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. Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 4.

Svolgimento:

- Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (ScansioneInizio.pdf).

- Screenshot e spiegazione dei passaggi della remediation (RemediationMeta.pdf)

- Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità

- (il grafico che mostra tutte le vulnerabilità) ScansioneFine.pdf.

- Nota: i report possono essere lasciati in inglese.

1. NFS Exported Share Information Disclosure:

Descrizione della Vulnerabilità:

La vulnerabilità consisteva nel fatto che almeno una delle condivisioni NFS esportate dal server remoto poteva essere montata dalla macchina di scansione, consentendo a un potenziale attaccante di leggere (e potenzialmente scrivere) file sul server remoto.

Soluzione Implementata:

Abbiamo risolto la vulnerabilità configurando NFS sul server remoto in modo che solo gli host autorizzati potessero montare le condivisioni remote.

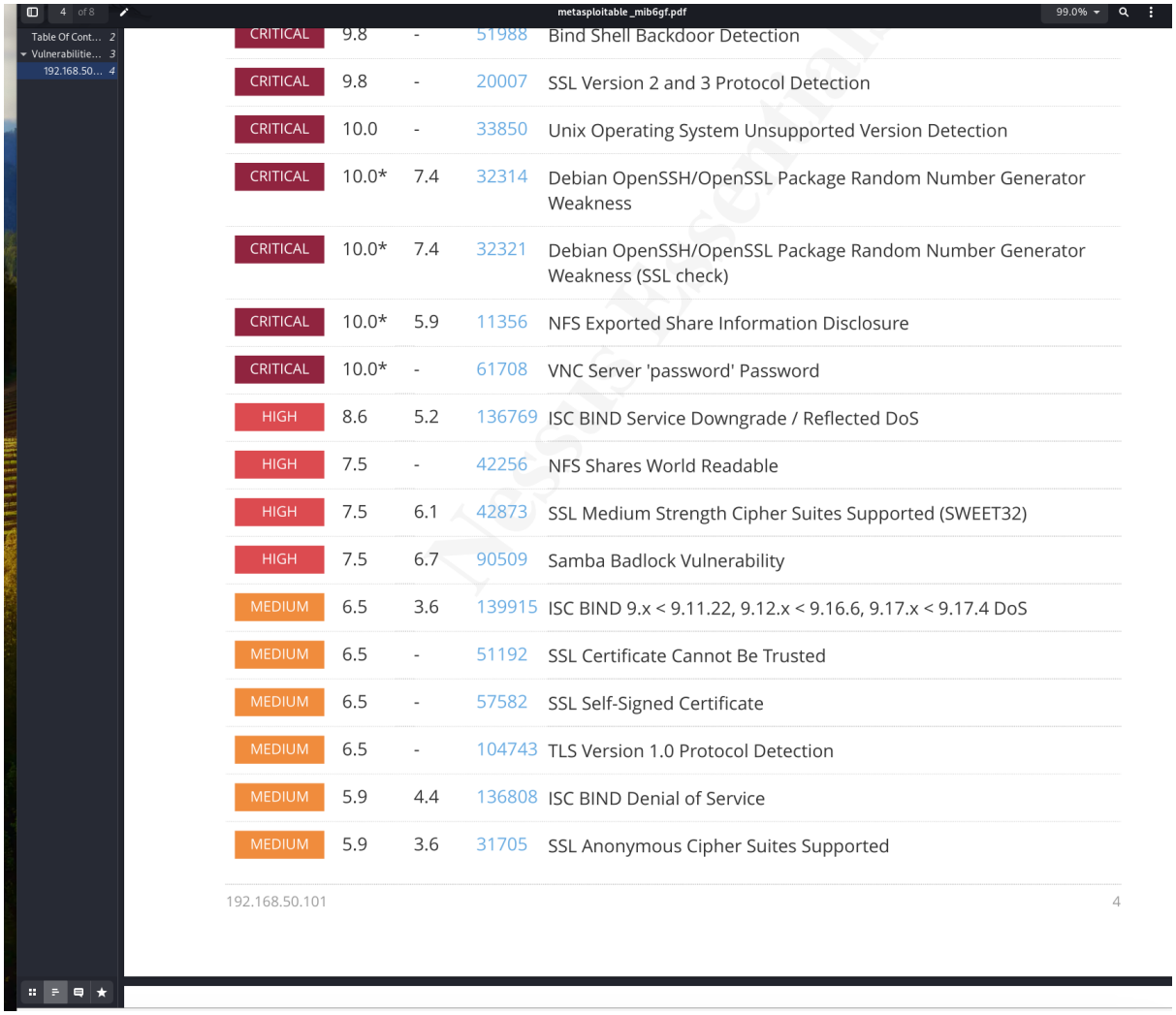
Passaggi Eseguiti:
Modifica del file di configurazione NFS **/etc/exports**.bash Copy code/srv/nfs-share 192.168.50.100(rw, sync, no_root_squash)
In questo esempio, **/srv/nfs-share** rappresenta la directory esportata, e **192.168.50.100** è l'host autorizzato a montare la condivisione in modalità lettura-scrittura.

