

# TP 9 Guillaume Sanchez

## Découverte de l'écosystème de la VM4

Après un scan de l'écosystème de la machine, NESSUS nous rapporte que 43 port sont ouvert :

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus SYN scanner	Port scanners	43

22, 135, 137, 139, 445, 1617, 3000, 3306, 3389, 3700, 4848, 5985, 7676, 8009, 8019, 8020, 8022, 8027, 8028, 8031, 8032, 8080, 8181, 8282, 8383, 8443, 8444, 8484, 8585, 8686, 9200, 9300, 47001, 49152, 49153, 49154, 49157, 49168, 49191, 49192, 49199, 49201, 49225, 49260

En cliquant dessus pour avoir plus d'information, il nous propose une description et une solution :

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

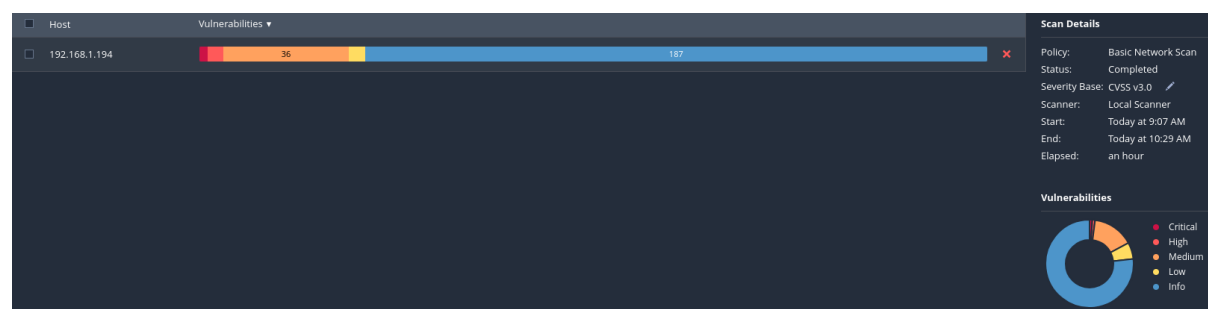
### Solution

Protect your target with an IP filter.

## Recherche des Vulnérabilités de la VM4

Après une découverte de l'écosystème, j'ai lancé un scan de vulnérabilité sur la machine. Le scan a trouvé en tout 45 vulnérabilités et 187 informations :

- 1 critique
- 4 fortes
- 36 moyennes
- 4 faibles



On peut voir plusieurs types de vulnérabilités, du ssl, du ssh, du smb etc. Certaines sont liées directement à des CVE.

Sev	CVSS	VPR	EPSS	Name	Family	Count	
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2	
MIXED	...	...	...	SSL (Multiple Issues)	General	51	
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1	
MIXED	...	...	...	TLS (Multiple Issues)	Service detection	17	
MIXED	...	...	...	IETF Md5 (Multiple Issues)	General	3	
MIXED	...	...	...	Openbsd Openssh (Multiple Issues)	Misc.	2	
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2	
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1	
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	7	
INFO	...	...	...	TLS (Multiple Issues)	General	13	

L'onglet qui a retenu mon attention, est le deuxième, beaucoup de problème lié au SSL. Dedans on y retrouve plus vulnérabilités :

HIGH	7.5	6.1	0.406	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5			SSL Certificate Cannot Be Trusted
MEDIUM	6.5			SSL Self-Signed Certificate
MEDIUM	5.3			SSL Certificate Expiry
MEDIUM	5.3			SSL Certificate with Wrong Hostname

La première vulnérabilité qui a une note de CVSSv3 de 7,5, concerne les ports 4848, 3820, 8181 et 8383 et est liée directement à une CVE : [CVE-2016-2183](#).

### SSL Medium Strength Cipher Suites Supported (SWEET32)

**Description**

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths of least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

**Solution**

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

**See Also**

<https://www.seebug.org/vulns/2016/2183/>  
<https://www.exploit-db.com/exploits/2183/>

**Output**

No output recorded.

No test details logs, please visit individual host

Port	Hosts
4848 /tcp /www	192.168.1.194
3820 /tcp /grip	192.168.1.194
8181 /tcp /www	192.168.1.194
8383 /tcp /www	192.168.1.194

**Plugin Details**

Severity: High  
ID: 42875  
Version: 1.22  
Type: remote  
Family: General  
Published: November 22, 2009  
Modified: February 12, 2023

**VPR Key Drivers**

Threat Reconn: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: PoC  
Age of Vuln: 730 days +  
Product Coverage: High  
CVSSv3 Impact Score: 3.6  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 6.1  
Exploit Prediction Scoring System (EPSS): 0.406  
Risk Factor: Medium  
CVSS v3.0 Base Score: 7.5  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:0/CWE:312/2016-2183  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:L/AU:N/C:P/N/A/N

**Vulnerability Information**

Vulnerability Pub Date: August 24, 2016  
In the News: true

**Reference Information**

CVE: CVE-2016-2183

Une seconde vulnérabilité qui a retenue mon attention est la “SSL Anonymous Cipher Suites Supported” qui concerne les port 8031 / tcp et qui est liée à une CVE : [CVE-2007-1858](#)

SSL Anonymous Cipher Suites Supported

**Description**

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

**Solution**

Reconfigure the affected application if possible to avoid use of weak ciphers.

**See Also**

<http://www.venous.org/76646666>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
8031/tcp	192.168.1.194 if

Plugin details

Severity: Medium

ID: 31702

Version: 1.91

Type: remote

Family: Service detection

Published: March 28, 2008

Modified: October 27, 2023

**VPE Key Drivers**

Threat Recon: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 738 days +

Product Coverage: Low

CVE(s) Impact Score: 3.8

Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 4.4

Exploit Prediction Scoring System (EPSS): 0.027

Risk Factor: Low

CVE(s) v3.0 Base Score: 6.9

CVE(s) v3.0 Vector: CVSS:3.0/AV/NA/C:H/PR:N/UI/N/SU:C/H/NA/NA

CVE(s) v3.0 Temporal Vector: CVSS:3.0/E/URL/O/R/C

CVE(s) v3.0 Temporal Score: 5.2

CVE(s) v3.0 Base Score: 2.9

CVE(s) v3.0 Temporal Score: 1.9

CVE(s) v2.0 Vector: CVSS2:AV/NA/C:H/NA/NC/PR/UN/AN

CVE(s) v2.0 Temporal Vector: CVSS2:ES/URL/O/R/C

**Vulnerability Information**

CPE: cpe:/o:apache:tomcat

Exploit Available: false

Exploit Ease: No known exploits are available

Vulnerability Pub Date: May 9, 2007

**Reference Information**

BD: 26462

CVE: CVE-2007-1858

Une autre vulnérabilité qui a retenu mon attention est la ” ICMP Timestamp Request Remote Date Disclosure” qui concerne le port “0 / icmp”, plus précisément, cela permet à un attaquant de connaître la date définie sur la machine ciblée et donc de contourner les protocoles d'authentification basés sur le temps.Elle est liée à une CVE : [CVE-1999-0524](#)

ICMP Timestamp Request Remote Date Disclosure

**Description**

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthorized, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

**Solution**

Filter out the ICMP timestamp requests (73), and the outgoing ICMP timestamp replies (14).

**Output**

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
0/icmp	192.168.1.194 if

Plugin details

Severity: Low

ID: 10114

Version: 1.56

Type: remote

Family: General

Published: August 1, 1999

Modified: October 7, 2024

**VPE Key Drivers**

Threat Recon: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 738 days +

Product Coverage: Very High

CVE(s) Impact Score: 1.4

Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 2.2

Exploit Prediction Scoring System (EPSS): 0.0037

Risk Factor: Low

CVE(s) v3.0 Base Score: 2.1

CVE(s) v3.0 Vector: CVSS:3.0/AV/L/AC/L/NA/NC/PR/N/A/N

**Vulnerability Information**

Vulnerability Pub Date: August 1, 1997

**Reference Information**

CVE: 200

CVE: CVE-1999-0524

Nessus nous parle également du fait que le Système d'exploitation Windows non pris en charge. En effet l'os n'est plus pris en charge et donc il est susceptible de contenir des failles de sécurité.

**CRITICAL** Unsupported Windows OS (remote)

**Description**  
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

**Solution**  
Upgrade to a supported service pack or operating system