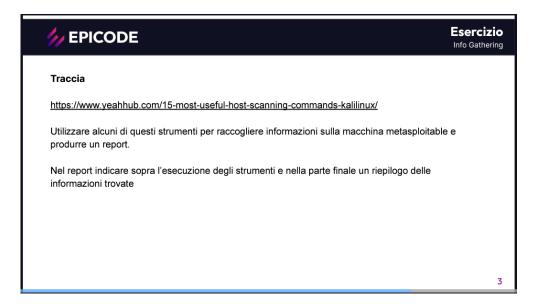
ESERCITAZIONE WEEK 10 DAY 5



Report

Macchina target: Metasploitable

Charles and	Disulant
Strumenti	Risultati
sudo nmap -sn -PE 192.168.50.101	Starting Nmap 7.94 (https://nmap.org) at 2024-01-
	13 12:30 EST
	Nmap scan report for 192.168.50.101
	Host is up (0.00024s latency).
	MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC)
	Nmap done: 1 IP address (1 host up) scanned in 13.06
	seconds
sudo netdiscover -r 192.168.50.101	File Actions Edit View Help Currently scanning: Finished! Screen View: Unique Hosts
	1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
	192.168.50.101 08:00:27:84:48:ba 1 60 PCS Systemtechnik GmbH
sudo crackmapexec 192.168.50.101	[*] First time use detected
	[*] Creating home directory structure
	[*] Creating default workspace
	[*] Initializing SMB protocol database
	[*] Initializing RDP protocol database
	[*] Initializing MSSQL protocol database
	[*] Initializing WINRM protocol database
	[*] Initializing SSH protocol database
	[*] Initializing LDAP protocol database
	[*] Initializing FTP protocol database
	[*] Copying default configuration file
	[*] Generating SSL certificate
	usage: crackmapexec [-h] [-t THREADS] [timeout
	TIMEOUT]
	[jitter INTERVAL] [darrell] [verbose]
	{smb,rdp,mssql,winrm,ssh,ldap,ftp}

	crackmapexec: error: argument protocol: invalid			
	choice: '192.168.50.101' (choose from 'smb', 'rdp',			
	'mssql', 'winrm', 'ssh', 'ldap', 'ftp')			
sudo nmap 192.168.50.101 -top- ports 10 -open	Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:36 EST			
	Nmap scan report for 192.168.50.101 Host is up (0.00032s latency).			
	1			
	Not shown: 3 closed tcp ports (reset) PORT STATE SERVICE			
	21/tcp open ftp			
	22/tcp open ssh			
	23/tcp open telnet			
	25/tcp open smtp			
	80/tcp open http			
	139/tcp open netbios-ssn			
	445/tcp open microsoft-ds			
	MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox			
	virtual NIC)			
	Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds			
sudo nmap 192.168.50.101 -p -sV - reason -dns-server ns	Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:37 EST			
1003011 -0113-301101 113	Error #486: Your port specifications are illegal.			
	Example of proper form: "-100,200-1024,T:3000-			
	4000,U:60000-"			
	QUITTING!			
sudo nmap -sS -sV -T4	Starting Nmap 7.94 (https://nmap.org) at 2024-01-			
192.168.50.101	13 12:39 EST			
	Nmap scan report for 192.168.50.101			
	Host is up (0.000061s 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			
	1			
	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			
	1			
	5432/tcp open postgresql PostgreSQL DB 8.3.0 -			
	8.3.7			
	1			

