- **Vendor:** EC-Council
- **Exam Code:** 312-50v11
- **Exam Name:** Certified Ethical Hacker Exam (CEH v11)
- **New Updated Questions from Braindump2go (Updated in March/2021)**

QUESTION 906
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

```
env x='(){ :;};echo exploit' bash 瑲 `cat/etc/passwd'
```

A. Removes the passwd file
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Display passwd content to prompt

Answer: D

QUESTION 907
joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud booker
B. Cloud consumer
C. Cloud carrier
D. Cloud auditor

Answer: B
Explanation:
The cloud client is that the principal stakeholder for the cloud computing service. A cloud client represents someone or organization that maintains a account with, and uses the service from a cloud provider. A cloud client browses the service catalog from a cloud provider, requests the acceptable service, sets up service contracts with the cloud provider, and uses the service.
The cloud client is also beaked for the service provisioned, and needs to arrange payments accordingly. Cloud consumers fulfilled SLAs to specify the technical performance necessities fulfilled by a cloud provider. SLAs will cover terms regarding the quality of service, security, remedies for performance failures. A cloud provider may also list within the SLAs a collection of promises explicitly not created to consumers, i.e. limitations, and obligations that cloud consumers should accept. A cloud client will freely select a cloud provider with better pricing and a lot of favourable terms. Typically, a cloud provider's evaluation policy and SLAs are non-negotiable, unless the customer expects serious usage and can be able to negotiate for better contracts. Depending on the services requested, the activities and usage scenarios will be totally different among cloud consumers.

QUESTION 908
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

A. verification
B. Risk assessment
C. Vulnerability scan
D. Remediation

Answer: D
Explanation:
Its allude to play out the means that utilization to alleviate the established weaknesses as per scan level. In this stage reaction group plan moderation cycle to cover weaknesses.
Prioritize proposals
Design an activity intend to execute the proposals Perform Root source examination
Apply the arrangements
Remediation errands:

QUESTION 909
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

A. Phishing malware
B. Zero-day malware
C. File-less malware
D. Logic bomb malware

Answer: A

QUESTION 910
While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed. What most likely happened?

A. Matt inadvertently provided the answers to his security questions when responding to the post.
B. Matt's bank-account login information was brute forced.
C. Matt Inadvertently provided his password when responding to the post.
D. Matt's computer was infected with a keylogger.

Answer: A

QUESTION 911
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan
B. TCP Maimon scan
C. app ping scan
D. ACK flag probe scan

Answer: C

QUESTION 912
What is the minimum number of network connections in a multi homed firewall?

A. 3

B. 5
C. 4
D. 2

Answer: A

QUESTION 913
which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. SSO
B. RADIUS
C. WPA
D. NTLM

Answer: A

QUESTION 914
Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.
B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
C. It is not ?a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Answer: B

QUESTION 915
Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_______to encrypt the message, and Bryan uses__________to confirm the digital signature.

A. Bryan's public key; Bryan's public key
B. Alice's public key; Alice's public key
C. Bryan's private key; Alice's public key
D. Bryan's public key; Alice's public key

Answer: C

QUESTION 916
Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

A. Dorian is signing the message with his public key. and Poly will verify that the message came from Dorian by using Dorian's private key.
B. Dorian Is signing the message with Polys public key. and Poly will verify that the message came from Dorian by using Dorian's public key.
C. Dorian is signing the message with his private key. and Poly will verify that the message came from Dorian by using Dorian's public key.
D. Dorian is signing the message with Polys private key. and Poly will verify mat the message came from Dorian by using Dorian's public key.

Answer: C

QUESTION 917
An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deckled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?

A. Flowmon
B. Robotium
C. Balenadoud
D. intenlFuzzer

Answer: A

QUESTION 918
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:
char buff[10];
buff[>o] - 'a':
What type of attack is this?

A. CSRF
B. XSS
C. Buffer overflow
D. SQL injection

Answer: D

QUESTION 919
Don, a student, came across a gaming app in a third-party app store and Installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?

A. SMS phishing attack
B. SIM card attack
C. Agent Smith attack
D. Clickjacking

Answer: D

QUESTION 920
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

QUESTION 921
You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.
What Is the best Linux pipe to achieve your milestone?

A. dirb https://site.com | grep "site"

B. curl -s https://sile.com | grep `'< a href-\'http" | grep "Site-com- | cut -d "V" -f 2
C. wget https://stte.com | grep "< a href=*http" | grep "site.com"
D. wgethttps://site.com | cut-d"http-

Answer: C

QUESTION 922
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.

