Topic 1 - Exam A

Question #1 *Topic 1*

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 **Most Voted**

C. AES

D. MD5 encryption algorithm

Correct Answer: *B*

Community vote distribution

B (92%) 8%

Question #2 *Topic 1*

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 **Most Voted**

C. CSRF

D. XSS

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Question #3 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #4 *Topic 1*

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 **Most Voted**

D. nmap -A --host-timeout 99 -T1

Correct Answer: *C*

Community vote distribution

C (91%) 9%

Question #5 *Topic 1*

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 **Most Voted**

C. WPA2-Enterprise

D. WPA2-Personal

Correct Answer: *B*

Community vote distribution

B (100%)

Question #6 *Topic 1*

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 **Most Voted**

D. idq.dll

Correct Answer: *C*

Community vote distribution

C (60%) A (40%)

Question #7 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

D (100%)

Question #8 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (87%) 13%

Question #9 *Topic 1*

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:] **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #10 *Topic 1*

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 **Most Voted**

C. Command and control

D. Exploitation

Correct Answer: *B*

Community vote distribution

B (91%) 9%

Question #11 *Topic 1*

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

Correct Answer: *A*

Community vote distribution

A (100%)

Question #12 *Topic 1*

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 **Most Voted**

C. Credentialed assessment

D. Distributed assessment

Correct Answer: *B*

Community vote distribution

B (100%)

Question #13 *Topic 1*

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 **Most Voted**

C. Website defacement

D. Web cache poisoning

Correct Answer: *B*

Community vote distribution

B (100%)

Question #14 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (53%) A (47%)

Question #15 *Topic 1*

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 **Most Voted**

C. WebSite-Watcher

D. WAFW00F

Correct Answer: *B*

Community vote distribution

B (75%) D (25%)

Question #16 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (88%) 13%

Question #17 *Topic 1*

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 **Most Voted**

B. Persistence

C. Cleanup

D. Preparation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #18 *Topic 1*

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #19 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

D (100%)

Question #20 *Topic 1*

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 **Most Voted**

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

Correct Answer: *A*

Community vote distribution

A (100%)

Question #21 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #22 *Topic 1*

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 **Most Voted**

B. Jamming signal attack

C. Wardriving

D. KRACK attack

Correct Answer: *A*

Community vote distribution

A (100%)

Question #23 *Topic 1*

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 **Most Voted**

D. EarthExplorer

Correct Answer: *C*

Community vote distribution

C (100%)

Question #24 *Topic 1*

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 **Most Voted**

C. Docker client

D. Docker registries

Correct Answer: *B*

Community vote distribution

B (80%) C (20%)

Question #25 *Topic 1*

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 **Most Voted**

B. Google image search

C. search.com

D. EarthExplorer

Correct Answer: *A*

Community vote distribution

A (100%)

Question #26 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #27 *Topic 1*

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 **Most Voted**

B. JSON-RPC

C. SOAP API

D. REST API

Correct Answer: *A*

Community vote distribution

A (100%)

Question #28 *Topic 1*

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. **Most Voted**

D. Topological scanning technique

Correct Answer: *C*

Community vote distribution

C (100%)

Question #29 *Topic 1*

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 **Most Voted**

D. Red hat

Correct Answer: *C*

Community vote distribution

C (69%) B (19%) 13%

Question #30 *Topic 1*

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 **Most Voted**

B. Slowloris

C. PLCinject

D. PyLoris

Correct Answer: *A*

Community vote distribution

A (100%)

Question #31 *Topic 1*

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 **Most Voted**

B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

Correct Answer: *A*

Community vote distribution

A (59%) B (41%)

Question #32 *Topic 1*

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 **Most Voted**

B. DNS rebinding attack

C. MarioNet attack

D. Clickjacking attack

Correct Answer: *A*

Community vote distribution

A (100%)

Question #33 *Topic 1*

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 **Most Voted**

B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

Correct Answer: *A*

Community vote distribution

A (75%) B (25%)

Question #34 *Topic 1*

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.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #35 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #36 *Topic 1*

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 **Most Voted**

D. Session fixation attack

Correct Answer: *C*

Community vote distribution

C (57%) D (43%)

Question #37 *Topic 1*

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 **Most Voted**

D. Desynchronization

Correct Answer: *C*

Community vote distribution

C (100%)

Question #38 *Topic 1*

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' **Most Voted**

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'

Correct Answer: *B*

Community vote distribution

B (71%) D (29%)

Question #39 *Topic 1*

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

A. RCPT

B. CHK

C. VRFY **Most Voted**

D. EXPN

Correct Answer: *C*

Community vote distribution

C (80%) D (20%)

Question #40 *Topic 1*

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 **Most Voted**

B. FTP

C. HTTPS

D. IP

Correct Answer: *A*

Community vote distribution

A (83%) B (17%)

Question #41 *Topic 1*

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.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #42 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (80%) A (20%)

Question #43 *Topic 1*

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. Most Voted

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.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #44 *Topic 1*

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 Most Voted

B. -sS

C. -Pn

D. -V

Correct Answer: *A*

Community vote distribution

A (100%)

Question #45 *Topic 1*

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

Correct Answer: *D*

Community vote distribution

D (100%)

Question #46 *Topic 1*

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #47 *Topic 1*

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. **Most Voted**

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.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #48 *Topic 1*

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #49 *Topic 1*

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>

Correct Answer: *C*

Community vote distribution

C (100%)

Question #50 *Topic 1*

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Viewing page 1 out of 7 pages.

Viewing questions **1-50** out of 302 questions