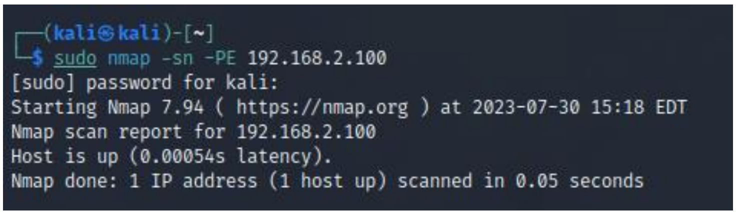
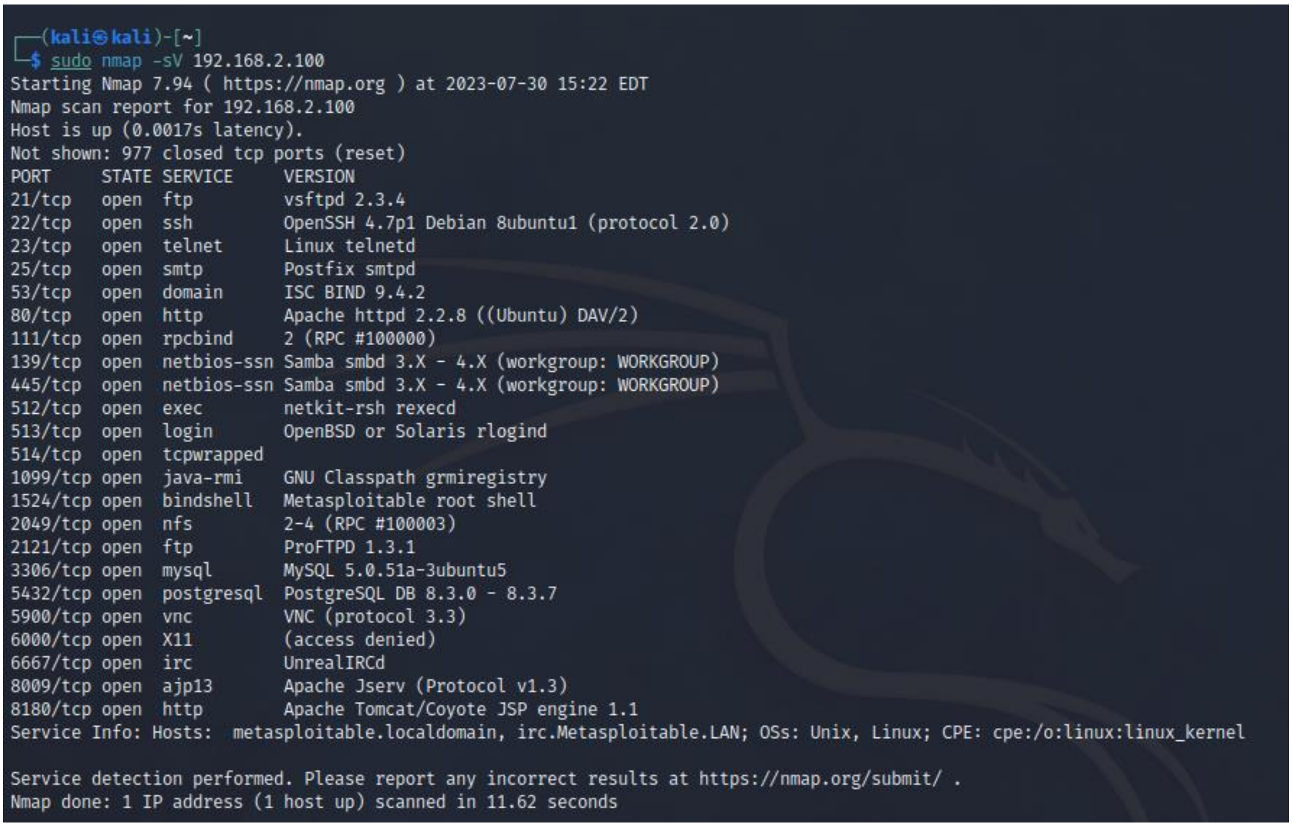
RACCOLTA INFORMAZIONI
METASPLOITABLE

1. Strumenti e comandi utilizzati
   - nmap -sn -PE
   - nmap -sV
   - nmap -sS -sV
   - nc -nvz
   - us -mT
   - us -mU
   - crackmapexec

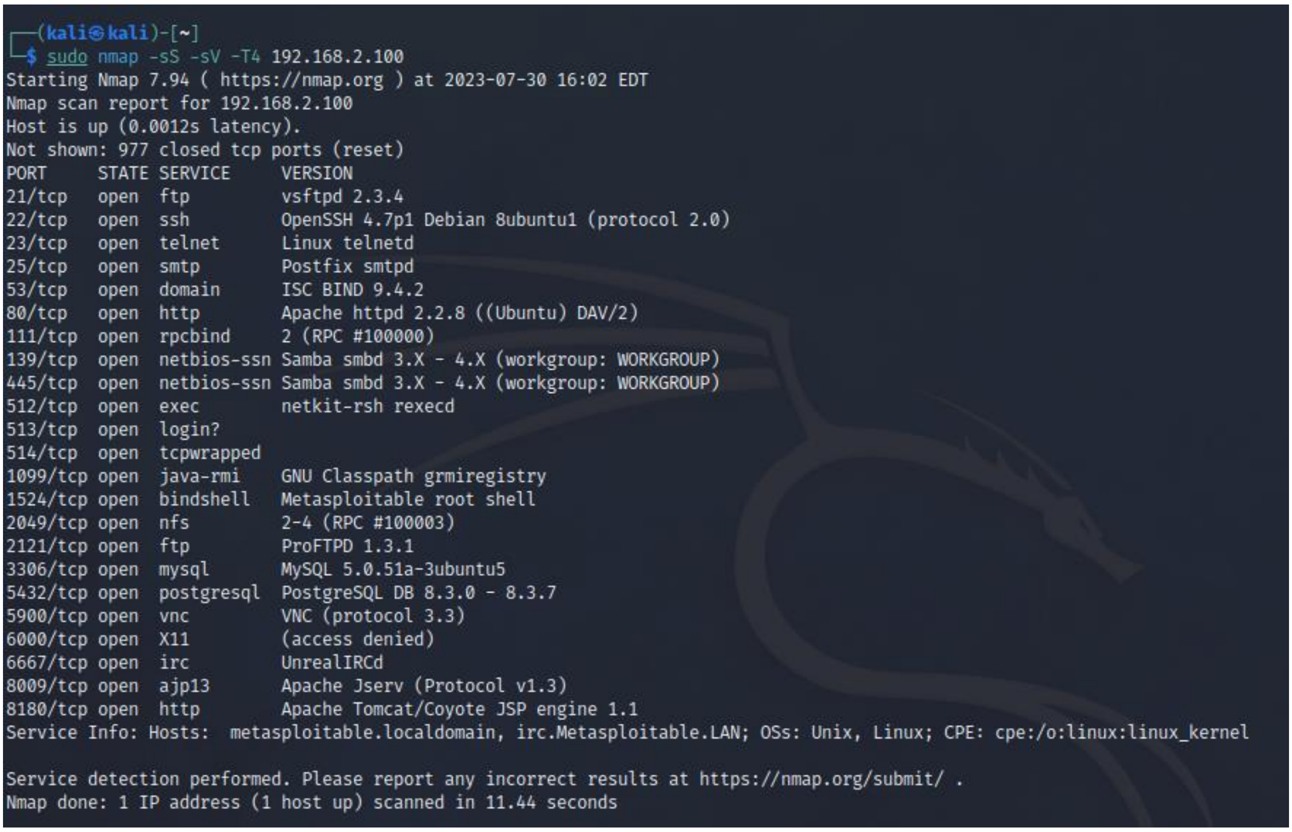
2. Informazioni raccolte



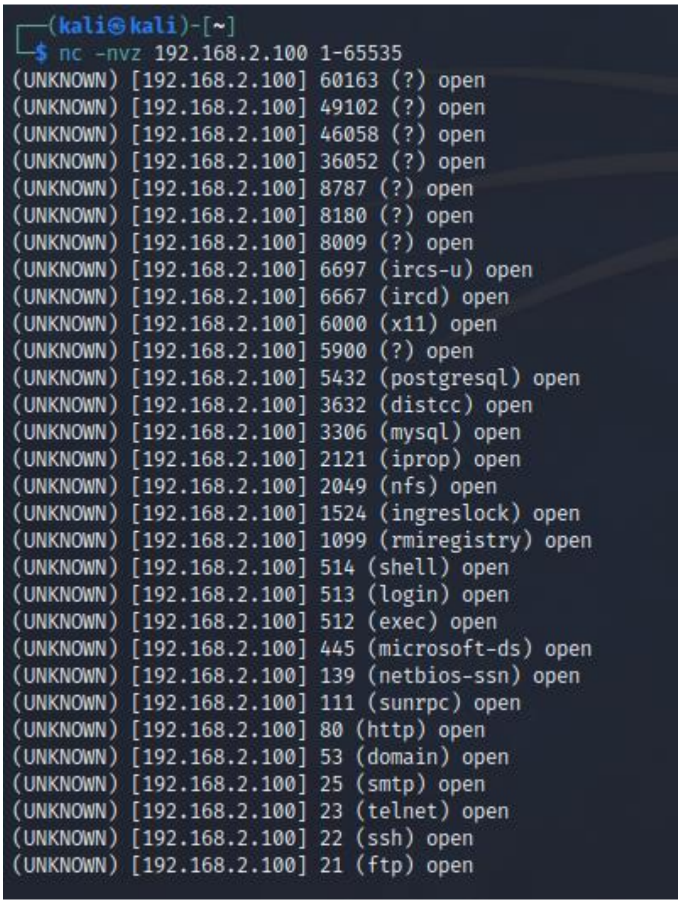
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.2.100
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-30 15:18 EDT
Nmap scan report for 192.168.2.100
Host is up (0.00054s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```



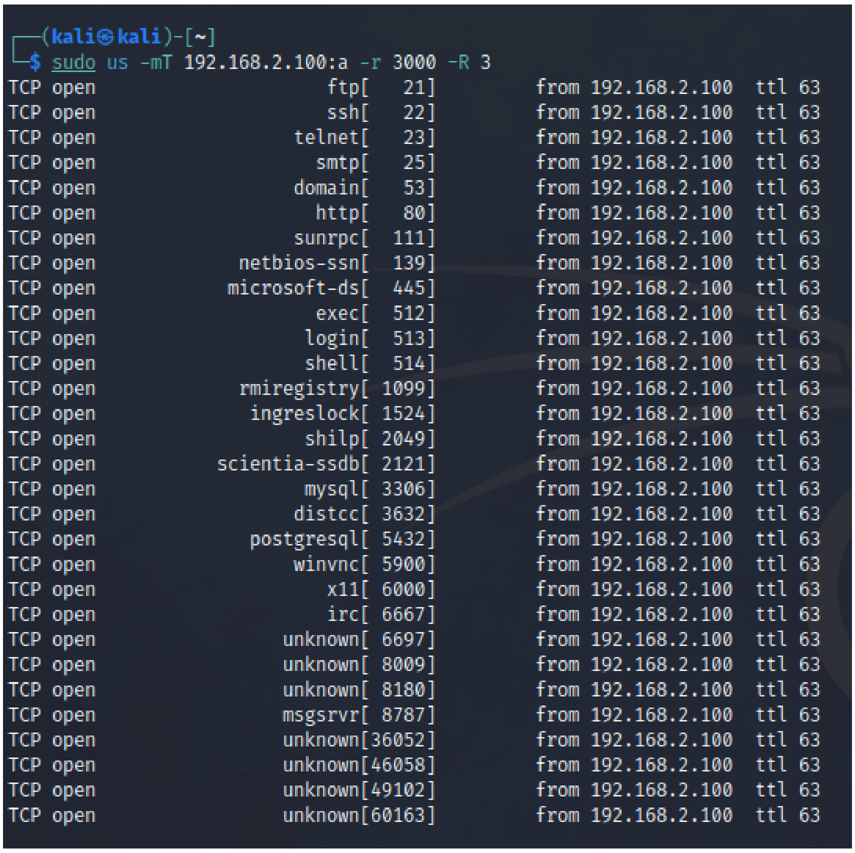
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.2.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-30 15:22 EDT
Nmap scan report for 192.168.2.100
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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       OpenBSD or Solaris rlogind
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       Apache Jserv (Protocol v1.3)
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 11.62 seconds
```



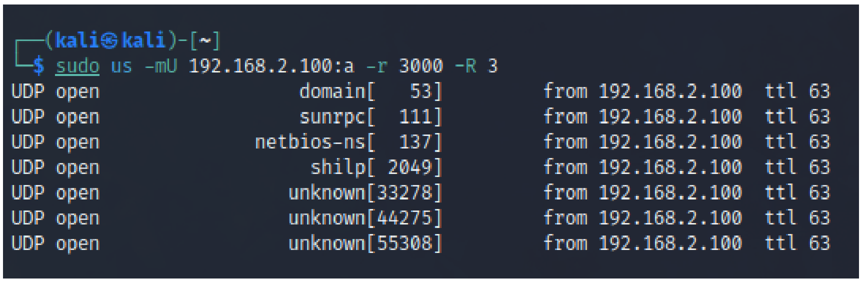
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.2.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-30 16:02 EDT
Nmap scan report for 192.168.2.100
