictable Session Token
C. Captured Session Token
D. Date/Time Session Token

Answer: B

NEW QUESTION 146
Benjamin, a professional hacker, was attempting to establish persistence on a compromised Windows system. For this purpose, he exploited a security limitation within the NTLM protocol and obtained valid NTLM hashes of Kerberos tickets. Next, Benjamin reused the password hashes for gaining access to other network resources.

Which of the following attacks did Benjamin launch in the above scenario?

A. Brute-force attack
B. Overpass-the-hash attack (OPtH)
C. Fingerprint attack
D. Distributed network attack

Answer: B

NEW QUESTION 147
Allen, a security professional in an organization, was suspicious about the activities in the network and decided to scan all the logs. In this process, he used a tool that automatically collects all the event logs from all the systems present in the network and transfers the real-time event logs from the network systems to the main dashboard.

Which of the following tools did Allen employ in the above scenario?

A. Intelius
B. BinText
C. Splunk
D. theHarvester

Answer: C

NEW QUESTION 148
n which of the following methods does an attacker leverage headers such as Host in the HTTP request message to crack passwords?

A. Brute-forcing
B. Password guessing
C. Attack password reset mechanism
D. “Remember Me” exploit

Answer: A

NEW QUESTION 149
In which of the following attack techniques does an attacker exploit an NFC-enabled Android device by establishing a remote connection with the target mobile device and taking full control of the device?

A. Advanced SMS phishing
B. Hooking
C. Spearphone attack
D. Tap ’n Ghost attack

Answer: D

NEW QUESTION 150
Melanie, a new employee in an organization, noted down her passwords in a document and saved it to the cloud. Brett, a professional hacker who targeted the organization, succeeded in accessing the file uploaded by Melanie and gathering sensitive information of the organization.

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

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

Answer: A

NEW QUESTION 151
You are performing a port scan with Nmap. You are in a hurry and conducting the scans at the fastest possible speed. What type of scan should you run to get very reliable results?

A. Stealth scan
B. XMAS scan
C. Fragmented packet scan
D. Connect scan

Answer: D

NEW QUESTION 152
Which of the following techniques is a black-box testing method that is used to identify coding errors and security loopholes in web applications and can prevent attacks such as buffer overflow, DoS, XSS, and SQL injection?

A. Application whitelisting
B. Application blacklisting
C. Runtime application self-protection
D. Application fuzz testing

Answer: D

NEW QUESTION 153
n which of the following attacks do attackers send request packets to the target network while pretending to be a legitimate host to scan the hosts located behind the firewall?

A. MAC address spoofing
B. Directory traversal
C. Spimming
D. Session hijacking

Answer: B

NEW QUESTION 154
Which of the following types of attack is a cross-protocol weakness that can communicate and initiate an attack on servers supporting recent SSLv3/TLS protocol suites?

A. Related-key attack
B. Padding oracle attack
C. DROWN attack
D. DUHK attack

Answer: C

NEW QUESTION 155
In which of the following attacks does an attacker use a method known as the “bricking” of a system, through which he sends emails, IRC chats, tweets, or videos with fraudulent content for hardware updates to the victim?

A. Recursive HTTP GET flood attack
B. UDP flood attack
C. Permanent denial-of-service attack
D. SYN flood attack

Answer: C

NEW QUESTION 156
Which of the following master components in the Kubernetes cluster architecture scans newly generated pods and allocates a node to them?

A. Kube-apiserver

B. Etcd cluster
C. Kube-scheduler
D. Kube-controller-manager

Answer: C

NEW QUESTION 157
In network security, an IDS is a system used for monitoring and identifying unauthorized access or abnormal activities on computers or local networks. Which of the following techniques can an attacker use to escape detection by the IDS?

A. Encrypted traffic
B. Eavesdropping
C. Vlan hopping
D. Covert channel

Answer: A

NEW QUESTION 158
Which type of assessment tools are used to find and identify previously unknown vulnerabilities in a system?

