Network Security Tools – ALL Commands with Usage (Side■by■Side)

1. Wireshark – Packet Analysis

`wireshark`	Launch Wireshark GUI.
`wireshark -i eth0`	Capture packets on a specific interface.
`wireshark -i eth0 -w capture.pcap`	Capture traffic and save to a PCAP file.
`wireshark capture.pcap`	Open an existing capture file.
`http`	Filter HTTP traffic.
`https / tls`	View encrypted HTTPS traffic.
`tcp`	Show TCP packets only.
`udp`	Show UDP packets only.
`dns`	Filter DNS queries and responses.
`ip.addr == 192.168.1.10`	Filter packets by IP address.
`ip.src == X`	Filter by source IP.
`ip.dst == X`	Filter by destination IP.
`tcp.port == 80`	Filter packets by port number.

2. Zenmap / Nmap – Network Scanning

`nmap 192.168.1.1`	Basic scan to check host availability.
`nmap 192.168.1.0/24`	Scan all hosts in a subnet.
`nmap -p 80,443 192.168.1.1`	Scan specific ports.
`nmap -p-`	Scan all 65535 ports.
`nmap -sS`	TCP SYN stealth scan.
`nmap -sT`	TCP connect scan.
`nmap -sU`	UDP scan.
`nmap -sV`	Detect service versions.
`nmap -O`	Detect operating system.
`nmap -A`	Aggressive scan (OS, version, scripts).
`nmap -F`	Fast scan of common ports.
`nmap --script vuln`	Run vulnerability detection scripts.

3. iptables – Linux Firewall

`iptables -L`	List all firewall rules.

`iptables -L -n -v`	List rules with numbers and packet counts.
`iptables -A INPUT -p tcp --dport 22 -j ACCEPT`	Allow SSH traffic.
`iptables -A INPUT -p tcp --dport 80 -j ACCEPT`	Allow HTTP traffic.
`iptables -A INPUT -p tcp --dport 443 -j ACCEPT`	Allow HTTPS traffic.
`iptables -A INPUT -s 192.168.1.50 -j DROP`	Block traffic from a specific IP.
`iptables -A INPUT -p tcp --dport 23 -j DROP`	Block Telnet service.
`iptables -D INPUT 1`	Delete rule by rule number.
`iptables -F`	Flush all firewall rules.
`iptables-save`	Save firewall rules permanently.

4. UFW – Uncomplicated Firewall

`ufw enable`	Enable the firewall.
`ufw disable`	Disable the firewall.
`ufw status`	Check firewall status.
`ufw status numbered`	View rules with numbers.
`ufw allow ssh`	Allow SSH access.
`ufw allow 80`	Allow HTTP traffic.
`ufw allow 443`	Allow HTTPS traffic.
`ufw deny 21`	Block FTP service.
`ufw allow from 192.168.1.10`	Allow traffic from a specific IP.
`ufw delete allow 80`	Delete an existing rule.
`ufw reset`	Reset firewall to default rules.