```
(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 13:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39909/tcp   mountd
|   100005  1,2,3      41094/udp   mountd
|   100021  1,3,4      37014/udp   nlockmgr
|   100021  1,3,4      55305/tcp   nlockmgr
|   100024  1          49781/tcp   status
|_  100024  1          49822/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, Speaks41ProtocolNew, Support41Auth,
SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag, SupportsCompression
|   Status: Autocommit
|_  Salt: [k)')9~3#RS-$jkZc`:@
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-07-02T18:00:15+00:00; +4s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:E0:46:9B (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

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
```

| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-07-02T13:59:00-04:00
|_clock-skew: mean: 1h20m06s, deviation: 2h18m37s, median: 3s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT   ADDRESS
1   0.55 ms 192.168.50.101

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 148.92 seconds

┌──(kali㉿kali)-[~]
└─$ **sudo nmap -sS 192.168.50.101**
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-03 14:18 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)

Sorgente	**Destinazione**	**PORT**	**STATE SERVICE**
192.168.50.100	192.168.50.101	21/tcp	open ftp
192.168.50.100	192.168.50.101	22/tcp	open ssh
192.168.50.100	192.168.50.101	23/tcp	open telnet
192.168.50.100	192.168.50.101	25/tcp	open smtp
192.168.50.100	192.168.50.101	53/tcp	open domain
192.168.50.100	192.168.50.101	80/tcp	open http
192.168.50.100	192.168.50.101	111/tcp	open rpcbind
192.168.50.100	192.168.50.101	139/tcp	open netbios-ssn
192.168.50.100	192.168.50.101	445/tcp	open microsoft-ds
192.168.50.100	192.168.50.101	512/tcp	open exec
192.168.50.100	192.168.50.101	513/tcp	open login
192.168.50.100	192.168.50.101	514/tcp	open shell
192.168.50.100	192.168.50.101	1099/tcp	open rmiregistry
192.168.50.100	192.168.50.101	1524/tcp	open ingreslock
192.168.50.100	192.168.50.101	2049/tcp	open nfs
192.168.50.100	192.168.50.101	2121/tcp	open ccproxy-ftp
192.168.50.100	192.168.50.101	3306/tcp	open mysql
192.168.50.100	192.168.50.101	5432/tcp	open postgresql
192.168.50.100	192.168.50.101	5900/tcp	open vnc
192.168.50.100	192.168.50.101	6000/tcp	open X11
192.168.50.100	192.168.50.101	6667/tcp	open irc
192.168.50.100	192.168.50.101	8009/tcp	open ajp13
192.168.50.100	192.168.50.101	8180/tcp	open unknown

MAC Address: 08:00:27:E0:46:9B (Oracle VirtualBox virtual NIC)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 14:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (conn-refused)
```

SORGENTE	DESTINAZIONE	PORT	STATE	SERVICE
192.168.50.100	192.168.50.101	21/tcp	open	ftp
192.168.50.100	192.168.50.101	22/tcp	open	ssh
192.168.50.100	192.168.50.101	23/tcp	open	telnet
192.168.50.100	192.168.50.101	25/tcp	open	smtp
192.168.50.100	192.168.50.101	53/tcp	open	domain
192.168.50.100	192.168.50.101	80/tcp	open	http
192.168.50.100	192.168.50.101	111/tcp	open	rpcbind
192.168.50.100	192.168.50.101	139/tcp	open	netbios-ssn
192.168.50.100	192.168.50.101	445/tcp	open	microsoft-ds
192.168.50.100	192.168.50.101	512/tcp	open	exec
192.168.50.100	192.168.50.101	513/tcp	open	login
192.168.50.100	192.168.50.101	514/tcp	open	shell
192.168.50.100	192.168.50.101	1099/tcp	open	rmiregistry
192.168.50.100	192.168.50.101	1524/tcp	open	ingreslock
192.168.50.100	192.168.50.101	2049/tcp	open	nfs
192.168.50.100	192.168.50.101	2121/tcp	open	ccproxy-ftp
192.168.50.100	192.168.50.101	3306/tcp	open	mysql
192.168.50.100	192.168.50.101	5432/tcp	open	postgresql
192.168.50.100	192.168.50.101	5900/tcp	open	vnc
192.168.50.100	192.168.50.101	6000/tcp	open	X11
192.168.50.100	192.168.50.101	6667/tcp	open	irc
192.168.50.100	192.168.50.101	8009/tcp	open	ajp13
192.168.50.100	192.168.50.101	8180/tcp	open	unknown

```
MAC Address: 08:00:27:E0:46:9B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```