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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       Apache Jserv (Protocol v1.3)
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 11.44 seconds
```



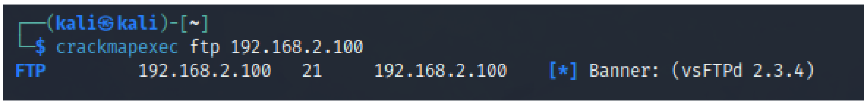
```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.2.100 1-65535
(UNKNOWN) [192.168.2.100] 60163 (?) open
(UNKNOWN) [192.168.2.100] 49102 (?) open
(UNKNOWN) [192.168.2.100] 46058 (?) open
(UNKNOWN) [192.168.2.100] 36052 (?) open
(UNKNOWN) [192.168.2.100] 8787 (?) open
(UNKNOWN) [192.168.2.100] 8180 (?) open
(UNKNOWN) [192.168.2.100] 8009 (?) open
(UNKNOWN) [192.168.2.100] 6697 (ircs-u) open
(UNKNOWN) [192.168.2.100] 6667 (ircd) open
(UNKNOWN) [192.168.2.100] 6000 (x11) open
(UNKNOWN) [192.168.2.100] 5900 (?) open
(UNKNOWN) [192.168.2.100] 5432 (postgresql) open
(UNKNOWN) [192.168.2.100] 3632 (distcc) open
(UNKNOWN) [192.168.2.100] 3306 (mysql) open
(UNKNOWN) [192.168.2.100] 2121 (iprop) open
(UNKNOWN) [192.168.2.100] 2049 (nfs) open
(UNKNOWN) [192.168.2.100] 1524 (ingreslock) open
(UNKNOWN) [192.168.2.100] 1099 (rmiregistry) open
(UNKNOWN) [192.168.2.100] 514 (shell) open
(UNKNOWN) [192.168.2.100] 513 (login) open
(UNKNOWN) [192.168.2.100] 512 (exec) open
(UNKNOWN) [192.168.2.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.2.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.2.100] 111 (sunrpc) open
(UNKNOWN) [192.168.2.100] 80 (http) open
