Top 20 from the list are strongly recommended.

1. Information Security

Information security is the process employed to safeguard information in any form (physical or electronic) from unauthorized access, disclosure, and destruction.

According to NIST, it involves protecting information systems from unauthorized activities to ensure confidentiality, integrity, and availability.

2. Cyber Security VS Information Security

Cyber Security

Cybersecurity focuses on safeguarding electronic data and preventing unauthorized access, disclosure, alteration, and destruction.

Its primary goal is to protect digital data and systems from unauthorized access, damage, or disruption.

Information Security

Information security is a broader discipline encompassing protecting all types of assets, whether in hard copy or digital form.

The main objective of information security is to reduce the risk of cyber-attacks and protect against unauthorized exploitation of systems, networks, and technologies.

3. What is CIA Triad ?

CIA Triad is an information security model meant to guide an organization’s security procedures and policies.

Confidentiality, Integrity, and Availability. These are the three core components of the CIA triad

- Confidentiality

Confidentiality ensures access to resources or data, which must be restricted to only authorized subjects or entities. Data encryption is a common method of ensuring confidentiality.

- Integrity

Integrity involves maintaining the consistency and accuracy of data over its entire life cycle.

Data must not be changed in transit, for example, when it is sent over the Internet or using a local area network

- availability

A vulnerability is a flaw, loophole, oversight, or error that can be exploited to violate the system's security policy.

For example, software or an application that has code vulnerable to a buffer or flow exploit.

4. Explain Vulnerabilty, Threats, Exploit and Risk.

- Vulnerabilty

A vulnerability is a flaw, loophole, oversight, or error that can be exploited to violate system security policy.

For example, a software or an application that has code vulnerable to a buffer or flow exploit.

- **Threats**

A threat is an event, natural or man-made, able to cause a negative impact on an organization.

- **Exploit**

An exploit is a defined way to breach the security of an IT system through a vulnerability.

- **Risk**
- It is a situation involving exposure to danger.

5. Define Indentification, Authentication, and Authorization?

Identification

Identification is the process of recognizing and uniquely identifying a user within a system or application. It establishes who the user is.

Authentication

Authentication is the process of verifying the identity of the user who has been identified. It ensures that the user is indeed who they claim to be.

Authorization

Authorization is the process of determining the permissions and access levels granted to the authenticated user. It defines what resources and actions the user is allowed to access within the system.

What level of access someone have ,i.e process of granting access and defining the specific resources for a user's needs.

6. What is 3 way handshake?

A three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server.

- **Step 1 (SYN):**

In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

- **Step 2 (SYN + ACK):**

The Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

- **Step 3 (ACK):**

In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

7. What is SSL/TLS handshake?

Top 20 from the list are strongly recommended.

In nutshell, SSL is obsolete and TLS is new name of older SSL protocol as modern encryption standard using by everybody. Technically, TLS is more accurate, but everyone knows SSL.

SSL	TLS
SSL stands for “Secure Socket Layer.”	TLS stands for “Transport Layer Security.”
Netscape developed the first version of SSL in 1995.	The first version of TLS was developed by the Internet Engineering Taskforce (IETF) in 1999.
SSL is a cryptographic protocol that uses explicit connections to establish secure communication between web server and client.	TLS is also a cryptographic protocol that provides secure communication between web server and client via implicit connections. It’s the successor of SSL protocol.
Three versions of SSL have been released: SSL 1.0, 2.0, and 3.0.	Four versions of TLS have been released: TLS 1.0, 1.1, 1.2, and 1.3.
All versions of SSL have been found vulnerable, and they all have been deprecated.	TLS 1.0 and 1.1 have been “broken” and are deprecated as of March 2020. TLS 1.2 is the most widely deployed protocol version.

8. Accounting V/S Auditing.

- **Accounting**
- The Process of tracking and recording system activities and resource access.
- **Auditing**
- The portion of accounting requires security professionals to examine logs of what was recorded.

