FACULDADE DE TECNOLOGIA SENAC GOIÁS

Projeto Integrador – Fundamentos de Redes de Computadores

Professor: Fernando Tsukahara

Alunos: Lúcio Torres, Nayara Lopes, Marciano Romeu e Silvanne Marinho

Relatório – Nmap

O Nmap é uma ferramenta para a exploração de informações das redes e tem como sua principal função escanear portas. Essas portas são fornecidas por meio de tabelas, contendo seu número e protocolo, estado e tipo de serviço, além de inúmeras outras informações que podem ser requisitadas de acordo com os objetivos do usuário. Elas podem ser classificadas em seis estados: aberto (*open*), fechado (*closed*), filtrado (*filtered*), não-filtrado (*unfiltered*), *open*|*filtered*, ou *closed*|*filtered.*

Para o levantamento dos dados da rede, foi instalado, inicialmente, o Nmap com os comandos para o acesso do administrador, usando o sudo su: ***apt-get install nmap***.

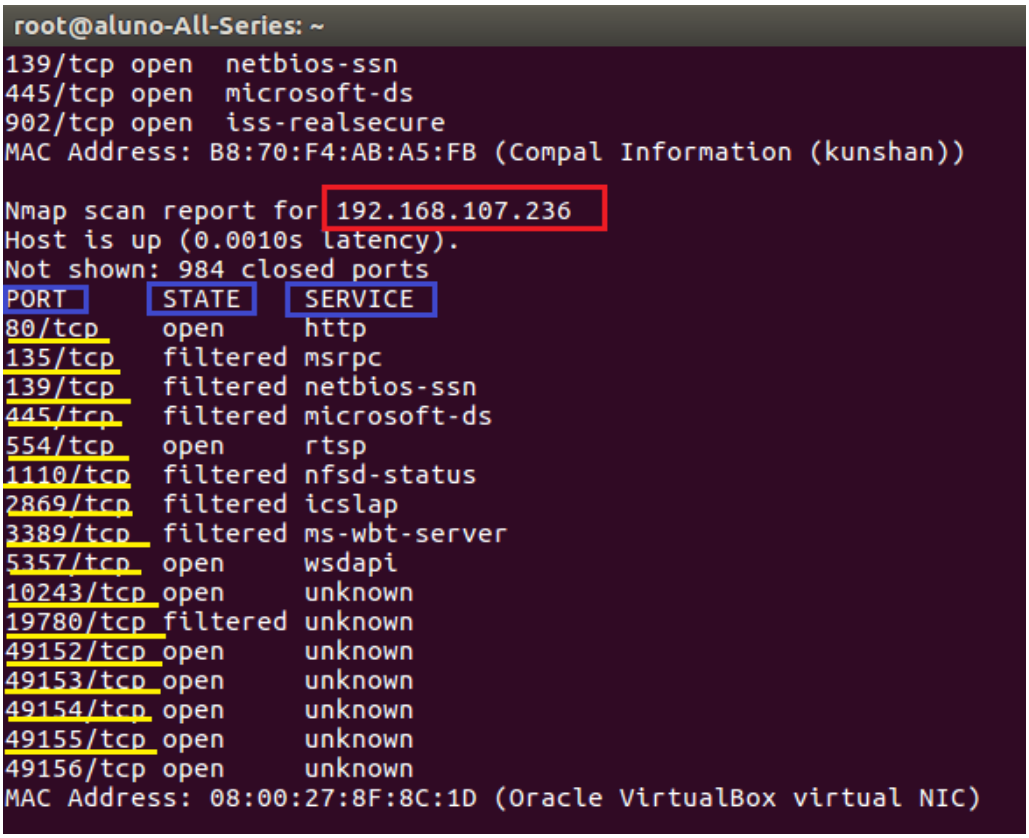

Figura 1. Print screen do terminal do Ubuntu: rede cabeada.

Após instalado, foi verificado o endereço de rede e utilizado o comando: ***nmap 192.168.107.0/24***, que escaneia todas as portas da rede, abertas ou não. Quando se escaneia todas as portas, esse processo pode demorar, como no caso, foram dois minutos e quarentas segundos. Dentro do laboratório onde foi rodado o arquivo, foram encontrados os seguinte Ips:

- 192.168.107.14 - 6 portas/tcp abertas de diferentes servidores.
- 192.168.107.18 - 6 portas/tcp abertas de diferentes servidores.
- 192.168.107.20 - 5 portas/tcp abertas de diferentes servidores.
- 192.168.107.29 - 5 portas/tcp abertas de diferentes servidores.
- 192.168.107.37 - 1 porta/tcp fechada servidor domain.
- 192.168.107.43 - 4 portas/tcp abertas de diferentes servidores.
- 192.168.107.239 - 1 porta/tcp abertado servidor.

