

FONTE DELLO SCAN	TARGET DELLO SCAN	TIPO DI SCAN	RISULTATI OTTENUTI
192,168,50,100	192,168,50,101	Scan TCP	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
192,168,50,100	192,168,50,101	Scan SYN	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 3632/tcp open distccd

192,168,50,100	192,168,50,101	Scan -A	<div>PORT STATE SERVICE VERSION</div> <div>21/tcp open ftp vsftpd 2.3.4</div> <div>ftp-syst:</div> <div>STAT:</div> <div>FTP server status:</div> <div>Connected to 192.168.50.100</div> <div>Logged in as ftp</div> <div>TYPE: ASCII</div> <div>No session bandwidth limit</div> <div>Session timeout in seconds is 300</div> <div>Control connection is plain text</div> <div>Data connections will be plain text</div> <div>vsFTPD 2.3.4 - secure, fast, stable</div> <div>End of status</div> <div>ftp-anon: Anonymous FTP login allowed (FTP code 230)</div> <div>22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)</div> <div>ssh-hostkey:</div> <div>1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)</div> <div>2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)</div> <div>23/tcp open telnet Linux telnetd</div> <div>25/tcp open smtp Postfix smtpd</div> <div>smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN</div> <div>53/tcp open domain ISC BIND 9.4.2</div> <div>dns-nsid:</div> <div>bind.version: 9.4.2</div> <div>80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)</div> <div>http-title: Metasploitable2 - Linux</div> <div>http-server-header: Apache/2.2.8 (Ubuntu) DAV/2</div> <div>111/tcp open rpcbind 2 (RPC #100000)</div> <div>rpcinfo:</div> <div>program version port/proto service</div> <div>100000 2 111/tcp rpcbind</div> <div>100000 2 111/udp rpcbind</div> <div>100003 2,3,4 2049/tcp nfs</div> <div>100003 2,3,4 2049/udp nfs</div> <div>100005 1,2,3 38345/tcp mountd</div> <div>100005 1,2,3 56439/udp mountd</div> <div>100021 1,3,4 40683/tcp nlockmgr</div> <div>100021 1,3,4 57828/udp nlockmgr</div> <div>100024 1 36786/tcp status</div> <div>100024 1 45322/udp status</div> <div>139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)</div> <div>445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)</div> <div>512/tcp open exec netkit-rsh rexecd</div> <div>513/tcp open login?</div> <div>514/tcp open shell Netkit rshd</div> <div>1099/tcp open java-rmi GNU Classpath grmiregistry</div> <div>1524/tcp open bindshell Metasploitable root shell</div> <div>MAC Address: 08:00:27:CD:BA:61 (Oracle VirtualBox virtual NIC)</div> <div>Device type: general purpose</div> <div>Running: Linux 2.6.X</div> <div>OS CPE: cpe:/o:linux:linux_kernel:2.6</div> <div>OS details: Linux 2.6.9 - 2.6.33</div> <div>Network Distance: 1 hop</div> <div>Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel</div> <div>Host script results:</div> <div>clock-skew: mean: -1h37m46s, deviation: 2h49m41s, median: -3h37m46s</div> <div>smb-os-discovery:</div> <div>OS: Unix (Samba 3.0.20-Debian)</div> <div>Computer name: metasploitable</div> <div>NetBIOS computer name:</div> <div>Domain name: localdomain</div> <div>FQDN: metasploitable.localdomain</div> <div>System time: 2024-07-03T06:24:37-04:00</div> <div>smb2-time: Protocol negotiation failed (SMB2)</div> <div>nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)</div> <div>smb-security-mode:</div> <div>account_used: <blank></div> <div>authentication_level: user</div> <div>challenge_response: supported</div> <div>message_signing: disabled (dangerous, but default)</div> <div>TRACEROUTE</div> <div>HOP RTT ADDRESS</div> <div>1 1.51 ms 192.168.50.101</div>
----------------	----------------	---------	---