C. Availability
D. Authentication

8. MD5 produces hash value of:

A. 64-bit
B. 128-bit C. 256-bit D. 5 12-bit

9. A Cryptographic Attack type where a cryptanalyst has access to a ciphertext but does not have access to the corresponding plaintext is called: A. Ciphertext Only Attack
B. Chosen Plaintext Attack
C. Adaptive Chosen Ciphertext Attack
D. Rubber Hose Attack

10. The most secure way to mitigate information theft from a laptop of an organization left in a public place is:
1. Use a strong login password
2. Hard Drive Encryption
3. Set a BIOS password
4. Back up

Answers

Chapter 1: Introduction to Ethical Hacking

1. B
Ethical Hackers always require legal permission.
2. B
Gray Box is a type of penetration testing, in which the pentester is provided with very limited prior knowledge of the system or any information on targets
3. C
White Hat Hackers always have legal permission to perform penetration testing against a target system.
4. C
Hacktivists draw the attention to target to deliver a message or promote an agenda.
5. A
Script Kiddies have no or very low knowledge about hacking.
6. C
White Box testing requires complete knowledge of a target.
7. D

Suicide Hackers are those who aim for destruction without worrying about punishment.
8. B & C
Penetration testing is required in an environment to perform an audit, find vulnerabilities and exploit them to address them before an attacker reaches them.
9. B
Gray Hats are those who work for both, offensively and defensively.
10. B
A vulnerability assessment is a process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

11. A
The Black Box is a type of penetration testing, in which the pentester is blind testing, or doubleblind testing, i.e. the pentester is provided with no prior knowledge of the system or any information of the target.
12. D
TOE stands for Target of Evaluation.

The vulnerability is a weak point or loophole in any system or network, which can be exploited by an attacker.

Chapter 2: Footprinting & Reconnaissance

1. A
Active and passive methods of reconnaissance are also popular for gaining information of target directly or indirectly. The overall purpose of this phase is to keep interaction with the target to gain information without any detection or alerting.
2. A
Footprinting is the basically the collection of every possible information regarding the target and target network.
3. A
Social Engineering in Information Security refers to the technique of psychological manipulation. This trick is used to gather information from directly or indirectly interfering human beings. 4. B
There is some advanced option that can be used to search for a specific topic using search engines. These advance search operators make the searching more appropriate and focused on a certain topic.
5. C
Wayback Machine is used to store/archive web pages so that you can look through them again later.
6. A
These websites gather information and reports of companies including legal news, press releases, financial information, analysis reports, and upcoming projects and plans as well. 7. A
DNS Record Type “A” refers Host IP Address.
8. B
DNS Record Type “A” refers Host IP Address, “MX” refers Domain’s Mail Server, “NS” refers Host’s Name Server and “SRV” reveals Service Records information.

9. D
Recong0-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features.
10. B
Website Footprinting includes monitoring and investigating about the target organization's official website for gaining information such as Software running, versions of these software's, operating systems, Sub-directories, database, scripting information, and other details. This information can be gathered by online service, as defined earlier, like netcraft.com or by using software such as Burp Suite, Zaproxy, Website Informer, Firebug, and others.
11. A
"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. WHOIS database is maintained by Regional Internet Registries (RIR).

Chapter 3: Scanning Networks

1. B
TCP is connection oriented. Once a connection is established, data can be sent bidirectionally. UDP is a simpler, connectionless internet protocol. Multiple messages are sent as packets in chunks using UDP. Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP packets.

2. A
There is three-way handshaking that is performed while establishing a TCP connection between hosts. This handshaking ensures successful, reliable and connection-oriented session between these hosts.
3. C & D
Telnet, nmap, Curl, Netcat are the tools that are popularly used for banner grabbing.
4. A
Proxy server anonymizes the web traffic to provide anonymity. When a user sends a request for any resources to the other publically available servers, proxy server acts as an intermediary for these requests.
5. A
Nmap in a nutshell, offers Host discovery, Port discovery, Service discovery, Operating System version information, Hardware (MAC) address information, Service version detection, Vulnerability & exploit detection.
6. D
TCP Flags includes SYN, ACK, URG, PSH, FIN & RST.
7. A
Consider Host A wants to communicate with Host B. TCP Connection will establish when host A sends a Sync packet to host B. Host B upon receipt of Sync packet from Host A, replies to Host A with Sync+Ack packet. Host A will reply with Ack packet when it receives Sync+Ack packet from Host B. After successful handshaking, TCP connection will be established.
8. B
Ping Sweep is a method of sending ICMP Echo Request packets to a range of IP

addresses instead of sending one by one requests and observing the response.
9. A
Full Open Scan is the type of Scanning technique, in which TCP Three-way handshaking session is initiated and completed.
10. A
Inverse TCP Flag Scanning is the scanning process, in which sender either send TCP probe with TCP flags, i.e. FIN, URG, and PSH, or without Flags. If TCP Flags are set, it is known as XMAS Scanning. In case, if there is no flag set, it is known as Null Scanning.

Chapter 4: Enumeration

1. A
In the phase of Enumeration, an attacker initiates active connections with the target system. Using this active connection, direct queries are generated to gain more information. These information help to identify the system attack points. Once attacker discovers attack points, it can gain unauthorized access using this collected information to reach assets.

2. A
NetBIOS is Network Basic Input / Output System program that allows the communication in between different applications running on different systems within a local area network.