9. Encription VS encoding Vs Hashing

- **Encryption vs Encoding vs Hashing :**

Concept	Purpose	Reversibility	Examples	Use Case
Encryption	Protect data confidentiality by transforming plaintext into ciphertext.	Reversible with the correct decryption key.	AES, RSA	Securing sensitive information during transmission and storage.
Encoding	Transform data into a different format for proper	Reversible using a decoding scheme.	Base64, ASCII, URL encoding	Data transmission, storage, and

Top 20 from the list are strongly recommended.

Concept	Purpose	Reversibility	Examples	Use Case
	interpretation by systems.			compatibility across platforms.
Hashing	Ensure data integrity by transforming data into a fixed-size string.	One-way process; original data cannot be recovered.	MD5, SHA-1, SHA-256	Password storage, data integrity checks, digital signatures.

10. TCP vs UDP

TCP	UDP
TCP:Transmission Control Protocol	UDP : User Datagram Protocol
It is a Connection Oriented protocol	It is a Connection less protocol
Acknowledgement is received	Acknowledgment is not received
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP)
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP)

11. What is OSI Model?

OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

OSI model consists of seven layers, and each layer performs a particular network function.

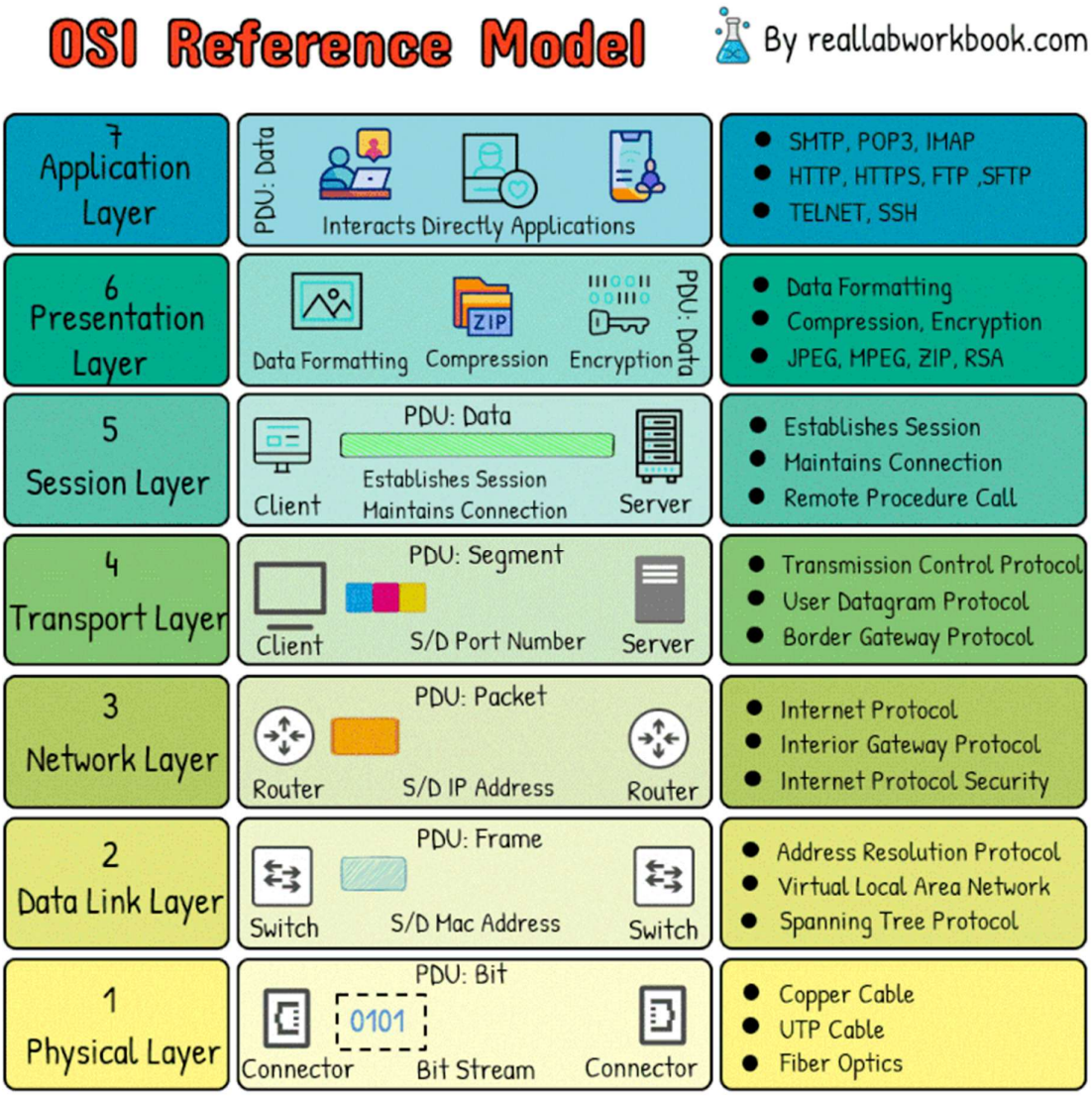
Upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software

He lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software.

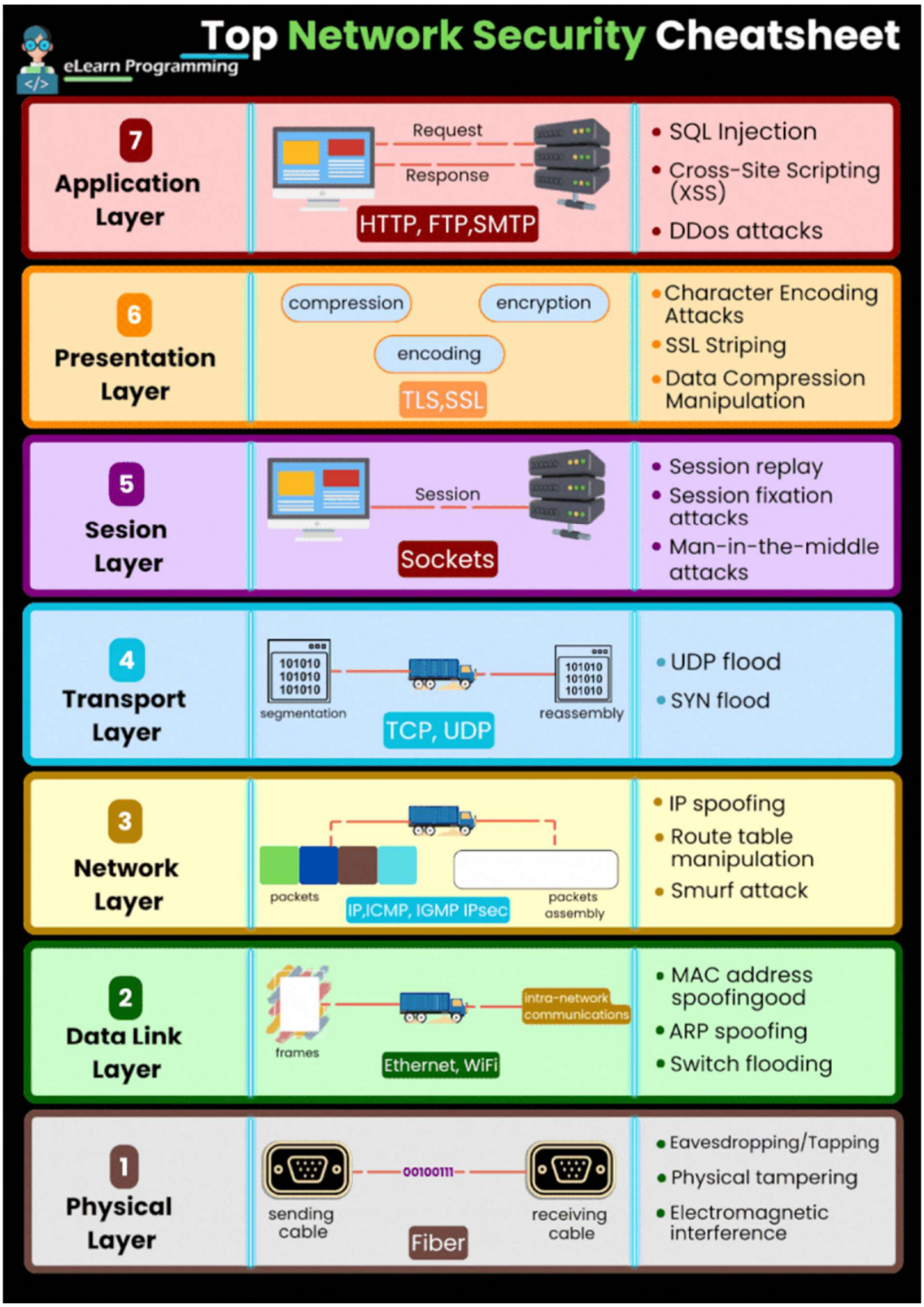
Top 20 from the list are strongly recommended.

