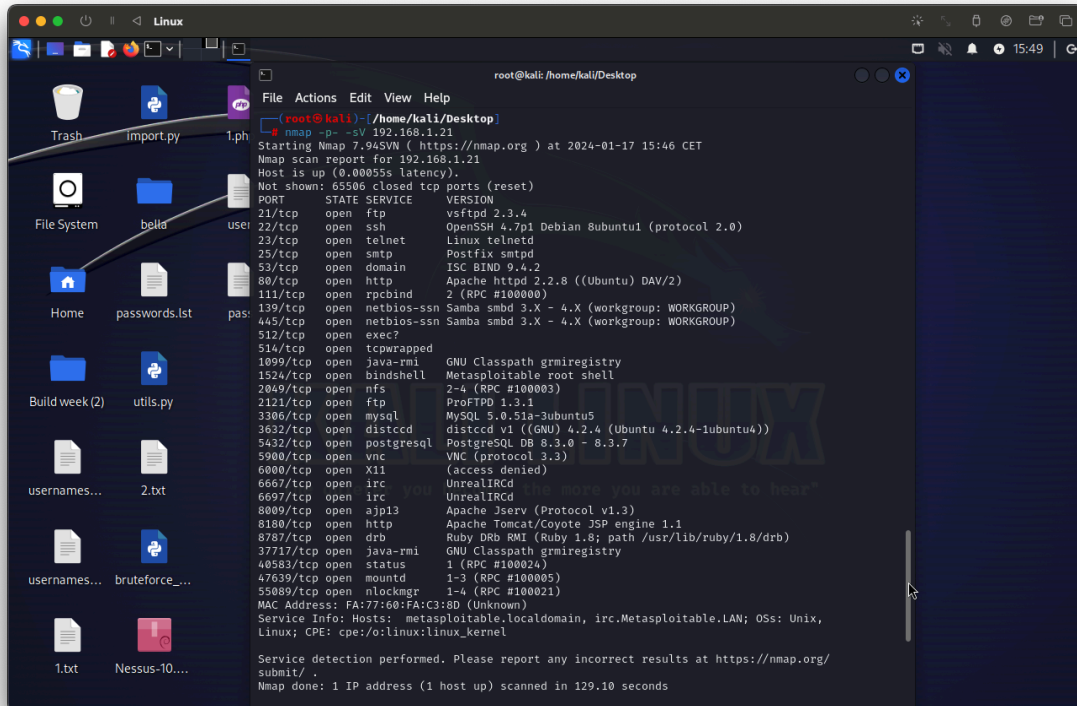


Consegna S6-L3

L'obiettivo è attaccare la macchina metasploitable su porte che potrebbero essere protette da password

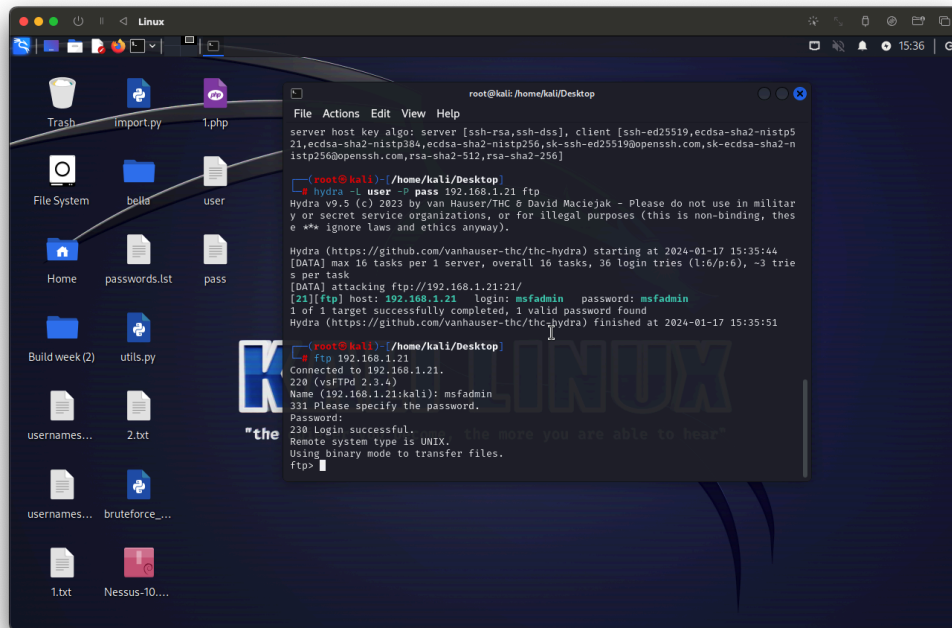
Prima di tutto occorre individuare le porte accessibili e i rispettivi servizi



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
root@kali ~ - /home/kali/Desktop
# nmap -p- -sV 192.168.1.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 15:46 CET
Nmap scan report for 192.168.1.21
Host is up (0.00055s latency).
Not shown: 65506 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?
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
3692/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
37717/tcp open  java-rmi     GNU Classpath grmiregistry
40583/tcp open  status       1 (RPC #100024)
47639/tcp open  mountd       1-3 (RPC #100005)
55089/tcp open  rlockmgr     1-4 (RPC #100021)
MAC Address: FA:77:60:FA:C3:6D (Unknown)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 129.10 seconds
```

Successivamente occorrono due file con utenti e password da testare
Attraverso hydra possiamo inserire i file e effettuare un brute force



Come è possibile notare hydra ha trovato l'username e la password