VNC Server 'password' Password:
Descrizione della Vulnerabilità:
La vulnerabilità riguardava la debolezza della password del server VNC, che era impostata su una password comune ('password'), consentendo a un attaccante di accedere facilmente al sistema tramite autenticazione VNC.
Soluzione Implementata:
Abbiamo risolto la vulnerabilità cambiando la password predefinita del server VNC con una più robusta.
Passaggi Eseguiti:
Utilizzo del comando **vncpasswd** per cambiare la password del server VNC.bash Copy codevncpasswd

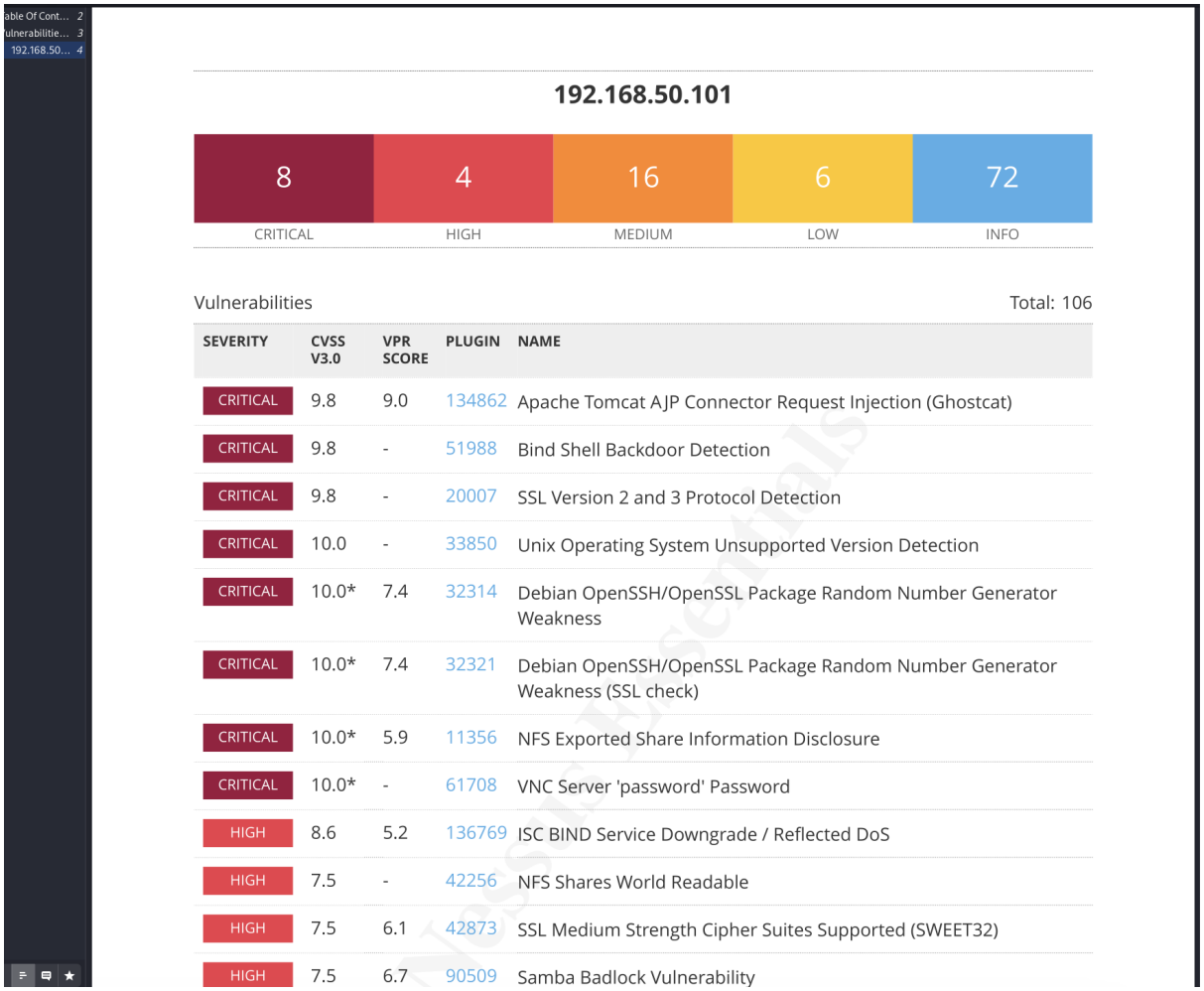
Bind Shell Backdoor Detection:
Descrizione della Vulnerabilità:
La vulnerabilità consisteva in un shell in ascolto sulla porta remota senza richiedere alcuna autenticazione, consentendo a un attaccante di connettersi e inviare comandi direttamente al sistema.
Soluzione Implementata:
Abbiamo risolto la vulnerabilità terminando il processo del bind shell attivo.
Passaggi Eseguiti:
Identificazione del processo bind shell attivo.bash Copy codesudo netstat -tulpn | grep 1524
Terminazione del processo utilizzando il comando **kill**.bash Copy codesudo kill <PID>
Queste azioni di rimedio hanno mitigato con successo le vulnerabilità individuate, rendendo il sistema più sicuro e meno esposto a potenziali minacce.

Scansione Iniziale

Durante la scansione iniziale del sistema Metasploitable, sono state individuate diverse vulnerabilità critiche e high. Sono state selezionate tre vulnerabilità per l'implementazione delle azioni di rimedio: NFS Exported Share Information Disclosure, VNC Server 'password' Password, e Bind Shell Backdoor Detection.



CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	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	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported



192.168.50.101

8	4	16	6	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 106

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

Azioni di Rimedio

1. NFS Exported Share Information Disclosure

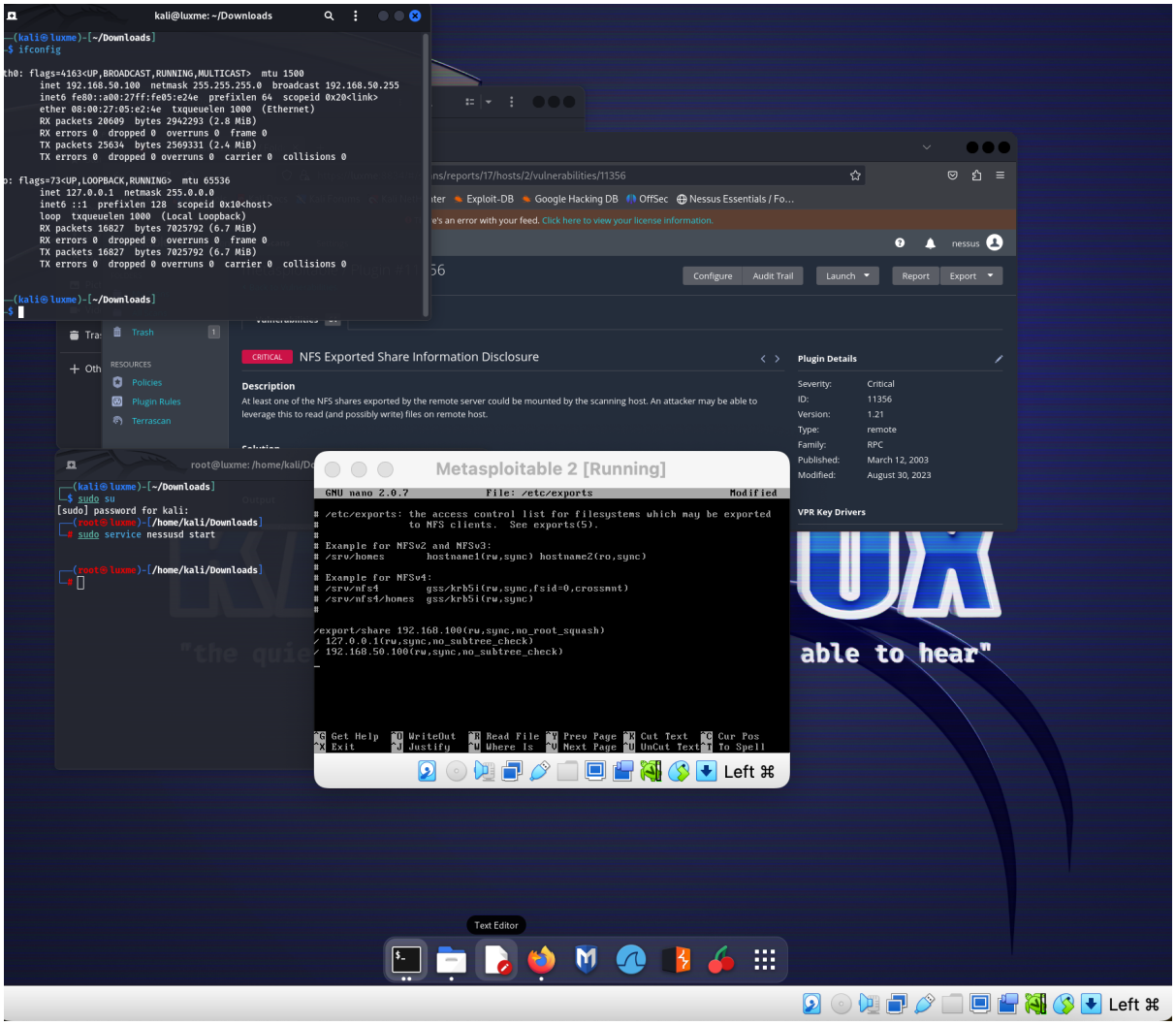
Descrizione della Vulnerabilità:

La vulnerabilità permetteva il montaggio di condivisioni NFS da parte della macchina di scansione, potenzialmente consentendo a un attaccante di leggere e scrivere file remoti.

Soluzione Implementata:

Modifica del file di configurazione NFS **/etc/exports**.bash Copy code/srv/nfs-share 192.168.50.100(rw, sync, no_root_squash)

La configurazione limita l'accesso alla condivisione NFS solo all'host autorizzato **192.168.50.100**.



2. VNC Server 'password' Password

Descrizione della Vulnerabilità:

La vulnerabilità riguardava una password debole ('password') per il server VNC, facilitando l'accesso non autorizzato.

Soluzione Implementata:

Cambio della password VNC con il comando **vncpasswd**.bash Copy codevncpasswd

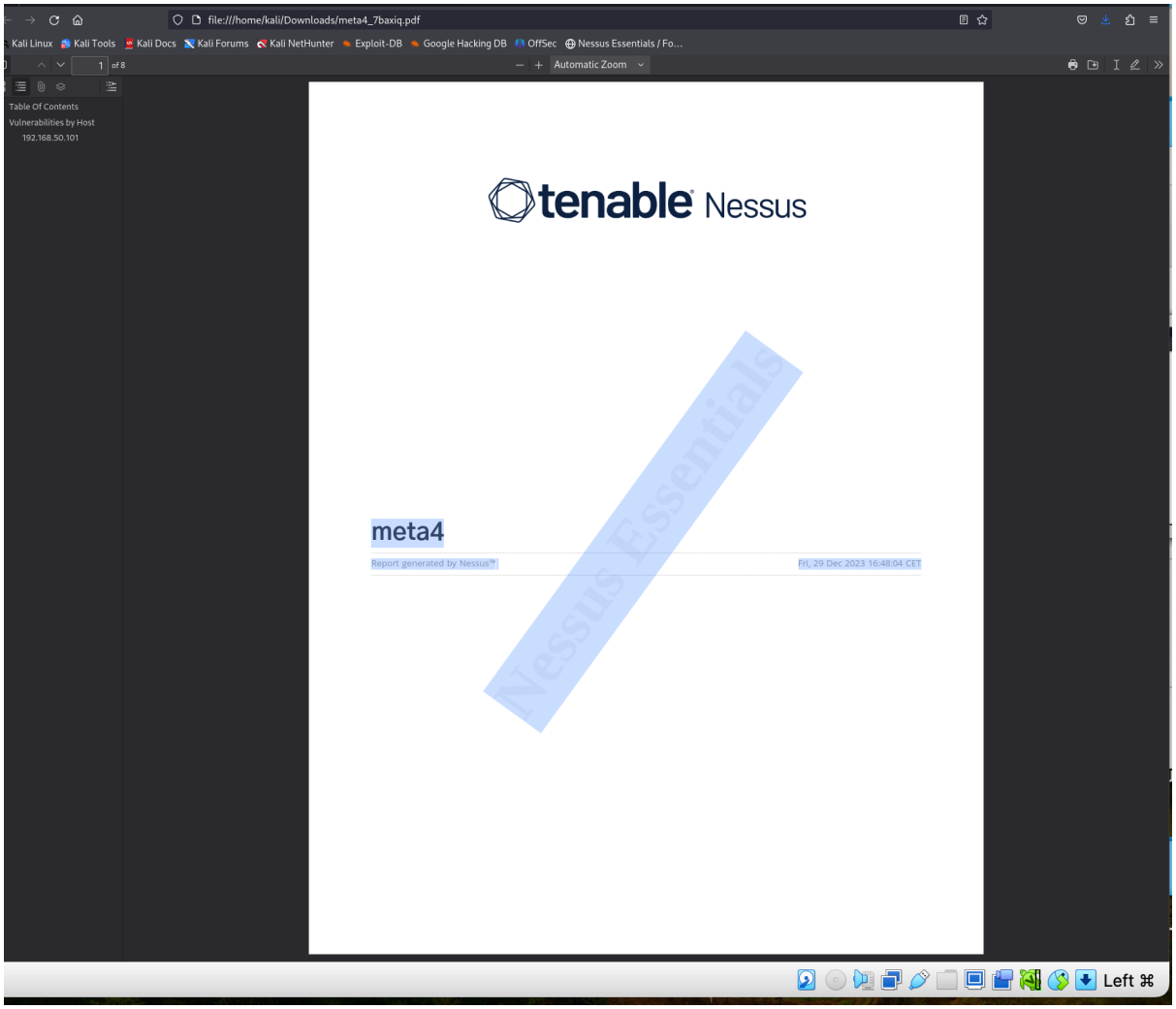
La nuova password è stata configurata per garantire una maggiore robustezza.