A. Depth assessment tools
B. Scope assessment tools
C. Application-layer vulnerability assessment tools
D. Active scanning tools

Answer: C

NEW QUESTION 159
Which of the following tools is used by an attacker to determine the relationships and real-world links among people, organizations, websites, Internet infrastructure, and documents?

A. Unicornscan
B. BillCipher
C. Maltego
D. Whonix

Answer: C

NEW QUESTION 160
Joe, a security professional in an organization, was instructed to simplify the decision-making capability of an organization for identified risks. In the process, he employed a method to scale risk by considering the probability, likelihood, and consequence or impact of the risk.

What is the method employed by Joe for the representation of risk severity?
A. Risk level

B. Risk identification
C. Risk treatment
D. Risk matrix

Answer: D

NEW QUESTION 161
Which of the following techniques allows an attacker to view the individual data bytes of each packet passing through a network as well as capture a data packet, decode it, and analyze its content according to predetermined rules?

A. Hardware protocol analyzer
B. Switch port stealing
C. SPAN port
D. CAM table

Answer: A

NEW QUESTION 162
Which of the following recommendations can help users store critical data securely on an iOS mobile device?

A. Avoid using hardware-backed 256-bit AES encryption to store critical data.
B. Specify Access Control Flags to authenticate keys.
C. Store only large chunks of data directly in the keychain.
D. Implement a mechanism to retain keychain data to ensure that the data are accessed after uninstalling an application.

Answer: B

NEW QUESTION 163
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

Answer: C

NEW QUESTION 164

Which of the following MIBs manages the TCP/IP-based Internet using a simple architecture and system?

A. WINS.MIB
B. DHCP.MIB
C. MIB_II.MIB
D. HOSTMIB.MIB

Answer: C

NEW QUESTION 165
Kevin, a professional hacker, was hired to take control of the target organization's Active Directory (AD) environment. For this purpose, Kevin configured a fake SMB server and initiated an MITM attack to steal valid users' NTLM hashes and get authenticated by the domain controller. He used the same hashes to obtain admin privileges from the AD to control all the domain users.

Which of the following attacks did Kevin launch in the above scenario?

A. PetitPotam hijacking
B. Distribution attack
C. MAC flooding
D. XSS attack

Answer: A

NEW QUESTION 166
Elijah, a malicious hacker, targeted an organization's cloud environment and created oversized HTTP requests to trick the origin web server into responding with error content, which can be cached at the CDN servers. The error-based content that is cached in the CDN server is delivered to legitimate users, resulting in a DoS attack on the target cloud environment.

Which of the following attacks did Elijah initiate in the above scenario?

A. Cloudborne attack
B. Wrapping attack
C. CPDoS attack
D. Golden SAML attack

Answer: C

NEW QUESTION 167
Which of the following attack techniques uses the cryptanalytic time-memory trade-off and requires less time than other techniques?\

A. Rainbow table attack

B. Distributed network attack
C. Toggle-case attack
D. PRINCE attack

Answer: A

NEW QUESTION 168
A hacker is attempting to see which protocols are supported by target machines or network. Which NMAP switch would the hacker use?

A. -sO
B. -sT
C. -sS
D. -sU

Answer: A

NEW QUESTION 169
Which of the following attacks is launched by an attacker to intercept and use a legitimate user's MAC address for receiving all the traffic destined for the user and gaining access to the network?\

A. MAC flooding
B. MAC spoofing
C. DNS cache poisoning
D. DHCP starvation

Answer: A

NEW QUESTION 170
Which of the following technique allows an attacker to see past versions and pages of the target website?

A. Run the Web Data Extractor tool
B. Go to Archive.org to see past versions of the company website
C. Recover cached pages of the website from Google search engine cache
D. Use Smart Whois to recover the old pages of the website

Answer: B

NEW QUESTION 171
Which of the following vulnerability assessment phases involves tasks such as system rescanning, dynamic analysis, and attack surface reviewing?