Port Information is revealed in scanning phase.
4. A
Explanation is given in the table below.

5. B
Explanation is given in the table below.

Option	Description
-a	With hostname, displays the NetBIOS name table and MAC address information
-A	With IP Address, displays the NetBIOS name table and MAC address information
-c	NetBIOS name cache information
-n	Displays the names registered locally by NetBIOS applications such as the server and redirector

6. D
Wireshark is not an example of SNMP Manager software. Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit and educational organizations.

7. B
There is no support for encryption in version 1 & 2c. SNMPv3 supports both encryption (DES) and hashing (MD5 or SHA).
8. B
SNMPv3 supports for both encryption (DES) and hashing (MD5 or SHA). Implementation of version 3 has three models. NoAuthNoPriv means no encryption and hashing will be used. AuthNoPriv means only MD5 or SHA based hashing will be used. AuthPriv means both encryption and hashing will be used for SNMP traffic.
9. A
NetBIOS service uses TCP port 139. NetBIOS over TCP (NetBT) uses the following TCP and UDP ports:

- UDP port 137 (name services)
- UDP port 138 (datagram services)
- TCP port 139 (session services)

10. B
NTP version 3 (NTPv3), and later versions support a cryptographic authentication technique between NTP peers.

Chapter 5: Vulnerability Analysis

1. B
Vulnerability assessment includes discovering weaknesses in an environment, design flaws and other security concerns, which can cause an Operating System, application or website to be misused. These vulnerabilities include misconfigurations, default configurations, buffer overflows, Operating System flaws, Open Services, and others. There are different tools available for network administrators and pentesters to scan for vulnerabilities in a network.
2. A

Creating Baseline is a pre-assessment phase of vulnerability assessment life-cycle in which pentester or network administrator who is performing assessment identifies the nature of corporate network, the applications and services. The pentester creates an inventory to all resources and assets, which helps to manage, prioritize the assessment. furthermore, he/she also maps the infrastructure, learns about the security controls, policies, and standards followed by the organization.
3. E

Risk Assessment includes scoping these identified vulnerabilities and their impact on the corporate network or on an organization. Similarly, remediation, verification and monitoring are the phase performed after Vulnerability Assessment.
4. C
Tree-based assessment is the assessment approach in which auditor follows different strategies for each component of an environment. For example, consider a scenario of an organization's network where different machines are live, the auditor may use an approach for Windows-based machines whereas another technique for Linux based servers.

5. D
Inference-based assessment is another approach to assist depending on the inventory of protocols in an environment. For example, if an auditor found a protocol, using inference based assessment approach, the auditor will investigate for ports and services related to that protocol. 6. C
The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.
7. C
U.S. National Vulnerability Database (NVD) was launched by National Institute of Standards and Technology (NIST).

8. D

Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit and educational organizations. It is a free, open source tool available for Windows, Linux, MAC, BSD, Solaris and other platforms natively.

Chapter 6: System Hacking

1. D
Non-Electronic Attacks or Nontechnical Attacks are the attacks, which do not require any technical understanding and knowledge. This is the type of attack that can be done by shoulder surfing, social engineering, and dumpster diving.

2. B
In Dictionary Attack, to perform password cracking, a password cracking application is used along with a dictionary file. This dictionary file contains entire dictionary or list of known & common words to attempt password recovery. This is the simplest type of password cracking. Usually,

systems are not vulnerable to dictionary attacks if they use strong, unique and alphanumeric passwords.
3. A
Brute Force Attack attempts to recover the password by trying every possible combination of characters. Each combination pattern is attempted until the password is accepted. Brute forcing is the common, and basic technique to uncover password.
4. D
Password Salting is the process of adding additional character in the password to one-way function. This addition of characters makes the password more difficult to reverse the hash. Major advantage or primary function of password salting is to defeat the dictionary attacks and precomputed attacks.
5. C
Metasploit Framework enables you to automate the process of discovery and

exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

6. A
Every possible combination of character is computed for the hash to create a rainbow table. When a rainbow table contains all possible pre-computed hashes, attacker captures the password hash of target and compares it with the rainbow table.
7. C
Password Salting is the process of adding additional character in the password to make it a oneway function. This addition of characters makes the password more difficult to reverse the hash. Major advantage or primary function of password salting is to defeat the dictionary attacks and pre-computed attacks.

Chapter 7: Malware Threats

1. B
Malware is abbreviated from the term Malicious Software. The term malware is an umbrella term, which defines a wide variety of potentially harmful software. This malicious software is specially designed for gaining access to target machines, stealing information and harming the target system.
2. D
The virus is a self-replicating program; it is capable of producing multiple copies of itself by attaching with another program of any format. These viruses can be executed as soon as they are downloaded, it may wait for the host to execute them as well as be in sleep for a predetermined time. The major characteristics of viruses are:

■ Infecting other files
■ Alteration of data
■ Transformation
■ Corruption
■ Encryption
■ Self-Replication

3. B
Static Analysis or Code Analysis is performed by fragmenting the resources of the binary file without executing it and studying each component. Disassembler such as IDA is used to disassemble the binary file.
4. B
Dynamic Analysis or Behavioral Analysis is performed by executing the malware on a host and observing the behavior of the malware. These behavioral analyses are performed in a Sandbox environment.
5. D
Trojan Deployment includes the following steps:

i. Create a Trojan using Trojan Construction Kit.
ii. Create a Dropper.
iii. Create a Wrapper.

iv. Propagate the Trojan.
v. Execute the Dropper.