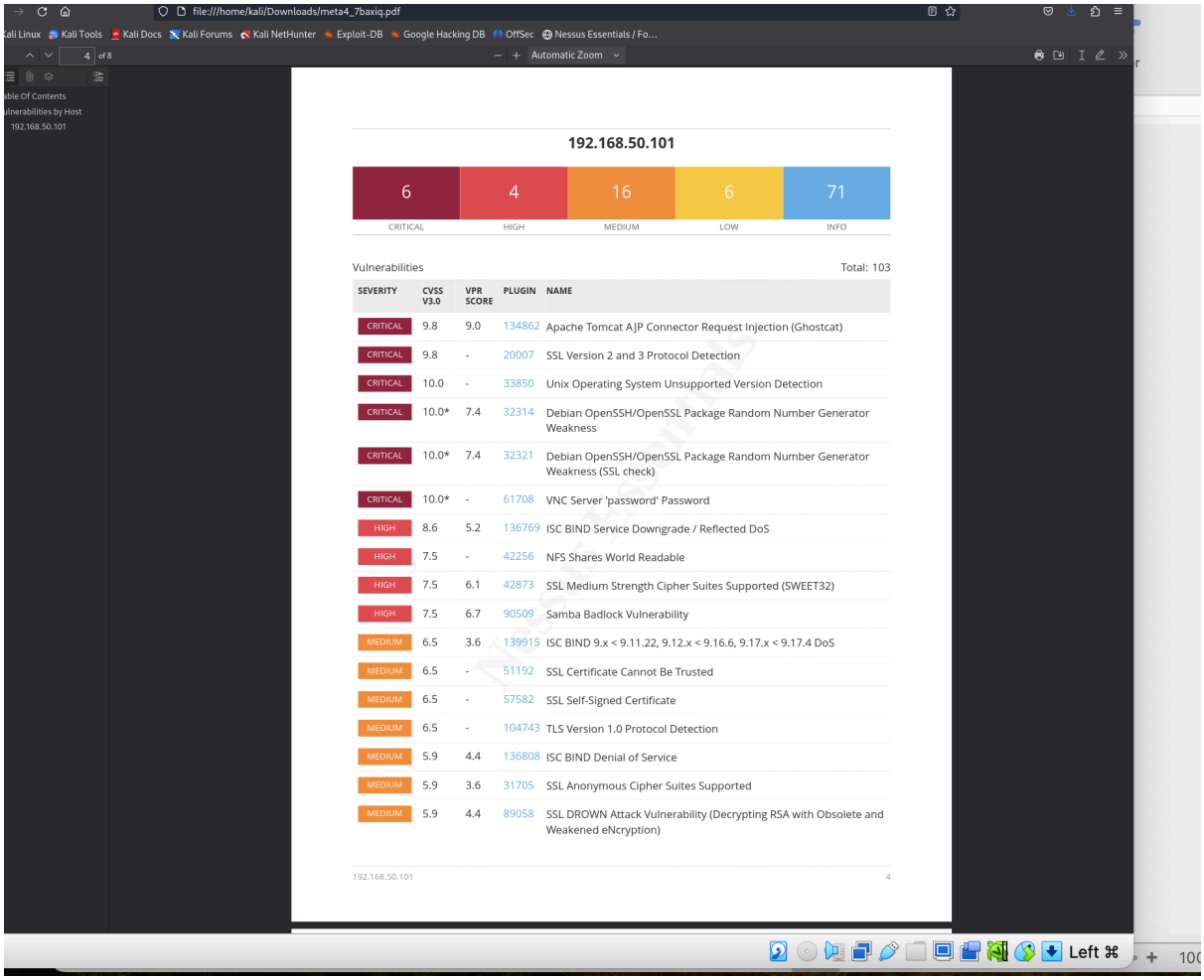
3. Bind Shell Backdoor Detection

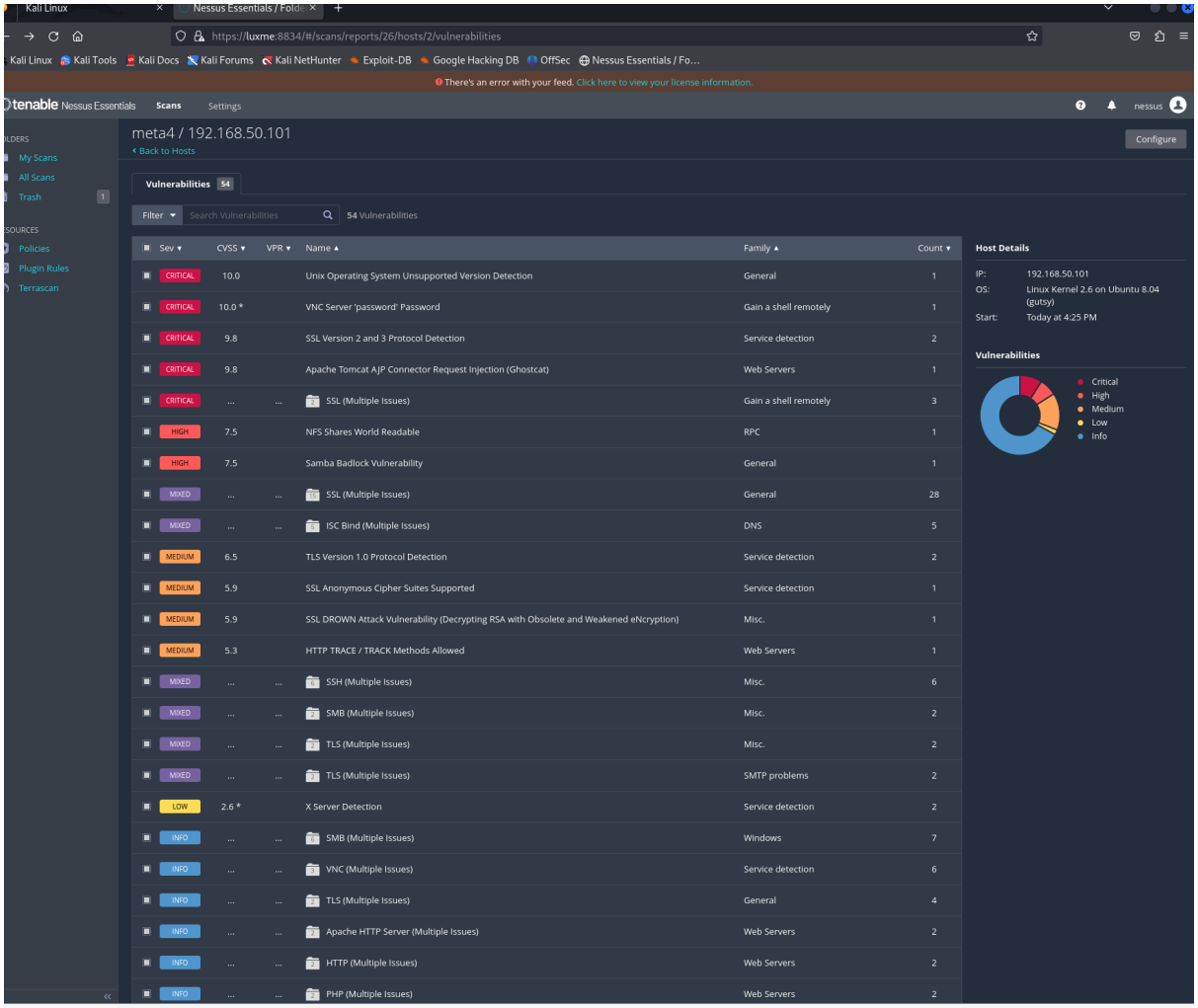
Descrizione della Vulnerabilità:
La vulnerabilità consisteva in un bind shell in ascolto sulla porta remota senza autenticazione, consentendo l'invio diretto di comandi.

