Qualys. Community Edition

Scan Results

February 28, 2024

Report Summary	
User Name:	Olusola Babajide Kassim
Login Name:	cyber6ub
Company:	CyberSola
User Role:	Manager
Address:	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Created:	02/28/2024 at 21:56:32 (GMT-0800)
Launch Date:	02/28/2024 at 19:55:21 (GMT-0800)
Active Hosts:	1
Total Hosts:	2
Type:	On demand
Status:	Canceled
Reference:	scan/1709178921.09358
Scanner Appliances:	CyberSola (Scanner 12.16.61-1, Vulnerability Signatures 2.5.993-2)
Duration:	01:03:17
Title:	Basic Wins7 Scan
Asset Groups:	-
IPs:	10.0.0.4, 10.0.0.6
Excluded IPs:	-
Options Profile:	Basic Net Scan

Summary of Vulnerabilities

Vulnerabilities Total	25	Security Risk (Avg)	5.0

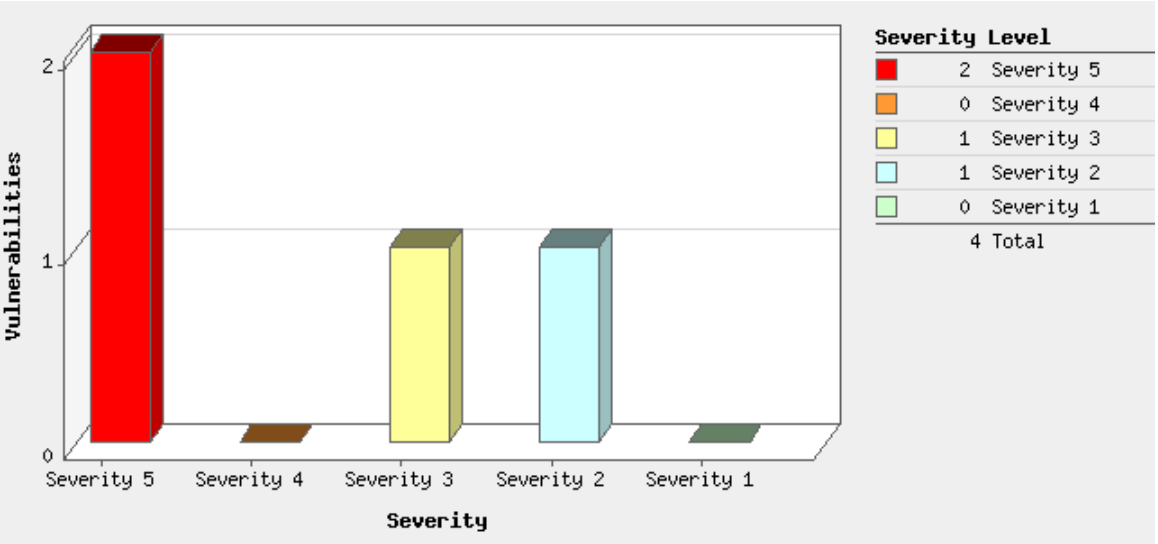
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	2	0	0	2
4	0	0	0	0
3	1	0	2	3
2	1	0	4	5
1	0	0	15	15
Total	4	0	21	25

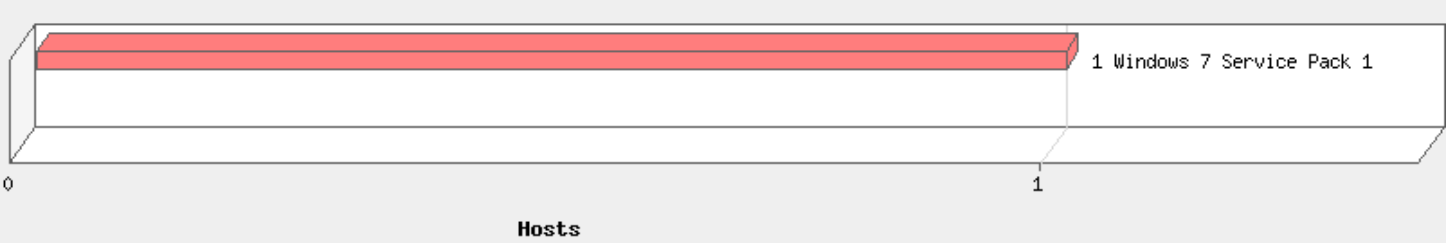
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
TCP/IP	0	0	8	8
Information gathering	0	0	7	7
SMB / NETBIOS	1	0	3	4
Windows	2	0	1	3
Security Policy	1	0	0	1
Total	4	0	19	23

