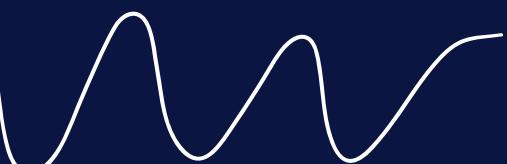


ACTIVITY



VALUTAZIONE DELLA VULNERABILITÀ



ha lo scopo di identificare ed assegnare un rischio alle vulnerabilità / configurazioni errate trovate nelle fasi precedenti, e preparare alla fase di exploit.

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

Mettere in comunicazione le due macchine (Kali Linux e Metasploitable) mettendoli sulla stessa rete.
Accesso Nessus



TRACCIA

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo)

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

- ☐ Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni
- ☐ Familiarizzare con alcune delle vulnerabilità note che troverete spesso.

COMMUNICAZIONE TRA MACCHINE

```
(kali㉿kali)-[~] $ ping 192.168.1.9
PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.
64 bytes from 192.168.1.9: icmp_seq=1 ttl=64 time=2.35 ms
64 bytes from 192.168.1.9: icmp_seq=2 ttl=64 time=8.09 ms
^C
--- 192.168.1.9 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 2.351/5.219/8.087/2.868 ms
```

NESSUS

The screenshot shows the Tenable Nessus interface. On the left, a terminal window displays the installation of the Nessus scanner on a Kali Linux system. The command run is:

```
$ sudo dpkg -i Nessus-10.6.1-debian10_amd64.deb
```

The output shows the scanner is installed and ready to use. On the right, the Nessus interface shows a list of scans. There are two scans listed: "Metasploitable 1" and "Metasploitable". Both are marked as "On Demand". The interface also includes a sidebar for "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Terrascan), and a "Tenable News" section.

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

Creazione di una nuova scansione su Nessus



NUOVA SCANSIONE

The screenshot shows the 'My Scans' page with a list of existing scans: 'Metasploitable 1' and 'Metasploitable'. The 'New Scan' button is highlighted with a red circle.

Per avviare una nuova scansione si clicca sul pulsante evidenziato nell'immagine affianco

poi si sceglie il tipo di scansione ma in questo caso era richiesto il Basic Network Scan

The screenshot shows the 'Scan Templates' page with various scan types: Host Discovery, Basic Network Scan, Advanced Scan, Advanced Dynamic Scan, Malware Scan, and Mobile Device Scan. The 'Basic Network Scan' option is highlighted with a red box.

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. It includes sections for Settings, Credentials, and Plugins. The 'Targets' section shows a text input field for 'Targets' with an example: '192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'. The 'Launch' button is highlighted with a red arrow.

infine si completa i campi richiesti per poi cliccare sul pulsante launch.

VALUTAZIONE DELLA VULNERABILITÀ

Risultato della scansione



NUOVA SCANSIONE

Scans

Metasploitable 1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 7:08 AM
- End: Today at 7:30 AM
- Elapsed: 22 minutes

Vulnerabilities

Severity	Count
Critical	12
High	7
Medium	25
Low	7
Info	133

Scans

Metasploitable 1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 7:08 AM
- End: Today at 7:30 AM
- Elapsed: 22 minutes

Vulnerabilities

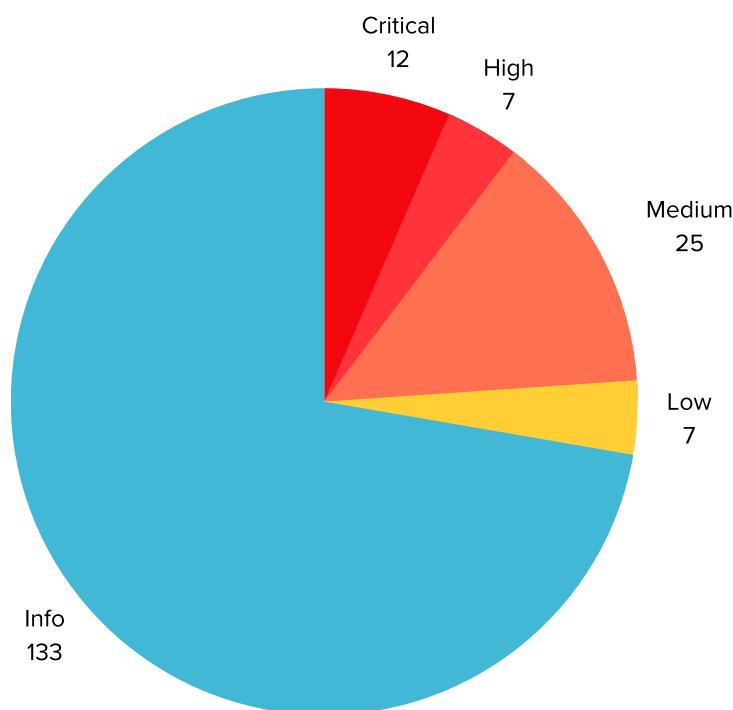
Sev	CVSS	VPR	Name	Family	Count
Critical	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1
Critical	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8		Bind Shell Backdoor Detection	Backdoors	1
Mixed	DNS (Multiple Issues)	DNS	4
Mixed	Apache Tomcat (Multiple Issues)	Web Servers	4
Critical	SSL (Multiple Issues)	Gain a shell remotely	3
Mixed	SSL (Multiple Issues)	Service detection	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