Na imagem acima (Figura 1), podemos ver um exemplo. O IP 192.168.107.236, com as seguintes portas: 80/tcp, 554/tcp, 5357/tcp, 10243/tcp, 49152/tcp, 49153/tcp, 49155/tcp e 49156/tcp. Essas portas estavam abertas, aceitando conexões e envio de dados. As portas 135/tcp, 139/tcp, 445/tcp, 1110/tcp, 2869/tcp, 3389/tcp e 19780/tcp estavam filtradas, isso significa que o Nmap não consegue determinar se elas estão abertas, porque uma filtragem de pacotes impede que as sondagens alcancem as portas.

Cada porta apresenta uma função, definida pelo serviço indicado no escaneamento. A porta 80/tcp está diretamente ligada à transferência de hipertexto, para transferir páginas World Wide Web; a porta 554/tcp se aplica ao serviço de streaming em tempo real; e a porta 5357/tcp é usada para descobertas de rede.

A porta 135/tcp se refere a um serviço de localização; a porta 139/tcp está ligada ao serviço de sessão NetBIOS; a porta 445/tcp é um serviço de diretório da Microsoft; a porta 1110/tcp serve para coletar informações de status de um cluster; a porta 2869/tcp pode dizer respeito ao proxy interno feito para o Firewall de Conexão com a Internet e para o Compartilhamento de Conexão da Internet da

Microsoft; e a porta 3389/tcp funciona para o servidor da microsoft para o Windows-Based Terminal.

As portas 10243/tcp, 19780/tcp, 49152/tcp, 49153/tcp, 49155/tcp, 49156/tcp apontam seus serviços como desconhecidos.

No IP 192.168.107.236 foram escaneadas 1000 portas, 984 fechadas, essas estavam acessíveis (recebem e respondem pacotes de sondagens do Nmap), porém não é possível visualizar nenhuma aplicação rodando nelas.

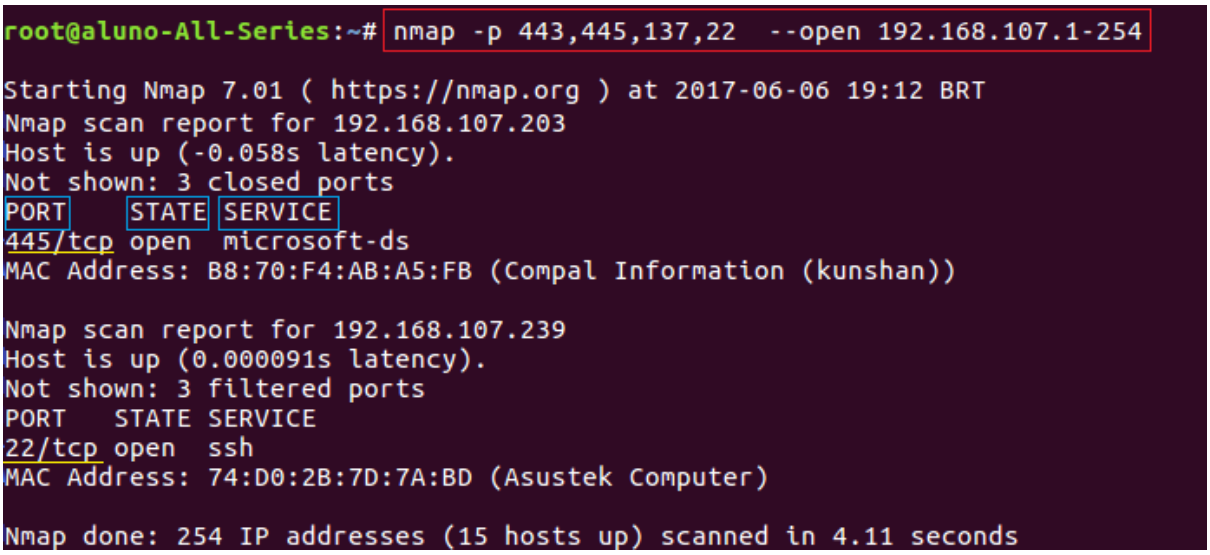

Figura 2: Print screen do terminal do Ubuntu: rede cabeada.