(UNKNOWN) [192.168.2.100] 53 (domain) open
(UNKNOWN) [192.168.2.100] 25 (smtp) open
(UNKNOWN) [192.168.2.100] 23 (telnet) open
(UNKNOWN) [192.168.2.100] 22 (ssh) open
(UNKNOWN) [192.168.2.100] 21 (ftp) open
```



```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT 192.168.2.100:a -r 3000 -R 3
TCP open                     ftp[   21]         from 192.168.2.100  ttl 63
TCP open                     ssh[   22]         from 192.168.2.100  ttl 63
TCP open                  telnet[   23]         from 192.168.2.100  ttl 63
TCP open                    smtp[   25]         from 192.168.2.100  ttl 63
TCP open                  domain[   53]         from 192.168.2.100  ttl 63
TCP open                    http[   80]         from 192.168.2.100  ttl 63
TCP open                  sunrpc[  111]         from 192.168.2.100  ttl 63
TCP open             netbios-ssn[  139]         from 192.168.2.100  ttl 63
TCP open            microsoft-ds[  445]         from 192.168.2.100  ttl 63
TCP open                    exec[  512]         from 192.168.2.100  ttl 63
TCP open                   login[  513]         from 192.168.2.100  ttl 63
TCP open                   shell[  514]         from 192.168.2.100  ttl 63
TCP open             rmiregistry[ 1099]         from 192.168.2.100  ttl 63
TCP open              ingreslock[ 1524]         from 192.168.2.100  ttl 63
