

TARGET	COMANDO	RISULTATO
192.168.60.101	nmap -sn -PE 192.168.60.101	nmap -sn -PE 192.168.60.101 Starting Nmap 7.94SVN ( <a href="https://nmap.org">https://nmap.org</a> ) at 2024-04-29 14:56 EDT Nmap scan report for 192.168.60.101 Host is up (0.0051s latency). MAC Address: 08:00:27:93:D0:C4 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
192.168.60.101	nmap -sS -sV -T5 192.168.60.101	Starting Nmap 7.94SVN ( <a href="https://nmap.org">https://nmap.org</a> ) at 2024-04-29 15:01 EDT Nmap scan report for 192.168.60.101 Host is up (0.010s 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? 25/tcp    open  smtp? 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? 513/tcp   open  login? 514/tcp   open  shell? 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  ccproxy-ftp? 3306/tcp  open  mysql? 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  unknown
192.168.60.101	nmap 192.168.60.101	Starting Nmap 7.94SVN ( <a href="https://nmap.org">https://nmap.org</a> ) at 2024-04-29 15:07 EDT Nmap scan report for 192.168.60.101 Host is up (0.0011s 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

192.168.60.101	nmap -O 192.168.60.101	Starting Nmap 7.94SVN ( <a href="https://nmap.org">https://nmap.org</a> ) at 2024-04-29 15:08 EDT Nmap scan report for 192.168.60.101 Host is up (0.0055s 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
192.168.60.101	nc -nvz 192.168.60.101 1-1024	(UNKNOWN) [192.168.60.101] 514 (shell) open (UNKNOWN) [192.168.60.101] 513 (login) open (UNKNOWN) [192.168.60.101] 512 (exec) open (UNKNOWN) [192.168.60.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.60.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.60.101] 111 (sunrpc) open (UNKNOWN) [192.168.60.101] 80 (http) open (UNKNOWN) [192.168.60.101] 53 (domain) open (UNKNOWN) [192.168.60.101] 25 (smtp) open (UNKNOWN) [192.168.60.101] 23 (telnet) open (UNKNOWN) [192.168.60.101] 22 (ssh) open (UNKNOWN) [192.168.60.101] 21 (ftp) open