Raccolta informazioni su macchina metasploitable 192.168.50.100

- **nmap -sn -PE <target>**
  - sn esegue un ping ai vari host nell'intervallo specificato. Se un host risponde, verrà elencato come attivo.

  -PE abilita la rilevazione tramite ICMP Echo Request.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:55 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00087s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

- **crackmapexec ssh <target>**
  interroga il servizio ssh sull'ip target

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.50.100
SSH         192.168.50.100  22     192.168.50.100   [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

- **nmap -sV <target>**

  esegue lo scan delle porte principali e della versione dei servizi attivi su ciasuna porta, analizza il sistema operativo della macchina target (banner grabbing)

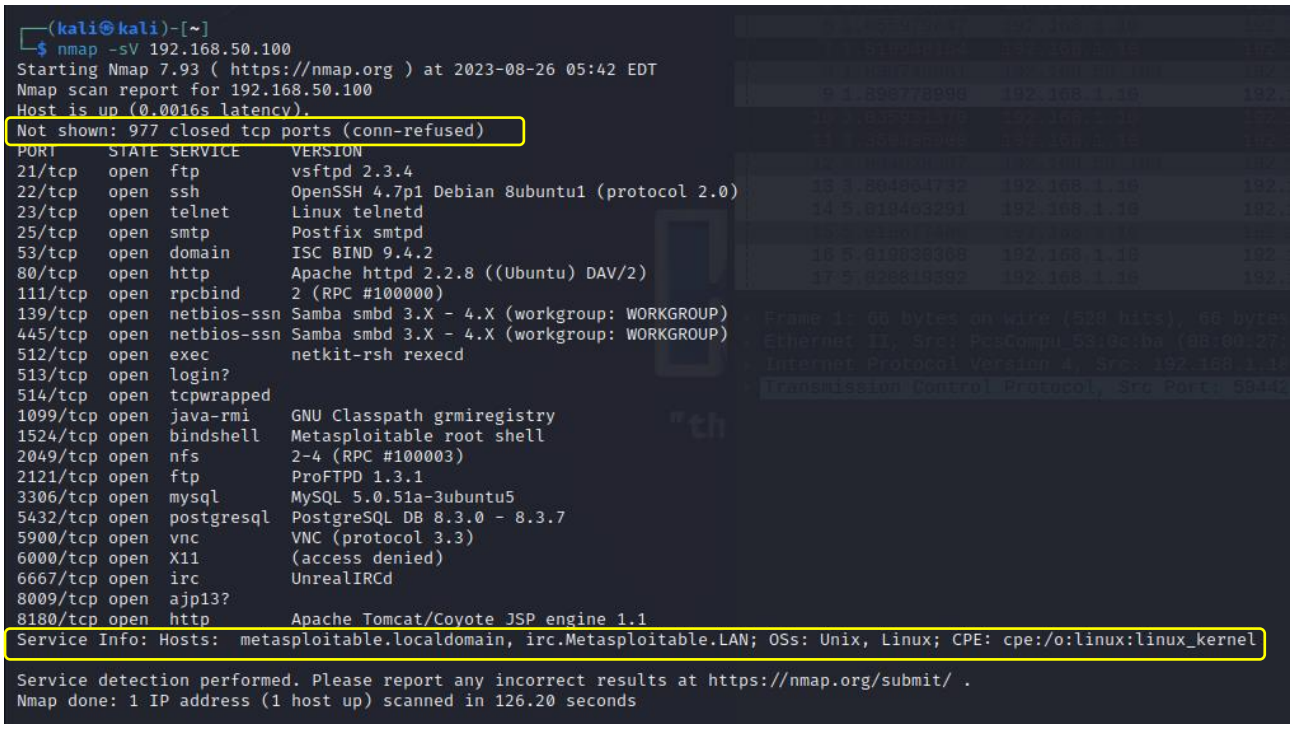
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:42 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.20 seconds
```

Report di Scansione

Indirizzo IP Target: 192.168.50.100

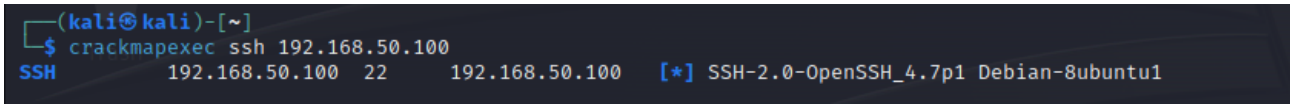
Dettagli Generali:

- L'host 192.168.50.100 è attivo.
- 977 porte TCP sono state rilevate come chiuse.
- Nomi Host Associati: metasploitable.localdomain e irc.Metasploitable.LAN.
- Sistemi operativi rilevati: Unix Linux, basato su kernel Linux, distribuzione Debian Ubuntu.



Servizi Rilevati:

1. **FTP** (File Transfer Protocol, utilizzato per il trasferimento file) su porte 21 e 2121: Utilizzano, rispettivamente vsftpd 2.3.4 e ProFTPD 1.3.1.
2. **SSH** (Secure Shell, utilizzato per stabilire connessioni sicure) su porta 22: Utilizza OpenSSH 4.7p1 con Debian 8ubuntu1 (protocollo 2.0). Confermato anche dal comando crackmapexec ssh



3. **Telnet** (protocollo che consente l'interazione con un dispositivo remoto emulando una sessione di terminale) su porta 23: Utilizza Linux telnetd
4. **SMTP** ("Simple Mail Transfer Protocol", protocollo di Internet utilizzato per la trasmissione di e-mail tra server) su porta 25: Implementato con Postfix smtpd.
5. **DNS** ("Domain Name System", utilizzato per risolvere nomi di dominio leggibili dall'uomo in indirizzi IP e viceversa) su porta 53: Utilizza ISC BIND 9.4.2.
6. **HTTP** ("HyperText Transfer Protocol" è il protocollo che i browser web utilizzano per comunicare con i server web e viceversa) su porte 80 e 8180: Utilizzano, rispettivamente, Apache httpd 2.2.8 su Ubuntu con supporto DAV/2 e Apache Tomcat/Coyote JSP engine 1.1.

7. **RPCBIND** su porta 111: Versione 2 (RPC #100000).

RPC (Remote Procedure Call):
RPC è un protocollo che permette a un programma di causare l'esecuzione di un procedimento (subroutine) in un altro spazio di indirizzi (tipicamente su un altro computer in una rete condivisa). In sostanza, con RPC, è possibile "chiamare" un programma o una funzione su un altro computer come se fosse locale.

RPCBIND:
RPCBIND è un server che converte i numeri di programma RPC in indirizzi universali. Quando un servizio è inizialmente avviato, si registra con RPCBIND indicando il numero di programma RPC e l'indirizzo universale specifico su cui ascolta. Quando un client desidera fare una chiamata RPC a un determinato numero di programma, può prima contattare RPCBIND per determinare l'indirizzo su cui il programma sta ascoltando.

8. **NetBIOS** (consente la comunicazione basata su sessioni tra computer in una rete, come la condivisione di file e di stampanti) sulle porte 139 e 445: Samba smbd versioni 3.X - 4.X con workgroup "WORKGROUP".