A. Verification
B. Remediation
C. Monitoring
D. Risk assessment

Answer: A

NEW QUESTION 172
Which of the following protocols is widely used in network management systems to monitor network-attached devices such as routers, switches, firewalls, printers, and servers?\

A. NBNS
B. SMTP
C. SNMP
D. NFS

Answer: C

NEW QUESTION 173
What results will the following command yield: nmap -sS -O -p 123-153 192.168.100.3?

A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

Answer: D

NEW QUESTION 174
Oscar, a professional hacker, was hired to discover the LDAP vulnerabilities in a target organizational network. Oscar initiated the manual LDAP enumeration process by using a Python script. In this process, he executed a command to retrieve the Directory System Agent (DSA)–specific entry (DSE) naming contexts.

Identify the Python script executed by Oscar in the above scenario.

A. pip3 install ldap3
B. get_info = ldap3.ALL
C. ntpdate
D. server.info

Answer: A

NEW QUESTION 175
Which of the following DNS records allows attackers to map the IP address to a hostname?

A. MX
B. PTR
C. CNAME
D. NS

Answer: B

NEW QUESTION 176
Which of the following elements of information security ensures that information is accessible only to authorized personnel and features controls such as data classification, data encryption, and proper disposal of equipment?

A. Confidentiality
B. Integrity
C. Availability
D. Authenticity

Answer: A

NEW QUESTION 177
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

Answer: D

NEW QUESTION 178
In which of the following threat modelling steps does the administrator break down an application to obtain details about the trust boundaries, data flows, entry points, and exit points?

A. Identify security objectives
B. Identify threats
C. Application overview
D. Decompose the application

Answer: D

NEW QUESTION 179
Which of the following techniques is used by an attacker to access all of an application's functionalities and employs an intercepting proxy to monitor all requests and responses?

A. Web spidering/crawling
B. Banner grabbing
C. Attacker-directed spidering
D. DNS interrogation

Answer: C

NEW QUESTION 180
David, a security analyst, was instructed to analyze a security incident in an organization's network. For this purpose, David followed the diamond model of intrusion analysis. In the analysis, David initially determined the relationship between the adversary and victim for understanding the goal or motivation of the adversary.

Identify the meta-feature of the diamond model that helped David in the above scenario.

A. Resource
B. Timestamp
C. Socio-political
D. Technology

Answer: C

NEW QUESTION 181
In which phase of a social engineering attack does an attacker indulges in dumpster diving?

A. Selecting target
B. Develop the relationship
C. Research on target
D. Exploit the relationship

Answer: C

NEW QUESTION 182
Clark, a professional hacker, has targeted Rick, a bank employee. Clark secretly installed a backdoor Trojan in Rick's laptop to leverage it and access Rick's files. After installing the Trojan, Clark obtained uninterrupted access to the target machine and used it for transferring and modifying files.

Which of the following types of Trojans did Clark install in the above scenario?

A. Win32/Simile
B. Zmist
C. Dharma
D. PoisonIvy

Answer: D

NEW QUESTION 183
Which of the following Nmap commands is used by an attacker to perform an IP protocol ping scan on a target device?

A. # nmap –sn –PS <target IP address>

B. # nmap –sn –PA <target IP address>
C. # nmap –sn –PO <target IP address>
D. # nmap –sn –PP <target IP address>

Answer: C

NEW QUESTION 184
In which of the following attacks does an attacker extract cryptographic secrets from a person by coercion or torture?

A. Rubber hose attack
B. Brute-force attack
C. Man-in-the-middle attack
D. Hash collision attack

Answer: A

NEW QUESTION 185
Which of the following hping command performs UDP scan on port 80?

A. hping3 -2 <IP Address> –p 80
B. hping3 -1 <IP Address> –p 80
C. hping3 –A <IP Address> –p 80
D. hping3 –F –P –U <IP Address> –p 80

Answer: A

NEW QUESTION 186
Smith, a professional hacker, targeted an organization to gain illegitimate access to its corporate network. For this purpose, he employed a vulnerability scanning tool and identified a bug in a host system running an outdated software version. Smith exploited that vulnerability to inject malicious code and gain remote access to the target host.

