



# 55/45 PRESENTAZIONE

by

Luca Lenzi, Mario Reitano, Giovanni Sannino

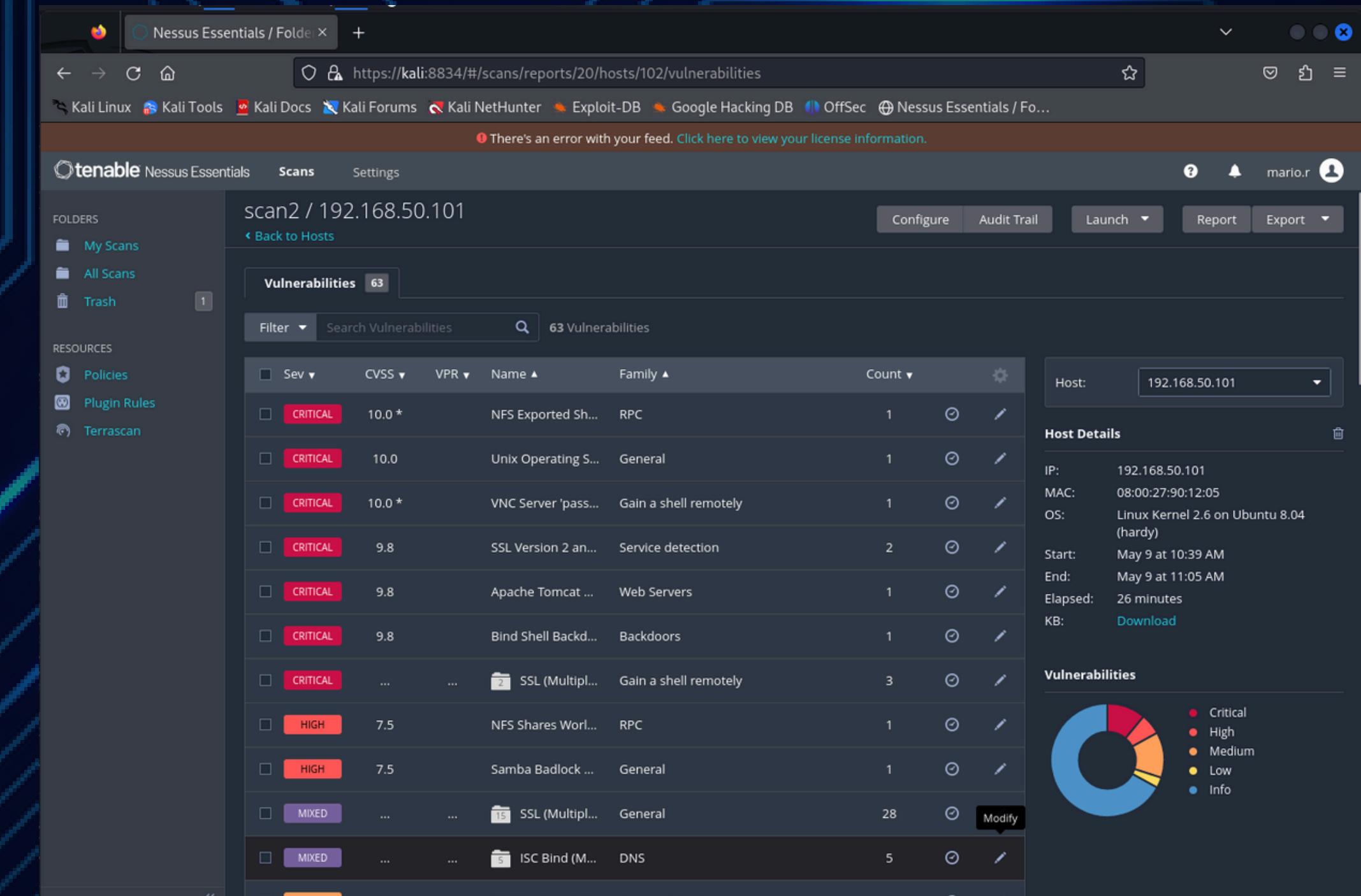
# Strumenti utilizzati

LABORATORI VIRTUALI  
METASPLOITABLE 2  
KALI LINUX

SCANNER DI RETE  
NESSUS  
NMAP

Traccia:

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.



# [1] VNC Server Password "password"

La password in questione è considerata "debole" o "facilmente rilevabile". Consigliamo l'utilizzo di una password più complessa, magari con l'utilizzo di maiuscole e caratteri speciali, per renderla più solida e meno facile da forzare in caso di attacchi "brute force".



scan2 / Plugin #61708

Vulnerabilities 63

CRITICAL VNC Server 'password' Password

**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	192.168.50.101

**Plugin Details**

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**

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**

Default Account:	true
Exploited by Nessus:	true

# [2] Unix Operating System Unsupported Version Detection

SCANZ / PLUGIN #33850

Configure Audit Trail Launch Report Export

Vulnerabilities 63

**CRITICAL** Unix Operating System Unsupported Version Detection

**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 (Server).  
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	192.168.50.101

Plugin Details

Severity:	Critical
ID:	33850
Version:	1.292
Type:	combined
Family:	General
Published:	August 8, 2008
Modified:	April 3, 2024

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/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

Unsupported by vendor: true

Reference Information

JAVA-2001-A-0502, 2001-A-0548

Abbiamo rilevato un sistema operativo obsoleto. L'azione consigliata è quella di installarne un nuovo seguendo le seguenti istruzioni. Ricordiamo inoltre che è buona norma mantere il sistema operativo costantemente aggiornato per avere una migliore protezione.

# Come risolvere?

Per cambiare il sistema operativo di una macchina virtuale Metasploitable 2, devi seguire questi passaggi:

- **Backup dei dati:** Prima di procedere con la modifica del sistema operativo, assicurati di fare un backup di tutti i dati importanti presenti sulla macchina virtuale Metasploitable 2. Questo è importante perché la modifica del sistema operativo comporterà la perdita di tutti i dati presenti sulla macchina virtuale.
- **Installazione del nuovo sistema operativo:** Scarica l'immagine ISO del sistema operativo che desideri installare sulla macchina virtuale. Puoi trovare molte distribuzioni Linux o altri sistemi operativi online gratuitamente. Utilizza il software di virtualizzazione che stai utilizzando per eseguire Metasploitable 2 (come VirtualBox o VMware) per creare una nuova macchina virtuale e installare il nuovo sistema operativo utilizzando l'immagine ISO scaricata.
- **Configurazione della nuova macchina virtuale:** Durante il processo di installazione del nuovo sistema operativo sulla nuova macchina virtuale, verranno richieste informazioni come nome utente, password, configurazioni di rete, ecc. Assicurati di configurare correttamente la nuova macchina virtuale secondo le tue preferenze e requisiti.



- **Test e verifica:** Dopo aver completato l'installazione del nuovo sistema operativo sulla nuova macchina virtuale, avvia la macchina virtuale e verifica che tutto funzioni correttamente. Assicurati che la nuova macchina virtuale sia accessibile e funzionante come previsto.
- **Eliminazione della vecchia macchina virtuale:** Una volta che hai verificato che la nuova macchina virtuale funziona correttamente e hai fatto il backup di tutti i dati importanti dalla vecchia macchina virtuale Metasploitable 2, puoi eliminare la vecchia macchina virtuale per liberare spazio di archiviazione e risorse di sistema.

Ricorda che la modifica del sistema operativo di una macchina virtuale comporta la perdita di tutti i dati presenti sulla vecchia macchina virtuale, quindi è importante eseguire il backup dei dati importanti prima di procedere



### Raccomandazioni utili:

Dopo aver risanato il sistema Metasploitable, è consigliabile implementare un firewall e configurare i permessi della porta interessata in modo che non sia più accessibile, prevenendo così la creazione di future backdoor.

Raccomandiamo inoltre di effettuare regolari controlli di sicurezza e di tenere sempre aggiornati i meccanismi di protezione per garantire la sicurezza continua del sistema.

scan2 / Plugin #51988

Configure Audit Trail Launch Report Export

Vulnerabilities 63

CRITICAL Bind Shell Backdoor Detection

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 :

```
----- 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 192.168.50.101

Plugin Details

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



Per risolvere il problema della backdoor, iniziamo con il controllo della porta in cui è situata. Possiamo farlo utilizzando il comando "netstat" per monitorare il traffico di rete direttamente sulla macchina Metasploitable. Tuttavia, data la limitata usabilità di questa opzione, consiglio l'uso di un port scanner esterno come Nmap o Nessus. Una volta identificata la porta in cui si trova la backdoor, valutiamo se è possibile manipolarla in modo sicuro. Se la porta è troppo fragile o pericolosa, è prudente ricorrere a un backup in cui la backdoor non è presente.

## Backdoor

Un altro processo di risoluzione per evitare di eseguire un backup potrebbe essere:

Procedendo con la linea di comando che vediamo nell'immagine a seguire abbiamo trovato l'informazione che rivela la backdoor la “PID” process ID, esso può essere eliminato rapidamente con il comando “kill” seguito dal PID in questione, tuttavia se non configuriamo differentemente la porta in questione il problema tornerà presto

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524          0.0.0.0:*
4495/xinetd                                         LISTEN
```



**GRAZIE**