6. C

The basic purpose of Crypter is it encrypt, obfuscate, and manipulate the malware and malicious programs. By using Crypter for hiding a malicious program, it becomes even more difficult for security programs such as anti-viruses to detect.

7. B

Wrapper is a non-malicious file that binds the malicious file to propagate the Trojan. It binds a malicious file to create and propagate the Trojan along with it to avoid detection. 8. A

A dropper is a software or program that is specially designed for delivering a payload on the target machine.

Chapter 8: Sniffing

1. C

In the process of Sniffing, an attacker gets connected to the target network to sniff the packets. Using Sniffers, which turns Network Interface Card (NIC) of the attacker's system into promiscuous mode, attacker captures the packet. Promiscuous mode is a mode of the interface, in which NIC responds for every packet it receives.

2. B

Passive Sniffing is the sniffing type, in which there is no need of sending additional packets or interfering the device such as hub to receive packets. As we know, hub broadcasts every packet to its ports, which helps the attacker to monitor all traffic passing through hub without any effort. 3. A

SPAN makes a copy of all frames destined for a port and copies them to the SPAN destination port. 4. A

Lawful Interception (LI) is a process of wiretapping with legal authorization, which allows law enforcement agencies to selectively wiretap the communication of individual user.

5. C

DAI is used with DHCP snooping, IP-to-MAC bindings can be a track from DHCP transactions to protect against ARP poisoning (which is an attacker trying to get your traffic instead of to your destination). DHCP snooping is required to build the MAC-to-IP bindings for DAI validation. 6. C

Following are the filters of Wireshark to filter the output:

Operator ==
eq
!=

ne
contains

Function

Equal
Equal
Not equal
Not equal
Contains specified value

Example

ip.addr == 192. 168. 1. 1
tcp.port eq 23
ip.addr != 192. 168. 1. 1
it.src ne 192. 168. 1. 1
http contains "http://www.ipspecialist.net"

Chapter 9: Social Engineering

1. C
4. A
Distributed Reflection Denial of Service Attack is the type of DoS attack, in which intermediary and Secondary victims are also involved in the process of launching a DoS attack. Attacker sends requests to the intermediary victim, which redirects the traffic towards the secondary victim. Secondary victim redirects the traffic toward the target. Involvement of intermediary and secondary victims is for spoofing the attack.
5. C
The attacker first collects the information about a large number of potentially vulnerable machines to create a Hit-list. Using this technique, the attacker finds the vulnerable machine and infects it. Once a machine is infected, the list is divided by assigning half of the list to the newly compromised system. The scanning process in Hit-list scanning runs simultaneously. This technique is used to ensure the spreading and installation of malicious code in a short period.
6. C
Infected machine probes IP addresses randomly form IP address space and scans them for vulnerability. When it finds a vulnerable machine, it breaks into it and infects it with the script that was used to infect itself. Random scanning technique spreads the infection very quickly as it compromises a large number of the host.
7. B
In the process of Autonomous Propagation, the attacker exploits and sends malicious code to the vulnerable system. The toolkit is installed and searches for other vulnerable systems. Unlike Central Source Propagation, it does not require any Central Source or planting toolkit on its own system.

8. A
Back-Chaining Propagation requires attack toolkit installed on attacker's machine. When an attacker exploits the vulnerable machine, it opens the connection on the infected system listening for file transfer. Then, the toolkit is copied from the attacker. Once toolkit is installed on the infected system, it will search for other vulnerable system and the process continuous.
9. B
Wavelet-based Signal Analysis is an automated process of detecting DoS/DDoS attacks by analysis of input signals. This automated detection is used to detect volume based anomalies. Wavelet analysis evaluates the traffic and filter on a certain scale whereas Adaptive threshold techniques are used to detect DoS attacks.
10. A
Change-Point detection is an algorithm, which is used to detect Denial-of-Service (DoS) attacks. This Detection technique uses non-parametric Cumulative Sum (CUSUM) algorithm to detect traffic patterns.

Phishing process is a technique in which fake email, which looks like legitimate email is sent to a target host. When the recipient opens the link, he is enticed for providing information. 2. A
Social Engineering is an act of stealing information from humans. As it does not have any interaction with target system or network, it is considered as a non-technical attack. 3. D
Human-based Social Engineering includes one-to-one interaction with the target. Social Engineer gathers sensitive information by tricking such as ensuring the trust, taking advantage of habits, behavior and moral obligation.
4. A
Insider attack includes attacks performed by an employee of an organization, which has been paid for it to do so by the competitor or attacker, or a disgruntled employee.
5. A
Spam Filtering is necessary to step to avoid phishing emails, which reduces the threat of unintentional clicking on spam emails.
6. B
Piggybacking is the technique, in which an unauthorized person waits for an authorized person to gain entry in a restricted area.
7. A
Tailgating is the technique, in which an unauthorized person gains access to the restricted area by following the authorized person.