9. **Exec** (parte della suite di comandi rsh, Remote Shell, in particolare si tratta di rexecd "Remote Execution Daemon", un demone che ascolta le richieste di esecuzione di comandi su una macchina remota) su porta 512: Utiliza netkit-rsh rexecd
10. **Login** (protocollo rlogin, remote login, permette a un utente di effettuare il login su un altro sistema host dalla sua postazione di lavoro o computer locale) su porta 513.
11. **Porta 514 tcpwrapped**

Tcpwrapped:

Funzione: `tcpwrapper` è una soluzione di sicurezza per Linux e altri sistemi UNIX-like che fornisce un controllo dell'accesso ai servizi di rete. Permette agli amministratori di definire quali host possono o non possono connettersi a servizi di rete sul sistema.

Come Funziona: Quando un servizio è "tcpwrapped", qualsiasi tentativo di connessione a quel servizio viene prima valutato dai `tcpwrappers`. Se l'host che tenta di connettersi è autorizzato, la connessione procede normalmente; in caso contrario, la connessione viene rifiutata.

File di Configurazione: Le regole per `tcpwrappers` sono solitamente definite nei file `/etc/hosts.allow` e `/etc/hosts.deny`.

12. **Java RMI** ("Remote Method Invocation" è un'API fornita dalla piattaforma Java che consente la chiamata di metodi su oggetti remoti presenti in diverse Java Virtual Machines) su porta 1099: Implementato con GNU Classpath grmiregistry.
13. **Bindshell** (vulnerabilità intenzionalmente inserita nella distribuzione Linux Metasploitable) su porta 1524

Una bind shell, in termini generali, è un tipo di backdoor che un attaccante pianta o sfrutta su un sistema vulnerabile. Una volta attivata, la bind shell "si lega" a una specifica porta di ascolto sul sistema compromesso.

Funzionamento:
Quando la bind shell viene eseguita, inizia ad ascoltare le connessioni in entrata sulla porta specificata, in questo caso la porta 1524. Qualsiasi utente che conosca l'esistenza di questa shell può connettersi a questa porta utilizzando strumenti standard come "netcat" o "telnet".
Una volta stabilita la connessione, l'utente ottiene una shell (un'interfaccia di comando) sul sistema compromesso. Nel contesto di Metasploitable e della porta 1524, questa shell ha privilegi di root, che è l'accesso amministrativo più alto su un sistema Linux.

14. **NFS** ("Network File System" è un protocollo utilizzato per condividere file tra computer in una rete) su porta 2049: Supporta versioni da 2 a 4 (RPC #100003).
15. **MySQL** (sistema di gestione di database relazionali) su porta 3306: Versione 5.0.51a-3ubuntu5.
16. **PostgreSQL** (sistema di gestione di database relazionali open source) su porta 5432: Versioni da 8.3.0 a 8.3.7.
17. **VNC** ("Virtual Network Computing"è un software che consente la visualizzazione grafica di un desktop remoto e l'interazione con esso attraverso una rete) su porta 5900: Utilizza il protocollo 3.3.
18. **X11** (noto anche come X Window System, è un protocollo di visualizzazione remota che fornisce una base per le interfacce utente grafiche – GUI - su sistemi Unix-like, come Linux e BSD. Consente di eseguire

applicazioni con una GUI su un sistema, il server, e di visualizzare e interagire con esse su un altro sistema, il client) su porta 6000: Accesso negato, il servizio non è configurato per accettare connessioni da client remoti o da indirizzi IP non autorizzati.

19. **IRC** (**"**Internet Relay Chat" è un protocollo di comunicazione utilizzato per la messaggistica di testo in tempo reale su Internet) su porta 6667: Usa UnrealIRCd.
20. **AJP13** ("Apache JServ Protocol" è un protocollo binario ottimizzato utilizzato per comunicare tra un server web come Apache e un server di applicazioni come Tomcat) su porta 8009: Implementato con Apache Jserv (Protocollo v1.3).