Question #251

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.

Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

A. [allinurl:]

B. [location:]

C. [site:]

D. [link:]

Question #252

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

What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WPA

B. WEP

C. WPA3

D. WPA2

Question #253

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.

Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

A. -Pn

B. -PU

C. -PP

D. -PY

Question #254

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker

checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Buffer overflow attack

B. Side-channel attack

C. Denial-of-service attack

D. HMI-based attack

Question #255

Given below are different steps involved in the vulnerability-management life cycle.

1) Remediation

2) Identify assets and create a baseline

3) Verification

4) Monitor

5) Vulnerability scan

6) Risk assessment

Identify the correct sequence of steps involved in vulnerability management.

A. 2 → 5 → 6 → 1 → 3 → 4

B. 2 → 4 → 5 → 3 → 6 → 1

C. 2 → 1 → 5 → 6 → 4 → 3

D. 1 → 2 → 3 → 4 → 5 → 6

Question #256

Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

A. DDoS attack

B. Evil twin attack

C. DNS cache flooding

D. MAC flooding

Question #257

What is the following command used for?

```
sqlmap.py -u "http://10.10.1.20/?p=1&forumaction=search" -dbs
```

A. Retrieving SQL statements being executed on the database

B. Creating backdoors using SQL injection

C. Enumerating the databases in the DBMS for the URL

D. Searching database statements at the IP address given

Question #258

Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.

What is the security model implemented by Jane to secure corporate messages?

A. Zero trust network

B. Secure Socket Layer (SSL)

C. Transport Layer Security (TLS)

D. Web of trust (WOT)

Question #259

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands.

Which of the following commands was used by Clark to hijack the connections?

A. btlejack -f 0x9c68fd30 -t -m 0x1fffffffff

B. btlejack -c any

C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

D. btlejack -f 0x129f3244 -j

Question #260

John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials.

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

A. IoT Inspector

B. AT&T IoT Platform

C. IoTSeeker

D. Azure IoT Central

Question #261

To hide the file on a Linux system, you have to start the filename with a specific character.

What is the character?

A. Tilde (~)

B. Underscore (_)

C. Period (.)

D. Exclamation mark (!)

Question #262

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.

Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

A. CAST-128

B. RC5

C. TEA

D. Serpent

Question #263

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering

B. App sandboxing

C. Jailbreaking

D. Social engineering

Question #264

Mirai malware targets IoT devices.

After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

A. MITM attack

B. Password attack

C. Birthday attack

D. DDoS attack

Question #265

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company.

Which information security standard is most applicable to his role?

A. FISMA

B. Sarbanes-Oxley Act

C. HITECH

D. PCI-DSS

Question #266

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

A. Kube-apiserver

B. Etcd cluster

C. Kube-controller-manager

D. Kube-scheduler

Question #267

According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

A. Cloud connector

B. Cloud broker

C. Cloud provider

D. Cloud carrier

Question #268

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network.

What is this hacking process known as?

A. Wardriving

B. Spectrum analysis

C. Wireless sniffing

D. GPS mapping

Question #269

Which among the following is the best example of the third step (delivery) in the cyber kill chain?

A. An intruder creates malware to be used as a malicious attachment to an email.

B. An intruder's malware is triggered when a target opens a malicious email attachment.

C. An intruder's malware is installed on a targets machine.

D. An intruder sends a malicious attachment via email to a target.

Question #270

Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering. Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. User impersonation

B. Insecure transmission of credentials

C. Password reset mechanism

D. Verbose failure messages

Question #271

Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WS-Work Processes

B. WS-Security

C. WS-Policy

D. WSDL

Question #272

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

A. Bluetooth

B. WPA2-Enterprise

C. WPA3-Personal

D. ZigBee

Question #273

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

A. PGP

B. SMTP

C. GPG

D. S/MIME

Question #274

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

A. Operational threat intelligence

B. Strategic threat intelligence

C. Tactical threat intelligence

D. Technical threat intelligence

Question #275

This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information.

What type of attack is this?

A. Union SQL injection

B. Error-based SQL injection

C. Time-based SQL injection

D. Blind SQL injection

Question #276

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.

What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"

B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."

C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

Question #277

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

A. Strategic threat intelligence

B. Operational threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Question #278

Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. Union SQL injection

B. Error-based injection

C. Blind SQL injection

D. Boolean-based blind SQL injection

Question #279

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

A. FISMA

B. PCI-DSS

C. SOX

D. ISO/IEC 27001:2013

Question #280

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

```
<!DOCTYPE blah [ < !ENTITY trustme SYSTEM "file:///etc/passwd" > ] >
```

A. SQLi

B. XXE

C. XXS

D. IDOR

Question #281

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

A. A list of all mail proxy server addresses used by the targeted host.

B. The internal command RCPT provides a list of ports open to message traffic.

C. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.