Chapter 10: Denial-of-Service

1. A
Denial-of-Service (DoS) is a type of attack, in which service offered by a system or a network is denied. Services may be denied, reducing the functionality or preventing the access to the resources even to the legitimate users.
2. B

Service Request Flood is a DoS attack, in which attacker flood the request towards a service such as Web application or Web server until all the services are overloaded.
3. C
The Permanent Denial-of-Service Attack is the DoS attack, which instead of focusing on denial of services, focuses on hardware sabotage. Affected hardware by PDoS attack is damaged and requires replacement or reinstallation of hardware. PDoS is performed by a method known as "Phlashing" that causes irreversible damage to the hardware, or "Bricking a system" by sending fraudulent hardware updates.
11. B
Botnet Defensive technique includes using RFC 3704 filtering. RFC 3704 is designed for Ingress filtering for multi-homed networks to limit the DDoS attacks. It denies the traffic with a spoofed address to access the network and ensure the trace to its source address.
12. C
Black Hole Filtering is a process of silently dropping the traffic (either incoming or outgoing traffic) so that the source is not notified about discarding of the packet.

Chapter 1 1: Session Hijacking

1. B
In Session Hijacking, the attacker intercepts the session and takes over the legitimate authenticated session. When a session authentication process is complete, and the user is authorized to use resources such as web services, TCP communication or other, the attacker takes

advantage of this authenticated session and places himself in between the authenticated user and the host.

2. D
SQL Injection Attacks uses SQL websites or web applications. It relies on the strategic injection of malicious code or script into existing queries.
3. A
Source Routing is a technique of sending the packet via selected route. In session hijacking, this technique is used to attempt IP spoofing as a legitimate host with the help of source routing to direct the traffic through the path identical to the victim's path.
4. A
To understand the Session Fixation Attack, assume an attacker, victim, and the web server; Attacker initiates a legitimate connection with the web server, issues a session ID or uses a new session ID. The attacker then sends the link to the victim with the established session ID for bypassing the authentication. When the user clicks the link and attempts to log into the website, web server continues the session as it is already established and authentication is performed.

Chapter 12: Evading IDS, Firewalls & Honeypots

1. D
Host-based IPS/IDS is normally deployed for the protection of specific host machine, and it works strictly with the Operating System Kernel of the host machine.
2. B
Bastion Host is a computer system that is placed in between public and private network. It is intended to be the crossing point where all traffic is passed through. Certain roles and responsibilities are assigned to this computer to perform.
3. B
An example of next-generation firewalls is Cisco ASA series with FirePOWER services. NGFW provides complete visibility into network traffic users, mobile devices, Virtual Machine (VM) to VM data communication, etc.
4. A
Honeypots are the devices or system that are deployed to trap attackers attempting to gain unauthorized access to the system or network as they are deployed in an isolated environment and being monitored. Typically, honeypots are deployed in DMZ and configured identically to a server. 5. D
Bandwidth and Volumetric Attacks are not appropriate to evade IPS/IDS. These attacks can be easily detected as IDS is constantly monitoring the anomaly and behavior of the network traffic.

6. B
Fragmentation is the process of splitting the packet into fragments. This technique is usually adopted when IDS and Host device is configured with different timeouts. For example, an IDS is configured with 10 Seconds of timeout whereas host is configured with 20 seconds of a timeout. Sending packets with 15 sec delay will bypass reassembly at IDS and reassemble at the host.

Chapter 13: Hacking Web Servers

1. D
Internet Information Services is an extensible web server created by Microsoft to used with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP. 2. C
Directory Traversal Attack is a type of attack, in which an attacker attempts using trial and error method to access restricted directories by applying dots and slash sequences. By accessing the directories outside the root directory, the attacker can reveal sensitive information about the system.
3. B
HTTP Response Splitting Attack the technique, in which an attacker sends response splitting request to the server. By this way, an attacker can add the header response, in result, the server

will split the response into two responses. The second response is under control of the attacker so that user can be redirected to the malicious website.

4. A
A hotfix is referred to a hot system, specially designed for a live production environment where fixes have been made outside a normal development and testing

to address the issue. 5. B
Patches are the pieces of software that is specially designed for fixing the issue. 6. A
The Microsoft Baseline Security Analyzer is a Windows-based Patch management tool powered by Microsoft. MBSA identifies the missing security updates and common security misconfigurations.

Chapter 14: Hacking Web Applications

1. C
Application Administrator is responsible for the management and configuration required for the web application. It ensures the availability and high performance of the web application. 2. B
CSS frameworks provide a basic structure for designing consistent solutions to tackle common recurring issues across front-end web development.
3. D
Server-side languages include Ruby on Rails, PHP, C#, Python and other languages.
4. A,B,C
The web application is working on the following layers:

■ *Presentation Layer:* Presentation Layer is responsible for displaying and presenting the information to the user on the client end
■ *Logic Layer:* Logic Layer is used to transform, query, edit, and otherwise manipulate information to and from the forms
■ *Data Layer:* Data Layer is responsible for holding the data and information for the application as a whole
5. B
Attacker by accessing the web application using low privilege account, can escalate the privileges
to access sensitive information. Different techniques are used such as URL, POST data, Query
string, cookies, parameter tampering, HTTP header, etc. to escalate privileges.

6. D
Canonicalization (sometimes standardization or normalization) is a process for converting data that has more than one possible representation into a "standard," "normal", or canonical form.

Chapter 15: SQL Injection

1. B
In an Inferential SQL Injection, no data is transferred from a web application; the i.e. attacker is unable to see the result of an attack hence referred as a Blind Injection.
2. A
In-Band SQL Injection is a category, which includes injection techniques using same communication channel to launch the injection attack and gather information from the response. 3. B
The SELECT statement is used to select data from a database. The data returned is

stored in a result table, called the result-set.
4. D
The UPDATE statement is used to modify the existing records in a table.

