

scansione Metasploitable tramite nessus

metasploitable ip 192.168.64.13

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 10	HIGH 7	MEDIUM 19	LOW 5	INFO 77
-----------------------	------------------	---------------------	-----------------	-------------------

Questi risultati sono stati ottenuti e 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 e ne restituisce le vulnerabilità che potrebbero essere utilizzate dai Hacker per ottenerne l'accesso]

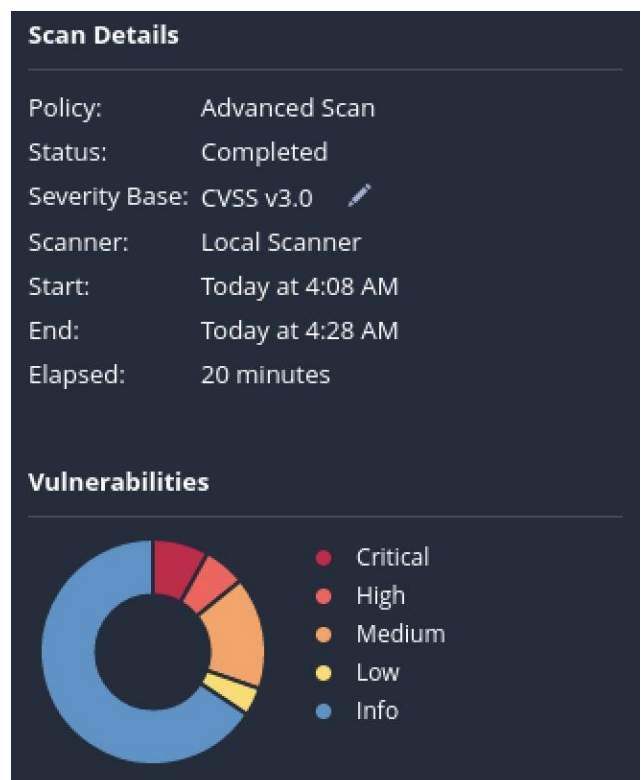
È fondamentale che le 10 vulnerabilità critiche vengano corrette nelle prime 24h in modo tale da garantire che nessuno dei sistemi interni venga compromesso. Per le restanti vulnerabilità, è necessario che venga attuata una soluzione nel corso dei prossimi 7 giorni.

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

Samba Badlock Vulnerability

VNC Server 'password' Password

rlogin Service Detection

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

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 <i>Samba Badlock</i>
VNC Server 'password' Password Exploit: auxiliary/scanner/vnc/vnc_login 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 -l 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