Fix Vulnerabilities

In questo report si riportano quelle che sono state le *Fix* ad alcune delle vulnerabilità, presenti sull'host Metasploitable, presentate nel report "*Scan Technical Report*".
La prima fase presenterà le vulnerabilità a cui è stata implementata una *Remediation* , mentre la seconda fase presenterà le vulnerabilità a cui è stata implementata una *Mitigation*. In entrambi i casi ciò ha il fine di ridurre il rischio di possibili attacchi.

Remediations

Di seguito sono riportate le vulnerabilità a cui è stata applicata una Remediation.

- **Critical 5900/tcp** → VNC password = 'password'

Accesso al server VNC facilmente accessibile tramite *Brute Force* o password debole ("password"). Per questo fix si ha cambiato password con una più sicura.

New password → 'sicu05ms'

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

Verifica Fix: Stabilendo una connessione vnc (vncviewer) da kali a meta con cui provare la precedente password facilmente decifrabile, ricevendo 'Authentication failure' si ha la prova del fix.

```
┌──(root㉿kali)-[/home/kali]
└─# vncviewer 192.168.50.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

- **Critical 1524/tcp** → Ingreslock backdoor

Rilevata una *backdoor* sulla porta 1524. Per questo fix si ha modificato il file di configurazione inetd.conf, commentando la riga ingreslock che permette l'esecuzione della Bind Shell.

```
  GNU nano 2.0.7                File: inetd.conf                      Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Riavvio del servizio → */etc/init.d/openbsd-inetd restart* + reboot di metasploitable

Verifica Fix: A seguito del riavvio, è stato verificato tramite Nmap che la porta 1524 risulta ora in stato closed e il tentativo di connessione via Netcat restituisce *Connection Refused*.

```
┌──(root㉿kali)-[/etc]
└─# nc -v 192.168.50.101 1524
192.168.50.101: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

- **High 21/tcp** → FTP Brute Force Logins (Default Creds)

Rilevate credenziali deboli o di default (msfadmin:msfadmin, postgres:postgres, user:user, service:service), impattante su più servizi (FTP, Telnet, SSH). Permette accesso non autorizzato e modifica dei file.

Per questo fix bisogna mettere in sicurezza i login delle utenze segnalate, cambiando le password

New password msfadmin → 'meta05sp'
New password postgres → 'pg05log'
New password user → 'us05er'
New password service → '$er05vis'

```
msfadmin@metasploitable:~$ passwd
Changing password for msfadmin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Verifica Fix: verificando la connessione ftp con vecchie credenziali deboli. Gli screen mostrano il cambio password e la verifica per msfadmin.

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.50.101
Connected to 192.168.50.101.
220 (vsFTPd 2.3.4)
Name (192.168.50.101:kali): msfadmin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

Mitigations

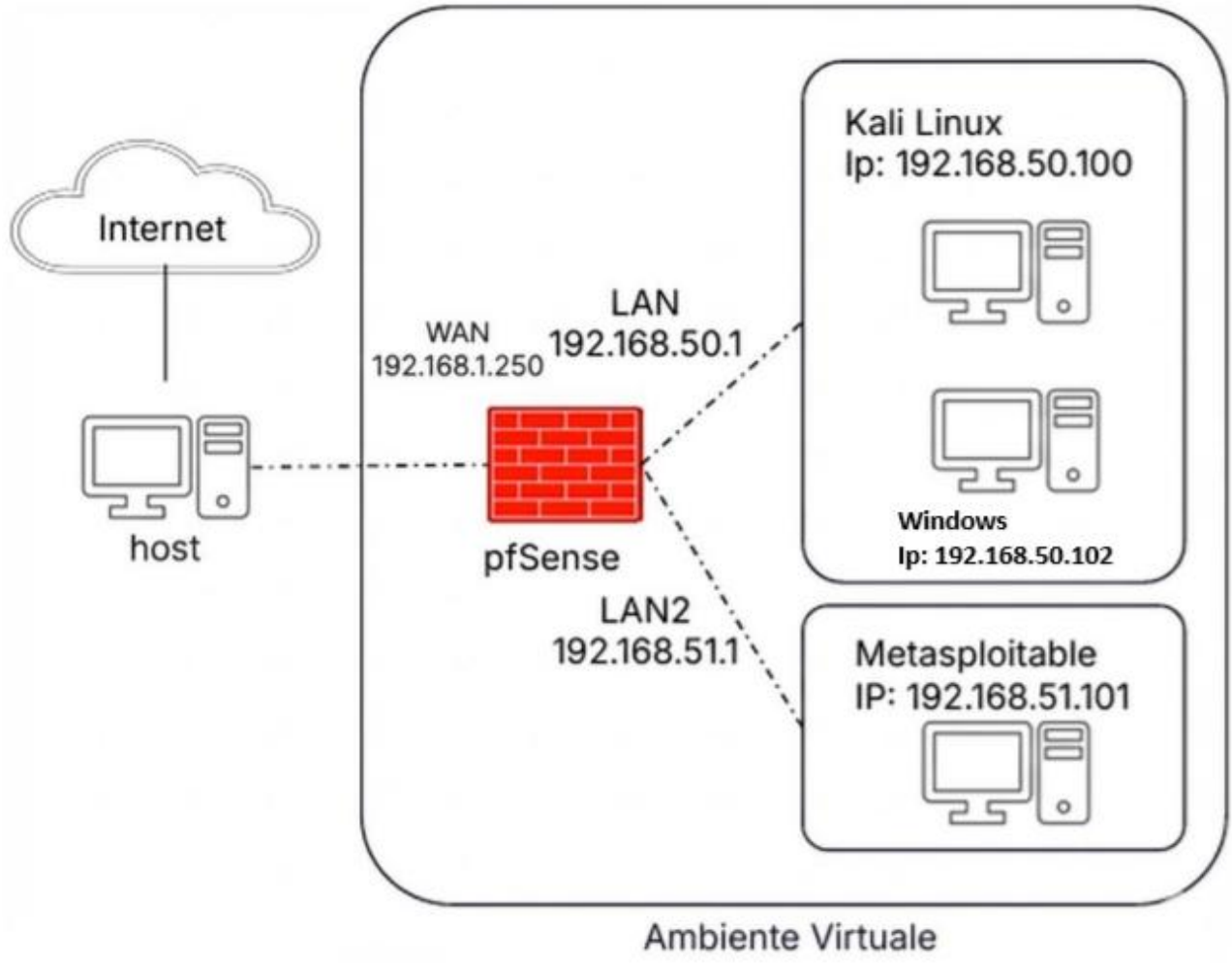
Di seguito sono riportate le vulnerabilità a cui è stata applicata una Mitigation, più nello specifico tramite il settaggio di regole Firewall, con l'utilizzo di Pfsense.

- **Medium 22/tcp** → Weak SSH Algorithms Supported

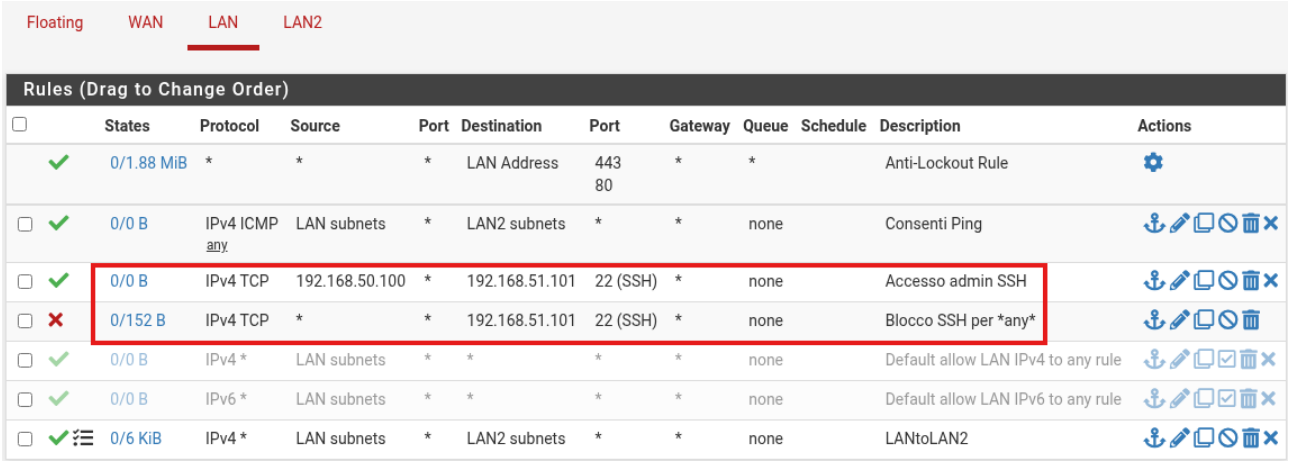
- **Low 22/tcp** → Weak MAC Algorithm(s) Supported

L'host Metasploitable supporta algoritmi di cifratura e MAC (Message Authentication Code) deboli (Arcfour, MD5, ssh-dss, gruppi DH piccoli).

Per questo Fix si ha configurato il Firewall *Pfsense* affinchè si applicasse una *Segmentation* dell'*Ambiente Virtuale* (come mostrato nell'immagine sottostante).



Con la creazione di 2 *rules* è stato applicato un approccio di *Whitelisting*: tutto il traffico verso la porta 22 è bloccato di default (Deny All), eccetto quello proveniente dall'IP di gestione autorizzato.



N.B.: l'ordine delle rules è cruciale, in questo modo prima verrà vista la regola che consente l'accesso dall'IP autorizzato (Kali) e poi verrà vista la regola che blocca l'accesso da qualunque altro host. Come ultima regola è presente il Pass di tutto il traffico iPv4 da LAN a LAN2, non disabilitata data la sua utilità nel consentire anche la scansione di gvm.
Questo vale per il modo di ragionare dei Firewall (*First Match Wins*)

Verifica Fix: Attraverso il comando Telnet da vm Windows (situata in LAN) si verifica il non raggiungimento alla porta 22 del target.

```
C:\Users\user>telnet 192.168.51.101 22
Connessione a 192.168.51.101...Impossibile aprire una connessione con l'host. sulla porta 22: Connessione non riuscita
```

Test raggiungimento da ip autorizzato(Kali):

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 22 192.168.51.101
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-23 15:03 -0500
Nmap scan report for 192.168.51.101
Host is up (0.0042s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

Conclusioni

In un sistema vulnerabile come Metasploitable andrebbero applicate Remediation più mirate, la mitigazione tramite Firewall è un ottimo modo per ridurre il rischio quando non si può fare a meno di modificare una configurazione vulnerabile, lasciando però un *Rischio Residuo*.

Durante il report sono state presentate le Remediation applicate in un momento antecedente alla Mitigation con Pfsense ed è per questo motivo che l'ip del target varia andando avanti con la lettura.