Windows Kernel Exploits

pentestlab.blog/category/red-team/page/120

April 24, 2017

Windows by default are vulnerable to several vulnerabilities that could allow an attacker to execute malicious code in order to abuse a system. From the other side patching systems sufficiently is one of the main problems in security. Even if an organization has a patching policy in place if important patches are not implemented immediately this can still give short window to an attacker to exploit a vulnerability and escalate his privileges inside a system and therefore inside the network.

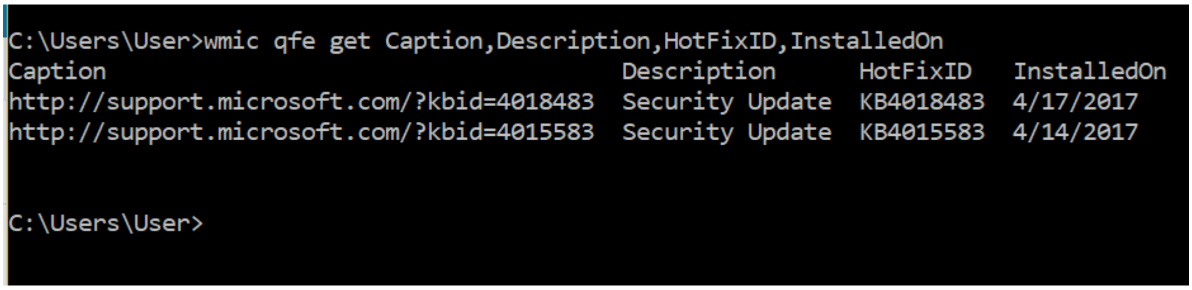
This article will discuss how to identify missing patches related to privilege escalation and the necessary code to exploit the issue.

Discovery of Missing Patches

The discovery of missing patches can be identified easily either through manual methods or automatic. Manually this can be done easily be executing the following command which will enumerate all the installed patches.

```
wmic qfe get Caption,Description,HotFixID,InstalledOn
```

The output will be similar to this:



```
C:\Users\User>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                      Description      HotFixID   InstalledOn
http://support.microsoft.com/?kbid=4018483  Security Update  KB4018483  4/17/2017
http://support.microsoft.com/?kbid=4015583  Security Update  KB4015583  4/14/2017


C:\Users\User>
```

Enumeration of Installed Patches

The HotFixID can be used in correlation with the table below in order to discover any missing patches related to privilege escalation. As the focus is on privilege escalation the command can be modified slightly to discover patches based on the KB number.

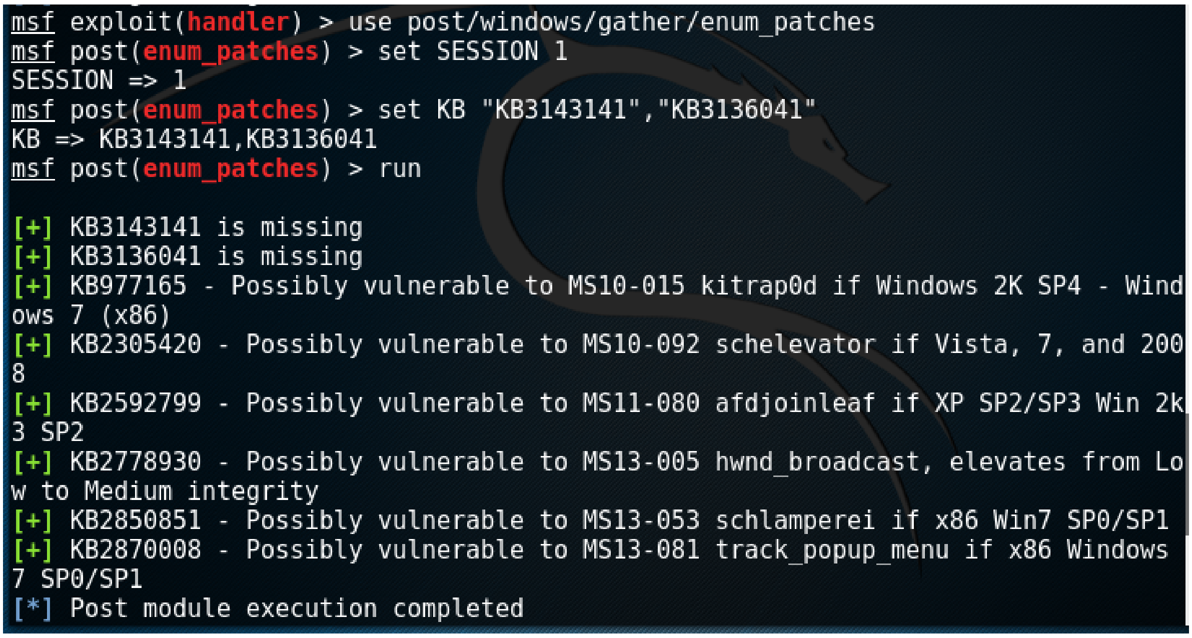
```
wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3136041"
/C:"KB4018483"
```