Na Figura 2, a partir da entrada “nmap -p 445,445,137,22 --open 192.168.107.1-254”, foram analisadas somente as portas especificadas (443, 445, 137 e 22) e abertas, delimitadas pelas opções “-p <faixa de portas>” e “--open”, em uma seleção de hosts da rede na qual se encontrava a máquina (1-254). Dentre os 254 endereços de IP escaneados, estando 15 hosts ativos. Foram, então, selecionadas duas das portas abertas como exemplo.

No IP 192.168.107.203, foram encontradas três portas fechadas, não exibidas, e apenas uma porta aberta, a 445/tcp. A porta 445/tcp, cujo servidor é o 'microsoft-ds', é usada para o compartilhamento de arquivos em uma rede e é um serviço implementado para as versões mais recentes do Windows.

Já para o IP 192.168.107.239, foram encontradas três portas filtradas e uma porta aberta, 22/tcp, de servidor 'ssh' (Secure Shell). Trata-se de uma porta utilizada para logins seguros e remotos, redirecionamento de portas e transferência de arquivos.

Para o escaneamento das portas nas redes Wi-Fi (Figura 3), cujo endereço é 192.168.40.0/21, foram realizados oito escaneamentos, dos

seguintes IPs: 192.168.40.0/24, 192.168.41.0/24, 192.168.42.0/24, 192.168.43.0/24, 192.168.44.0/24, 192.168.45.0/24, 192.168.46.0/24 e 192.168.47.0/24.

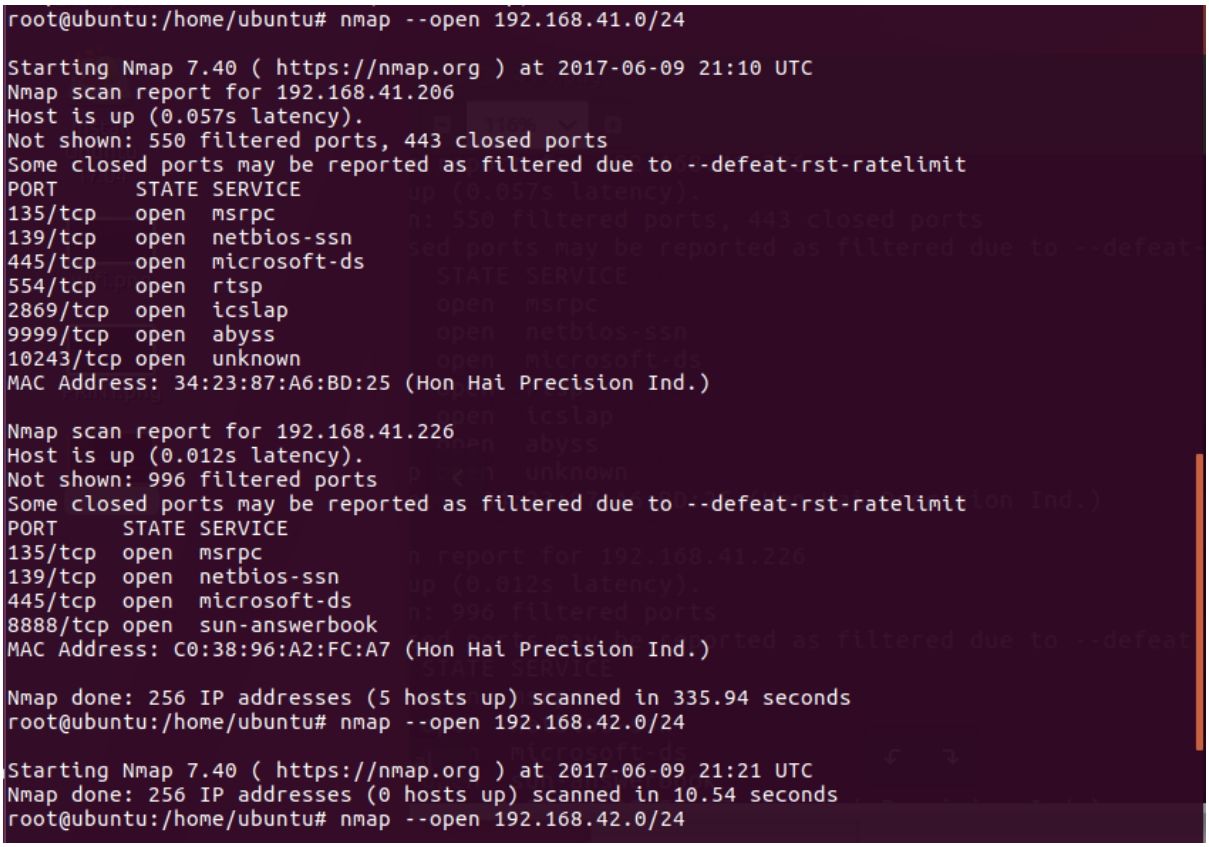

Imagem 3. Print screen do terminal do Ubuntu: rede wi-fi.