Identify the type of vulnerability exploited by Smith in the above scenario.

A. Weak encryption
B. Default installations/default configurations
C. Unpatched application
D. Design flaws

Answer: C

NEW QUESTION 187
Max, a security professional, was tasked with monitoring web applications to identify any existing security flaws that can be exploited by attackers. While monitoring the application, Max noticed that the application is downloading updates from unauthorized or untrusted sources without conducting sufficient security checks.

Identify the type of application security risk noticed by Max in the above scenario.

A. Software and data integrity failures
B. Insecure design
C. Server-side request forgery
D. Injection

Answer: A

NEW QUESTION 188
Oliver, an encryption specialist at an organization, was instructed to implement a secure communication technique for the corporate network. For this purpose, Oliver employed an encryption technology that uses a cipher mode of operation, which requires an initialization vector (IV) and a secret key for encryption. In this mode of operation, the first block of plaintext is XORed with the IV and the resultant is sent as input to the block cipher encryption algorithm, along with the secret key. Then, the cipher block is used to perform XOR with the next plaintext block, and this process continues for the encryption of all the plaintext blocks.

Which of the following cipher modes of operation is demonstrated in the above scenario?

A. Cipher block chaining (CBC) mode
B. Counter mode
C. Cipher feedback (CFB) mode
D. Electronic code book (ECB) mode

Answer: C

NEW QUESTION 189
Which of the following types of jailbreaking uses a loophole in SecureROM to disable signature checks and thereby load patch NOR firmware?

A. Userland exploit
B. iBoot exploit
C. Bootrom exploit
D. Tethered jailbreaking

Answer: C

NEW QUESTION 190
Which of the following protocols uses AES-GCMP 256 for encryption and ECDH and ECDSA for key management?

A. WPA
B. WPA2
C. WEP
D. WPA3

Answer: D

NEW QUESTION 191
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

Answer: D

NEW QUESTION 192
Which of the following viruses combines the approach of file infectors and boot record infectors and attempts to simultaneously attack both the boot sector and executable or program files?

A. System or boot-sector viruses
B. Multipartite viruses
C. Macro viruses
D. Cluster viruses

Answer: B

NEW QUESTION 193
Which of the following tool determines the OS of the queried host by looking in detail at the network characteristics of the HTTP response received from the website?

A. Netcraft
B. Nmap
C. Wireshark
D. Netcat

Answer: D

NEW QUESTION 194
Which of the following is a password cracking technique that tests all possible character combinations, including combinations of uppercase characters from A to Z, numbers from 0 to 9, and lowercase characters from a to z?

A. Phishing attack
B. Guessing
C. Brute-force attack
D. Dictionary attack

Answer: C

NEW QUESTION 195
Which of the following methods is an adaptive SQL injection testing technique used to discover coding errors by inputting a massive amount of random data and observing the changes in the output?

A. Static testing
B. Function testing
C. Fuzz testing
D. Dynamic testing

Answer: C

NEW QUESTION 196
Which of the following GNU radio tools is used to capture and listen to incoming signals on an audio device?

A. uhd_rx_cfile
B. uhd_siggen_gui
C. uhd_rx_nogui
D. uhd_ft

Answer: C

NEW QUESTION 197
If an attacker uses ../ (dot-dot-slash) sequence to access restricted directories outside of the webserver root directory, then which attack did he perform?

A. DNS amplification attack
B. DoS attack
C. Directory traversal attack
D. HTTP response splitting attack

Answer: C

NEW QUESTION 198
Which of the following commands displays various options that a user can utilize to obtain a list of words from a target website?