S.N	OSI Layer	Function	Protocols
1	Application Layer	Application layer interface directly interacts with the application and provides common web application services	HTTP, FTP, SMTP, POP, SNMP, DHCP
2	Presentation Layer	Translate, encrypt, and compress data	SSL, TLS, ASCII, JPEG, MPEG
3	Session Layer	To establish, manage, and terminate sessions	NetBios, PPTP, RPC, SIP, SSH
4	Transport Layer	Provide Reliable end to end communication solution - Form **Semgments**	TCP, UDP, SCTP, DCCP, SPX
5	Network Layer	- Move packet from source to destination - Internetworking, Addressing - Form **Packets**	IP, ICMP, ARP, OSPF, BGP, RIP
6	Data Link Layer	- Framing, error detection and correction, acknowledgment, flow control, ensuring well-defined reliable service interface to the network layer, encapsulating packets from network layer to frames, etc - Form **Frames**	Bridge, Switch, Ethernet, PPP, HDLC
7	Physical Layer	- Controls the way unstructured, raw, bit-stream data is sent and received over a physical medium. - Composed of the electrical, optical, and physical components of the network. - Form **Bits**	Coax, Fiber, Wireless, RJ45, Bluetooth

Top 20 from the list are strongly recommended.



Top 20 from the list are strongly recommended.



12. TCP/IP Model

Top 20 from the list are strongly recommended.

TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers

- **1. Process/Application Layer** Application + Presentation + Session Layer
- **2. Host-to-Host/Transport Layer** - transport layer
- **3.Internet Layer** - Network layer
- **4.Network Access/Link Layer** - Data Link Layer + Physical Layer

13. What is OWASP ?

OWASP Top 10 is an online document on OWASP's website that provides ranking of and remediation guidance for the top 10 most critical web application security risks

"Open Web Application Security Proect" is list of most common web application vulnerabilty. It was first updated in 2013 and now it's latest release is 2021.

14. What is pentesting and types of pentesting

Penetration testing is also known as pen testing or ethical hacking. It describes the intentional launching of simulated cyberattacks that seek out exploitable vulnerabilities in computer systems, networks, websites, and applications.

The type of penetration testing normally depends on the scope and the organizational wants and requirements. This can classfied in to 3 types

- **Black Box Penetration Testing**

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system.

- **White Box Penetration Testing**

It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

- **Grey Box Penetration Testing** In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system.

15. What is ports and most common network ports and services.

Protocol is a set of rule by definition in computer networking, Protocol is a standard way for computers to exchange information each protocol has a port number assigned to it

There are 65,535 ports in total

Top 20 from the list are strongly recommended.