Alternatively this can be done automatically via Metasploit, Credential Nessus Scan or via a custom script that will look for missing patches related to privilege escalation.

Metasploit

There is a Metasploit module which can quickly identify any missing patches based on the Knowledge Base number and specifically patches for which there is a Metasploit module.

```
post/windows/gather/enum_patches
```

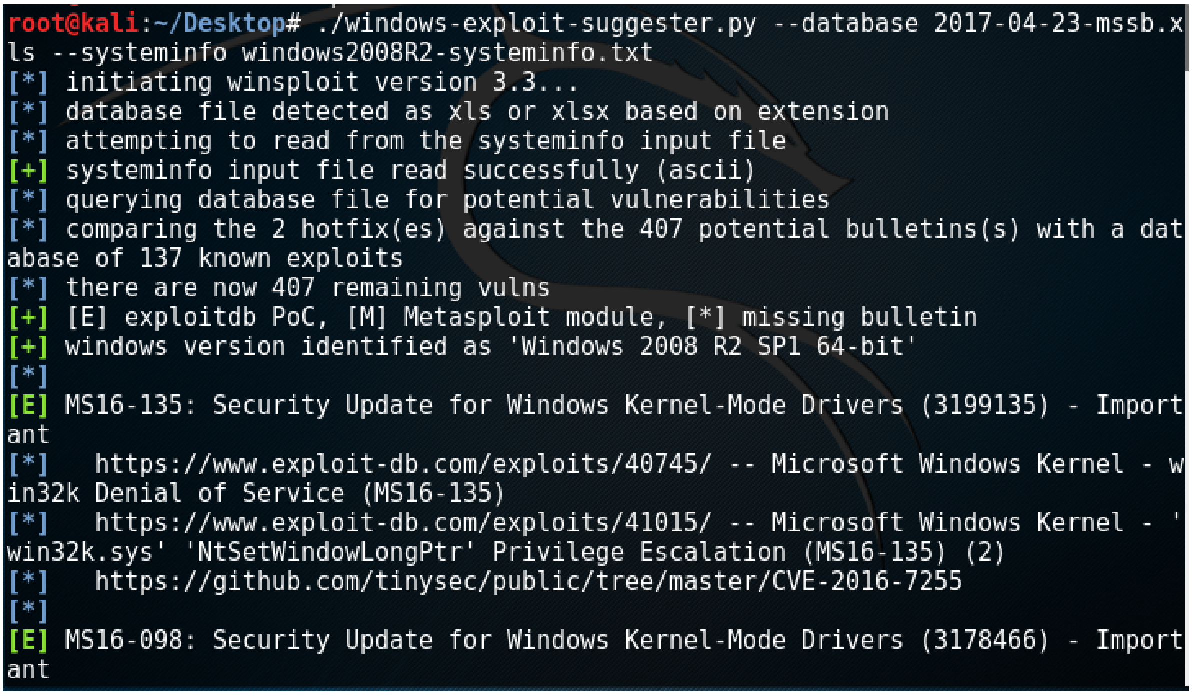


```
msf exploit(handler) > use post/windows/gather/enum_patches
msf post(enum_patches) > set SESSION 1
SESSION => 1
msf post(enum_patches) > set KB "KB3143141","KB3136041"
KB => KB3143141,KB3136041
msf post(enum_patches) > run

[+] KB3143141 is missing
[+] KB3136041 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Wind
ows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 200
8
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k
3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Lo
w to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows
7 SP0/SP1
[*] Post module execution completed
```