A. cewl www.certifiedhacker.com
B. cewl.rb --help
C. cewl --email www.certifiedhacker.com
D. dnsrecon -r 162.241.216.0-162.241.216.255

Answer: B

NEW QUESTION 199
Which of the following DoS attack detection techniques analyzes network traffic in terms of spectral components? It divides incoming signals into various frequencies and examines different frequency components separately.

A. Activity profiling
B. Wavelet-based signal analysis
C. Change-point detection
D. Signature-based analysis

Answer: B

NEW QUESTION 200
Given below are the different phases involved in the web API hacking methodology.

1. Detect security standards
2. Identify the target
3. Launch attacks
4. Identify the attack surface

What is the correct sequence of phases followed in the web API hacking methodology?

A. 1 -> 2 -> 3 -> 4
B. 2 -> 1 -> 4 -> 3
C. 4 -> 2 -> 3 -> 1
D. 2 -> 4 -> 3 -> 1

Answer: B

NEW QUESTION 201
Which of the following layers in the IoT architecture is responsible for bridging the gap between two endpoints and performs functions such as message routing, message identification, and subscribing?

A. Internet layer
B. Access gateway layer
C. Middleware layer
D. Edge technology layer

Answer: C

NEW QUESTION 202
Given below are the steps to exploit a system using the Metasploit framework.

1. Verify exploit options
2. Configure an active exploit
3. Select a target
4. Launch the exploit
5. Select a payload

What is the correct sequence of steps through which a system can be exploited?

A. 1 -> 3 -> 2 -> 4 -> 5
B. 2 -> 1 -> 3 -> 5 -> 4
C. 4 -> 5 -> 1 -> 2 -> 3
D. 3 -> 1 -> 2 -> 5 -> 4

Answer: D

NEW QUESTION 203
In which of the following malware components does an attacker embed notorious malware files that can perform the installation task covertly?

A. Injector
B. Obfuscator
C. Dropper
D. Packer

Answer: C

NEW QUESTION 204
Which of the following is an open-source technology that provides PaaS through OS-level virtualization and delivers containerized software packages?

A. Serverless computing
B. Virtual machines
C. Docker
D. Microservices

Answer: C

NEW QUESTION 205
Information gathered from social networking websites such as Facebook, Twitter, and LinkedIn can be used to launch which of the following types of attacks?

A. Smurf attack
B. Social engineering attack
C. SQL injection attack
D. Distributed denial of service attack

Answer: B

NEW QUESTION 206
Which of the following types of external keyloggers works on the principle of converting electromagnetic sound waves into data?

A. PS/2 and USB keylogger
B. Bluetooth keylogger
C. Wi-Fi keylogger
D. Acoustic/CAM keylogger

Answer: D

NEW QUESTION 207
Which of the following policies addresses the areas listed below:

- Issue identification (ID) cards and uniforms, along with other access control measures to the employees of a particular organization.
- Office security or personnel must escort visitors into visitor rooms or lounges.
- Restrict access to certain areas of an organization in order to prevent unauthorized users from compromising security of sensitive data.

A. Special-access policies
B. Physical security policies
C. Password security policies
D. Defense strategy

Answer: B

NEW QUESTION 208
Which of the following is the entity in the NIST cloud deployment reference architecture that manages cloud services in terms of use, performance, and delivery and maintains the relationship between cloud providers and consumers?

A. Cloud provider
B. Cloud carrier
C. Cloud auditor
D. Cloud broker

Answer: D

NEW QUESTION 209
Which of the following cryptographic protocols allows two parties to establish a shared key over an in secure channel?

A. DSA
B. RSA
C. Diffie–Hellman
D. YAK

Answer: C

NEW QUESTION 210
In a GNSS spoofing technique, attackers block and re-broadcast the original signals for masking the actual signal sent to the targeted receiver. In this manner, the attackers manipulate the original signal with false positioning data and delay timings. Identify this technique.

A. Meaconing method
B. Cancellation methodology
C. Drag-off strategy
D. Interrupting the lock mechanism

Answer: A

NEW QUESTION 211
In which of the following types of injection attack does an attacker inject carriage return (\r) and linefeed (\n) characters into user input to trick a web server, web application, or user?