Functions of Ports

Service	Port Number	Function	Service	Port Number	Function
FTP	20, 21	File Transfer Protocol **Use:** Transfer files (Upload and Download)	**MySQL**	3306	MySQL Database **Use:** Connects to MySQL databases
SSH	22	Secure Shell **Use:** Encrypts the connection for remote login	**PostgreSQL**	5432	PostgreSQL Database **Use:** Connects to PostgreSQL databases
Telnet	23	**Use:** Establishes a connection for remote login **Note:** Does not encrypt data like SSH	**Oracle**	1521	Oracle Database **Use:** Connects to Oracle databases
RDP	3389	Remote Desktop Protocol **Use:** Connects to remote Windows computers	**LDAP**	389	Lightweight Directory Access Protocol **Use:** Accesses directory services
DNS	53	Domain Name System **Use:** Maps URLs to IP addresses	**SMB**	445	Server Message Block **Use:** File sharing and network communication
SMTP	25	Simple Mail Transfer Protocol **Use:** Sending emails	**NetBIOS**	137, 138, 139	Network Basic Input/Output System **Use:** Network file sharing and service discovery
POP3	110	Post Office Protocol v3	**MSSQL**	1433	Microsoft SQL Server **Use:** Connects to

Top 20 from the list are strongly recommended.

Service	Port Number	Function	Service	Port Number	Function
		Use: Receiving emails			Microsoft SQL Server databases
IMAP4	143	Internet Message Access Protocol v4 **Use:** Receiving emails (new version)	**VNC**	5900	Virtual Network Computing **Use:** Remote desktop access
HTTP	80	Hypertext Transfer Protocol **Use:** Connects to web pages on the internet	**Syslog**	514	System Logging Protocol **Use:** Sends system log or event messages to a logging server
HTTPS	443	Hypertext Transfer Protocol Secure **Use:** Secure protocol using TLS/SSL certificates	**SNMP**	161	Simple Network Management Protocol **Use:** Network device management and monitoring
ARP	N/A	Address Resolution Protocol **Use:** Maps IP addresses to MAC addresses for routing in IP subnets			

Common Ports and services

Service	Port Number	Service	Port Number
FTP	20, 21	**SMTP**	25
SSH	22	**POP3**	110
Telnet	23	**IMAP4**	143

Top 20 from the list are strongly recommended.

Service	Port Number	Service	Port Number
RDP	3389	**HTTP**	80
DNS	53	**HTTPS**	443
ARP	N/A	**MySQL**	3306
PostgreSQL	5432	**Oracle**	1521
LDAP	389	**SMB**	445
NetBIOS	137, 138, 139	**MSSQL**	1433
VNC	5900	**Syslog**	514
SNMP	161		

16. DNS Working

Step	Description
1. Initial Query	When searching for www.example.com, the browser and OS first check their local cache for the corresponding IP address.
2. Cache Miss	If no record is found, the OS queries the "Resolving Name Server" (RNS) for the IP address. The RNS checks its own cache.
3. Root Name Servers	If the RNS does not have the record, it queries the Root Name Servers, which provide addresses of the TLD Name Servers for .com.
4. TLD Name Servers	The RNS queries the .com TLD Name Servers, which provide the address of the Authoritative Name Servers for example.com.
5. Authoritative Name Servers	The Authoritative Name Servers for example.com provide the IP address of www.example.com. The RNS caches this result and returns it to the OS.

17. SSH Handshake Process

Step	Description
1. Client Initiates	The SSH client initiates a connection to the SSH server by sending a connection request.

Top 20 from the list are strongly recommended.

Step	Description
2. Server Responds	The SSH server responds with its public key and a set of supported encryption algorithms.
3. Key Exchange	The client and server exchange cryptographic keys to agree on a shared secret for encryption.
4. Authentication	The client sends an authentication request (username and password, or key-based authentication).
5. Server Verifies	The server verifies the client's credentials. If valid, it sends an acknowledgment.
6. Secure Connection	Once authentication is successful, both the client and server establish an encrypted session.

18. SSH Handshake Process

Step	Description
1. Client Initiates	The SSH client initiates a connection to the SSH server by sending a connection request.
2. Server Responds	The SSH server responds with its public key and a set of supported encryption algorithms.
3. Key Exchange	The client and server exchange cryptographic keys to agree on a shared secret for encryption.
4. Authentication	The client sends an authentication request (username and password, or key-based authentication).
5. Server Verifies	The server verifies the client's credentials. If valid, it sends an acknowledgment.
6. Secure Connection	Once authentication is successful, both the client and server establish an encrypted session.

19. Give the name of few tools used in penetration testing.

BurSuite

Top 20 from the list are strongly recommended.

Tool	Description	Key Features
Proxy	Allows users to view and modify the contents of requests and responses while they are in transit.	- View and modify requests/responses - Forward to other tools - Configurable proxy settings
Intruder	Automates customized attacks against web applications.	- Brute-force attacks - Dictionary attacks - Rate limiting tests
Repeater	Manually manipulates and reissues individual HTTP requests to analyze responses.	- Send, modify, and reissue requests - Detailed response analysis
Decoder	Decodes and encodes data using common methods like URL, HTML, Base64, and Hex.	- Common encoding/decoding methods - Analyzes data in parameters or headers
Scanner	Automatically scans web applications for vulnerabilities.	- Automated vulnerability scanning - Detailed reports - Customizable scan settings
Comparer	Compares two sets of data to identify differences, useful for analyzing responses or request variations.	- Compare requests/responses - Highlight differences - Useful for analyzing changes
Sequencer	Analyzes the randomness of tokens and session identifiers to assess their strength and predictability.	- Token randomness analysis - Session identifier analysis - Statistical reports
Extender	Allows users to add custom functionality to Burp Suite through extensions and plugins.	- Add and manage extensions - Customize Burp Suite's capabilities - Support for third-party plugins

Top 20 from the list are strongly recommended.

Common command of SQLMap and Nmap

SQLmap and Nmap

SQLmap	Command/Example	Nmap	Command/Example
Run on a Single URL	sqlmap -u "http://example.com"	**Ping Scan**	nmap -sn <target>
Run on a Single Parameter	sqlmap -p <parameter> -u "http://example.com"	**Host Scan**	nmap -sn <target IP range>
Enumerate Databases	sqlmap -u "http://example.com?id=1" --dbs	**OS Scanning**	nmap -O <target IP>
Enumerate Tables	sqlmap -u "http://example.com?id=1" -D <db_name> --tables	**Most Popular Ports**	nmap --top-ports 20 <target>
Enumerate Columns	sqlmap -u "http://example.com?id=1" -D <db_name> -T <table_name> --columns	**Output to a File**	nmap -oN output.txt nmap -oX output.xml
Dump Data	sqlmap -u "http://example.com?id=1" -D <db_name> -T <table_name> --dump	**Service Version Detection**	nmap -sV <target>
Use a Proxy	sqlmap -u "http://example.com" --proxy="http://proxy_ip:proxy_port"	**Script Scanning**	nmap --script=<script_name> <target>
Set User-Agent	sqlmap -u "http://example.com" --user-agent="CustomAgent"	**TCP SYN Scan**	nmap -sS <target>
Set Level	sqlmap -u "http://example.com" --level=<level>	**UDP Scan**	nmap -sU <target>
Set Threads	sqlmap -u "http://example.com" --threads=<num>	**Aggressive Scan**	nmap -A <target>
WAF Bypass	sqlmap -u "http://example.com" --tamper=<script>	**Traceroute Scan**	nmap --traceroute <target>

Top 20 from the list are strongly recommended.