6667/tcp open irc				
### ### ##############################				
engine 1.1 MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC) 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 65:55 seconds Sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 345 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 38 (http) open (UNKNOWN) [192.168.50.101] 38 (http) open (UNKNOWN) [192.168.50.101] 32 (stente) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101]		8009/tcp open ajp13 Apache Jserv (Protocol v1.3)		
MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC) 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 P address (1 host up) scanned in 65.55 seconds sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 132 (exec) open (UNKNOWN) [192.168.50.101] 132 (exec) open (UNKNOWN) [192.168.50.101] 132 (ship) open (UNKNOWN) [192.168.50.101] 32 (ship) open (UNKNOWN) [192.168.50.101] 32 (ship) open (UNKNOWN) [192.168.50.101] 32 (ship) open (UNKNOWN) [192.168.50.101] 22 (shi) open (UNKNOWN)		8180/tcp open http Apache Tomcat/Coyote JSP		
virtual NIC 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 Pa address (1 host up) scanned in 65.55 seconds		engine 1.1		
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel		MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox		
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 65.55 seconds sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 24 (telnet) open (UNKNOWN) [192.168.50.101] 24 (telnet) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 26 (smtp) open (UNKNOWN) [192.		virtual NIC)		
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 65.55 seconds (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 45 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (metbios-ssn) open (UNKNOWN) [192.168.50.101] 131 (sunrpc) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [19		Service Info: Hosts: metasploitable.localdomain,		
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 65.55 seconds (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (metbios-ssn) open (UNKNOWN) [192.168.50.101] 133 (domain) open (UNKNOWN) [192.168.50.101] 23 (tehnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (tehnet) open (UNKNOWN) [192.168.50.101] 23 (tehnet) open (UNKNOWN) [192.168.50.101] 24 (ftp) open (UNKNOWN) [192.168.50.101] 25 (ssh) open (UNKNOWN) [192.168.50.101] 25 (ssh) open (UNKNOWN) [192.168.50.101] 26 (irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:		
incorrect results at https://nmap.org/submit/. Nmap done: 1 Paddress (1 host up) scanned in 65.55 seconds Sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 134 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (http) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 24 (ssh) open (UNKNOWN) [19		•		
incorrect results at https://nmap.org/submit/. Nmap done: 1 Paddress (1 host up) scanned in 65.55 seconds Sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 134 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (http) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 24 (ssh) open (UNKNOWN) [19		_		
incorrect results at https://nmap.org/submit/. Nmap done: 1 Paddress (1 host up) scanned in 65.55 seconds Sudo nc -nvz 192.168.50.101 1-1024 (UNKNOWN) [192.168.50.101] 514 (shell) open (UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 134 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 130 (http) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 24 (ssh) open (UNKNOWN) [19		Service detection performed. Please report any		
Nmap done: 1 Paddress (1 host up) scanned in 65.55 seconds				
Seconds		;		
Sudo nc -nvz 192.168.50.101 1-1024				
(UNKNOWN) [192.168.50.101] 513 (login) open (UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 repbind 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)	sudo nc -nvz 192.168.50.101 1-1024			
(UNKNOWN) [192.168.50.101] 512 (exec) open (UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 131 (sunrpc) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 21 (sth) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 24 (ssh) open (UNKNOWN) [192.168.50.101] 25 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 23 (ssh) open (UNKNOWN) [192.168.50.101] 24 (ssh) open (UNKNOWN) [192.168.50.101] 25 (ssh) open (UNKNOWN) [192.168.50.101] 26 (ssh) ope				
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 111 (sunrpc) open (UNKNOWN) [192.168.50.101] 30 (http) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH 4.7p1 Debian-8ubuntu1 Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open helnet Samba smbd 3.X - 4.X (workgroup: WORKGROUP)		, , , , , , , , , , , , , , , , , , , ,		
open (UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 111 (sunrpc) open (UNKNOWN) [192.168.50.101] 35 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH, 4.7p1 Debian-8ubuntu1 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 nethios-ssn Smtpd 53/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)		, , , , , , ,		
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.50.101] 111 (sunrpc) open (UNKNOWN) [192.168.50.101] 38 (http) open (UNKNOWN) [192.168.50.101] 33 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 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)				
open (UNKNOWN) [192.168.50.101] 111 (sunrpc) open (UNKNOWN) [192.168.50.101] 80 (http) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SH-2.0-OpenSSH _4.7p1 Debian-8ubuntu1 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 smtp Postfix smtpd 53/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 enetbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)				
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open (UNKNOWN) [192.168.50.101] 80 (http) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)				
(UNKNOWN) [192.168.50.101] 80 (http) open (UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 22 (smtp) open (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 rebbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)		-		
(UNKNOWN) [192.168.50.101] 53 (domain) open (UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 21 (ftp) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)				
(UNKNOWN) [192.168.50.101] 25 (smtp) open (UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 21 (ftp) open (UNKNOWN) [192.168.50.101] 21 (ftp) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)		, , , , , , , , , , , , , , , , , , , ,		
(UNKNOWN) [192.168.50.101] 23 (telnet) open (UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 recbind 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)				
(UNKNOWN) [192.168.50.101] 22 (ssh) open (UNKNOWN) [192.168.50.101] 21 (ftp) open sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 recbind 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)		, , , , , , , , , , , , , , , , , , , ,		
(UNKNOWN) [192.168.50.101] 21 (ftp) open sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 recbind 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)				
sudo nc -nv 192.168.50.101 22 (UNKNOWN) [192.168.50.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01-13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 repoind 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)				
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 sudo nmap -sV 192.168.50.101 Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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 recbind 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)	sudo nc -nv 192.168.50.101 22			
Starting Nmap 7.94 (https://nmap.org) at 2024-01- 13 12:44 EST Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)				
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)	sudo nmap -sV 192.168.50.101	Starting Nmap 7.94 (https://nmap.org) at 2024-01-		
undergoing ARP Ping Scan Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)		13 12:44 EST		
Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)		Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1		
0.00% done Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)		undergoing ARP Ping Scan		
Nmap scan report for 192.168.50.101 Host is up (0.000075s 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)		Parallel DNS resolution of 1 host. Timing: About		
Host is up (0.000075s 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)		0.00% done		
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)		Nmap scan report for 192.168.50.101		
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)		Host is up (0.000075s latency).		
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)		Not shown: 977 closed tcp ports (reset)		
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)		PORT STATE SERVICE VERSION		
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)		21/tcp open ftp vsftpd 2.3.4		
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)		22/tcp open ssh OpenSSH 4.7p1 Debian		
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)		8ubuntu1 (protocol 2.0)		
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)		23/tcp open telnet Linux telnetd		
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)		25/tcp open smtp Postfix smtpd		
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)		53/tcp open domain ISC BIND 9.4.2		
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)		80/tcp open http Apache httpd 2.2.8 ((Ubuntu)		
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)		DAV/2)		
(workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)		111/tcp open rpcbind 2 (RPC #100000)		
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)		139/tcp open netbios-ssn Samba smbd 3.X - 4.X		
(workgroup: WORKGROUP)		(workgroup: WORKGROUP)		
		445/tcp open netbios-ssn Samba smbd 3.X - 4.X		
E13/ton anon avec mother rehighered		(workgroup: WORKGROUP)		
S12/tcp Open exec		512/tcp open exec netkit-rsh rexecd		
513/tcp open login?		513/tcp open login?		
514/tcp open shell Netkit rshd		514/tcp open shell Netkit rshd		
1099/tcp open java-rmi GNU Classpath grmiregistry		1099/tcp open java-rmi GNU Classpath grmiregistry		
1524/tcp open bindshell Metasploitable root shell		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: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC) 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 65.42 seconds -mtu=512 Starting Nmap 7.94 (https://nmap.org) at 2024-01sudo nmap 192.168.50.101 13 12:46 EST Nmap scan report for 192.168.50.101 Host is up (0.000084s 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 MAC Address: 08:00:27:84:48:BA (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds