30 Days Cybersecurity Daily Diary:-

Day 1:-
a) Introduction to Cybersecurity
b) Learned the meaning of cybersecurity.
c) Studied why systems and networks need protection from cyber attacks.
d) Discussed basic types of cyber threats.

Day 2:-
a) IP Address
b) Studied what an IP address is.
c) Learned how IP addresses identify devices in a network.
d) Understood public and private IP basics.

Day 3:-
a) IP Address Classes
b) Learned Class A, B, C, D, and E IP addresses.
c) Studied their ranges and use cases.
d) Identified which classes are commonly used.

Day 4:-
a) CIDR
b) Studied CIDR notation like /8, /16, /24.
c) Learned how CIDR replaces class-based networking.
d) Practiced simple CIDR examples.

Day 5:-
a) Subnetting
b) Learned why subnetting is used in networks.
c) Studied how a network is divided into subnets.
d) Understood advantages of subnetting.

Day 6:-
a) Subnet Mask
b) Studied subnet masks and their format.
c) Learned how subnet masks separate network and host bits.
d) Practiced basic subnet mask calculations.

Day 7:-
a) TCP/IP Model
b) Learned the layers of TCP/IP model.
c) Studied functions of each layer.
d) Understood how data flows through the model.

Day 8:-
a) OSI Model
b) Studied the 7 layers of OSI model.
c) Learned the role of each layer.
d) Compared OSI model with TCP/IP model.

Day 9:-
a) TCP and UDP
b) Learned the difference between TCP and UDP.
c) Studied features of TCP like reliability.
d) Studied features of UDP like speed.

Day 10:-
a) Network Devices
b) Studied hub, switch, router, and firewall.
c) Learned how each device works.
d) Identified where each device is used.

Day 11:-
a) DHCP
b) Learned what DHCP is.
c) Studied how DHCP assigns IP addresses automatically.
d) Understood benefits of DHCP.

Day 12:-
a) DHCP DORA Process
b) Learned Discover, Offer, Request, Acknowledge steps.
c) Studied how a device gets an IP address.
d) Practiced DORA flow explanation.

Day 13:-
a) DNS
b) Learned what DNS is.
c) Studied how domain names convert to IP addresses.
d) Understood importance of DNS in networking.

Day 14:-
a) Disk Partitioning
b) Learned about disk partitions.
c) Studied file systems.
d) Understood why partitioning is needed.

Day 15:-
a) Ping Command
b) Used ping command to test connectivity.
c) Studied ICMP concept.
d) Learned how to analyze ping results.

Day 16:-
a) Traceroute
b) Learned traceroute command.
c) Studied how packets travel across networks.
d) Identified delays and hops.

Day 17:-
a) Nmap
b) Learned what Nmap is.
c) Studied basic Nmap commands.
d) Scanned network for open ports.

Day 18:-
a) Nmap Scanning Techniques
b) Learned SYN scan and service scan.
c) Studied OS detection.
d) Analyzed scan results.

Day 19:-

a) Wireshark
b) Learned Wireshark interface.
c) Captured live network traffic.
d) Studied packet structure.

Day 20:-
a) Wireshark Filters
b) Learned basic display filters.
c) Filtered specific protocols.
d) Analyzed filtered packets.

Day 21:-
a) Metasploit Framework
b) Learned purpose of Metasploit.
c) Studied penetration testing basics.
d) Explored framework modules.

Day 22:=
a) msfconsole
b) Used msfconsole commands.
c) Searched and selected exploits.
d) Executed exploits in lab setup.

Day 23:-
a) Burp Suite
b) Learned Burp Suite components.
c) Intercepted HTTP requests.
d) Studied web request structure.

Day 24:=
a) Burp Suite Tools
b) Used Repeater tool.
c) Used Intruder for testing inputs.
d) Analyzed application responses.

Day 25:-
a) Hydra
b) Learned Hydra tool basics.
c) Studied brute-force attack concept.
d) Performed password testing in lab.

Day 26:-
a) Medusa
b) Learned Medusa tool usage.
c) Compared Medusa with Hydra.
d) Tested login services.

Day 27:-
a) Bettercap
b)Learned Bettercap basics.
c) Studied man-in-the-middle attacks.
d) Observed network traffic manipulation.

Day 28:-
a) Ettercap
b) Learned Ettercap features.

c) Studied ARP poisoning.
d) Sniffed LAN traffic in lab.

Day 29:-
a) Autopsy
b) Learned digital forensics basics.
c) Used Autopsy tool.
d) Analyzed disk and file evidence.

Day 30:-
a) Revision and Ethics
b) Revised all networking and security topics.
c) Learned ethical hacking rules.
d) Understood legal responsibilities in cybersecurity.