Metasploit – Patches Enumeration

Windows Exploit Suggester

Gotham Digital Security released a tool with the name Windows Exploit Suggester which compares the patch level of a system against the Microsoft vulnerability database and can be used to identify those exploits that could lead to privilege escalation. The only requirement is that requires the system information from the target.



```
root@kali:~/Desktop# ./windows-exploit-suggester.py --database 2017-04-23-mssb.x
ls --systeminfo windows2008R2-systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 407 potential bulletins(s) with a dat
abase of 137 known exploits
[*] there are now 407 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Import
ant
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - w
in32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - '
win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Import
ant
```

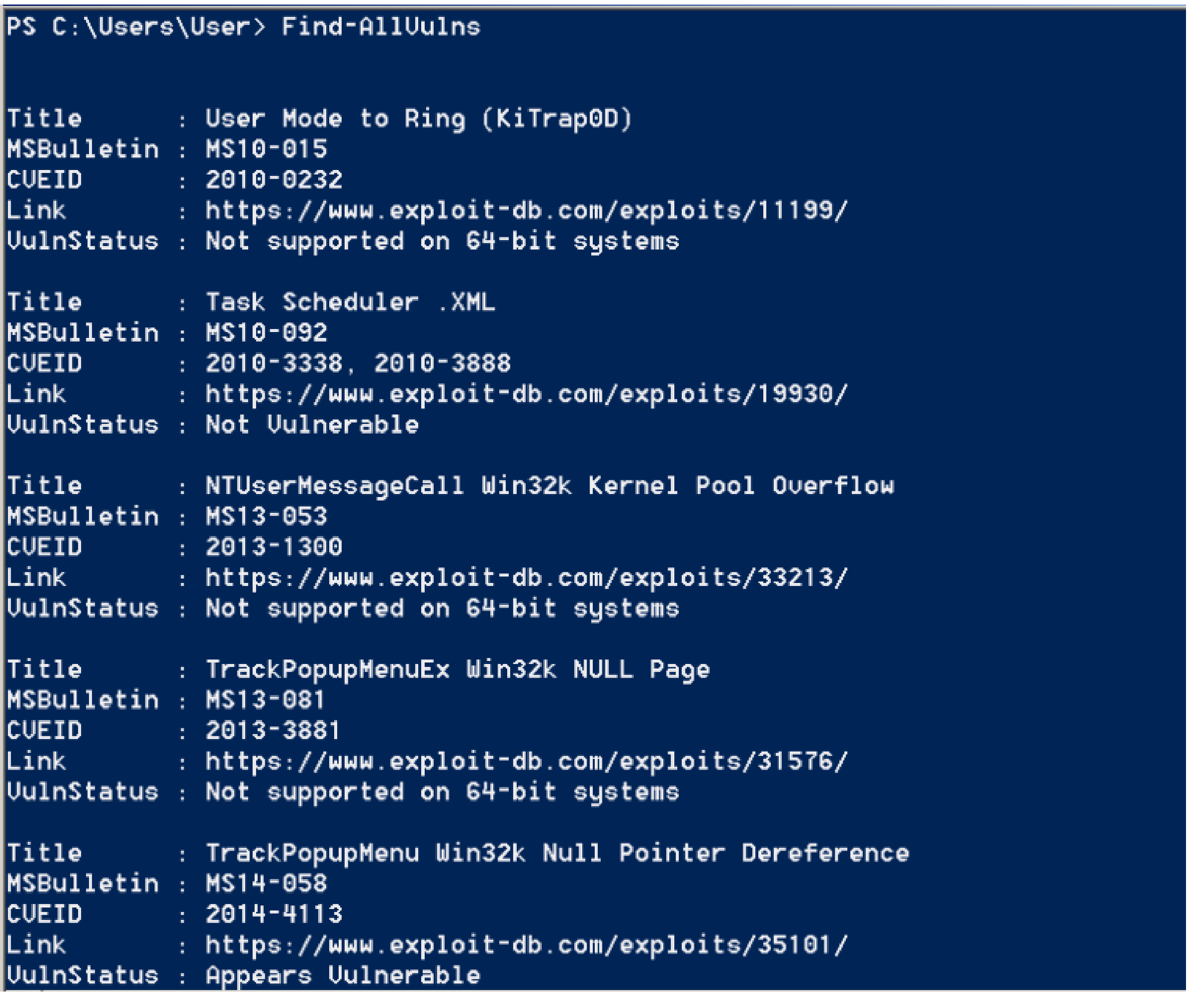
Windows Exploit Suggester

PowerShell

There is also a PowerShell script which target to identify patches that can lead to privilege escalation. This script is called Sherlock and it will check a system for the following:

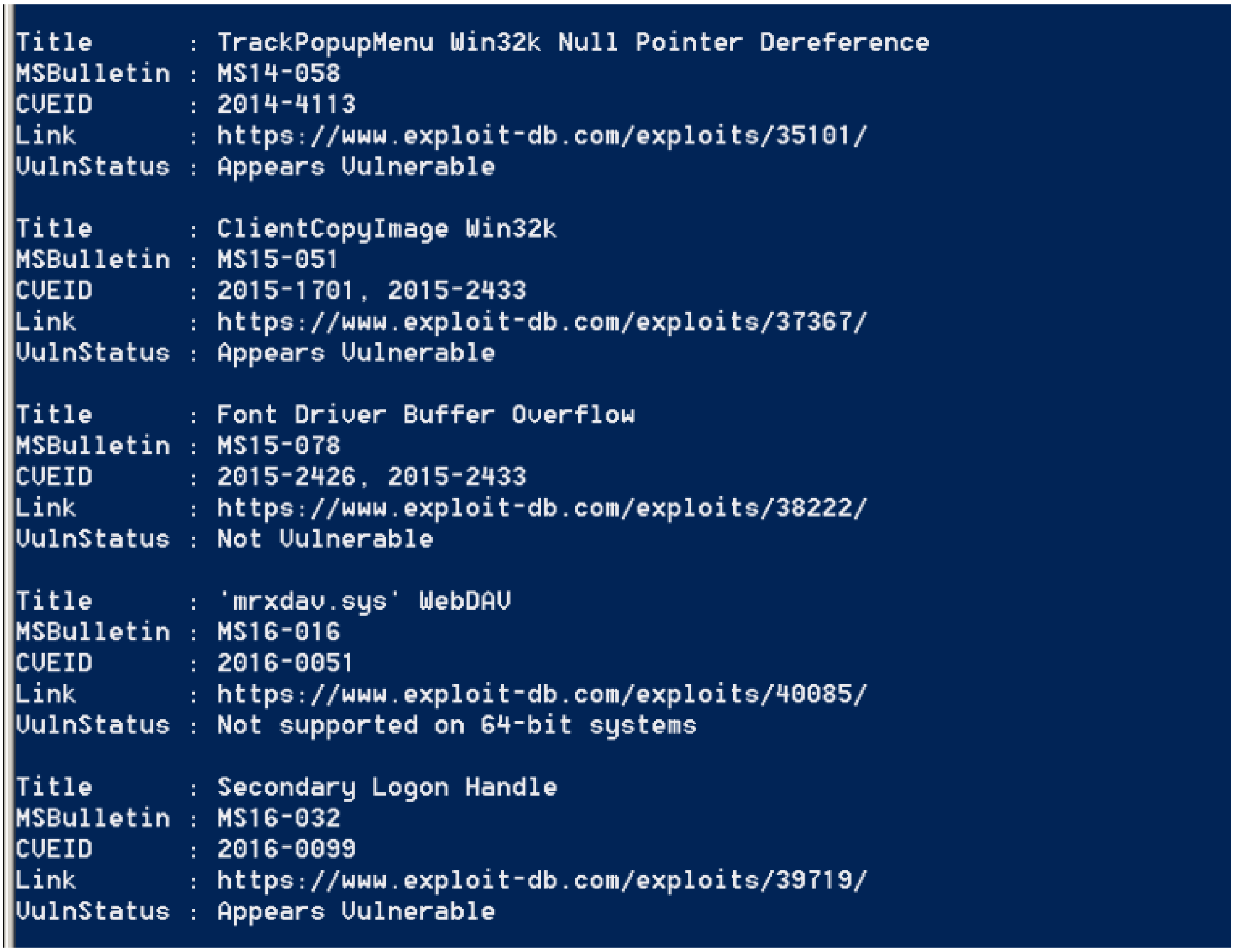
- MS10-015 : User Mode to Ring (KiTrap0D)
- MS10-092 : Task Scheduler
- MS13-053 : NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081 : TrackPopupMenuEx Win32k NULL Page
- MS14-058 : TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051 : ClientCopyImage Win32k
- MS15-078 : Font Driver Buffer Overflow
- MS16-016 : 'mrxdav.sys' WebDAV
- MS16-032 : Secondary Logon Handle
- CVE-2017-7199 : Nessus Agent 6.6.2 – 6.10.3 Priv Esc

