

OpenVAS

Learn the basics of threat and vulnerability management using Open Vulnerability Assessment Scanning

Task 7 Practical Vulnerability Management

Question: **When did the scan start in Case 001?**

Answer: **Feb 28, 00:04:46**

Host Summary							
Host	Start	End	High	Medium	Low	Log	False Positive
10.10.148.71	Feb 28, 00:04:46	Feb 28, 00:21:02	1	3	1	0	0
Total: 1			1	3	1	0	0

Question: **When did the scan end in Case 001?**

Answer: **Feb 28, 00:21:02**

Host Summary							
Host	Start	End	High	Medium	Low	Log	False Positive
10.10.148.71	Feb 28, 00:04:46	Feb 28, 00:21:02	1	3	1	0	0
Total: 1			1	3	1	0	0

Question: **How many ports are open in Case 001?**

Answer: **3**

Port Summary for Host 10.10.148.71	
Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
general/tcp	Low
445/tcp	High

Question: **How many total vulnerabilities were found in Case 001?**

Answer: **5**

Security Issues for Host 10.10.148.71	
High (CVSS: 9.3) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)	445/tcp
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.	

1

Medium (CVSS: 5.0) NVT: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)	2	135/tcp
Summary Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.		
Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)	3	3389/tcp
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.		
Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)	4	3389/tcp
Summary The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.		
Low (CVSS: 2.6) NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)	5	general/tcp
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.		

Question: What is the highest severity vulnerability found? (MSxx-xxx)

Answer: MS17-010

Security Issues for Host 10.10.148.71		
High (CVSS: 9.3) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)		445/tcp
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.		

Question: What is the first affected OS to this vulnerability?

Answer: Microsoft Windows 10 x32/x64 Edition

Security Issues for Host 10.10.148.71		
High (CVSS: 9.3) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)		445/tcp
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.		
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.		
Impact Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.		
Solution Solution type: VendorFix Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory		
Affected Software/OS Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2		

Question: What is the recommended vulnerability detection method?

Answer: Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability

Security Issues for Host 10.10.148.71	
High (CVSS: 9.3) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)	445/tcp
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.	
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.	
Impact Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.	
Solution Solution type: VendorFix Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory	
Affected Software/OS Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2	
Vulnerability Insight Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.	
Vulnerability Detection Method Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability. Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676) Version used: \$Revision: 11874 \$	

END.