D. Reveals the daily outgoing message limits before mailboxes are locked.

Question #282

When considering how an attacker may exploit a web server, what is web server footprinting?

A. When an attacker creates a complete profile of the site's external links and file structures

B. When an attacker uses a brute-force attack to crack a web-server password

C. When an attacker implements a vulnerability scanner to identity weaknesses

D. When an attacker gathers system-level data, including account details and server names

Question #283

An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages.

What is the attack performed in the above scenario?

A. Cache-based attack

B. Timing-based attack

C. Downgrade security attack

D. Side-channel attack

Question #284

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.

What is the framework used by James to conduct footprinting and reconnaissance activities?

A. OSINT framework

B. WebSploit Framework

C. Browser Exploitation Framework

D. SpeedPhish Framework

Question #285

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders

B. Using wget to perform banner grabbing on the webserver

C. Flooding the web server with requests to perform a DoS attack

D. Downloading all the contents of the web page locally for further examination

Question #286

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 -

Window Size: 5840 -

What the OS running on the target machine?

A. Windows OS

B. Mac OS

C. Linux OS

D. Solaris OS

Question #287

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files.

What is the type of injection attack Calvin's web application is susceptible to?

A. CRLF injection

B. Server-side template injection

C. Server-side JS injection

D. Server-side includes injection

Question #288

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

A. Infoga

B. NCollector Studio

C. Netsparker

D. WebCopier Pro

Question #289

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components.

What is the attack technique used by Stephen to damage the industrial systems?

A. HMI-based attack

B. SMishing attack

C. Reconnaissance attack

D. Spear-phishing attack

Question #290

In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.

What is the tool used by Hailey for gathering a list of words from the target website?

A. CeWL

B. Orbot

C. Shadowsocks

D. Psiphon

Question #291

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept steal, modify, and block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

A. Wireshark

B. BetterCAP

C. DerpNSpoof

D. Gobbler

Question #292

George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities.

Which of the following anonymizers helps George hide his activities?

A. https://www.baidu.com

B. https://www.guardster.com

C. https://www.wolframalpha.com

D. https://karmadecay.com

Question #293

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

A. Key stretching

B. Public key infrastructure

C. Key derivation function

D. Key reinstallation

Question #294

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages.

What is the type of spyware that Jake used to infect the target device?

A. DroidSheep

B. Androrat

C. Trident

D. Zscaler

Question #295

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

A. Frequency/voltage tampering

B. Optical, electromagnetic fault injection (EMFI)

C. Temperature attack

D. Power/clock/reset glitching

Question #296

Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy.

What is the type of attack Bob performed on Kate in the above scenario?

A. SIM card attack

B. aLTEr attack

C. Spearphone attack

D. Man-in-the-disk attack

Question #297

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

Which of the following techniques is employed by Dayn to detect honeypots?

A. Detecting honeypots running on VMware

B. Detecting the presence of Snort_inline honeypots

C. Detecting the presence of Honeyd honeypots

D. Detecting the presence of Sebek-based honeypots

Question #298

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash

B. net view

C. macof

D. ntptrace

Question #299

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

A. Key archival

B. Certificate rollover

C. Key escrow

D. Key renewal

Question #300

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

A. Secure development lifecycle

B. Security awareness training

C. Vendor risk management

D. Patch management

Question #301

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system

A. Worm

B. Rootkit

C. Adware

D. Trojan

Question #302

Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Question #303

Which Nmap switch helps evade IDS or firewalls?

A. -D

B. -n/-R

C. -T

D. -oN/-oX/-oG

Question #304

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .stm

B. .cms

C. .rss

D. .html

Question #305

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 × 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key (Km1) and a rotation key (Kr1) for performing its functions.

What is the algorithm employed by Harper to secure the email messages?

A. CAST-128

B. AES

C. GOST block cipher

D. DES

Question #306

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

A. No ABAC validation

B. Business logic flaws

C. Improper use of CORS

D. Code injections

Question #307

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

A. Website footprinting

B. Dark web footprinting

C. VPN footprinting

D. VoIP footprinting

Question #308

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

A. Cloudborne attack

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

C. Metadata spoofing attack

D. Cloud cryptojacking

Question #309

Which of the following tactics uses malicious code to redirect users' web traffic?

A. Spear-phishing

B. Phishing

C. Spimming

D. Pharming