A. Dos attack
B. DHCP spoofing
C. ARP cache poisoning
D. DNS hijacking

Answer: A
Explanation:
A Distributed Denial of Service (DDoS) attack may be a non-intrusive internet attack made to require down the targeted website URL or slow it down by flooding the network, server or application with fake traffic. When against a vulnerable resource- intensive endpoint, even a small amount of traffic is enough for the attack to succeed.Distributed Denial of Service (DDoS) attacks are threats that website owners must familiarize themselves with as they're a critical piece of the safety landscape. Navigating the varied sorts of DDoS attacks are often challenging and time consuming. to assist you understand what a DDoS attack is and the way to stop it, we've written the subsequent guide.
Understanding a DDoS AttackThe objective of a DDoS attack is to stop legitimate users from accessing your website URL. For a DDoS attack to achieve success , the attacker must send more requests than the victim server can handle. differently successful attacks occur is when the attacker sends bogus requests.
How does a DDoS Attack Work?The DDoS attack will test the bounds of an internet server, network, and application resources by sending spikes of faux traffic. Some attacks are just short bursts of malicious requests on vulnerable endpoints like search functions. DDoS attacks use a military of zombie devices called a botnet. These botnets generally contains compromised IoT devices, websites, and computers.When a DDoS attack is launched, the botnet will attack the target and deplete the appliance resources. A successful DDoS attack can prevent users from accessing an internet site or slow it down enough to extend bounce rate, leading to financial losses and performance issues. What is the Goal Behind a DDoS Attack?The main goal of an attacker that's leveraging a Denial of Service (DoS) attack method is to disrupt an internet site availability:?the web site can become slow to reply to legitimate requests.?the web site are often disabled entirely, making it impossible for legitimate users to access it.Any sort of disruption, counting on your configuration, are often devastating to your business.

QUESTION 923
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. Twofish encryption algorithm
B. HMAC encryption algorithm
C. IDEA
D. Blowfish encryption algorithm

Answer: A

QUESTION 924
At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Actions on objectives
B. Weaponization
C. installation
D. Command and control

Answer: D

QUESTION 925
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externaIsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?

A. website defacement
B. Server-side request forgery (SSRF) attack
C. Web server misconfiguration
D. web cache poisoning attack

Answer: B

QUESTION 926
infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance
B. Maintaining access
C. Scanning
D. Gaming access

Answer: D
Explanation:
This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're 㨢 Password cracking ?Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.?Password attacks ?Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 927
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own public key to encrypt the message.
B. Use Mane's public key to encrypt the message.
C. Use his own private key to encrypt the message.
D. Use Marie's private key to encrypt the message.

Answer: B

QUESTION 928
A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A. Credentialed assessment
B. Database assessment

C. Host-based assessment
D. Distributed assessment

Answer: C
Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.
What it Measures Host
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities ?those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

QUESTION 929
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A. <1B>
B. <00>
C. <03>
D. <20>

Answer: C

QUESTION 930
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU
B. GPU
C. UEFI
D. TPM

Answer: D

QUESTION 931
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?

A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted

Answer: B

QUESTION 932
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
What Information-gathering technique does this best describe?

A. WhOiS lookup
B. Banner grabbing
C. Dictionary attack
D. Brute forcing

Answer: C

QUESTION 933
Robin, a professional hacker, targeted an organization's network to sniff all the traffic.
During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch inthe network so that he could make it a root bridge that will later allow him to sniff all the traffic in thenetwork.
What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack
B. VLAN hopping attack
C. DNS poisoning attack
D. STP attack

Answer: C

QUESTION 934
Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

A. Fed RAMP
B. PCIDSS
C. SOX
D. HIPAA

Answer: C
Explanation:
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.
The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

QUESTION 935
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker client
B. Docker objects
C. Docker daemon

D. Docker registries

Answer: B

QUESTION 936
Which ios jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

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

Answer: B
Explanation:
A semi-tethered jailbreak is one that allows a handset to finish a boot cycle when being pwned, however jailbreak extensions won't load till a laptop-based jailbreak application is deployed over a physical cable association between the device and also the computer in question.
Semi-tethered jailbreaks aren't as difficult as tethered jailbreaks as a result of you'll be able to power cycle your device and expect to use it commonly thenceforth, like creating phone calls and causing text messages. On the opposite hand, jailbreak tweaks won't initialize on the freshly-booted device and jailbreak-based apps like Cydia and Filza can merely crash on launch them till the device is shod back to a jailbroken state. Just as the name implies, a semi-`tethered' jailbreak necessitates a physical cable association between the device and also the laptop once running the jailbreak tool to patch the kernel and reinitialize the jailbroken state, however the nice issue here is that you simply will still access important core smartphone practicality in an exceedingly pinch after you don't have a laptop near .
The spic-and-span checkra1n jailbreak tool for macOS (and before long Windows) could be a prime example of a semi-tethered jailbreak, and may pwn A7-A11-equipped devices as previous because the iPhone 5s and as new because the iPhone X.

QUESTION 937
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex

Answer: A

QUESTION 938
A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?

A. Slowloris attack
B. Session splicing
C. Phlashing
D. Desynchronization

Answer: A

QUESTION 939
Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied

positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on jane?

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

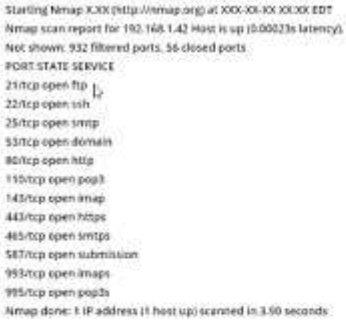
Answer: D

QUESTION 940
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

QUESTION 941
Consider the following Nmap output:



```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

What command-line parameter could you use to determine the type and version number of the web server?

A. -sv
B. -Pn
C. -V
D. -ss

Answer: D

QUESTION 942
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

A. DNS cache snooping
B. DNSSEC zone walking
C. DNS tunneling method
D. DNS enumeration

Answer: C

QUESTION 943
which type of virus can change its own code and then cipher itself multiple times as it replicates?

A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Encryption virus

Answer: A
Explanation:
A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now- infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.Like other viruses, a stealth virus can take hold of the many parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected `infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse.The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.

QUESTION 944
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program

Answer: B

QUESTION 945
An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

A. Phishing
B. Vlishing
C. Spoofing
D. DDoS

Answer: D