5. B
SELECT [column 1, column2, ...] FROM [table_name] Here, column 1, column2, ... are the field names of the table you want to select data from. If you want to select UserID field available in the table "Employees", use the following syntax:
SELECT *UserID* FROM *Employees*

6. B
SQL is a standard language for accessing and manipulating databases. SQL stands for Structured Query Language.

Chapter 16: Hacking Wireless Networks

1. A
Service Set Identifier (SSID) is the name of an Access Point. Technically, SSID is a token, that is used to identify 802. 1 1 networks (Wi-Fi) of 32 bytes. The Wi-Fi network broadcasts the SSID

continuously (if enabled). This broadcasting is basically intended for identification and presence of a wireless network.

2. C
Open System Authentication process requires six frame communication between client and the responder to complete the process of authentication.
3. A
Shared Key authentication mode requires four frames to complete the process of authentication. 4. D
IEEE 802. 1x is focused solution for WLAN framework offering Central Authentication. IEEE 802. 1x is deployed with Extensible Authentication Protocol (EAP) as WLAN Security Solution. 5. A
Omnidirectional antennas are those antennas that radiate uniformly in all directions. The radiation pattern is often described as Doughnut shaped. Most common use of omnidirectional antennas is in radio broadcasting, cell phone, and GPS. Types of the omnidirectional antenna includes Dipole Antenna and Rubber Ducky Antenna.
6. A
WEP uses 24-bit Initialization Vector (IV) to create a stream cipher RC4 with Cyclic Redundant Check (CRC) to ensure confidentiality and integrity. Standard 64-bit WEP uses the 40-bit key, 128- bit WEP uses 104-bit key & 256-bit WEP uses a 232-bit key. Authentications used with WEP are Open System Authentication and Shared Key Authentication.
7. B
Temporal Key Integrity Protocol (TKIP) ensures per packet key by dynamically generating a new key for each packet of 128-bit to prevent a threat that is vulnerable to WEP.

8. D

BlueSmack is the type of DoS attack for Bluetooth. In BlueSmacking, the target device is overflowed by the random packets. Ping of death is used to launch this Bluetooth attack, flooding a large number of echo packets causes DoS.

9. A
BlueBugging is another type of Bluetooth attack, in which an attacker exploits a Bluetooth device to gain access and compromise its security. BlueBugging is a technique to remotely access the Bluetooth enabled device.
10. C
Airpcap is a Windows-based 802. 1 1 Wireless Traffic Capture device that fully integrates with Wireshark. It delivers information about wireless protocols and radio signals, enabling the capture and analysis of low-level 802. 1 1 wireless traffic including control frames, management frames, and power information in the Wireshark UI. Once AirPcap is installed, Wireshark displays a special toolbar that provides direct control of the AirPcap adapter during wireless data capture. 11. D

Wireless Intrusion Prevention System (WIPS) is a network device for wireless networks. It monitors the wireless network, protects it against unauthorized access points and performs automatic intrusion prevention. By monitoring the radio spectrum, it prevents rogue access points and generates alerts for network administrator about detection.

Chapter 17: Hacking Mobile Platforms

1. A
Jailbreaking allows the root access to an iOS device, which allows downloading unofficial applications. Jailbreaking is popular for removing restrictions, installation of additional software, malware injection, and software piracy.
2. A
In Tethered Jailbreaking, when the iOS device is rebooted, it will no longer have a patched kernel.

It may be stuck in a partially started state. With Tethered Jailbreaking, a computer is required to boot the device each time; i.e. the device is re-jailbroken each time. Using Jailbreaking tool, the device is started with the patched kernel.

3. B
Blackberry App world is official application distribution service.
4. A
The basic purpose of implementing Mobile Device Management (MDM) is deployment, maintenance, and monitoring of mobile devices that make up BYOD solution. Devices may include the laptops, smartphones, tablets, notebooks or any other electronic device that can be moved outside the corporate office to home or some public place and then gets connected to corporate office by some means.

Chapter 18: IoT Hacking

1. B

The architecture of IoT depends upon five layers, which are as follows:

I. Application Layer
II. Middleware Layer
III. Internet Layer
IV. Access Gateway Layer

V. Edge Technology Layer

2. A

Middleware Layer is for device and information management.

3. C

Access Gateway Layer is responsible for protocol translation and messaging.

4. B

Device-to-Cloud Model is another model of IoT device communication, in which IoT devices are directly communicating with the application server.

5. A

Rolling code or Code hopping is another technique to exploit. In this technique, attackers capture the code, sequence or signal coming from transmitter devices along with simultaneously blocking the receiver to receive the signal. This captured code will be later used to gain unauthorized access.

Chapter 19: Cloud Computing

1. A

Infrastructure-as-a-Services, (IaaS) also known as Cloud infrastructure service is a self-service model. IaaS is used for accessing, monitoring and managing purpose. For example, instead of purchasing additional hardware such as firewall, networking devices, server and spending money for deployment, management, and maintenance, IaaS model offers cloud-based infrastructure to deploy remote data centers.

2. A

Software-as-a-Service (SaaS) is one of the most popular types of Cloud Computing Service that is most widely used. On-demand software is centrally hosted to be accessible by users using client via browsers. An example of SaaS is office software such as office 365, Cisco WebEx, Citrix GoToMeeting, Google Apps, messaging software, DBMS, CAD, ERP, HRM, etc.

