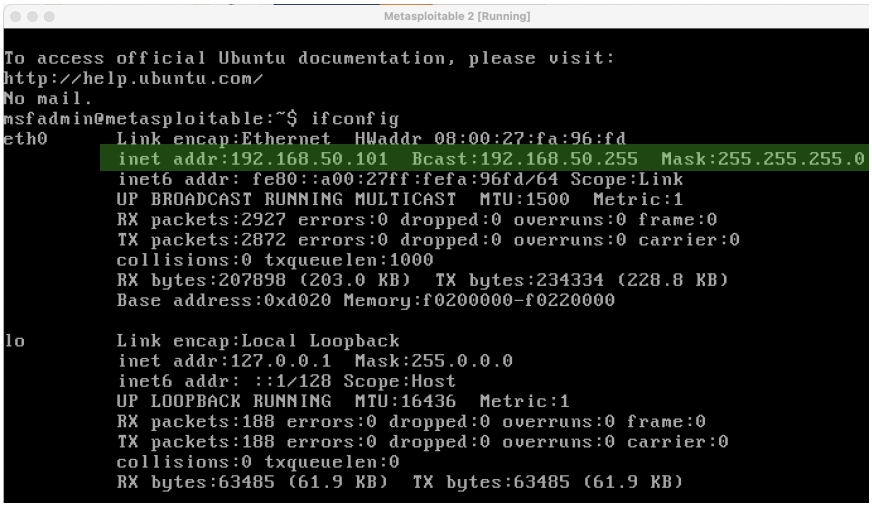
PROGETTO MODULO 3

Sappiamo che la configurazione di rete di ***Metasploitable*** è
——————>



1) SCANSIONE DELLE PORTE E DEI SERVIZI

Tramite il comando `nmap` si esegue una scansione delle porte e dei servizi in esecuzione su *Metasploitable*.

Utilizzo: `nmap -sV -o 192.168.50.101`

dove:
`-sV` ho i dettagli su i servizi che sono in esecuzione e la versione dei software associati ai questi sevizi.
`- o` cerca di determinare il sistema operativo in uso sulla macchina.

Così si possono identificare i servizi di rete disponibili e accessibili, dando una visione generale sulle potenziali vulnerabilità sulla macchina.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 09:42 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00081s 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  shell       Netkit rshd
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
MAC Address: 08:00:27:FA:96:FD (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: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.10 seconds
```

Legenda:

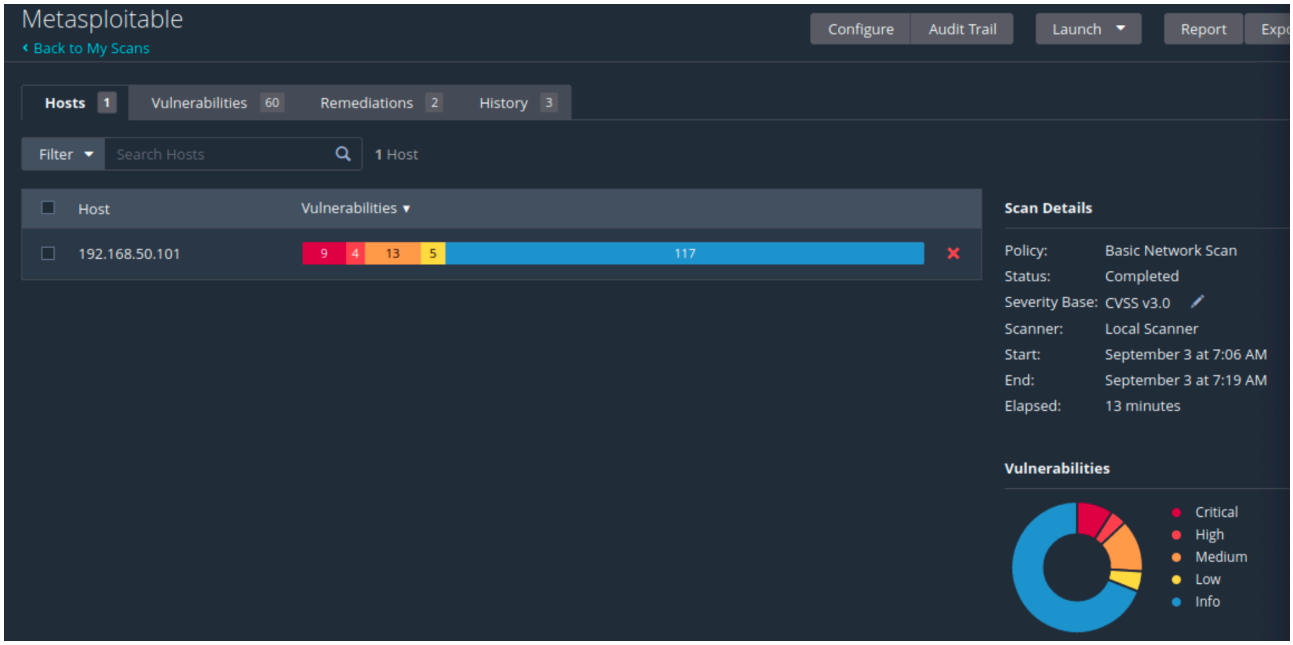
servizi di rete disponibili e accessibili
Versione dei software associati ai servizi
Sistema Operativo

2) ANALISI DELLE VULNERABILITÀ

Effettuo l'analisi delle vulnerabilità tramite Nessus.
Dove si è riscontrato un totale di 148 vulnerabilità della sicurezza.
Divise in:

- **CRITICHE** : 9
- **ALTE** : 4
- **MEDIE** : 13
- **BASSE** : 5
- **Informazioni** : 117

Come si evince dal PDF -> **ScansioneInizio.pdf**



Le vulnerabilità critiche dovranno essere risolte per prime.

3) REMEDIATION ACTION

File pdf —> **RemediationMeta.pdf**

4) SCANSIONE FINALE

File pdf —> **ScansioneFine.pdf**