

# S5 L4

## Svolgimento Progetto

Giulia Salani

# Consegna

## Traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono: Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni Familiarizzare con alcune delle vulnerabilità note che troverete spesso.

Svolgimento

1. Ho installato Nessus su Kali, con scheda di rete in bridged.
2. Ho impostato la NIC in internal e modificato l'IP di Kali in modo che fosse sulla stessa rete di Meta.
3. A questo punto ho fatto partire la scansione su Meta.

Questo il riepilogo della scansione, con la distribuzione delle vulnerabilità per gravità:

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nessus Essentials / Folder x +

https://kali:8834/#/scans/reports/5/hosts

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

giusal

**Metasploitable**

Configure Audit Trail Launch Report Export

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Hosts 1 Vulnerabilities 65 Remediations 2 Notes 2 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.32.102	10 5 22 7 128

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 1:07 PM  
End: Today at 1:39 PM  
Elapsed: 32 minutes

**Vulnerabilities**

Donut chart showing vulnerability distribution by severity:

- Critical
- High
- Medium
- Low
- Info

CTRL (DESTRA)

13:40 21/12/2023

Nella tab «Vulnerabilities» è possibile approfondire una per una:

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nessus Essentials / Folder

https://kali:8834/#/scans/reports/5/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

giusal

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Metasploitable

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 65 Remediations 2 Notes 2 History 1

Filter Search Vulnerabilities 65 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
MIXED	...	...	SSL (Multiple Issues)	General	28	
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	

Plugin ID: 89058

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 1:07 PM

End: Today at 1:39 PM

Elapsed: 32 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

CTRL (DESTRA)

14:00 21/12/2023

Nella tab «Remediations», invece, è indicato come porvi rimedio:

The screenshot shows the Nessus Essentials web interface within a Kali Linux virtual machine. The browser address bar displays `https://kali:8834/#/scans/reports/5/remediations`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area is titled 'Metasploitable' and shows the 'Remediations' tab selected. A table lists two remediation actions:

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1

On the right, 'Scan Details' are provided: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 1:07 PM, End: Today at 1:39 PM, Elapsed: 32 minutes. The bottom of the image shows the Windows taskbar with various application icons and the system clock indicating 14:31 on 21/12/2023.

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

**CRITICAL** NFS Exported Share Information Disclosure**Description**

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Output**

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.32.102

La vulnerabilità indica che almeno una delle condivisioni NFS (Network File System) sul server remoto può essere montata dall'host di scansione. Questo potrebbe consentire a un attaccante di accedere e potenzialmente modificare file sul server attraverso NFS. Per mitigare, occorre limitare l'accesso NFS solo agli host autorizzati e configurare correttamente le autorizzazioni e le regole di firewall.

&lt; &gt;

**Plugin Details**

✎

Severity: Critical  
ID: 11356  
Version: 1.21  
Type: remote  
Family: RPC  
Published: March 12, 2003  
Modified: August 30, 2023

**VPR Key Drivers**

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Unproven  
Age of Vuln: 730 days +  
Product Coverage: Low  
CVSSv3 Impact Score: 5.9  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 5.9  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
/I:C/A:C

**Vulnerability Information**



Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

CRITICAL

## Unix Operating System Unsupported Version Detection

&lt; &gt;

## Plugin Details



## Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

## Solution

Upgrade to a version of the Unix operating system that is currently supported.

## Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .
```

For more information, see : <https://wiki.ubuntu.com/Releases>

To see debug logs, please visit individual host

Port ▲

Hosts

N/A

192.168.32.102

La vulnerabilità indica che il sistema Unix sul host remoto utilizza una versione non più supportata, rendendolo vulnerabile a potenziali minacce poiché non riceverà ulteriori patch di sicurezza dal produttore. Per mitigare, occorre aggiornare a una versione supportata o implementare misure di sicurezza aggiuntive per proteggere il sistema.

Severity: Critical  
ID: 33850  
Version: 1.289  
Type: combined  
Family: General  
Published: August 8, 2008  
Modified: October 18, 2023

## Risk Information

Risk Factor: Critical

## CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

## Vulnerability Information

Unsupported by vendor: true

## Reference Information

IAVA: 0001-A-0502, 0001-A-0648

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

**CRITICAL** VNC Server 'password' Password

&lt; &gt;

## Plugin Details

✎

**Description**

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**

Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.32.102

Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

**Risk Information**

Attack Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
C/A:C

**Vulnerability Information**

Default Account: true  
Exploited by Nessus: true

Questa vulnerabilità indica che il server VNC sull'host remoto è protetto da una password debole, come evidenziato dal fatto che Nessus è riuscito ad accedere utilizzando una password comune come 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare questa debolezza per assumere il controllo del sistema. Per mitigare, modificare immediatamente la password VNC passando ad una complessa e robusta e considerare l'implementazione di misure aggiuntive come l'uso di certificati, VPN o autenticazione a due fattori per rafforzare la sicurezza.

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

CRITICAL

## SSL Version 2 and 3 Protocol Detection

&lt; &gt;

## Plugin Details



## Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications.

Although SSL/TLS has a secure means for choosing the highest supported version of protocol (the client always chooses the highest version it and the server support nothing better), many web browsers implement this in an unsafe manner (e.g. POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communication. The use of SSL 3.0 will not meet the PCI SSC's definition of 'strong cryptography'.

## Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

## See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u?b06c7e95>  
<http://www.nessus.org/u?247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u?5d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

La vulnerabilità indica che il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, versioni vulnerabili a diversi difetti crittografici come schemi di padding insicuri e rinegoziazione non sicura. Questi difetti possono consentire a un attaccante di condurre attacchi di tipo "man-in-the-middle" o decifrare comunicazioni. È consigliato disabilitare completamente questi protocolli e utilizzare invece TLS 1.2 o versioni successive con suite crittografiche approvate.

Severity: Critical  
ID: 20007  
Version: 1.34  
Type: remote  
Family: Service detection  
Published: October 12, 2005  
Modified: April 4, 2022

## Risk Information

Risk Factor: Critical

## CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

## Vulnerability Information

In the news: true

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

CRITICAL

## Apache Tomcat AJP Connector Request Injection (Ghostcat)

&lt; &gt;

## Plugin Details

✎

## Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

## Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

## See Also

<http://www.nessus.org/u?8ebe6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eafcf70>

## Output

Nessus was able to exploit the issue using the following request:

```
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F ..
0x0010: 61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00 as
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .ld
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 ocal
00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep
63 63 65 70 74 2D 4C 61 6F 67 75 61 67 65 00 00 cept-Lan
```

Collapse Menu (/)

La vulnerabilità riguarda una vulnerabilità di lettura/inclusione file nel connettore AJP. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web o, se consentito, caricare codice maligno JSP per eseguire codice a distanza (RCE). Per mitigare, aggiorna la configurazione AJP per richiedere autorizzazione e/o esegui un aggiornamento del server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successive.

Severity: Critical  
ID: 134862  
Version: 1.42  
Type: remote  
Family: Web Servers  
Published: March 24, 2020  
Modified: September 25, 2023

## VPR Key Drivers

Great Recency: No recorded events  
Great Intensity: Very Low  
Exploit Code Maturity: High  
Age of Vuln: 730 days +  
Product Coverage: Very High  
SSV3 Impact Score: 5.9  
Great Sources: No recorded events

## Risk Information

Vulnerability Priority Rating (VPR): 9.0  
Risk Factor: High  
CVSS v3.0 Base Score 9.8  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N  
E:N/S:U/C:H/I:H/A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H  
URL:O/RC:C  
CVSS v3.0 Temporal Score: 9.4

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

**CRITICAL** Bind Shell Backdoor Detection

&lt; &gt;

Plugin Details

✎

**Description**

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution**

Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output**

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 li
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.32.102

Severity: Critical  
ID: 51988  
Version: 1.10  
Type: remote  
Family: Backdoors  
Published: February 15, 2011  
Modified: April 11, 2022

**Risk Information**

Risk Factor: Critical  
**SS v3.0 Base Score 9.8**  
SS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N  
:N/S:U/C:H/I:H/A:H  
SS v2.0 Base Score: 10.0  
SS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
C/A:C

La vulnerabilità indica che su una determinata porta remota è in ascolto una shell senza alcun meccanismo di autenticazione. Questo scenario potrebbe consentire a un attaccante di connettersi alla porta e inviare comandi direttamente, ottenendo un accesso non autorizzato al sistema. Per mitigare il rischio, è essenziale implementare misure di sicurezza come l'autenticazione o, se non necessario, disabilitare l'ascolto della shell sulla porta specificata.

Hosts 1

Vulnerabilities 65

Remediations 2

Notes 2

History 1

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**Description**

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

**Solution**

Consider all cryptographic material generated on the remote host to be guessable. In re-generated.

**See Also**<http://www.nessus.org/u?107f9bdc><http://www.nessus.org/u?f14f4224>**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.32.102
25 / tcp / smtp	192.168.32.102

**Plugin Details**

Severity:	Critical
ID:	32321
Version:	1.27
Type:	remote
Family:	Gain a shell remotely
Published:	May 15, 2008
Modified:	November 16, 2020

**VPR Key Drivers**

Great Recency:	No recorded events
Great Intensity:	Very Low
Exploit Code Maturity:	Functional
Age of Vuln:	730 days +
Product Coverage:	Low
SSV3 Impact Score:	5.9
Great Sources:	No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR):	7.4
Risk Factor:	Critical
SS v2.0 Base Score:	10.0
SS v2.0 Temporal Score:	8.3
SS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/C/A:C
CVSS v2.0 Temporal Vector:	CVSS2#E:F/RL:OF/RC:C

La vulnerabilità indica che il certificato x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu affetto da un difetto nel generatore di numeri casuali della sua libreria OpenSSL. A causa di questa mancanza di entropia, un attaccante potrebbe facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare le sessioni o eseguire un attacco "man-in-the-middle". Per risolvere, è necessario rigenerare il certificato con una versione corretta di OpenSSL e sostituire i certificati compromessi.