3. D

Community Clouds are accessed by multiple parties having common goals and shared resources.

4. D

Cloud Consumer uses service from Cloud Providers.

5. B

Cloud Broker is an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Chapter 20: Cryptography

1. A
Being the oldest and most widely used technique in the domain of cryptography, Symmetric Ciphers use the same secret key for the encryption and decryption of data.

2. A
Being the oldest and most widely used technique in the domain of cryptography, Symmetric Ciphers use the same secret key for the encryption and decryption of data. Most widely used symmetric ciphers are AES and DES.
3. B
Stream Cipher is a type of symmetric key cipher that encrypts the plain text one by one. 4. A
DES algorithm consists of 16 rounds, processing the data with the 16 intermediary round keys of 48-bit generated from 56-bit cipher key by a Round Key Generator. Similarly, DES reverse cipher computes the data in clear text format from cipher text using the same cipher key. 5. A
Subject field represents Certificate holder's name.

6. C
RSA key length varies from 5 12 to 2048 with 1024 being the preferred one.
7. B

The message digested is the cryptographic hashing technique that is used to ensure the integrity of a message.

8. B
The MD5 algorithm is one from the message digest series. MD5 produces a 128-bit hash value that is used as a checksum to verify the integrity.
9. A
A Ciphertext Only Attack is a cryptographic attack type where a cryptanalyst has access to a ciphertext but does not have access to the corresponding plaintext. The attacker attempts to extract the plain text or key by recovering plain text messages as much as possible to guess the key. Once the attacker has the encryption key, he/she can decrypt all messages.
10. B
Disk Encryption refers to the encryption of disk to secure files and directories by converting into an encrypted format. Disk encryption encrypts every bit on disk to prevent unauthorized access to data storage.

Acronyms

- AAA Authentication, Authorization & Accounting
- ACK Acknowledgement
- ACL Access Control List
- AD Active Directory
- ADS Alternate Data Streams
- AES Advanced Encryption Standard
- AP Access Point
- API Application Programming Interface
- AppSec Application Security
- APT Advanced Persistent Threat
- ARP Address Resolution Protocol
- AS Authentication Server
- ASA Adaptive Security Appliance
- ASCII American Standard Code for Information Interchange • ASR Aggregation Services Router
- ATM Asynchronous Transfer Mode
- BC Business Continuity
- BCP Business Continuity Planning
- BER Basic Encoding Rules
- BGP Border Gateway Protocol
- BIA Business Impact Analysis
- BLE Bluetooth Low Energy
- BSSID Basic Service Set Identifier
- C&A Certification and Accreditation
- C&C Command and Control
- CA Certificate Authority
- CAM Content-Addressable Memory
- CC Common Criteria
- CCIE Cisco Certified Internetworking Expert
- CCMP Counter Mode Cipher Block Chaining Message Authentication Code Protocol
- CDDI Copper DDI
- CEH Certified Ethical Hacker
- CHFI Computer Hacking Forensics Investigator
- CIA Confidentiality Integrity Availability
- CISSP Certified Information Systems Security Professional • CMF Content Management Framework

- CMM Capability Maturity Model
- COBIT Control Objectives for Information and related Technology • CRC Cyclic Redundant Check
- CSA Control Self-Assessment
- CSO Chief Security Officer
- CSPP Connection String Parameters Pollution
- CSRF Cross-Site Request Forgery
- CUE Continuing Education Units
- CUSUM Cumulative Sum
- CVE Common Vulnerabilities and Exposures
- CVSS Common Vulnerability Scoring Systems
- CWS Cloud Web Security
- DAC Discretionary Access Control
- DAI Dynamic ARP Inspection
- DCOM Distributed Component Object Model
- DES Data Encryption Standard
- DHCP Dynamic Host Configuration Protocol
- DLL Dynamic Link Libraries
- DLP Data Loss Prevention
- DMCA Digital Millennium Copyright Act
- DMZ Demilitarized Zone
- DNA Distributed Network Attack
- DNS Domain Name System
- DoDAF Department of Defense Architecture Framework • DoS Denial-of-Service
- DPI Deep Packet Inspection
- DR Disaster Recovery
- DRDoS Distributed Reflection Denial of Service
- DRP Disaster Recovery Plan
- DSA Digital Signature Algorithm
- DSA Directory System Agent
- EAL Evaluation Assurance Level
- EAP Extensible Authentication Protocol
- EBCDICM Extended Binary-Coded Decimal Interchange Mode • EC2 Elastic Cloud Compute
- EDI Electronic Data Interchange
- EISA Enterprise Information Security Architecture • EK Endorsement

