

S5-L3

abbiamo utilizzato nmap per eseguire le scansioni su meta e su windows, dalle scansioni su nmap abbiamo notato che su meta ci sono diverse porte aperte, la principale differenza tra (tcp e syn) e la velocità della scansione.

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.20.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:46 CET
Nmap scan report for 192.168.20.102
Host is up (0.00096s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now active. Monitor the filter reload progress.

Filtering WAN LAN LAN2

Rules (Drag to Change Order)						
	States	Protocol	Source	Port	Destination	
<input type="checkbox"/>	States	*	*	*	LAN Address	
<input type="checkbox"/>	States	tcp	*	*	tcp 21-23	
<input type="checkbox"/>	States	tcp	LAN subnets	*	*	
<input type="checkbox"/>	States	tcp	LAN subnets	*	*	

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.20.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:48 CET
Nmap scan report for 192.168.20.102
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Filtering WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	
<input checked="" type="checkbox"/>	States	*	*	*	LAN Address	
<input type="checkbox"/>	States	tcp	*	*	tcp 21-23	
<input type="checkbox"/>	States	tcp	LAN subnets	*	*	
<input type="checkbox"/>	States	tcp	LAN subnets	*	*	

```
(kali㉿kali)-[~]  
$ sudo nmap -sT 192.168.20.102  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:50 CET  
Nmap scan report for 192.168.20.102  
Host is up (0.0071s latency).  
Not shown: 977 closed tcp ports (conn-refused)
```

```
(kali㉿kali)-[~]  
$ sudo nmap -Pn 192.168.20.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 14:26 CET  
Nmap scan report for 192.168.20.101  
Host is up.  
All 1000 scanned ports on 192.168.20.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 215.70 seconds
```

```
(kali㉿kali)-[~]  
$ sudo nmap -sV 192.168.20.102  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:53 CET  
Nmap scan report for 192.168.20.102  
Host is up (0.00097s 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 11.53 seconds
```