TCP open                   shilp[ 2049]         from 192.168.2.100  ttl 63
TCP open           scientia-ssdb[ 2121]         from 192.168.2.100  ttl 63
TCP open                   mysql[ 3306]         from 192.168.2.100  ttl 63
TCP open                  distcc[ 3632]         from 192.168.2.100  ttl 63
TCP open              postgresql[ 5432]         from 192.168.2.100  ttl 63
TCP open                  winvnc[ 5900]         from 192.168.2.100  ttl 63
TCP open                     x11[ 6000]         from 192.168.2.100  ttl 63
TCP open                     irc[ 6667]         from 192.168.2.100  ttl 63
TCP open                 unknown[ 6697]         from 192.168.2.100  ttl 63
TCP open                 unknown[ 8009]         from 192.168.2.100  ttl 63
TCP open                 unknown[ 8180]         from 192.168.2.100  ttl 63
TCP open                 msgsrvr[ 8787]         from 192.168.2.100  ttl 63
TCP open                 unknown[36052]         from 192.168.2.100  ttl 63
TCP open                 unknown[46058]         from 192.168.2.100  ttl 63
TCP open                 unknown[49102]         from 192.168.2.100  ttl 63
TCP open                 unknown[60163]         from 192.168.2.100  ttl 63
```



```
┌──(kali㉿kali)-[~]
└─$ sudo us -mU 192.168.2.100:a -r 3000 -R 3
UDP open                  domain[   53]         from 192.168.2.100  ttl 63