Key

- E-PHI Electronic Protected Health Information
- ESCA EC-Council Certified Security Analyst
- FDDI Fiber Distributed Data Interface
- FEPRA Family Education Rights and Privacy Act • FHSS Frequency-hopping Spread Spectrum
- FINRA Financial Industry Regulatory Authority • FIPS Federal Information Processing Standard • FISMA Federal Information Security Management Act • FPP Fire Prevention Plan
- FTK Forensic Toolkit
- FTP File Transfer Protocol
- GCE Google Compute Engine
- GHDB Google Hacking Database
- GLBA Gramm-Leach-Bliley Act
- GRC Governance, Risk Management, and Compliance • GSM Global System for Mobile Communication • HBA Host Bus Adapters
- HDD Hard Disk Drives
- HFS Hierarchical File System
- HIDS Host-based Intrusion Detection System • HIPAA Health Insurance Portability and Accountability Act • HIPS Host-based Intrusion Prevention System • HMAC Hashed Message Authentication Code • HRU Harrison-Ruzzo-Ullman
- HSS Health and Human Services
- HSSI High-Speed Serial Interface
- HTTP Hyper Text Transfer Protocol
- IA Information Assurance
- IaaS Infrastructure-as-a-Service
- IAM Identity and Access Management
- IAO Information Asset Owner
- ICMP Internet Control Message Protocol
- ICS Industrial Control Systems
- ICT Information and Communication Technology • ICV Integrity Check Value
- IDS Intrusion Detection System
- IEC International Electro-Technical Commission • IGMP Internet Group Management Protocol • IIS Internet Information Services
- IKE Internet Key Exchange

- ILT Instructor-led Training
- IMAP Internet Message Access Protocol
- IoT Internet-of-Things
- IP Intellectual Property
- IP Internet Protocol
- IPR Intellectual Property Rights
- IPS Intrusion Prevention System
- IPSec Internet Protocol Security
- IPX Internetwork Packet Exchange
- IRP Incident Response Plan
- ISACA Information Systems Audit and Control Association
- ISAF Information Systems Security Assessment Framework
- ISDN Integrated Services Digital Network
- ISE Identity Service Engine
- ISM Information Security Management
- ISO International Organization for Standardization
- ISP Internet Service Provider
- ISR Integrated Services Router
- ITIL Information Technology Infrastructure Library
- ITSEC Information Technology Security Evaluation Criteria
- ITSM IT Service Management
- IV Initialization Vector
- JPEG Joint Photographic Experts Group
- JTFTI Joint Task Force Transformation Initiative
- KDC Key Distribution Center
- L2F Layer 2 Forwarding
- L2TP Layer 2 Tunneling Protocol
- LAN Local Area Network
- LDAP Lightweight Directory Access Protocol
- LI Lawful Interception
- Li-Fi Light Fidelity
- LOIC Low Orbit Ion Cannon
- LPF Line Print Daemon
- LPT License Penetration Tester
- LPWAN Low-Power Wide Area Networking (LPWAN)
- LSC Local Security Committee
- MAC Mandatory Access Control
- MAC Media Access Control
- MBR Master Boot Record

- MBSA Microsoft Baseline Security Analyzer
- MD5 Message Digest 5
- MDM Mobile Device Management
- MEC Multi-chassis Ether channel
- MIB Management Information Base
- MIC Message Integrity Check
- MIDI Musical Instrument Digital Interface
- MITM Man-in-the-middle
- MODAF Ministry of Defense Architecture Framework
- MPEG Moving Picture Experts Group
- MSDU MAC Service Data Unit
- NAT Network Address Translation
- NFC Near Field Communication
- NFS Network File System
- NGFW Next Generation firewalls
- NGIPS Next-Generation Intrusion Prevention System
- NIC Network Interface Card
- NIDS Network-based Intrusion Detection System
- NIST National Institute of Standards & Technology
- NNTP Network News Transport Protocol
- NSA National Security Agency
- NTLM NT LAN Manager
- NTP Network Time Protocol
- NVD National Vulnerability Database
- OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation • OEP Occupant Emergency Plan
- OFDM Orthogonal Frequency Division Multiplexing
- OPEX Operational Expense
- ORM Online Reputation Management
- OSA Open System Authentication
- OSHA Occupational Safety and Health Administration • OSI Open System Interconnection
- OSPF Open Shortest Path First
- OSSTMM Open Source Security Testing Methodology Manual • OTP One-Time Password
- OUI Organizationally Unique Identifier
- OUI Object Unique Identifier

• OWASP Open Web Application Security Project

• PaaS Platform-as-a-Service

• PACL Port Access Control List

• PASTA Process for Attack Simulation and Threat Analysis • PCI-DSS Payment Card Industry Data Security Standard

• PGP Pretty Good Privacy

• PII Personally Identifiable Information • PKI Public Key Infrastructure

• PLC Power-Line Communication

• PMK Pairwise Master key

• POP3 Post Office Protocol version 3

• PP Protection Profile

• PPP Point-to-Point Protocol

• PPTP Point-to-Point Tunneling Protocol • PRISM Planning Tool for Resource Integration • RAID Redundant Array of Inexpensive Disks • RARP Reverse Address Resolution Protocol • RAT Remote Access Trojans