A. Server-side JS injection
B. Server-side includes injection
C. Log injection
D. CRLF injection

Answer: D

NEW QUESTION 212
Given below are the different steps by which an attacker can reveal a hidden SSID using the aircrack-ng suite.

1. Start airodump-ng to discover SSIDs on the interface
2. Run airmon-ng in the monitor mode
3. Switch to airodump to view the revealed SSID
4. De-authenticate the client to reveal the hidden SSID using Aireplay-ng

What is the correct sequence of steps used for revealing a hidden SSID using the aircrack-ng suite?

A. 1 -> 2 -> 3 -> 4
B. 2 -> 1 -> 4 -> 3
C. 2 -> 3 -> 1 -> 4
D. 2 -> 4 -> 3 -> 1

Answer: D

NEW QUESTION 213
Robert is a user with a privileged account and he is capable of connecting to the database. Rock wants to exploit Robert's privilege account. How can he do that?

A. Access the database and perform malicious activities at the OS level

B. Reject entries that contain binary data, escape sequences, and comment characters.
C. Use the most restrictive SQL account types for applications.
D. Design the code in such a way it traps and handles exceptions appropriately.

Answer: A

NEW QUESTION 214
Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk
B. Deny the risk
C. Mitigate the risk
D. Initiate the risk

Answer: C

NEW QUESTION 215
Which of the following is an HTTP header field used by an attacker to identify a client system's IP address that initiates a connection to a web server through an HTTP proxy?

A. Referer
B. User-Agent
C. X-Forwarded-For
D. Proxy-Authorization

Answer: C

NEW QUESTION 216
Which of the following technologies is an advanced version of conventional cloud technology and is often used in solutions that require the processing of small and urgent operations within a timespan of milliseconds, where the gateway intelligence is performed within devices such as programmable automation controllers?

A. Edge computing
B. Fog computing
C. Serverless computing
D. Docker networking

Answer: B

NEW QUESTION 217
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

Answer: C

NEW QUESTION 218
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

Answer: C

NEW QUESTION 219
Which of the following Nbtstat parameters lists the current NetBIOS sessions and their status with the IP addresses?

A. -S
B. -s
C. -c
D. -R

Answer: A

NEW QUESTION 220
InfoTech Security hired a penetration tester Sean to do physical penetration testing. On the first day of his assessment, Sean goes to the company posing as a repairman and starts checking trash bins to collect the sensitive information.
What is Sean trying to do?

A. Trying to attempt social engineering using phishing
B. Trying to attempt social engineering by eavesdropping
C. Trying to attempt social engineering by shoulder surfing
D. Trying to attempt social engineering by dumpster diving

Answer: D

NEW QUESTION 221

Javier is asked to explain to IT management as to why he is suggesting replacing the existing company firewall. Javier states that many external attackers are using forged internet addresses against the firewall and is concerned that this technique is highly effective against the existing firewall. What type of firewall Javier would have deployed?

A. Packet filtering firewall is deployed because it is unable to prevent these types of attacks.
B. Host-based firewall is deployed because the attackers are outside the network.
C. Circuit-level proxy firewall is deployed because it prevents these types of attacks.
D. Host-based firewall is deployed because the attackers are inside the network.

Answer: C

NEW QUESTION 222
Identify the attack in which an attacker captures the data from an employee's entry tag and copies it to another tag using a new chip to make unauthorized entry into the targeted organization's premises.

A. Key reinstallation attack
B. RFID cloning attack
C. Bluejacking
D. DNS rebinding attack

Answer: B

NEW QUESTION 223
Which of the following types of antennas is useful for transmitting weak radio signals over very long distances – on the order of 10 miles?

A. Omnidirectional
B. Parabolic grid
C. Unidirectional
D. Bidirectional

Answer: B
NEW QUESTION 224
An attacker sends an e-mail containing a malicious Microsoft office document to target WWW/FTP servers and embed Trojan horse files as software installation files, mobile phone software, and so on to lure a user to access them.

