

REPORT 2

**Remediation delle
Vulnerabilità di Meta
M3W12-D4**

22 / 11 / 2024

Cybersecurity Analyst

Remediation delle Vulnerabilità su Metasploitable
Matteo Madonia

SOMMARIO

1. Traccia e consegna_____	Pag. 2
2. Considerazioni iniziali - Remediation_____	Pag. 2
3. Informazioni preliminari_____	Pag. 2
4. Informazioni generali VM_____	Pag. 2
5. Report della scansione iniziale_____	Pag. 3
6. Intervention priority Timeline delle Vulnerabilità _____	Pag. 8
7. Remediation delle Vulnerabilità note_____	Pag. 9
8. Considerazioni finali _____	Pag. 18



1. Traccia e consegna

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche 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.

Consegna numero 2: Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf

2

2. Considerazioni iniziali - Remediation

In seguito alla scansione di Vulnerability Assessment effettuata con il tool professionale Nessus, sono state individuate molte Vulnerabilità CRITICHE su porte aperte e servizi in ascolto. In seguito all'analisi e individuazione di 4 di esse, procediamo ora alla fase di REMEDIATION per la correzione di tali vulnerabilità, nell'ottica di diminuire drasticamente l'indice di criticità e ridurre il fattore RISCHIO ad un RISCHIO RESIDUO.

Nota bene: si riporta nuovamente di seguito il report estratto dal tool Nessus in seguito alla scansione.

3. Informazioni preliminari

MV in esame:

- KALI LINUX: VM source scheda di rete in Bridge
- Metasploitable: VM target oggetto d'esame, scheda di rete in Bridge

Firewall:

- iptables

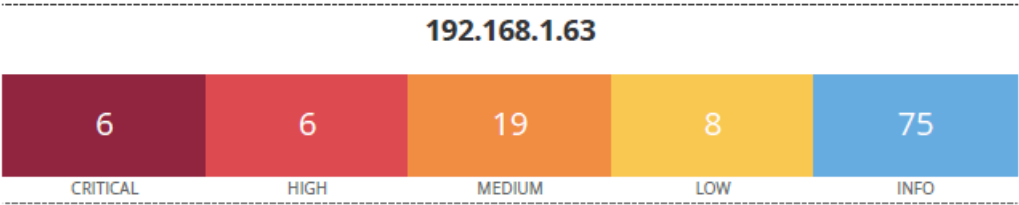
4. Informazioni generali VM

- IP VM target: 192.168.1.63/24 (Metasploitable) – rilasciato in DHCP
- IP VM source: 192.168.1.109/24 (Kali Linux) – rilasciato in DHCP

Nota Bene: gli indirizzi IP durante i report potrebbero subire variazioni, in quanto rilasciati in DHCP, per aver eseguito gli esercizi in momenti e luoghi differenti, quindi diverse reti.

5.Report della scansione iniziale

LEGENDA:
Richiesta Remediation su Vulnerabilità = ➡



Vulnerabilities

Total: 114

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6661	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.1395	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonir
MEDIUM	6.5	4.4	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server

MEDIUM	5.9	4.4	0.9717	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9434	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.0114	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.4	0.6115	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.9736	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	0.9736	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	0.9749	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version

INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	10437	NFS Share Export List

INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	10180	Ping the remote host
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported

INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

6. Intervention priority timeline delle Vulnerabilità



61708 - VNC Server 'password' Password – Porta tcp/5900/vnc	46882 - UnrealIRCd Backdoor Detection – Porta tcp/6667/irc	32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness Porta tcp/22/ssh E 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	51988 - Bind Shell Backdoor Detection – Porta tcp/1524/wild_shell
CRITICA	CRITICA	CRITICA	CRITICA
Richiesto intervento immediato, nell’arco di pochi giorni	Richiesto intervento immediato, nell’arco di pochi giorni	Richiesto intervento immediato, nell’arco di pochi giorni	Richiesto intervento immediato, nell’arco di pochi giorni; precedenza ai primi 3 descritti

7. Remediation delle Vulnerabilità note

- 61708 - VNC Server 'password' Password – Porta tcp/5900/vnc

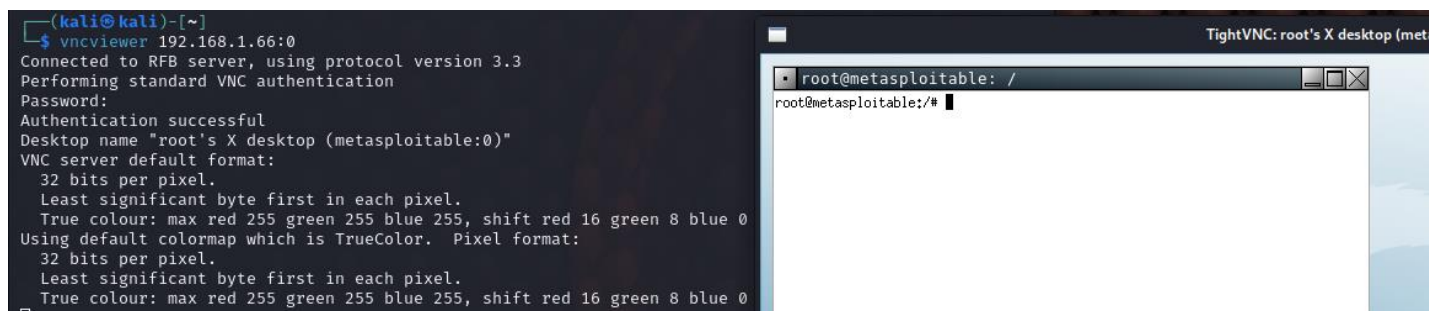
Per il diminuire il fattore di RISCHIO CRITICO ad un livello di fattore di RISCHIO RESIDUO accettabile, la strada più semplice è quella di disabilitare l'accesso remoto al server VNC sulla macchina, ma in caso di occorrenza non risulterebbe più attivo e quindi utilizzabile.

Procediamo quindi con la variazione della password di default 'password', in una molto più sicura ed efficiente, utilizzando una struttura alfa-numerica contenente inoltre simboli speciali

Premessa:

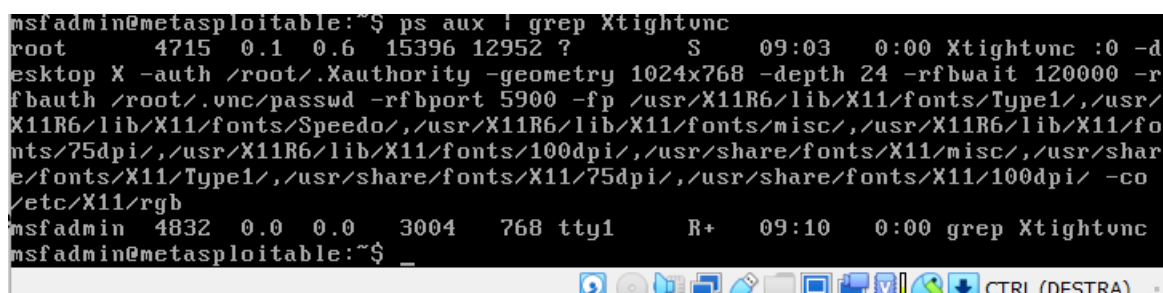
VM Metasploitable attiva – indirizzo scheda di rete rilasciato in DHCP 192.168.1.66

1. Con il comando `vncviewer 192.168.1.66:0` da shell Kali linux verificare la connessione con il server sulla sessione :0 (la sessione :0 corrisponde alla porta 5900) inserendo la password di default impostata da Meta: 'password' – login di connessione avvenuta con successo



2. Prendere il comando da shell di Meta come amministratore (Root): `sudo su`
E' importante eseguire i prossimi STEP come ROOT!!
3. Verificare con il comando `ps aux | grep Xtightvnc` su Meta che il servizio VNC su Meta sia attivo e in esecuzione come segue:

Il servizio è attivo sulla sessione :0



4. Impostare la nuova password per il server VNC sulla sessione :0 con il seguente comando: vncpasswd
Seguire attentamente tutte le istruzioni

```
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

E' stata impostata la password: Met@100! (anche per la sola visualizzazione)

5. Terminare il processo della sessione vncserver :0 come segue: comando vncserver -kill :0
Questo e il prossimo step sono necessari per il refresh del processo del server VNC

```
root@metasploitable:~# vncserver -kill
TightVNC server version 1.2.9

Usage: vncserver [<OPTIONS>] [:<DISPLAY#>]
       vncserver -kill :<DISPLAY#>

<OPTIONS> are Xtightvnc options, or:

    -name <DESKTOP-NAME>
    -depth <DEPTH>
    -geometry <WIDTH>x<HEIGHT>
    -httpport number
    -basehttpport number
    -alwaysshared
    -nevershared
    -pixelformat rgb<NNN>
    -pixelformat bgr<NNN>

See tightvncserver and Xtightvnc manual pages for more information.
root@metasploitable:~# vncserver -kill :0
Killing Xtightvnc process ID 4740
```

6. Riattivare il processo vncserver :0 come segue: comando vncserver :0

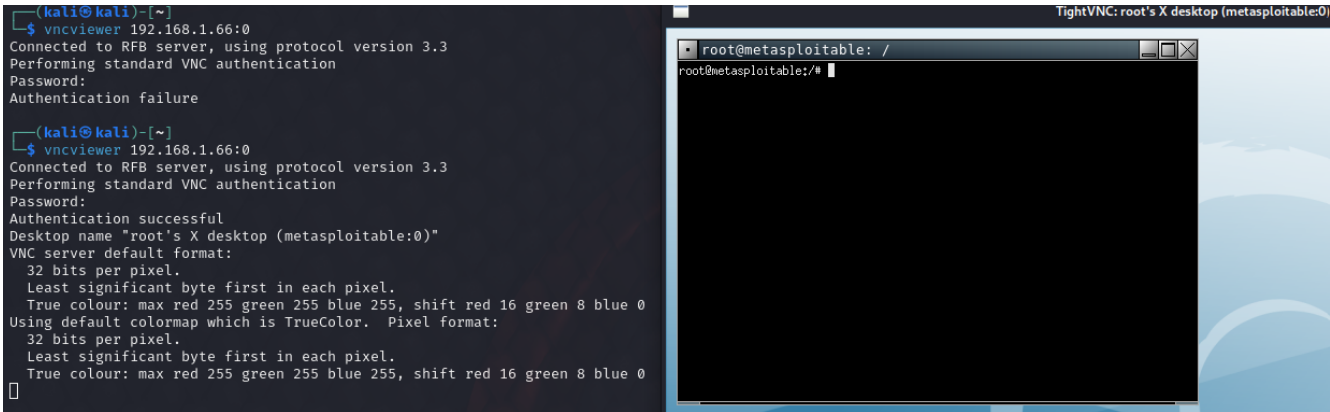
```
root@metasploitable:~# vncserver :0

New 'X' desktop is metasploitable:0

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:0.log

root@metasploitable:~#
```

7. Da shell di Kali Linux riprovare il collegamento al server VNC di Meta, sulla sessione :0, corrispondente alla porta aperta 5900, come segue con il comando: `vncviewer 192.168.1.66:0`
NOTA BENE: nel primo step di autenticazione ho inserito la password 'password' che Meta usa di default -> autenticazione fallita!
Nel secondo step ho utilizzato la Password da me impostata: `Met@100!` -> autenticazione avvenuta con successo!



8. Effettuare una prova di scansione con il tool di VA Nessus e verificare che la vulnerabilità non si trovi più in un range di CRITICITA' elevata, come di seguito:

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/>	INFO				VNC Server Security Type Detection	Service detection
<input type="checkbox"/>	INFO				VNC Server Unencrypted Communication Detection	Service detection
<input type="checkbox"/>	INFO				VNC Software Detection	Service detection

Possiamo concludere che le operazioni di REMEDIATION per questa vulnerabilità sono andate a buon fine, che con il cambio della password di default in una più forte e sicura, la criticità è diminuita drasticamente, ottenendo un rischio residuo più che accettabile.

- 51988 - Bind Shell Backdoor Detection – Porta tcp/1524/wild_shell

Per il diminuire il fattore di RISCHIO CRITICO ad un livello di fattore di RISCHIO RESIDUO accettabile, è possibile in questo caso, chiudere tutte le porte non necessarie, come per la porta tcp/1524. Su questa porta aperta e servizio in ascolto, con accesso senza autenticazione, potrebbe essere presente una backdoor che mi permette di eseguire una shell di comando chiamata BINDSHELL, ovvero una tipologia di shell remota, sfruttabile da un hacker per un possibile attacco di rete.

Prendiamo in considerazione il firewall presente sui sistemi Linux, iptables, per ridurre la criticità della vulnerabilità, chiudendo la porta. Procediamo come di seguito:

1. Verificare che la porta 1524 sia aperta: aperta, verificato con la scansione di VA di Nessus
2. Verifica della presenza di una bindshell sulla porta tcp 1524, tramite tool netcat da shell Kali Linux, come segue:

La connessione sul servizio in ascolto è avvenuta con successo e senza alcuna autorizzazione, ho preso il comando di root da Kali Linux sul target Metasploitable: posso fare qualsiasi tipo di modifica, vedere le impostazioni della scheda di rete e addirittura modificarle. Ho trovato quindi una BINDSHELL.

```
(kali@kali)-[~]
$ nc 192.168.1.66 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:6b:d4
          inet addr:192.168.1.66  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:6bd4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39525 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25900 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4457684 (4.2 MB)  TX bytes:11327678 (10.8 MB)
          Base address:0xd240 Memory:f0820000-f0840000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:428 errors:0 dropped:0 overruns:0 frame:0
          TX packets:428 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:184385 (180.0 KB)  TX bytes:184385 (180.0 KB)

root@metasploitable:/#
```

3. Con il firewall iptables, presente sui sistemi Linux, andiamo a chiudere la porta tcp/1524 non necessaria, come segue: NOTA BENE: è importante eseguire questo comando come ROOT

```
msfadmin@metasploitable:/$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/# sudo iptables -A INPUT -p tcp --dport 1524 -j REJECT
root@metasploitable:/#
```

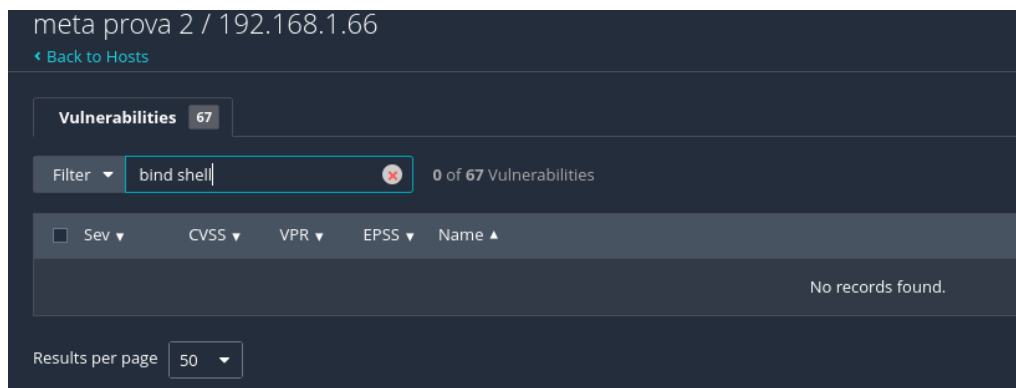
- Verifichiamo e riproviamo ora, sempre con il tool netcat su shell Kali Linux, la connessione con il servizio in ascolto sulla porta tcp/1524, come segue:

l'impostazione del firewall è andata a buon fine, la porta ora risulta chiusa e non raggiungibile per una connessione remota (ingreslock)

```
(kali㉿kali)-[~]  
$ netcat 192.168.1.66 1524  
(UNKNOWN) [192.168.1.66] 1524 (ingreslock) : Connection refused  
(kali㉿kali)-[~]  
$
```

- Effettuare una prova di scansione con il tool di VA Nessus e verificare che la vulnerabilità non si trovi più in un range di CRITICITA' elevata, o addirittura non compaia in quanto la porta risulta chiusa, come di seguito:

filtrando le vulnerabilità, la **Bind Shell Backdoor Detection**, non appare nella lista delle vulnerabilità note; REMEDIATION avvenuta con successo



Possiamo concludere che le operazioni di REMEDIATION per questa vulnerabilità sono andate a buon fine, con la chiusura della porta tcp/1524, la criticità si è annullata, non potendo quindi più connettersi con il servizio che prima era in ascolto, richiamando un Bind-shell per il controllo della vittima, ottenendo un rischio residuo ottimo.

- 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness Portatcp/22/ssh

E

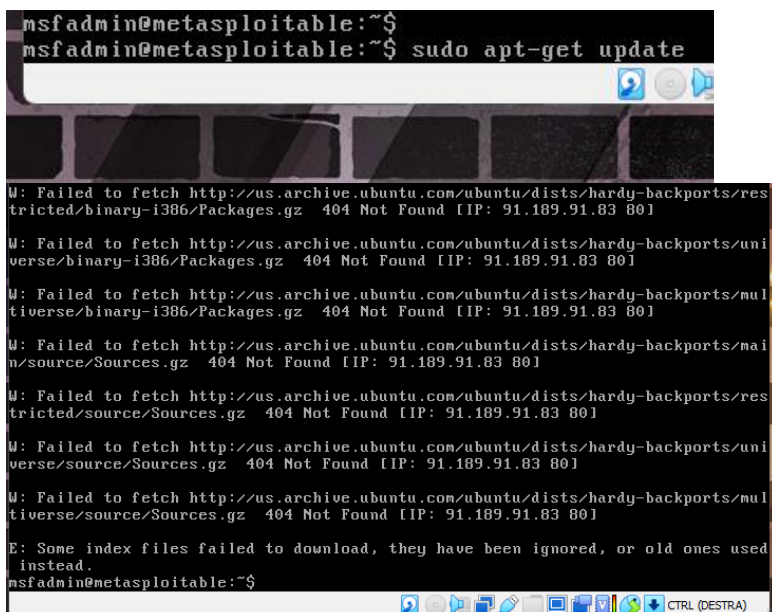
- 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Questo tipo di vulnerabilità presenta particolari problematiche circa l’ RNG, il generatore di numeri casuali, utilizzato in OpenSSH e OpenSSL, protocolli utilizzati per l’ invio sicuro di informazioni.

Alcuni dei protocolli come SSH (su porta TCP 22), che si basano su chiavi crittografiche forti per garantire comunicazioni sicure, potrebbero essere esposti a rischio della sicurezza se l’ RNG non funziona correttamente o non viene aggiornato.

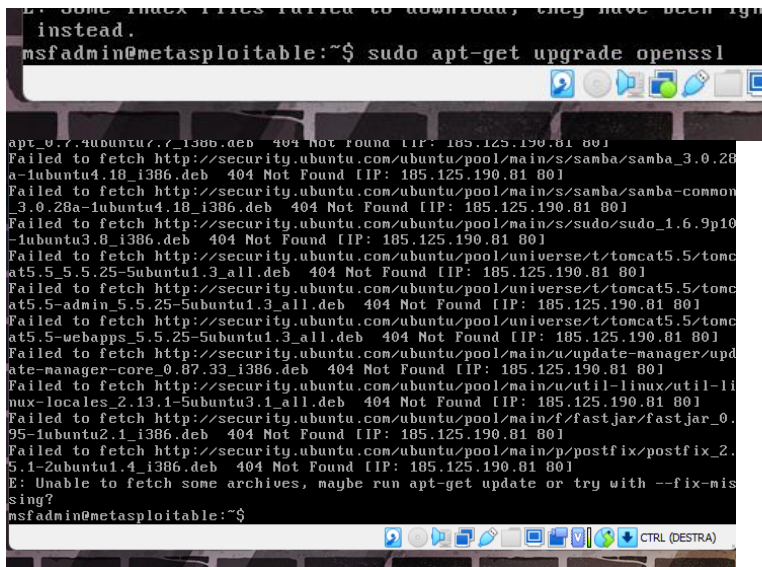
Possiamo provare in questo caso, per abbassare drasticamente la criticità della vulnerabilità, un metodo diverso, procedendo con l’ aggiornamento delle Chiavi ssh Keygen, come segue:

1. Effettuiamo un update con il seguente comando: `sudo apt-get update`



```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ sudo apt-get update  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/restricted/binary-i386/Packages.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/universe/binary-i386/Packages.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/multiverse/binary-i386/Packages.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/main/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/restricted/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/universe/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]  
U: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/hardy-backports/multiverse/source/Sources.gz 404 Not Found [IP: 91.189.91.83 80]  
E: Some index files failed to download, they have been ignored, or old ones used instead.  
msfadmin@metasploitable:~$
```

2. Effettuiamo un upgrade con il seguente comando: `sudo apt-get upgrade openssl`



```
E: Some index files failed to download, they have been ignored,
instead.
msfadmin@metasploitable:~$ sudo apt-get upgrade openssl

apt_0.7.4ubuntu7.2_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba_3.0.28a-1ubuntu4.18_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba-common_3.0.28a-1ubuntu4.18_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/s/sudo/sudo_1.6.9p10-1ubuntu3.8_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5_5.5.25-Subuntu1.3_all.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5-admin_5.5.25-Subuntu1.3_all.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/universe/t/tomcat5.5/tomcat5.5-webapps_5.5.25-Subuntu1.3_all.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/u/update-manager/update-manager-core_0.87.33_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/u/util-linux/util-linux-locales_2.13.1-5ubuntu3.1_all.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/f/fastjar/fastjar_0.95-1ubuntu2.1_i386.deb 404 Not Found [IP: 185.125.190.81 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/p/postfix/postfix_2.5.1-2ubuntu1.4_i386.deb 404 Not Found [IP: 185.125.190.81 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
msfadmin@metasploitable:~$
```

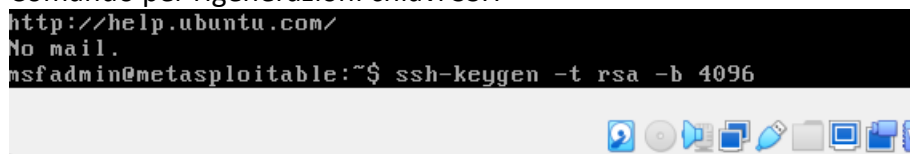
3. Effettuiamo un `sudo reboot`, per il riavvio della VM



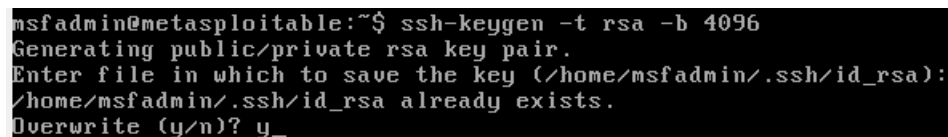
```
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
msfadmin@metasploitable:~$ sudo reboot
```

4. Una volta riavviata la macchina, procediamo con l'aggiornamento delle chiavi ssh – Keygen, con il seguente comando: `ssh-keygen -t rsa -b 4096`

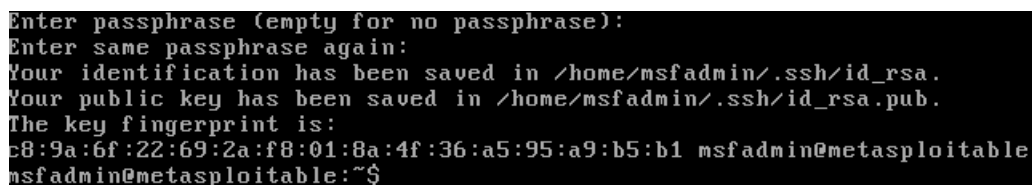
Comando per rigenerazioni chiavi SSH



```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096
```



```
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
Overwrite (y/n)? y_
```



```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
c8:9a:6f:22:69:2a:f8:01:8a:4f:36:a5:95:a9:b5:b1 msfadmin@metasploitable
msfadmin@metasploitable:~$
```


5. Procediamo con una prova di scansione con il tool di VA Nessus per verificare che la vulnerabilità non si trovi più in un range di CRITICITA' elevata:

le operazioni di REMEDIATION sopra eseguite hanno avuto successo, con un esito positivo; le vulnerabilità non presentano più un indice di criticità elevato; per un attaccante sarà più difficile decodificare una chiave crittografata, per intercettare un servizio attivo di tipo SSH/SSL.

meta prova 3 / 192.168.1.103 / SSH (Multiple Issues)

ConfigureAudit TrailLaunchReport

Back to Vulnerabilities

Vulnerabilities66

ssh6 of 6 Vulnerabilities

Sev	CVSS	VPR	EPSS	NiFamily	Count	
MEDIUM	4.3 *			SSMisc.	1	
LOW	3.7	3.4	0.6115	SSMisc.	1	
LOW	3.7			SSMisc.	1	
LOW	2.6 *			SSMisc.	1	
INFO				SSMisc.	1	
INFO				SSMisc.	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:30 PM
End: Today at 1:38 PM
Elapsed: 8 minutes

Vulnerabilities

Critical

High

- 46882 - UnrealIRCd Backdoor Detection – Porta tcp/6667/irc

Per effettuare una REMEDIATION per questa vulnerabilità, procediamo in questo caso a bloccare il servizio attivo sulla porta tcp/6667 e a chiudere la porta, come segue:

1. Procediamo al bloccaggio del servizio

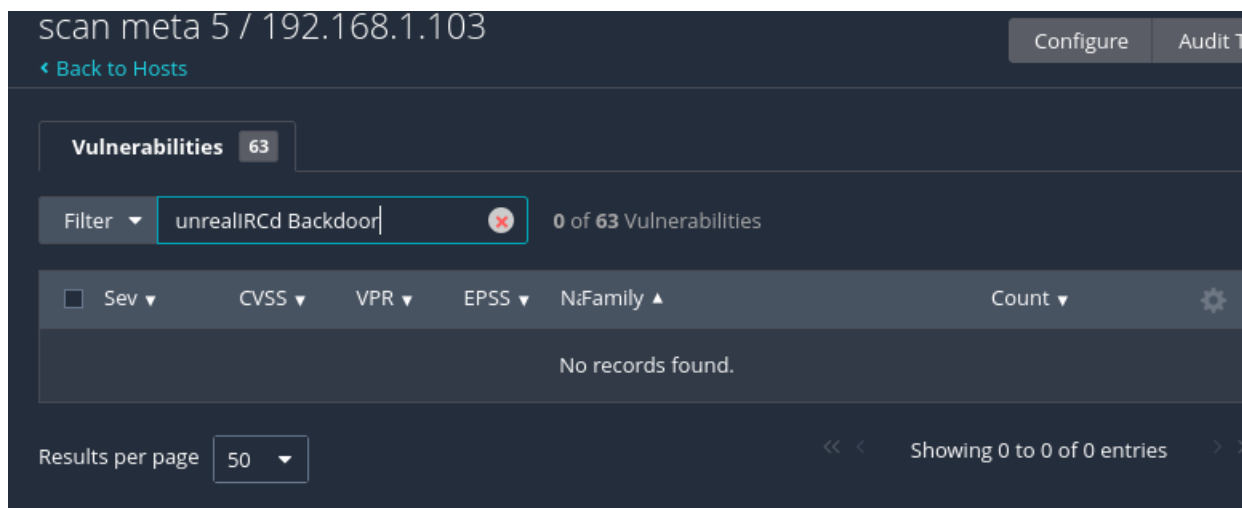
```
msfadmin@metasploitable:~$ sudo ufw deny 6667
[sudo] password for msfadmin:
Rules updated
msfadmin@metasploitable:~$ _
```

2. Impostiamo una Policy firewall con iptables, impostando la porta in 'DROP'

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# sudo iptables -A INPUT -p tcp --dport 6667 -j DROP
root@metasploitable:/home/msfadmin#
```

3. Procediamo con una prova di scansione con il tool di VA Nessus per verificare che la vulnerabilità non si trovi più in un range di CRITICITA' elevata:

le operazioni di REMEDIATION sopra eseguite hanno avuto successo, con un esito positivo; le vulnerabilità non presentano più un indice di criticità elevato; per un attaccante sarà più difficile sfruttare questa porta per un attacco. Nella scansione, la stessa non viene più rilevata, eliminando quindi la criticità della vulnerabilità.



8. Considerazioni finali

Le vulnerabilità di sistemi operativi su porte aperte e servizi attivi in rete, sono al giorno d'oggi una tematica da non sottovalutare, da monitorare costantemente nel tempo e che richiede continuo aggiornamento di patch ecc.

Molte aziende sottovalutano questa tematica, perché magari ignare della reale e potenziale gravità economica, intellettuale, personale, finanziaria ecc. che un attacco Hacker potrebbe causare.

E' per questo che il ruolo del Cybersecurity Analyst e Specialist è di fondamentale importanza.