Scansione completa su target Metasploitable 2 tramite Nessus

Nessus®
vulnerability scanner

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.

NESSUS :

Nessus è un software di scansione delle vulnerabilità ampiamente utilizzato nel campo della sicurezza informatica. Sviluppato dalla società Tenable Network Security, Nessus aiuta a identificare e valutare le vulnerabilità nei sistemi informatici, consentendo agli amministratori di sistema e agli specialisti della sicurezza di prendere misure preventive per proteggere i sistemi da attacchi informatici.

Le caratteristiche principali di Nessus includono:

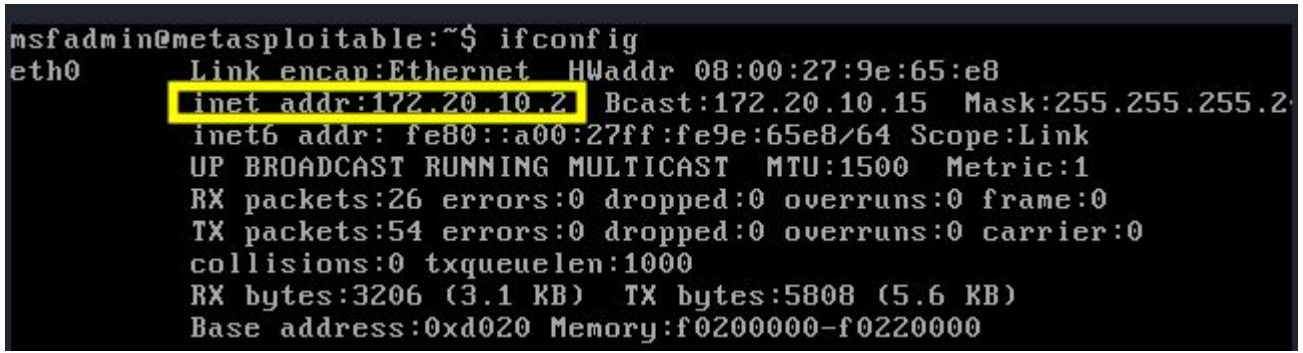
1. **Scansione automatica**: Nessus esegue scansioni automatiche dei dispositivi di rete e dei sistemi informatici per individuare potenziali vulnerabilità.
2. **Database di vulnerabilità**: Il software dispone di un ampio database che contiene informazioni dettagliate su varie vulnerabilità conosciute.
3. **Politiche di scansione personalizzabili**: Gli utenti possono definire politiche di scansione personalizzate per adattarsi alle esigenze specifiche del loro ambiente di rete.
4. **Report dettagliati**: Nessus genera report dettagliati che forniscono informazioni sulle vulnerabilità rilevate, consentendo agli amministratori di sistema di prendere decisioni informate sulla sicurezza.
5. **Integrazione con altri strumenti di sicurezza**: Nessus può essere integrato con altri strumenti e sistemi di sicurezza per una gestione più efficace delle minacce.

Operazione 1:

Il nostro scopo consiste nel scannerizzare la Metasploitable 2 per mezzo del software Nessus.

In primis bisogna trovare l'IP della Metasploitable 2 :

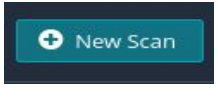
Una volta avviata la macchina virtuale con sopra la Metasploitable 2 lanciamo il comando ***ifconfig***, in modo tale da poter visualizzare l'IP.



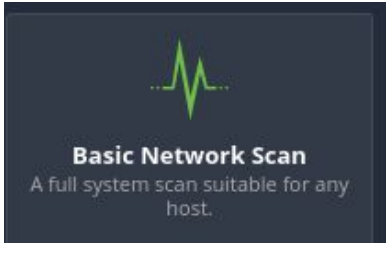
Operazione 2 :

Andiamo a configurare il software Nessus per iniziare una nuova scansione di rete :

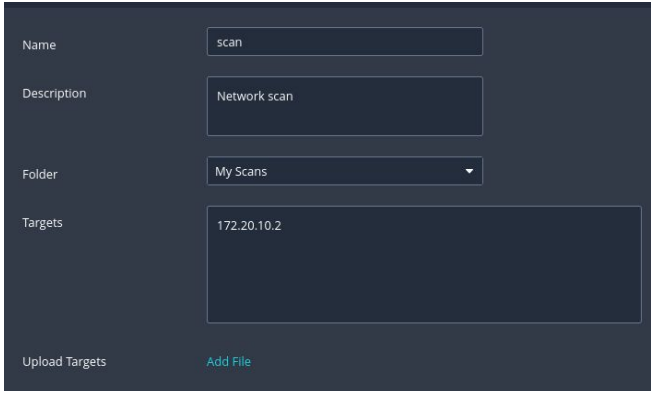
- Apriamo il software Nessus ritrovabile al url : https://localhost:8834 , dopo aver effettuato il login dobbiamo creare un nuovo scan (1)
- Selezioniamo tra le varie opzioni di scan la seguente **BASIC NETWORK SCAN** : (2)
- Andiamo ora ad inserire l'IP (TROVATO PRIMA) del target da scansionare e definire un nome per il nostro SCAN e una breve descrizione (3)
- Una volta completato lo step 3 andremo a lanciare lo SCAN (4)
- Una volta terminato lo scan verranno individuati tutti i problemi i quali esporremo nella pagina successiva e vedremo i vari passaggi per risolverli



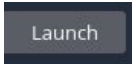
(1)



(2)



(3)



(4)

Risultato dello SCAN

Vulnerabilità’ riscontrate :

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	DNS (Multiple Issues)	DNS	5
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5

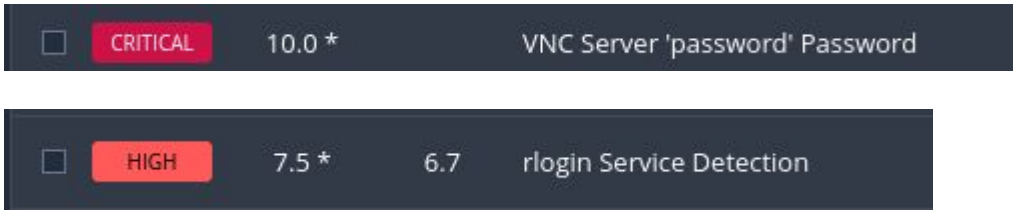
Host Details

IP:	172.20.10.2
MAC:	08:00:27:9E:65:E8
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 5:45 AM
End:	Today at 6:05 AM
Elapsed:	20 minutes
KB:	Download

Vulnerabilities

Risoluzione delle vulnerabilità' riscontrate

Procederemo ora con la risoluzione delle seguenti vulnerabilità' :



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.

🔑 VNC (Virtual Network Computing) is a remote desktop-sharing system that allows users to control and operate a computer over a network. While it offers convenience and remote access capabilities, it also presents a potential vulnerability that attackers can exploit.
VNC Port 5900, is the default port VNC servers use for communication.

Per verificare se il server VNC e attivo sulla Metasploitable 2, dobbiamo effettuare uno scan della macchina Metasploitable2 attraverso la nostra macchina Kali Linux, per mezzo della utility nmap (Security Scanner, Port Scanner, & Network Exploration Tool) :

- **nmap** -sV 172.20.10.2 -p 5900

Se VNC risulta attivo per avviare una istanza di connessione desktop remota ci basterà' lanciare il comando tramite kali linux :

- **vncviewr** 172.20.10.2
- tenteremo ora il login con password : 'password', come riscontrato da Nessus, il risultato sara' una connessione avvenuta

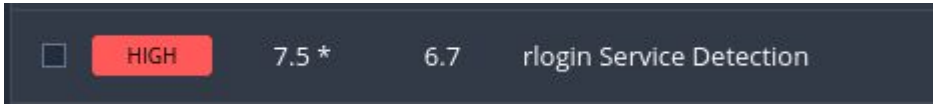
Per modificare la password ci basterà' accedere alla Metasploitable 2 e digitare il seguente comando :

- **vncpasswd**

Dovremmo poi digitare la nuova password

```
$ vncpasswd
Password:
Verify:
```

rlogin Service Detection



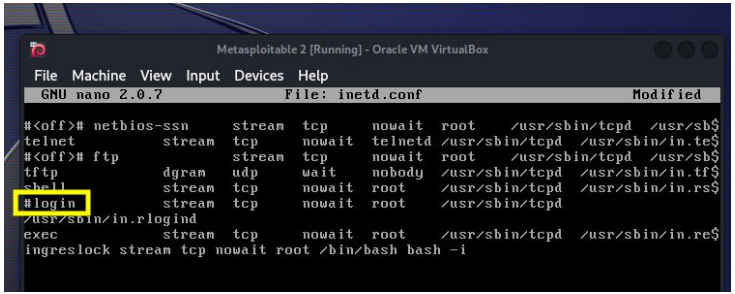
Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

In questo caso la soluzione si tratta di commentare la riga **login** all interno del file **/etc/inetd.conf** della Metasploitable 2



Risultati

Una volta eseguiti i vari passaggi di risoluzione delle problematiche di rischio, se proviamo a fare un nuovo scan con Nessus vedremo che i problemi prima rilevati ora non ci sono piu' :