Identify by which method the attacker is trying to bypass the firewall.

A. Bypassing firewall through external systems
B. Bypassing firewall through MITM attack
C. Bypassing firewall through content
D. Bypassing WAF using XSS attack

Answer: C

NEW QUESTION 225
Which of the following DHCPv4 messages is sent by a client to the server to relinquish the network address and cancel the remaining lease?

A. DHCPRelease
B. DHCPRequest
C. DHCPInform
D. DHCPOffer

Answer: A

NEW QUESTION 226
Which of the following attacks involves unauthorized use of a victim's computer to stealthily mine digital currency?

A. Cloud cryptojacking
B. Cloudborne attack
C. Cryptanalysis attack
D. Metadata spoofing attack

Answer: A

NEW QUESTION 227
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 webservers. The engineer decides to start by using netcat to port 80. The engineer receives this output:

HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2017 01:41:33 GMT
Date: Mon, 16 Jan 2017 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369

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

A. Cross-site scripting
B. Banner grabbing
C. SQL injection

D. Whois database query

Answer: B

NEW QUESTION 228
Billy, a software engineer, received a call from an unknown number claiming to be from the bank in which he has an account. The caller stated that Billy needs to verify his account because of a suspicious online transaction. Billy was suspicious of this request and did not provide any details.

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

A. Impersonation
B. Eavesdropping
C. Shoulder surfing
D. Dumpster diving

Answer: A

NEW QUESTION 229
Which of the following tools allows attackers to exploit a flaw in the BLE pairing process and quickly brute force a temporary key (TK)?

A. Netcraft
B. crackle
C. Sublist3r
D. Spokeo

Answer: B

NEW QUESTION 230
Which of the following scanning techniques used by attackers involves resetting the TCP connection between a client and server abruptly before the completion of the three-way handshake signals?

A. TCP connect scan
B. Stealth scan
C. Inverse TCP flag scan
D. Xmas scan

Answer: C

NEW QUESTION 231
Finch, a professional hacker, wanted to maintain persistence within a compromised ICS network. For this purpose, he manipulated the variables required for the functioning of programmable logic controllers (PLCs) with malicious code to retain access to the network even after the compromised device is restarted.

Which of the following techniques did Finch employ to maintain persistence on the target ICS network?

A. Project file infection
B. Intranet DNS spoofing
C. Autonomous propagation
D. Double tagging

Answer: A

NEW QUESTION 232
Ray, a professional hacker, helps malicious attackers in finding vulnerabilities in the target organization. He also helps organizations by checking its limitations and suggesting best practices for making its IT infrastructure more secure.

What is the hacker class to which Ray belongs?

A. Black hats
B. White hats
C. Suicide hackers
D. Gray hats

Answer: D

NEW QUESTION 233
Ethan, a blackhat hacker, created a fake social media account impersonating an organization's helpdesk account and started connecting with disgruntled individuals via social media posts. He started posting fake service links on social media. When victims click on the link, they are redirected to another site requesting them to provide their details.

Which of the following types of attacks did Ethan perform in the above scenario?

A. Angler phishing
B. Eavesdropping
C. Dumpster diving
D. Diversion theft

Answer: A

NEW QUESTION 234
Name an attack where the attacker connects to nearby devices and exploits the vulnerabilities of the Bluetooth protocol to compromise the device?

A. Rolling code attack
B. Jamming attack
C. DDoS attack

D. BlueBorne attack

Answer: D

NEW QUESTION 235
Which of the following techniques is used to detect rogue Aps?

A. RF scanning
B. Passphrases
C. AES/CCMP encryption
D. Non-discoverable mode

Answer: A

NEW QUESTION 236
A certificate authority (CA) generates a key pair that will be used for encryption and decryption of e-mails. The integrity of the encrypted e-mail is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. E-mail server certificate

Answer: B

NEW QUESTION 237
David, a professional hacker, is performing an attack on a target organization. He has gathered information on its vulnerabilities and created a malicious payload to exploit the target network. He is now planning to inject the payload into the target system by using a phishing email.

Which phase of the cyber kill chain methodology is David in?

A. Reconnaissance
B. Exploitation
C. Delivery
D. Installation

Answer: C

NEW QUESTION 238
Which of the following attributes of the Findings element in a vulnerability scanning report contains the host's name and address?

A. <OS>
B. <Node>
C. <Date>

D. Services

Answer: B

NEW QUESTION 239
Where should a web server be placed in a network in order to provide the most security?

A. Inside an unsecured network
B. Outside an unsecured network
C. Inside DeMilitarized Zones (DMZ)
D. Outside a secure network

Answer: C

NEW QUESTION 240
Jim, a professional hacker, launched an APT attack on an organization. He was successful in entering the target network and extending access in the target network. He is now maintaining access with the use of customized malware and repackaging tools.

Which of the following phases of the APT lifecycle involves maintaining access to the target system, starting from evading endpoint security devices, until there is no further use of the data and assets?

A. Preparation
B. Cleanup
C. Initial intrusion
D. Persistence

Answer: D

NEW QUESTION 241
Which of the following is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities?

A. CVSS
B. NIST
C. OWASP
D. IETF

Answer: A

NEW QUESTION 242
Which of the following is the regulation that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization?

A. The Federal Information Security Management Act (FISMA)
B. ISO/IEC 27001:2013
C. The Digital Millennium Copyright Act (DMCA)
D. Sarbanes Oxley Act (SOX)

Answer: B

NEW QUESTION 243
In which of the following phases of MITRE ATT&CK for ICS does an attacker use various methods to gather information and gain knowledge regarding the data and domains of the target ICS infrastructure?
Lateral movement
Collection
Command and control
Inhibit response functio

Answer: B

NEW QUESTION 244
Teela, Inc. is running an application with debug enabled on one of its systems. Under which category of vulnerabilities can this flaw be classified?

A. Design flaws
B. Operating system flaws
C. Misconfiguration
D. Unpatched servers

Answer: C

NEW QUESTION 245
Which of the following techniques is applied to routers for blocking spoofed traffic and preventing spoofed traffic from entering the Internet?

A. Ingress filtering
B. Egress filtering
C. Using random initial sequence numbers
D. Using firewalls and filtering mechanisms

Answer: A

NEW QUESTION 246
Which of the following types of honeypots simulates only a limited number of services and applications of a target system or network?

A. Medium-interaction honeypots
B. Low-interaction honeypots
C. High-interaction honeypots
D. Pure honeypots

Answer: B

NEW QUESTION 247
An attacker uses the following SQL query to perform an SQL injection attack

SELECT * FROM users WHERE name = ‘’ OR ‘1’=‘1';

Identify the type of SQL injection attack performed.

A. Tautology
B. Illegal/logically incorrect query
C. UNION SQL injection
D. End-of-line comment

Answer: A

NEW QUESTION 248
Which of the following regional internet registries (RIRs) provides services related to the technical coordination and management of Internet number resources in Canada, the United States, and many Caribbean and North Atlantic islands?

A. AFRINIC
B. ARIN
C. APNIC
D. LACNIC

Answer: B

NEW QUESTION 249
Which of the following indicators in the OSINT framework indicates a URL that contains the search term, where the URL itself must be edited manually?

A. (T)
B. (D)
C. (R)
D. (M)

Answer: D

NEW QUESTION 250
Charlie, a professional hacker, was hired to enumerate critical information from the target organization’s Active Directory (AD) environment. In this process, he executed a PowerView command that retrieves information related to the currently active domain user.

Identify the command executed by Charlie in the above scenario.

A. Find-LocalAdminAccess
B. (Get-DomainPolicy)."SystemAccess"
C. Get-DomainSID
D. Get-NetLoggedon -ComputerName <computer-name>

Answer: B