VALUTAZIONE DELLA VULNERABILITÀ

Report



VULNERABILITÀ



AGENDA

- 1 Critical
- 1 High
- 1 Medium
- 1 Low
- 1 Info

Approfondimento delle prime 4 vulnerabilità critiche:

<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	<input type="radio"/>	<input type="button" value="edit"/>
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	<input type="radio"/>	<input type="button" value="edit"/>
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	<input type="radio"/>	<input type="button" value="edit"/>
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	<input type="radio"/>	<input type="button" value="edit"/>

1) NFS Exported Share Information Disclosure:

è una vulnerabilità in cui le informazioni condivise tramite NFS sono diffuse in modo non autorizzato. Questo può accadere se la configurazione del sistema NFS non è adeguatamente protetta.

Soluzioni:

- Impostare i permessi di condivisione in modo che solo gli utenti autorizzati possano accedere ai dati condivisi.
- Limitare l'accesso NFS solo agli host o alle reti autorizzate.
- Mantenere tutti i software di sistema e le implementazioni NFS aggiornate.
- Monitorare e registrare l'accesso NFS per individuare attività sospette o non autorizzate.

VALUTAZIONE DELLA VULNERABILITÀ

Report



2) Unix Operating System Unsupported Version Detection:

si riferisce a una pratica di sicurezza in cui si cerca di identificare e rilevare versioni non supportate del sistema operativo Unix (una famiglia di sistemi operativi multiutente e multitasking) in esecuzione su un sistema o su una rete.

Soluzione:

- Mantenere aggiornato il sistema operativo o pianificare l'aggiornamento a una versione più recente o supportata

3) VNC Server 'password' Password:

VNC (Virtual Network Computing) è un sistema di controllo remoto che consente agli utenti di accedere e controllare un computer da un'altra posizione tramite una connessione di rete.

Soluzioni:

- Password forte: Questa password dovrebbe essere complessa e difficile da indovinare contenente almeno 8 caratteri tra lettere maiuscole e minuscole, alfanumerici e speciali.
- Crittografia: È consigliabile utilizzare una connessione VNC cifrata per proteggere i dati scambiati tra il client e il server.
- Autenticazione a due fattori: Se possibile, utilizzare l'autenticazione a due fattori per il server VNC. Questo aggiunge un ulteriore livello di sicurezza richiedendo un secondo metodo di autenticazione oltre alla password.
- Firewall e filtraggio degli indirizzi IP: Limitare l'accesso al server VNC utilizzando un firewall o il filtraggio degli indirizzi IP.
- Aggiornamenti: Assicurarsi che il software VNC e il sistema operativo siano aggiornati

4) Bind Shell Backdoor Detection:

è un processo di individuare e rilevare una "bind shell backdoor" o una "backdoor a shell di bind". Una backdoor è una porta d'accesso nascosta o un meccanismo che consente a un attaccante di ottenere accesso non autorizzato a un sistema o a una rete. La "bind shell" è un tipo di backdoor che crea una shell interattiva sul sistema di destinazione e permette all'attaccante di controllare il sistema da remoto.

Soluzioni:

- Uso di firewall
- Monitoraggio del traffico
- Aggiornamenti di sicurezza regolari
- Pratiche di autenticazione solide per ridurre le possibilità di compromissione del sistema