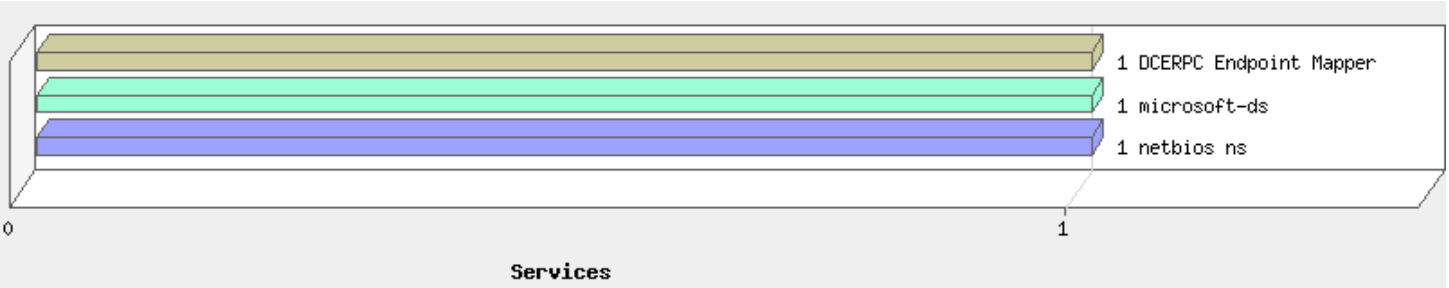
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

10.0.0.6 (windows-7-enter, WINDOWS-7-ENTER) Windows 7 Service Pack 1

Vulnerabilities (4)

5 Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers

QID:	91345
Category:	Windows
Associated CVEs:	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, CVE-2017-0147
Vendor Reference:	MS Shadow Brokers, MS17-010
Bugtraq ID:	96703,96704,96705,96707,96709,96706
Service Modified:	02/09/2024
User Modified:	-

Edited: No
PCI Vuln: Yes

THREAT:

Microsoft Server Message Block (SMB) Protocol is a Microsoft network file sharing protocol used in Microsoft Windows.
The Microsoft SMB Server is vulnerable to multiple remote code execution vulnerabilities due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
This security update is rated Critical for all supported editions of Windows XP, Windows 2003, Windows 8, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 Service Pack 1, Windows Server 2012 and 2012 R2, Windows 8.1 and RT 8.1, Windows 10 and Windows Server 2016.

UPDATE: 14 May 2017. Signature for this QID has been updated to detect the patch released by Microsoft for end-of-life operating systems Windows XP, Windows 2003 and Windows 8.

IMPACT:

A remote attacker could gain the ability to execute code by sending crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.
The latest version of the Petya ransomware is spreading over Windows SMB and is reportedly using the ETERNALBLUE exploit.

SOLUTION:

Customers are advised to refer to Microsoft Advisory MS17-010 (https://technet.microsoft.com/en-us/security/bulletin/MS17-010) or How to verify that MS17-010 is installed (https://support.microsoft.com/eu-es/help/4023262/how-to-verify-that-ms17-010-is-installed) for more details.
Workaround:Disable SMBv1
Refer to KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012) for more information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
MS17-010: Windows Vista Service Pack 2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows Vista x64 Edition Service Pack 2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows Server 2008 for 32-bit Systems Service Pack 2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows Server 2008 for x64-based Systems Service Pack 2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows 7 for 32-bit Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212)
MS17-010: Windows 7 for x64-based Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212)
MS17-010: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212)
MS17-010: Windows 7 for 32-bit Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012215)
MS17-010: Windows 7 for x64-based Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012215)
MS17-010: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012215)
MS17-010: Windows 8.1 for 32-bit Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012213)
MS17-010: Windows 8.1 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012213)
MS17-010: Windows Server 2012 R2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012213)
MS17-010: Windows 8.1 for 32-bit Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012216)
MS17-010: Windows 8.1 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012216)
MS17-010: Windows Server 2012 R2 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012216)
MS17-010: Windows RT 8.1 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012216)
MS17-010: Windows Server 2012 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012214)
MS17-010: Windows Server 2012 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012217)
MS17-010: Windows 10 for 32-bit Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012606)
MS17-010: Windows 10 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012606)
MS17-010: Windows 10 Version 1511 for 32-bit Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013198)
MS17-010: Windows 10 Version 1511 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013198)
MS17-010: Windows 10 Version 1607 for 32-bit Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013429)
MS17-010: Windows 10 Version 1607 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013429)
MS17-010: Windows Server 2016 for x64-based Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013429)
MS17-010: Windows Server 2003 Systems (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows XP Service Pack 3 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
MS17-010: Windows 8 (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2017-0143
Description: Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010) - Core Security Category : Exploits/Remote

Reference: CVE-2017-0143

Description: Microsoft Windows SMB Remote Code Execution (MS17-010) Detector - Core Security Category : Exploits/Remote

Reference: CVE-2017-0143
Description: Microsoft Windows SMB Pool Overflow EternalRomance Remote Code Execution Exploit (MS17-010) - Core Security Category : Exploits/Remote

Metasploit

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/linux/ssh/quantum_dxi_known_privkey
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/linux/ssh/quantum_dxi_known_privkey
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/linux/ssh/quantum_dxi_known_privkey
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/mipsbe/meterpreter_reverse_http
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref :

/modules/exploit/windows/iis/ms01_023_printer

Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/iis/ms01_023_printer
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/iis/ms01_023_printer
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/iis/ms01_023_printer
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/iis/ms01_023_printer
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/iis/ms01_023_printer
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/multi/browser/adobe_flash_opaque_background_uaf
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/multi/browser/adobe_flash_opaque_background_uaf
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/exploit/multi/browser/adobe_flash_opaque_background_uaf
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/fileformat/deepburner_path
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/fileformat/deepburner_path
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/fileformat/deepburner_path

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/http/jira_collector_traversal

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0146

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/http/jira_collector_traversal

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/http/jira_collector_traversal

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/browser/hp_loadrunner_writefilestring

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0146

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/browser/hp_loadrunner_writefilestring

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/browser/hp_loadrunner_writefilestring

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/auxiliary/scanner/http/hp_imc_som_file_download

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0146

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/auxiliary/scanner/http/hp_imc_som_file_download

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/auxiliary/scanner/http/hp_imc_som_file_download

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_psexec

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/payload/linux/mipsle/exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0144
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0145
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0146
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0147
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec

Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/linux/http/f5_icontrol_exec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/auxiliary/scanner/smb/smb_ms17_010
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_psexec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_psexec
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/exploit/windows/smb/smb_doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0144
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0147
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/exploit/windows/smb/doublepulsar_rce
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/auxiliary/admin/smb/ms17_010_command
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/auxiliary/admin/smb/ms17_010_command
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution - Metasploit Ref : /modules/auxiliary/admin/smb/ms17_010_command
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue_win8
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/auxiliary/admin/http/openbravo_xxe
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/sqli/oracle/dbms_export_extension
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/post/linux/gather/enum_nagios_xi
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/post/linux/gather/enum_nagios_xi
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution - Metasploit Ref : /modules/post/linux/gather/enum_nagios_xi
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0144
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0145
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0146
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0147
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0148
Description: MS17-010 SMB RCE Detection - Metasploit Ref : /modules/exploit/multi/misc/wireshark_lwres_getaddrbyname
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/encoder/x86/nonalpha
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/antivirus/symantec_endpoint_manager_rce

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144

Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0145

Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0146

Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0147

Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0148

Description: DOUBLEPULSAR Payload Execution and Neutralization - Metasploit Ref : /modules/auxiliary/scanner/http/brute_dirs

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/doublepulsar_rce.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd

Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/browser/symantec_altirisdeployment_runcmd
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/payload/linux/x64/meterpreter/bind_tcp
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/unix/local/setuid_nmap

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0144

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0145

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0146

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0147

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0148

Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+ - Metasploit Ref : /modules/exploit/linux/http/linksys_wvbr0_user_agent_exec_noauth

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue_win8.py

Reference: CVE-2017-0143

Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0144

Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount

Link:

https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145

Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution - Metasploit Ref : /modules/post/windows/manage/vss_mount
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue

Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/exploit/windows/smb/ms17_010_eternalblue
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Metasploit Ref : /modules/auxiliary/scanner/http/dlink_dir_session_cgi_http_login
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb


The Exploit-DB

Reference: CVE-2017-0148
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0147
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0146
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0145
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0144
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0147
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0146
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0148
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0145
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0144
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0143
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit) - The Exploit-DB Ref : 41891
Link: http://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0144
Description: Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 42030
Link: http://www.exploit-db.com/exploits/42030

Reference: CVE-2017-0144
Description: Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 42031
Link: http://www.exploit-db.com/exploits/42031

Reference: CVE-2017-0144
Description: Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 42315
Link: http://www.exploit-db.com/exploits/42315

Reference: CVE-2017-0143
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) - The Exploit-DB Ref : 41987
Link: http://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0147
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) - The Exploit-DB Ref : 43970
Link: http://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0146
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) - The Exploit-DB Ref : 43970
Link: http://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0143
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) - The Exploit-DB Ref : 43970
Link: http://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0148
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0147
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0146
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0145
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0144

Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0143
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) - The Exploit-DB Ref : 47456
Link: http://www.exploit-db.com/exploits/47456

exploitdb

Reference: CVE-2017-0146
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0143
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)
Link: https://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0143
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0143
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0143
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0145
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0145
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0145
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0146
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)
Link: https://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0146
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0146
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0144
Description: Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/42031

Reference: CVE-2017-0144
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0144
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0144
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0144
Description: Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/42315

Reference: CVE-2017-0144
Description: Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/42030

Reference: CVE-2017-0147
Description: Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)
Link: https://www.exploit-db.com/exploits/43970

Reference: CVE-2017-0147
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0147
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0147
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

Reference: CVE-2017-0148
Description: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Link: https://www.exploit-db.com/exploits/41987

Reference: CVE-2017-0148
Description: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Link: https://www.exploit-db.com/exploits/41891

Reference: CVE-2017-0148
Description: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)
Link: https://www.exploit-db.com/exploits/47456

saint

Reference: CVE-2017-0144
Description: Windows SMB PsImpersonateClient null token vulnerability
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/windows_psimpersonateclient_null_token

Reference: CVE-2017-0146
Description: Windows SMBv1 Transaction race condition
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/windows_smbv1_eternalsynergy

Reference: CVE-2017-0143
Description: Windows SMBv1 Remote Command Execution
Link: https://my.saintcorporation.com/cgi-bin/exploit_info/windows_smbv1_eternalblue

packetstorm

Reference: CVE-2017-0144
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0144
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0144
Description: Microsoft Windows 7/2008 R2 x64 EternalBlue Remote Code Execution
Link: https://packetstormsecurity.com/files/142603/Microsoft-Windows-7-2008-R2-x64-EternalBlue-Remote-Code-Execution.html

Reference: CVE-2017-0144
Description: Microsoft Windows 8/2012 R2 x64 EternalBlue Remote Code Execution
Link: https://packetstormsecurity.com/files/142602/Microsoft-Windows-8-2012-R2-x64-EternalBlue-Remote-Code-Execution.html

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0145
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Reference: CVE-2017-0145
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Reference: CVE-2017-0146
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance / EternalSynergy / EternalChampion SMB Remote Windows Code Execution
Link: https://packetstormsecurity.com/files/146236/MS17-010-EternalRomance-EternalSynergy-EternalChampion-SMB-Remote-Windows-C