The output of this tool can be seen below:



```
PS C:\Users\User> Find-AllVulns


Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Appears Vulnerable
```

Sherlock – Missing Patches



```
Title       : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin  : MS14-058
CVEID       : 2014-4113
Link        : https://www.exploit-db.com/exploits/35101/
VulnStatus  : Appears Vulnerable

Title       : ClientCopyImage Win32k
MSBulletin  : MS15-051
CVEID       : 2015-1701, 2015-2433
Link        : https://www.exploit-db.com/exploits/37367/
VulnStatus  : Appears Vulnerable

Title       : Font Driver Buffer Overflow
MSBulletin  : MS15-078
CVEID       : 2015-2426, 2015-2433
Link        : https://www.exploit-db.com/exploits/38222/
VulnStatus  : Not Vulnerable

Title       : 'mrxdav.sys' WebDAV
MSBulletin  : MS16-016
CVEID       : 2016-0051
Link        : https://www.exploit-db.com/exploits/40085/
VulnStatus  : Not supported on 64-bit systems

Title       : Secondary Logon Handle
MSBulletin  : MS16-032
CVEID       : 2016-0099
Link        : https://www.exploit-db.com/exploits/39719/
VulnStatus  : Appears Vulnerable
```

Sherlock – Identification of Privilege Escalation Patches

Privilege Escalation Table

The following table has been compiled to assist in the process of privilege escalation due to lack of sufficient patching.

Operating System	Description	Security Bulletin	KB	Exploit
Windows Server 2016	Windows Kernel Mode Drivers	MS16-135	3199135	Exploit Github
Windows Server 2008 ,7,8,10 Windows Server 2012	Secondary Logon Handle	MS16-032	3143141	GitHub ExploitDB Metasploit
Windows Server 2008, Vista, 7	WebDAV	MS16-016	3136041	Github

Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, Windows 2012	Windows Kernel Mode Drivers	MS15-051	3057191	GitHub ExploitDB Metasploit
Windows Server 2003, Windows Server 2008, Windows Server 2012, 7, 8	Win32k.sys	MS14-058	3000061	GitHub ExploitDB Metasploit
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	AFD Driver	MS14-040	2975684	Python EXE ExploitDB Github
Windows XP, Windows Server 2003	Windows Kernel	MS14-002	2914368	Metasploit
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	Kernel Mode Driver	MS13-005	2778930	Metasploit ExploitDB GitHub
Windows Server 2008, 7	Task Scheduler	MS10-092	2305420	Metasploit ExploitDB
Windows Server 2003, Windows Server 2008, 7, XP	KiTrap0D	MS10-015	977165	Exploit ExploitDB GitHub Metasploit
Windows Server 2003, XP	NDProxy	MS14-002	2914368	Exploit ExploitDB ExploitDB Github
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	Kernel Driver	MS15-061	3057839	Github

Windows Server 2003, XP	AFD.sys	MS11-080	2592799	EXE Metasploit ExploitDB
Windows Server 2003, XP	NDISTAPI	MS11-062	2566454	ExploitDB
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	RPC	MS15-076	3067505	Github
Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012	Hot Potato	MS16-075	3164038	GitHub PowerShell HotPotato
Windows Server 2003, Windows Server 2008, 7, XP	Kernel Driver	MS15-010	3036220	GitHub ExploitDB
Windows Server 2003, Windows Server 2008, 7, XP	AFD.sys	MS11-046	2503665	EXE ExploitDB