UDP open                  sunrpc[  111]         from 192.168.2.100  ttl 63
UDP open              netbios-ns[  137]         from 192.168.2.100  ttl 63
UDP open                   shilp[ 2049]         from 192.168.2.100  ttl 63
UDP open                 unknown[33278]         from 192.168.2.100  ttl 63
UDP open                 unknown[44275]         from 192.168.2.100  ttl 63
UDP open                 unknown[55308]         from 192.168.2.100  ttl 63
```



```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ftp 192.168.2.100
FTP         192.168.2.100  21    192.168.2.100   [*] Banner: (vsFTPd 2.3.4)
```

Con le scansioni effettuate, di cui sono stati riportati i risultati nelle schermate precedenti, abbiamo raccolto informazioni circa le porte aperte sulla macchina Metasploitable e i relativi demoni (servizi).
Tramite il comando *crackmapexec* è stato rilevato che il server FTP di default su sistemi Unix-like, ovvero vsFTPd nella versione 2.3.4, risulta compromesso dalla vulnerabilità indentificata con il CVE (Common Vulnerabilities and Exposures) n. 2011-2523[1] tramite la quale è poi possibile una backdoor attraverso la quale viene aperta una shell sulla porta 6200-tcp. In rete sono presenti istruzioni volte allo sfruttamento di tale vulnerabilità[2].

[1] https://nvd.nist.gov/vuln/detail/CVE-2011-2523

[2] https://www.exploit-db.com/exploits/49757