• RFID Radio Frequency Identification

• RIP Routing Information Protocol

• RIR Regional Internet Registries

• RMF Risk Management Framework

• ROSI Return on Security Investment

• RoT Root of Trust

• RPC Remote Procedure Call

• RSA Rivest Shamir Adleman

• RST Reset

• RTBHF Remotely Triggered Black Hole Filtering • RTG Real Traffic Grabber

• SaaS Software-as-a-Service

• SAM Security Account Manager

• SAN Storage Area Network

• SC Security Committee

• SCA Security Control Assessment

• SCADA Supervisory Control and Data Acquisition • SCP Secure Copy Protocol

• SDLC Security Development Life Cycle

• SEC Security Exchange Commission

• SEI Software Engineering Institute

- SET Secure Electronic Transaction
- SFR Security Functional Requirements • SFTP SSH File Transfer Protocol
- SHA Secure Hashing Algorithm
- SIEM Security Information & Event Management • SKA Shared Key Authentication
- SKIP Simple Key Management for Internet Protocols • SLA Service Level Agreement
- SLIP Serial Line Internet Protocol • SMS Short Messaging Service
- SMTP Simple Mail Transfer Protocol • SNMP Simple Network Management Protocol • SOAP Simple Object Access Protocol • SOC Service Organization Control • SONET Synchronous Optical Network • SOX Sarbanes Oxley Act
- SPAN Switched Port Analyzer
- SPI Sensitive Personal Information • SQL Structured Query Language
- SRK Storage Root Key
- SRPC Secure Remote Procedure Call • SSAE Standards for Attestation Engagements • SSD Solid-State Drives
- SSDP Simple Service Discovery Protocol • SSH Secure Shell
- SSID Service Set Identifier
- SSL Secure Sockets Layer
- ST Security Target
- STRIDE Spoofing, Tampering, Repudiation,

Denial-of-Service (DoS), Elevation of Privilege • SWG Secure Web Gateway

- SYN Synchronization
- TCP Transmission Control Protocol Information Disclosure,

- TCSEC Trusted Computer System Evaluation Criteria • TFTP Trivial File Transfer Protocol
- TGS Ticket-Granting Server
- TGT Tick-Granting-Ticket
- TIFF Tagged Image File Format
- TKIP Temporal Key Integrity Protocol
- TLS Transport Layer Security
- TOE Target of Evaluation
- TOGAF The Open Group Architectural Framework • TPM Trusted

Platform Module

- TTL Time-to-Live
- UCA User-Styled Custom Application
- UDP User Datagram Protocol
- UI User Interface
- UPnP Universal Plug and Play
- UTC Universal Time Coordinates
- VBA Visual Basic for Application
- VBR Volume Boot Record
- VM Virtual Machines
- VOIP Voice Over IP
- VPN Virtual Private Network
- VPN Virtual Private Network
- VRF Virtual Routing Forwarding
- VSAT Very Small Aperture Terminal
- WAF Web Application Firewall
- WAP Wireless Access Point
- WAS Windows Process Activation Services • WBT Web-based Training
- WEP Wired Equivalent Privacy
- Wi-Fi Wireless Fidelity
- WLAN Wireless Local Area Network (WLAN) • WLC Wireless LAN Controller
- WMAN Wireless Metropolitan Area Network (WMAN) • WPA Wi-Fi Protected Access
- WPAN Wireless Personal Area Network (Wireless PAN) • WWAN Wireless Wide Area Network (WWAN) • WWW World Wide Web
- XSS Cross-Site Scripting
- ZBF Zone-based Firewall

Appendix B: References

References

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP. 800- 12r 1.pdf
https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phonestablets-and-mobile-internet-devices-what-the-future-has-in-store
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html
https://msdn.microsoft.com/en-us/library/ff64864 1.aspx
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfdenl.html
https://www.ietf.org/rfc/rfc3704.txt
www.cisco.com
https://msdn.microsoft.com
www.intel.com
https://meraki.cisco.com
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html
#wp737 14 1 http://www.cisco.com/web/services/downloads/smart-solutions-maximize-federal-capabilities-formission-success.pdf
http://www.cisco.com/c/en/us/support/docs/availability/high-availability/ 15 1 14-NMSbestpractice.html
http://www.ciscopress.com/articles/article.asp?p=2 1802 10&seqNum=5
http://www.pearsonitcertification.com/articles/article.aspx?p=2 168927&seqNum=7
http://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/ 1-3/configuration/guide/pi_ 13_cg/ovr.pdf
http://www.cisco.com/c/en/us/products/security/security-manager/index.html
http://www.cisco.com/c/en/us/about/security-center/dnssec-best-practices.html
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/ 15-s/sec-usr-ssh 15-sbook/sec-secure-copy.html
http://www.ciscopress.com/articles/article.asp?p=25477&seqNum=3
http://www.cisco.com/c/en/us/products/security/ids42 15-sensor/index.html

About Our Products

Other Network & Security related products from IPSpecialist LTD are:

- CCNA Routing & Switching Technology Workbook
- CCNA Security v2 Technology Workbook
- CCNA Service Provider Technology Workbook
- CCDA Technology Workbook
- CCDP Technology Workbook
- CCNP Route Technology Workbook
- CCNP Switch Technology Workbook
- CCNP Troubleshoot Technology Workbook

- CCNP Security SENSS Technology Workbook
- CCNP Security SIMOS Technology Workbook
- CCNP Security SITCS Technology Workbook
- CCNP Security SISAS Technology Workbook
- CompTIA Network+ Technology Workbook
- CompTIA Security+ v2 Technology Workbook
- Certified Information System Security Professional (CISSP) Technology

Workbook
- CCNA CyberOps SECFND Technology Workbook
- Certified Block Chain Expert Technology Workbook
- Certified Cloud Security Professional (CCSP) Technology Workbook

Upcoming products are:

- CompTIA Pentest+ Technology Workbook
- CompTIA A+ Core 1 (220-1001) Technology Workbook • CompTIA A+ Core 2 (220-1002) Technology Workbook • CompTIA Cyber Security Analyst CySA+ Technology Workbook • CompTIA Cloud+ Technology Workbook
- CompTIA Server+ Technology Workbook

Note from the Author:
If you enjoyed this book and it has helped you along your certification, please consider rating and reviewing it. Your feedback is very important to us.
Link to Product Page: