EPICODE

CYBER SECURITY & ETHICAL HACKING

PROJECT

Presented by: Aguglia Andrea

TRACCIA:

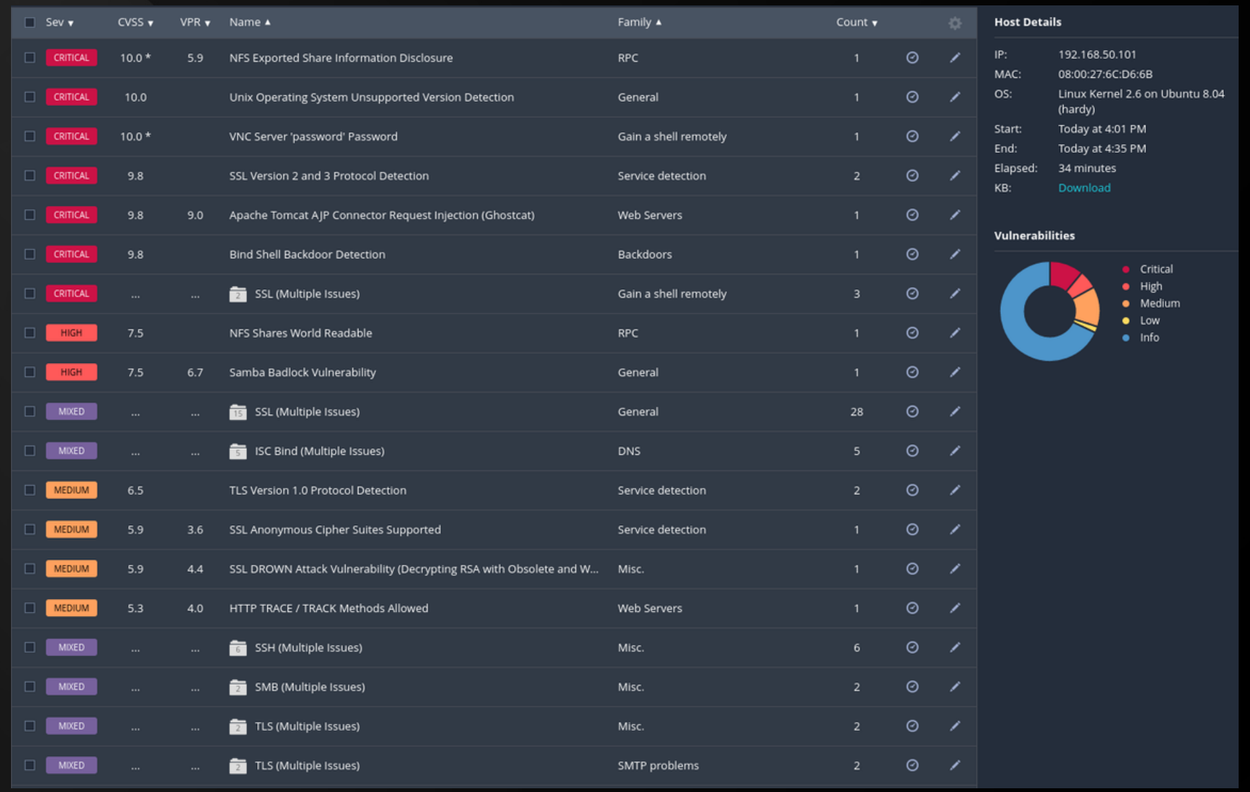
- *Effettuare una scansione completa sul target Metasploitable.*
- *Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.*

Nessus

Nessus è uno strumento di scansione delle vulnerabilità ampiamente utilizzato nel campo della sicurezza informatica.

Identificazione dei Rischi

Nessus svolge un'analisi approfondita dei rischi associati alla macchina Metasploitable 2, esaminando attentamente diverse criticità che vengono categorizzate in livelli quali Critical, High, Medium e Low. Questa valutazione dettagliata consente di identificare e classificare accuratamente le vulnerabilità presenti sulla macchina in questione, fornendo una panoramica chiara e strutturata dei potenziali punti deboli.



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 *		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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and W...	Misc.	1
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2

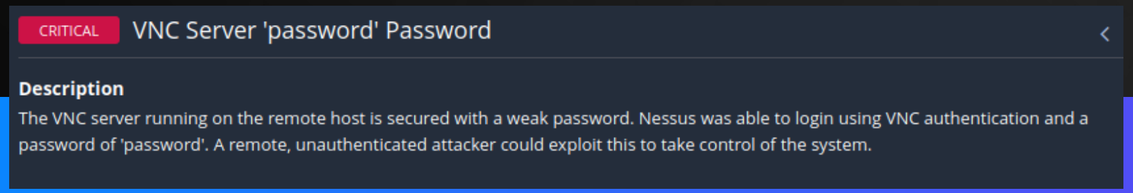
Host Details

IP:	192.168.50.101
MAC:	08:00:27:6C:D6:6B
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 4:01 PM
End:	Today at 4:35 PM
Elapsed:	34 minutes
KB:	Download

Vulnerabilities

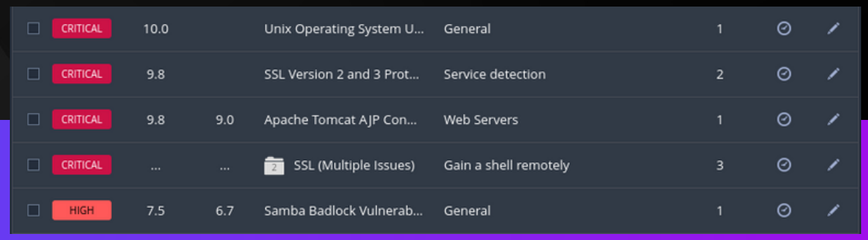
Prima Vulnerabilità

Problema



Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito a effettuare l'accesso utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

Soluzione



Per esplorare questa vulnerabilità, mi sono avventurato nel contesto di Metasploit. Ho eseguito il comando “vncpasswd”, il quale mi ha richiesto di inserire una nuova password con una lunghezza massima di otto caratteri.

Seconda Vulnerabilità

Problema

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare questa situazione per leggere (e eventualmente scrivere) file sull'host remoto.

Soluzione

CRITICAL	10.0		Unix Operating System U...	General	1		
CRITICAL	9.8		SSL Version 2 and 3 Prot...	Service detection	2		
CRITICAL	9.8	9.0	Apache Tomcat AJP Con...	Web Servers	1		
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5	6.7	Samba Badlock Vulnerab...	General	1		

Per esaminare la seconda vulnerabilità, considerando la facilità con cui le informazioni sono accessibili a un host non autorizzato, c'è il rischio che quest'ultimo possa leggere o scrivere sul nostro server da remoto.
Ho utilizzato Metasploit per condurre questa indagine, introducendo una serie di comandi significativi. Inizialmente, abbiamo eseguito il comando "sudo su" per elevare i privilegi, seguito da "sudo /etc/exports" per accedere e modificare il file di configurazione. Successivamente, al fine di esplorare e mitigare la vulnerabilità individuata, ho proceduto all'eliminazione dell'ultima riga all'interno del suddetto file.

```
  GNU nano 2.0.7              File: /etc/exports

# /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)
#

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

Seconda Vulnerabilità

Problema

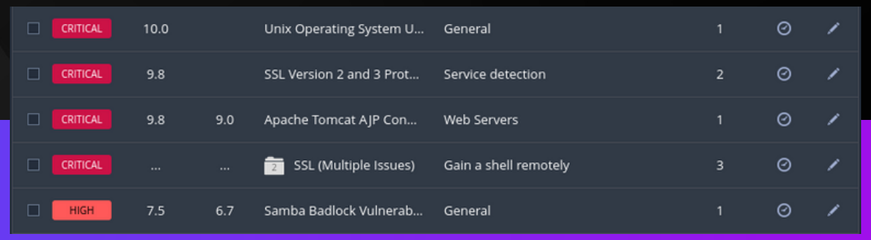
CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Su una porta remota è in ascolto una shell senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione



CRITICAL	10.0		Unix Operating System U...	General	1		
CRITICAL	9.8		SSL Version 2 and 3 Prot...	Service detection	2		
CRITICAL	9.8	9.0	Apache Tomcat AJP Con...	Web Servers	1		
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5	6.7	Samba Badlock Vulnerab...	General	1		

Per affrontare la terza vulnerabilità, abbiamo notato la presenza di una shell in ascolto su una porta remota senza autenticazione necessaria. Questo scenario potrebbe essere sfruttato da un attaccante per inviare comandi da remoto. Per mitigare questa situazione, mi sono avvalso di Metasploit e abbiamo emesso il seguente comando per chiudere la porta come indicato da Nessus: **lsof -i :1524**.

```
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4454 root   12u  IPv4  12019       TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin# kill 4454
root@metasploitable:/home/msfadmin# kill -9 4454
bash: kill: (4454) - No such process
root@metasploitable:/home/msfadmin#
```