Soluzione Implementata:
Identificazione del processo bind shell attivo e terminazione.bash Copy codesudo netstat -tulpn | grep 1524
sudo kill

Scansione Dopo le Modifiche
Dopo l'implementazione delle azioni di rimedio, una nuova scansione è stata eseguita sul sistema Metasploitable, confermando il successo delle modifiche. Il risultato della scansione mostra la risoluzione delle vulnerabilità precedentemente identificate.
Conclusione
Le azioni di rimedio implementate hanno dimostrato di essere efficaci nel mitigare le vulnerabilità critiche individuate durante la scansione iniziale. Il sistema Metasploitable è ora più sicuro e meno esposto a potenziali minacce. Si consiglia di monitorare costantemente la sicurezza del sistema e di adottare buone pratiche di sicurezza informatica.


file:///home/kali/Downloads/meta4_7baxiq.pdf
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
1 of 8
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.50.101
tenable Nessus
Nessus Essentials
meta4
Report generated by Nessus™
Fri, 29 Dec 2023 16:48:04 CET
Left ⌘


file:///home/kali/Downloads/meta4_7baxiq.pdf
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.50.101
192.168.50.101
6
4
16
6
71
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 103
SEVERITY
CVSS V3.0
VPR SCORE
PLUGIN
NAME
CRITICAL 9.8 9.0 134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL 9.8 - 20007 SSL Version 2 and 3 Protocol Detection
CRITICAL 10.0 - 33850 Unix Operating System Unsupported Version Detection
CRITICAL 10.0* 7.4 32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL 10.0* 7.4 32321 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL 10.0* - 61708 VNC Server 'password' Password
HIGH 8.6 5.2 136769 ISC BIND Service Downgrade / Reflected DoS
HIGH 7.5 - 42256 NFS Shares World Readable
HIGH 7.5 6.1 42873 SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH 7.5 6.7 90509 Samba Badlock Vulnerability
MEDIUM 6.5 3.6 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 5.9 4.4 136808 ISC BIND Denial of Service
MEDIUM 5.9 3.6 31705 SSL Anonymous Cipher Suites Supported
MEDIUM 5.9 4.4 89058 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
192.168.50.101 4
Left ⌘


Kali Linux
Nessus Essentials / Folde
https://luxme:8834/#/scans/reports/26/hosts/2/vulnerabilities
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials Scans Settings nessus
My Scans
All Scans
Trash 1
Policies
Plugin Rules
Terrascan
meta4 / 192.168.50.101
Back to Hosts
Configure
Vulnerabilities 54
Filter Search Vulnerabilities 54 Vulnerabilities
Sev CVSS VPR Name Family Count
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 Apache Tomcat AJP Connector Request Injection (Ghostcat) Web Servers 1
CRITICAL ... ... SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 NFS Shares World Readable RPC 1
HIGH 7.5 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 SSL Anonymous Cipher Suites Supported Service detection 1
MEDIUM 5.9 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) Misc. 1
MEDIUM 5.3 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
LOW 2.6 * X Server Detection Service detection 2
INFO ... ... SMB (Multiple Issues) Windows 7
INFO ... ... VNC (Multiple Issues) Service detection 6
INFO ... ... TLS (Multiple Issues) General 4
INFO ... ... Apache HTTP Server (Multiple Issues) Web Servers 2
INFO ... ... HTTP (Multiple Issues) Web Servers 2
INFO ... ... PHP (Multiple Issues) Web Servers 2
Host Details
IP: 192.168.50.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 4:25 PM
Vulnerabilities
Critical
High
Medium
Low
Info