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.

Svolgimento:

Configurata la rete interna su VirtualBox tra Kali Linux e Metaspoitable in modo che possano comunicare tra di loro.

Sono stati utilizzati 2 tool per il Port Scanner e il Vulnerability Scanner.

Avviati i 2 sistemi operativi è stato utilizzato il comando «PING» per confermare che i 2 dispositivi comunicassero.

Da Kali Linux, utilizzando il Port Scanner **NMAP** è stato eseguito il comando

nmap –sV –sT –O 192.168.50.101

per verificare quali porte, servizi e versioni utilizza Metaspoitable.

```
└─# nmap -sV -sT -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 09:25 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disab
led. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:58:0A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li
nux:linux_kernel

OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.46 seconds
```

Dopo è stato eseguito il tool Vulnerability Scanner **NESSUS** sull'indirizzo IP 192.168.50.101.
Dopo un'accurate ricerca sono state trovate diverse vulnerabilità su quel sistema.

192.168.50.101

8	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 8

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

Vulnerabilità: VNC Server 'password' Password.
È stato riscontrato che sul server VNC ci sia una password, per accedervi, molto debole.

Soluzione:
Cambiare la password.

Usando il comando

vncviewer 192.168.50.101

sono riuscito ad accedere da remoto a Metaspoitable ed eseguendo

vncpasswd

sono riuscito a cambiare la password usando caratteri speciali, maiuscoli, minuscoli e numeri, portando la vulnerabilità da livello CRITICAL a livello INFO.

192.168.50.101

0	0	0	0	3
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19288	VNC Server Security Type Detection
INFO	N/A	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	10342	VNC Software Detection