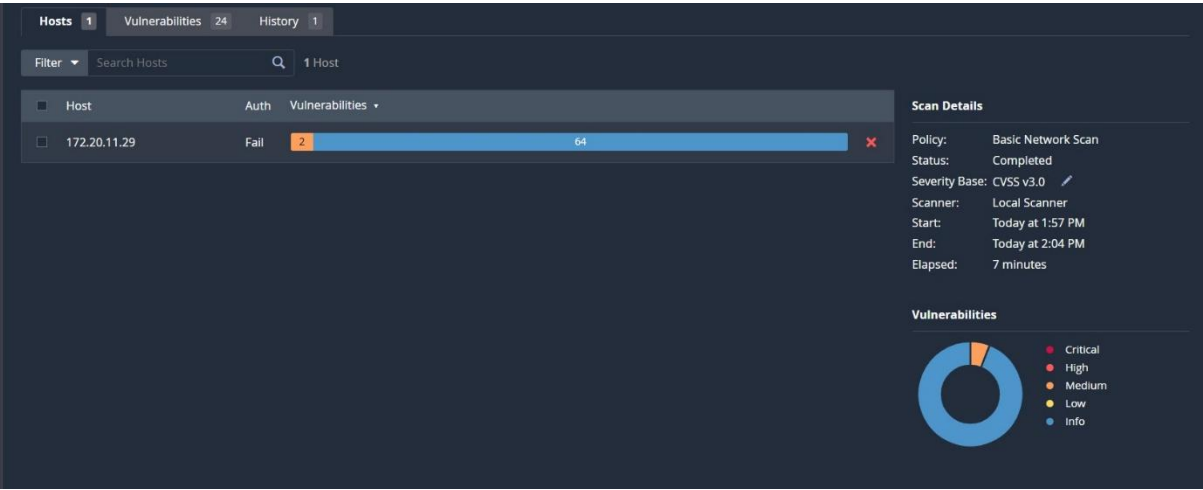


# Basic Networking Scan



Vulnerabilities 24

Filter Search Vulnerabilities 24 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
MEDIUM	5.3			SMB Signing not required	Misc.	1	
MIXED	...	...	...	SSL (Multiple Issues)	General	4	
INFO	...	...	...	SMB (Multiple Issues)	Windows	6	
INFO	...	...	...	HTTP Microsoft Windows (Multiple Issues)	ervers	2	
INFO	...	...	...	Microsoft Windows (Mult...	Windows	2	
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2	
INFO	...	...	...	Netstat Portscanner (SSH)	Port scanners	23	
INFO	...	...	...	DCE Services Enumeration	Windows	8	
INFO	...	...	...	Service Detection	Service detection	3	
INFO	...	...	...	Common Platform Enumerati...	General	1	
INFO	...	...	...	Device Type	General	1	
INFO	...	...	...	Host Fully Qualified Domain N...	General	1	
INFO	...	...	...	MySQL Server Detection	Databases	1	

**Host Details**

IP: 172.20.11.29  
OS: Windows 11  
Start: Today at 1:57 PM  
End: Today at 2:04 PM  
Elapsed: 7 minutes  
KB: [Download](#)  
Auth: Fail

**Vulnerabilities**

Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	1

**MEDIUM** SMB Signing not required

**Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**

<http://www.nessus.org/u7df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u774b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u7a3cac4ea>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	172.20.11.29

**Plugin Details**

Severity: Medium  
ID: 57608  
Version: 1.20  
Type: remote  
Family: Misc.  
Published: January 19, 2012  
Modified: October 5, 2022

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score: 5.3**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C  
CVSS v3.0 Temporal Score: 4.6  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Temporal Score: 3.7  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N  
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

**Vulnerability Information**

Exploit Available: true  
Exploit Ease: Exploits are available  
Vulnerability Pub Date: January 17, 2012

Vulnerabilities24

Search Vulnerabilities

4 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/>	MEDIUM	6.5		SSL Certificate Cannot Be Trusted	General	1	
<input type="checkbox"/>	INFO			SSL Certificate Information	General	1	
<input type="checkbox"/>	INFO			SSL Cipher Suites Supported	General	1	
<input type="checkbox"/>	INFO			SSL Perfect Forward Secrecy Cip...	General	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:57 PM  
End: Today at 2:04 PM  
Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Search Vulnerabilities

5 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/>	INFO			Microsoft Windows SMB Service ...	Windows	2	
<input type="checkbox"/>	INFO			Microsoft Windows SMB NativeL...	Windows	1	
<input type="checkbox"/>	INFO			Microsoft Windows SMB Version...	Windows	1	
<input type="checkbox"/>	INFO			Microsoft Windows SMB2 and S...	Windows	1	
<input type="checkbox"/>	INFO			Windows NetBIOS / SMB Remot...	Windows	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:57 PM  
End: Today at 2:04 PM  
Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Search Vulnerabilities

2 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/>	INFO			HTTP Server Type and Version	Web Servers	1	
<input type="checkbox"/>	INFO			HyperText Transfer Protocol (HT...	Web Servers	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:57 PM  
End: Today at 2:04 PM  
Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Search Vulnerabilities

2 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/>	INFO			Microsoft Windows NTLMSSP Au...	Windows	1	
<input type="checkbox"/>	INFO			WMI Not Available	Windows	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:57 PM  
End: Today at 2:04 PM  
Elapsed: 7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Search Vulnerabilities

2 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	EPSS	Name	Family	Count	
<input type="checkbox"/>	INFO				TLS Version 1.2 Protocol Detection	Service detection	1	
<input type="checkbox"/>	INFO				TLS Version 1.3 Protocol Detection	Service detection	1	

Scan Details

Policy:

Status:

Severity Base:

Scanner:

Start:

End:

Elapsed:

Basic Network Scan

Completed

CVSS v3.0

Local Scanner

Today at 1:57 PM

Today at 2:04 PM

7 minutes

Vulnerabilities

Critical

High

Medium

Low

Info