SQLmap	Command/Example	Nmap	Command/Example
Exit on Error	sqlmap -u "http://example.com" --ignore-errors	**Full TCP Connect Scan**	nmap -sT <target>
WAF Bypass using Cookies	sqlmap -u "http://example.com" --cookie="cookie_data"	**Version Detection Scan**	nmap -sV --version-all <target>
WAF Bypass using User-Agent	sqlmap -u "http://example.com" --user-agent="CustomAgent"	**Idle Scan**	nmap -sI <target>
WAF Bypass using Referer Header	sqlmap -u "http://example.com" --referer="http://referrer.com"	**OS and Version Detection**	nmap -O -sV <target>
WAF Bypass with Delays	sqlmap -u "http://example.com" --delay=5	**TCP ACK Scan**	nmap -sA <target>
WAF Bypass with Custom Payload	sqlmap -u "http://example.com" --tamper="random_case"	**IP Protocol Scan**	nmap -sO <target>

20. Some Basic Vulnerabilty and terms.

- Application Vulnerabilities

Software system flaws or weaknesses in an application that could be exploited to compromise the security of the application. Software system flaws or weaknesses in an application that could be exploited to compromise the security of the application.

- Buffer Overflow

Buffer Overflows occur when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage.

- Credentials Management

A credentials management attack attempts to breach username/password pairs and take control of user accounts.

Top 20 from the list are strongly recommended.

- CRLF Injection

CRLF Injection attacks refer to the special character elements "Carriage Return" and "Line Feed." Exploits occur when an attacker is able to inject a CRLF sequence into an HTTP stream.

- Cross-Site Request Forgery

Cross-Site Request Forgery (CSRF) is a malicious attack that tricks the user's web browser to perform undesired actions so that they appear as if an authorized user is performing those actions.

- Cross-Site Scripting

XSS vulnerabilities target scripts embedded in a page that are executed on the client-side (in the user's web browser) rather than on the server-side.

- Directory Traversal

Directory traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.

- Encapsulation

Encapsulation refers to a programming approach that revolves around data and functions contained, or encapsulated, within a set of operating instructions.

- Error Handling

Error Handling vulnerabilities occur when a system reveals detailed error messages or codes generated from stack traces, database dumps, and a wide variety of other problems, including out of memory, null pointer exceptions, and network timeout errors.

- Failure to Restrict URL Access

One of the common vulnerabilities listed on the Open Web Application Security Project's (OWASP) Top 10. The OWASP Top 10 details the most critical vulnerabilities in web applications.

- Insecure Cryptographic Storage

Insecure Cryptographic Storage is a common vulnerability that occurs when sensitive data is not stored securely from internal users.

- Insufficient Transport Layer Protection

Insufficient transport layer protection is a security weakness caused by applications not taking any measures to protect network traffic.

- LDAP Injection

LDAP injection is the technique of exploiting web applications that use client-supplied data in LDAP statements without first stripping potentially harmful characters from the request.

- Malicious Code

Analysis tools are designed to uncover any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

- OS Command Injection

Top 20 from the list are strongly recommended.

Command injection refers to a class of critical application vulnerabilities involving dynamically generated content. Attackers execute arbitrary commands on a host operating system using a vulnerable application.

- Race Condition

A race condition attack happens when a computing system that's designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously.

- SQL Injection

SQL injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command, which is executed by a web application, exposing the back-end database.

- Null Byte Injection

The null character is a control character with the value zero.

It is also possible to pass the null character in the URL, which creates a vulnerability known as Null Byte Injection and can lead to security exploits.

In the URL it is represented by %00.

Ex- Image with the name hello.gif and can be changed to hello.phpA.gif. Try replacing the hex value of A (\x60) with null byte which is (\x00)

- Port Knocking :

In computer networking, port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports.

- Command Injection

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating

system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell.

- 'ShellShock Vulnerability

Shellshock is a security bug causing Bash to execute commands from environment variables unintentionally.

Since the environment variables are not sanitized properly by Bash before being executed, the attacker can send commands to the server through HTTP requests and get them executed by the web server operating system.

An attacker can potentially use CGI to send a malformed environment variable to a vulnerable Web server. Because the server uses Bash to interpret the variable, it will also run any malicious command tacked-on to it.