Scan Report

February 22, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 6.87.153.210". The scan started at Sat Feb 22 08:40:22 2025 UTC and ended at Sat Feb 22 08:46:05 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
6.87.153.210	2	0	0	12	0
Total: 1	2	0	0	12	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 14 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 6.87.153.210

Host scan start	Sat Feb 22 08:40:40 2025 UTC
Host scan end	Sat Feb 22 08:46:05 2025 UTC

Service (Port)	Threat Level
445/tcp	High
general/tcp	High
445/tcp	Log
general/CPE-T	Log
135/tcp	Log
general/tcp	Log
general/SMBClient	Log
2638/tcp	Log
general/icmp	Log
139/tcp	Log

2.1.1 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

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
The vendor has released updates. Please see the references for more information.

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: `2019-05-03T10:54:50+0000`

References
```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

[return to 6.87.153.210]

2.1.2 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result
`cpe:/o:microsoft:windows_xp`

... continues on next page ...

... continued from previous page ...

Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "Windows XP" Operating System on the remote host has reached the end of life
↪.
CPE: cpe:/o:microsoft:windows_xp
EOL date: 2014-04-08
EOL info: https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Microsoft%20Windows%20XP&Filter=FilterNO

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:microsoft:windows_xp
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 6.87.153.210]

2.1.3 Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary
Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result
SMB signing is disabled on this host

Log Method

... continues on next page ...

... continued from previous page ...

Details: Microsoft SMB Signing Disabled
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: $Revision: 11003 $

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 2000 LAN Manager
Detected OS: Windows 5.1

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-04-24T11:06:32+0000

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
Only SMBv1 is enabled on remote target

Log Method
Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: $Revision: 10898 $

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

A CIFS server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 6.87.153.210]

2.1.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
6.87.153.210|cpe:/o:microsoft:windows_xp

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References
Other:
URL:http://cpe.mitre.org/

[return to 6.87.153.210]

2.1.5 Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

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.
The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A DCE endpoint resolution service seems to be running on this port.

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this port.

Log Method
Details: DCE/RPC and MSRPC Services Enumeration
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: $Revision: 11885 $

[return to 6.87.153.210]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Windows XP
CPE: cpe:/o:microsoft:windows_xp
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows 5.1; SMB Str
↪ing: Windows 2000 LAN Manager
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
```

Log Method

... continues on next page ...

... continued from previous page ...

Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 27.37.47.110 to 6.87.153.210:
27.37.47.110
6.87.153.210

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 6.87.153.210]

2.1.7 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script reports information about the SMB server of the remote host collected with the 'smbclient' tool.

Vulnerability Detection Result
Error getting SMB-Data -> SESSION SETUP FAILED: NT_STATUS_INVALID_PARAMETER

Log Method

... continues on next page ...

. . . continued from previous page . . .

Details: SMB Test with 'smbclient'
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: $Revision: 13274 $

[return to 6.87.153.210]

2.1.8 Log 2638/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result
```
Nmap service detection (unknown) result for this port: sybase
This is a guess. A confident identification of the service was not possible.
Hint: If you're running a recent nmap version try to run nmap with the following
↪ command: 'nmap -sV -Pn -p 2638 6.87.153.210' and submit a possible collected
↪fingerprint to the nmap database.
```

Log Method
Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: $Revision: 12934 $

References
```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 6.87.153.210]

2.1.9 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

[return to 6.87.153.210]

2.1.10 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
`A SMB server is running on this port`

Log Method
Details: `SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 13541 $`

[return to 6.87.153.210]