Reference: CVE-2017-0146
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Reference: CVE-2017-0147
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0147

Description: MS17-010 EternalRomance / EternalSynergy / EternalChampion SMB Remote Windows Code Execution
Link: https://packetstormsecurity.com/files/146236/MS17-010-EternalRomance-EternalSynergy-EternalChampion-SMB-Remote-Windows-C

Reference: CVE-2017-0147
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0148
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0148
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0143
Description: Microsoft Windows MS17-010 SMB Remote Code Execution
Link: https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

Reference: CVE-2017-0143
Description: DOUBLEPULSAR Payload Execution / Neutralization
Link: https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance / EternalSynergy / EternalChampion SMB Remote Windows Code Execution
Link: https://packetstormsecurity.com/files/146236/MS17-010-EternalRomance-EternalSynergy-EternalChampion-SMB-Remote-Windows-C

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://packetstormsecurity.com/files/142548/MS17-010-EternalBlue-SMB-Remote-Windows-Kernel-Pool-Corruption.html

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

canvas

Reference: CVE-2017-0146
Description: ms17_010
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/ms17_010

Reference: CVE-2017-0143
Description: ms17_010
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/ms17_010

Reference: CVE-2017-0143
Description: ETERNALBLUE
Link: http://exploitlist.immunityinc.com/home/exploitpack/CANVAS/ETERNALBLUE

metasploit

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0146
Description: MS17-010 SMB RCE Detection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0148
Description: MS17-010 SMB RCE Detection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0148
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0146
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/admin/smb/ms17_010_command.rb

Reference: CVE-2017-0147
Description: MS17-010 SMB RCE Detection
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0147
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0143
Description: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_psexec.rb

Reference: CVE-2017-0143
Description: MS17-010 SMB RCE Detection

Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0144
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0144
Description: MS17-010 SMB RCE Detection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/smb/smb_doublepulsar_rce.rb

Reference: CVE-2017-0145
Description: MS17-010 SMB RCE Detection
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

cisa-alerts

Reference: CVE-2017-0144
Description: CISA Adds 15 Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2022/02/10/cisa-adds-15-known-exploited-vulnerabilities-catalog

Reference: CVE-2017-0144
Description: Petya Ransomware
Link: https://cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

Reference: CVE-2017-0143
Description: Top 10 Routinely Exploited Vulnerabilities
Link: https://us-cert.cisa.gov/ncas/alerts/aa20-133a

Reference: CVE-2017-0143
Description: Top 10 Routinely Exploited Vulnerabilities
Link: https://www.cisa.gov/uscert/ncas/alerts/aa20-133a

Reference: CVE-2017-0143
Description: Top 10 Routinely Exploited Vulnerabilities
Link: https://cisa.gov/news-events/cybersecurity-advisories/aa20-133a

Reference: CVE-2017-0143
Description: Top 10 Routinely Exploited Vulnerabilities
Link: https://us-cert.cisa.gov/ncas/alerts/AA20-133a

Reference: CVE-2017-0144
Description: Petya Ransomware
Link: https://www.cisa.gov/ncas/alerts/TA17-181A

Reference: CVE-2017-0145
Description: Petya Ransomware
Link: https://cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

Reference: CVE-2017-0145
Description: Petya Ransomware
Link: https://www.cisa.gov/ncas/alerts/TA17-181A

Reference: CVE-2017-0145
Description: CISA Adds 15 Known Exploited Vulnerabilities to Catalog
Link: https://cisa.gov/news-events/alerts/2022/02/10/cisa-adds-15-known-exploited-vulnerabilities-catalog

0day.today

Reference: CVE-2017-0143
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0143
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0143
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

Reference: CVE-2017-0143
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0143
Description: Microsoft Windows SMB MS17-010 EternalRomance / EternalSynergy / EternalChampion Remote Code Executi
Link: https://0day.today/exploit/29702

Reference: CVE-2017-0148
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0147
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

Reference: CVE-2017-0147
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0147
Description: Microsoft Windows SMB MS17-010 EternalRomance / EternalSynergy / EternalChampion Remote Code Executi
Link: https://0day.today/exploit/29702

