scansione Metasploitable tramite nessus

metasploitable ip 192.168.64.13
MAC Address D2:5A:A964:5C:D1

Come richiesto dall'azienda "XXX" è stato condotto un vulnerability scanner su Metasploitable
Sono state riscontrate un totale di 118 vulnerabilità di sicurezza
la ripartizione delle vulnerabilità è la seguente:

CRITICAL	HIGH	MEDIUM	LOW	INFO
10	7	19	5	77

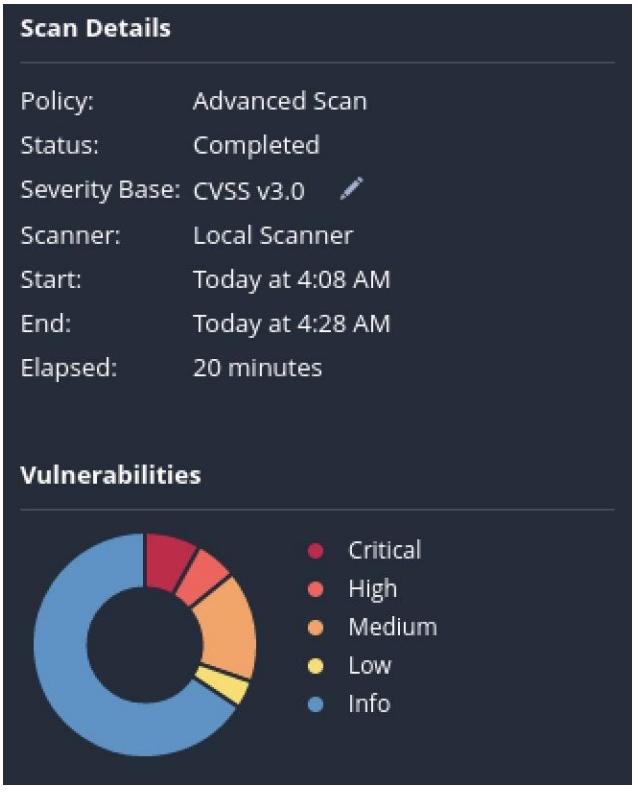
Questi risultati sono stati ottenuti è raccolti utilizzando uno scanner di vulnerabilità open source noto come NESSUS
[versione utilizzata: Nessus Essential 10.3.0 ubuntu1804]

[**nessus** è uno strumento di scansione della sicurezza che esegue la scansione di una macchina mirata o di una serie di macchine è ne restituisce le vulnerabilità che potrebbero essere utilizzate dai Hacker per ottenerne l'accesso]

È fondamentale che le 10 vulnerabilità critiche vengano corrette nelle prime 24h in modo tale da garantire che nessuno dei sistemi interni venga compromesso. Per le restanti vulnerabilità, è necessario che venga attuata una soluzione nel corso dei prossimi 7 giorni.

Sommario manageriale
Come richiesto è stato condotto un VS sulla macchina vulnerabile metasploitable. Durante l'esecuzione del test sono stati identificati i seguenti rischi:

- sono state rilevate 118 vulnerabilità di cui 10 di importanza critica da risolvere entro le 24h successive
- le restanti vulnerabilità verranno risolte in base allo schema di classificazione delle stesse mostrato qui di fianco



Al termine del rapporto, si raccomanda di controllare regolarmente (una volta a settimana) il livello di sicurezza di tutti i sistemi informatici al fine di garantire il minimo rischio per l'organizzazione

❒ Vulnerabilità identificate e soluzioni da adottare

NFS Exported Share Information Disclosure

Samba Badlock Vulnerability

VNC Server 'password' Password

rlogin Service Detection

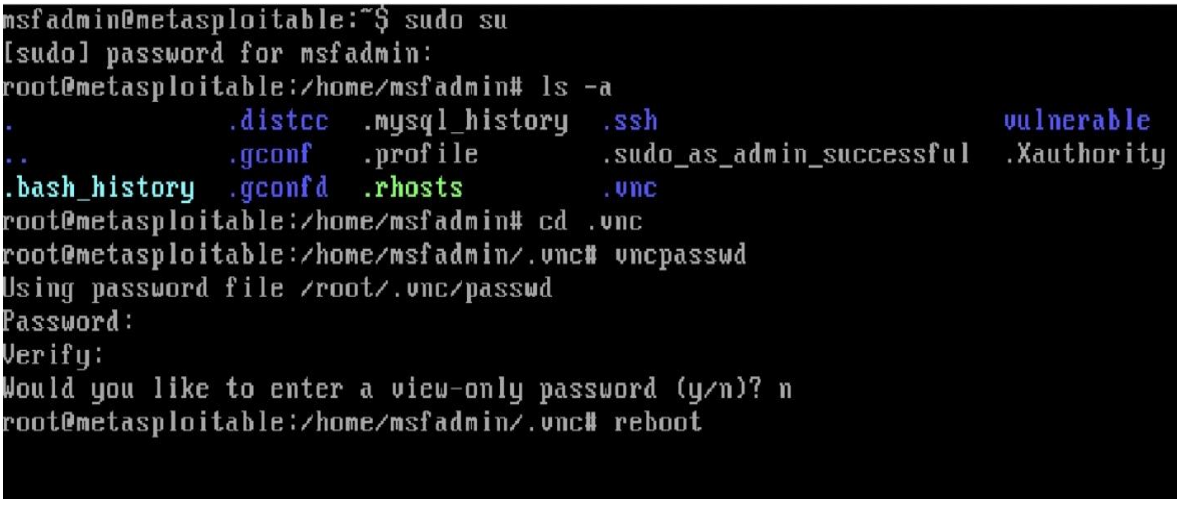
Di seguito è possibile trovare una tabella di questi exploit insieme alle relative risoluzioni

NFS Exported Share Information Disclosure grado Gravità (CVSSv2[0-10]): 10	**RIMEDIO:** Bisogna modificare il file 'exports' che si trova all'interno della sottocartella del root /etc
Samba Badlock Vulnerability Exploit: exploit/samba/usermap_script grado Gravità (CVSSv2[0-10]): 5	**RIMEDIO:** L'aggiornamento a Samba versione 4.2.11, 4.3.8 o 4.4.2 eliminerà la vulnerabilità *Samba Badlock*
VNC Server 'password' Password grado Gravità (CVSSv2[0-10]): 10	**RIMEDIO:** La password predefinita del server VNC deve essere modificata da "password" per garantire l'assenza di accessi non autorizzati
rlogin Service Detection Exploit: rlogin -1 root <RHOST> grado Gravità (CVSSv2[0-10]): 8	**RIMEDIO:** commentare la riga 'login' in etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e usare invece SSH

❒ Risoluzioni:

VNC Server 'password' Password-RIMEDIO

Alla fine del processo riavviare la macchina.



NFS Exported Share Information Disclosure

```
  GNU nano 2.0.7                File: exports                          Modified

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/       192.168.64.13(rw,sync,no_root_squash,no_subtree_check)
```

le modifiche da apportare sono le seguenti: cambiare "*" con l'indirizzo ip della nostra macchina.
Alla fine del processo riavviare la macchina.

In seguito a questi rimedi la successiva scansione con nessus appare così:

Vulnerabilities — Total: 114

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator
CRITICAL	10.0*	46882	UnrealIRCd Backdoor Detection
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	136808	ISC BIND Denial of Service
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	10205	rlogin Service Detection
HIGH	7.5*	10245	rsh Service Detection