A partir do comando "nmap -O --open <IP/24>", foram identificadas 40 diferentes portas abertas, todas elas de protocolo tcp, algumas identificáveis pelo seu serviço (32) e outras desconhecidas (8). São elas:

- 22/tcp - ssh (Secure Shell): porta utilizada para logins seguros e remotos, redirecionamento de portas e transferência de arquivos;
- 23/tcp - telnet: comunicação de texto sem encriptação;
- 25/tcp - smtp (Simple Mail Transfer Protocol): usada para roteamento de e-mail entre servidores;
- 53/tcp - domain: transferências de zona DNS, sincronização e transferência de configurações;
- 80/tcp - http: transferência de hipertexto, para transferir páginas World Wide Web;
- 135/tcp - msrpc: serviço de localização;

- 139/tcp - netbios-ssn: serviço de sessão do NetBIOS;
- 211/tcp - 914c-g: Texas Instruments 914C/G Terminal;
- 311/tcp - asip-webadmin: ferramenta de gerenciamento de workgroup da Apple;
- 443/tcp - https (Hyper Text Transfer Protocol Secure): transmissão segura de hipertexto;
- 445/tcp - microsoft-ds: serviço de diretório da Microsoft;
- 554/tcp - rtsp (Real Time Streaming Protocol): streaming em tempo real;
- 631/tcp - ipp (Internet Printing Protocol): impressão na internet;
- 902/tcp - iss-realsecure: ISS RealSecure Sensor;
- 912/tcp - apex-mesh: APEX relay-relay service;
- 1688/tcp - nsjtp-data: está ligado aos dados do Network ScanJet Transfer Protocol;
- 1801/tcp - msmq (Microsoft Message Queuing): enfileiramento de mensagens;
- 2103/tcp - zephyr-clt: Zephyr serv-hm connection;
- 2105/tcp - eklogin: Kerberos (v4) encrypted rlogin;
- 2107/tcp - msmq-mgmt: enfileiramento de mensagens;
- 2869/tcp - icslap: proxy interno feito para o Firewall de Conexão com a Internet e para o Compartilhamento de Conexão da Internet da Microsoft;
- 2968/tcp - enpp: Rtvscan (Symantec Antivirus) para servidores Novell NetWare;
- 3306/tcp - mysql: Miralix SMS Client Connector;
- 6646/tcp - unknown: Cisco Intercloud Fabric tunnel e jogos que usem essa porta;
- 5357/tcp - wsdapi: usado pelo Microsoft Network Discovery;
- 5432/tcp - postgresql: sistema de bando de dados PostgreSQL;
- 5800/tcp - vnc-http (Virtual Network Computing): protocolo de desktop remoto VNC para uso em HTTP;
- 5900/tcp - vnc: protocolo de desktop remoto VNC;
- 7676/tcp - imqbrokerd: iMQ Broker Rendezvous;
- 8080/tcp - http-proxy: Jakarta Tomcat;
- 8081/tcp - blackice-icecap: console de usuário ICECap;
- 8082/tcp - blackice-alerts: alertas BlackIce;

- 8090/tcp - unknown: alternativa HTTP para a porta 8080;
- 8888/tcp - sun-answerbook: servidor Sun Answerbook HTTP;
- 9999/tcp - abyss: interface remota de gerenciamento do servidor web Abyss;
- 10243/tcp - unknown: Windows Media Player Network Sharing Service;
- 49152/tcp - unknown: apliações que utilizam portas dinâmicas/randômicas/configuráveis;
- 49153/tcp - unknown: gerador de análises para reconhecer idiomas;
- 49154/tcp - unknown: Xsan Filesystem Access;
- 49157/tcp - unknown;
- 49158/tcp - unknown;
- 62078/tcp - iphone-sync: usado pelo iPhone durante a sincronização.