Reference: CVE-2017-0147
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0147
Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0148
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0148

Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0148
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

Reference: CVE-2017-0148
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0146
Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0146
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0146
Description: Microsoft Windows SMB MS17-010 EternalRomance / EternalSynergy / EternalChampion Remote Code Executi
Link: https://0day.today/exploit/29702

Reference: CVE-2017-0146
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0146
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0147
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0143
Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0144
Description: Microsoft Windows 8 / 2012 R2 (x64) - EternalBlue SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27803

Reference: CVE-2017-0144
Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0144
Description: Microsoft Windows 7 / 2008 R2 (x64) - EternalBlue SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27802

Reference: CVE-2017-0144
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0144
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0144
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0144
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

Reference: CVE-2017-0145
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

Reference: CVE-2017-0145
Description: Microsoft Windows - Uncredentialed SMB RCE (MS17-010) Exploit
Link: https://0day.today/exploit/27613

Reference: CVE-2017-0145
Description: Microsoft Windows MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit
Link: https://0day.today/exploit/27786

Reference: CVE-2017-0145
Description: Microsoft Windows - SrvOs2FeaToNt SMB Remote Code Execution (MS17-010) Exploit
Link: https://0day.today/exploit/27752

Reference: CVE-2017-0145
Description: DOUBLEPULSAR - Payload Execution and Neutralization Exploit
Link: https://0day.today/exploit/33313

Reference: CVE-2017-0146
Description: SMB DOUBLEPULSAR Remote Code Execution Exploit
Link: https://0day.today/exploit/33895

github-exploits

Reference: CVE-2017-0143
Description: Ascotbe/Kernelhub exploit repository
Link: https://github.com/Ascotbe/Kernelhub

Reference: CVE-2017-0143
Description: k4u5h41/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/k4u5h41/MS17-010_CVE-2017-0143

Reference: CVE-2017-0143
Description: fanicia/security-notes exploit repository
Link: https://github.com/fanicia/security-notes

Reference: CVE-2017-0148
Description: HakaKali/CVE-2017-0148 exploit repository
Link: https://github.com/HakaKali/CVE-2017-0148

Reference: CVE-2017-0143
Description: 1nf1n17yk1ng/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/1nf1n17yk1ng/MS17-010_CVE-2017-0143

Reference: CVE-2017-0143
Description: crypticdante/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/crypticdante/MS17-010_CVE-2017-0143

Reference: CVE-2017-0144
Description: kimocoder/eternalblue exploit repository
Link: https://github.com/kimocoder/eternalblue

Reference: CVE-2017-0143
Description: n3ov4n1sh/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/n3ov4n1sh/MS17-010_CVE-2017-0143

Reference: CVE-2017-0143

Description: H3xL00m/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/H3xL00m/MS17-010_CVE-2017-0143

Reference: CVE-2017-0143
Description: c0d3cr4f73r/MS17-010_CVE-2017-0143 exploit repository
Link: https://github.com/c0d3cr4f73r/MS17-010_CVE-2017-0143

coreimpact
Reference: CVE-2017-0143
Description: MS17-010 support update 2
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev
Reference: CVE-2017-0143
Description: Microsoft Windows SMBv1 Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2017-0144
Description: Microsoft SMBv1 Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2017-0145
Description: Microsoft SMBv1 Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2017-0146
Description: Microsoft Windows SMB Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2017-0147
Description: Microsoft Windows SMBv1 Information Disclosure Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Reference: CVE-2017-0148
Description: Microsoft SMBv1 Server Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

gist
Reference: CVE-2017-0144
Description: Windows x64 and x86 kernel shellcode for eternalblue exploit
Link: https://gist.github.com/worawit/05105fce9e126ac9c85325f0b05d6501

Reference: CVE-2017-0144
Description: Eternalblue exploit for Windows 7/2008
Link: https://gist.github.com/worawit/bd04bad3cd231474763b873df081c09a

Reference: CVE-2017-0144
Description: Eternalblue exploit for Windows 8/2012
Link: https://gist.github.com/worawit/074a27e90a3686506fc586249934a30e

google-0day-itw
Reference: CVE-2017-0144
Description: Microsoft Windows Buffer overflow in SMB File Extended Attributes (EternalBlue)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2017-0145
Description: Microsoft Windows Unspecified type confusion in SMB (EternalRomance)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2017-0146
Description: Microsoft Windows Race condition in SMB transactions (EternalChampion)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2017-0147
Description: Microsoft Windows Information leak in SMB transactions (EternalChampion)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

Reference: CVE-2017-0143
Description: Microsoft Windows Type confusion in SMB messages (EternalSynergy)
Link: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

ASSOCIATED MALWARE:

Qualys Cloud Threat DB

Malware ID: Lucifer
Type: Ransomware
Link: https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

Malware ID: Conti
Type: Ransomware
Link: https://www.fortinet.com/blog/threat-research/affiliates-cookbook-firsthand-peek-into-operations-and-tradecraft-of-conti

Malware ID: NotPetya
Type: Ransomware
Link: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Malware ID: Petya
Type: Ransomware
Link: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Malware ID: Ryuk
Type: Ransomware
Link: https://cybersecurity.bd.com/bulletins-and-patches/ryuk-ransomware

Malware ID: STOP
Type: Ransomware
Link: https://www.cyberswachhtakendra.gov.in/alerts/STOP_ransomware.html

Malware ID: Satan
Type: Ransomware
Link: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Malware ID: UIWIX
Type: Ransomware
Link: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Malware ID: WannaCry
Type: Ransomware
Link: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

Malware ID: Lucifer
Type: Ransomware
Link: https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

RESULTS:

Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers detected on port 445 over TCP.

5 EOL/Obsolete Operating System: Microsoft Windows 7 Detected

QID:	105793
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	EOL-Windows 7
Bugtraq ID:	-
Service Modified:	07/18/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

After 10 years, support for Windows 7 is coming to an end on January 14, 2020.
Microsoft will no longer provide security updates or support for PCs running the Windows 7 operating system. After this date, this product will no longer receive free:
- Technical support for any issues
- Software updates
- Security updates or fixes
- Computers running the Windows 7 operating system will continue to work even after support ends. However, using unsupported software may increase the risks from viruses and other security threats.
Affected Versions:Windows 7

IMPACT:

Microsoft no longer provides security updates. Obsolete software is more vulnerable to viruses,malware and other attacks.

SOLUTION:

The Vendor has advised (https://www.microsoft.com/en-us/windows/windows-7-end-of-life-support-information) customers to update to the latest supported version of Windows 10 (https://www.microsoft.com/en-in/windows/get-windows-10).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Obsolete operating system Microsoft Windows 7 detected remotely

3 SMB Signing Disabled or SMB Signing Not Required

QID:	90043
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/25/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.
Please refer to Microsoft's article 887429 (http://support.microsoft.com/kb/887429) and The Basics of SMB Signing (covering both SMB1 and SMB2) (https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2) for information on enabling SMB signing.
For Windows Server 2008 R2, Windows Server 2012, please refer to Microsoft's article Require SMB Security Signatures (http://technet.microsoft.com/en-us/library/cc731957.aspx) for information on enabling SMB signing. For group policies please refer to Microsoft's article Modify Security Policies in Default Domain Controllers Policy (http://technet.microsoft.com/en-us/library/cc731654)
For UNIX systems
To require samba clients running "smbclient" to use packet signing, add the following to the "[global]" section of the Samba configuration file:
client signing = mandatory

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

 2 NetBIOS Name Accessible

QID:	70000
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WINDOWS-7-ENTER

Information Gathered (21)

3 NetBIOS Bindings Information

QID:	70004
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be accessible to external networks, and should be firewalled.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Service	NetBIOS Suffix
WINDOWS-7-ENTER	Workstation Service	0x0
WORKGROUP	Domain Name	0x0
WINDOWS-7-ENTER	File Server Service	0x20
WORKGROUP	Browser Service Elections	0x1e
WORKGROUP	Master Browser	0x1d
..__MSBROWSE__.	Master Browser	0x1

3 RPC Portmapper Information

QID:	125001
Category:	Forensics
Associated CVEs:	CVE-1999-0632
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2024
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The result section shows the information received by making an RPC call to the portmapper on the target host. It shows the list of all registered RPC programs.

IMPACT:

N/A

SOLUTION:

Check to be sure that the information reported adheres to your security policy.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

RPC detected on UDP port 500.
RPC detected on UDP port 138.
RPC detected on UDP port 1900.

2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/26/2024
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 7 Service Pack 1	CIFS via TCP Port 445	
Windows 2008 R2/7	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	TCP/IP Fingerprint	U3414:135

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc
Microsoft Security Account Manager	1.0	49158			\pipe\lsass
Microsoft Service Control Service	2.0	49155			
Microsoft Spool Subsystem	1.0	49159			
Microsoft Task Scheduler	1.0				\PIPE\atsvc
(Unknown Service)	1.0	49152			\PIPE\InitShutdown
(Unknown Service)	1.0				\PIPE\InitShutdown
Security Center	1.0	49153			\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0	49153			\pipe\eventlog

DHCP Client LRPC Endpoint	1.0	49153	\pipe\eventlog
NRP server endpoint	1.0	49153	\pipe\eventlog
Event log TCPIP	1.0	49153	\pipe\eventlog
AppInfo	1.0	49154	\PIPE\srvsvc, \PIPE\atsvc
XactSrv service	1.0	49154	\PIPE\atsvc
IP Transition Configuration endpoint	1.0	49154	\PIPE\atsvc
IKE/Authip API	1.0	49154	\PIPE\atsvc
(Unknown Service)	1.0	49154	\PIPE\atsvc
(Unknown Service)	1.0		\pipe\trkwks
Remote Fw APIs	1.0	49159	

 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 135, the host's uptime is 0 days, 0 hours, and 11 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

 1 DNS Host Name

QID: 6
Category: Information gathering
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/04/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
10.0.0.6	No registered hostname

1 Network Adapter MAC Address

QID:	43007
Category:	Hardware
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

It is possible to obtain the MAC address information of the network adapters on the target system. Various sources such as SNMP and NetBIOS provide such information. This vulnerability test attempts to gather and report on this information in a table format.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Method	MAC Address	Vendor
NBTSTAT	08:00:27:96:CB:B6	CADMUS COMPUTER SYSTEMS

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 288 seconds

Start time: Thu, Feb 29 2024, 03:55:52 GMT

End time: Thu, Feb 29 2024, 04:00:40 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
Windows-7-Enter	NTLM DNS
WINDOWS-7-ENTER	NTLM NetBIOS
WINDOWS-7-ENTER	NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering

Associated CVEs:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/22/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:

N/A

SOLUTION:

For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:11
TCP	445	0:01:00
UDP	137	0:00:56
UDP	138	0:00:07

UDP	500	0:00:12
UDP	1900	0:00:12

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default
CIFS Version	SMB v2.1

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
500	isakmp	isakmp	unknown
1900	unknown	unknown	unknown

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2023
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	microsoft-ds	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	03:57:36 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1043	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2801	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 161	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 40422	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 3700	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 21544	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7308	Port Unreachable

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WINDOWS-7-ENTER

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is -2147483648 with a standard deviation of 1903075126. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(20272 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 8 milli seconds

1 NetBIOS Workgroup Name Detected

QID:	82062
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/01/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS workgroup or domain name for this system has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WORKGROUP

Appendix

Hosts Scanned (IP)

10.0.0.6

Target distribution across scanner appliances

CyberSola : 10.0.0.4, 10.0.0.6

Hosts Not Scanned

Scan Canceled by User (IP) (1)

10.0.0.4

Options Profile

Basic Net Scan

Scan Settings	
Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco/Network SSH:	Disabled
Unix Least Privilege Authentication:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled

MS SharePoint:	Disabled
Sybase:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled
NGINX:	Disabled
Infoblox:	Disabled
BIND:	Disabled
Cisco_APIC:	Disabled
Overall Performance:	Normal
Additional Certificate Detection:	
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

Severity	Level	Description
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.