Laboratório – Detecção de ameaças e vulnerabilidades

1. Objetivos

Use Nmap, um scanner de porta e ferramenta de mapeamento de rede, para detectar ameaças e vulnerabilidades em um sistema.

1. Histórico/Cenário

O Network Mapper, ou Nmap, é um utilitário de código aberto usado para descoberta de rede e auditoria de segurança. Os administradores também usam o Nmap para monitorar hosts ou gerenciar agendamentos de atualizações de serviços. O Nmap determina quais hosts estão disponíveis em uma rede, quais serviços, sistemas operacionais e filtros de pacotes ou firewalls estão sendo executados.

1. Recursos necessários

* PC com Ubuntu 16.0.4 LTS instalado em uma máquina virtual. Você pode usar a VM dos laboratórios concluídos no capítulo 2.
  1. Abra uma janela de terminal no Ubuntu.
     1. Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Usuário: **cisco**

Senha: **password**



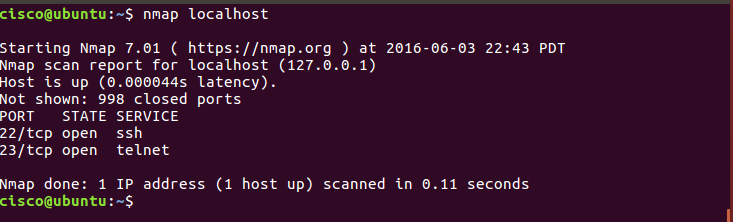
* + 1. Clique no ícone de **terminal** para abrir um terminal.



* 1. Execute o Nmap.

No prompt de comando, digite o seguinte comando para executar uma varredura básica nesse sistema Ubuntu:

cisco@ubuntu:~$ **nmap localhost**



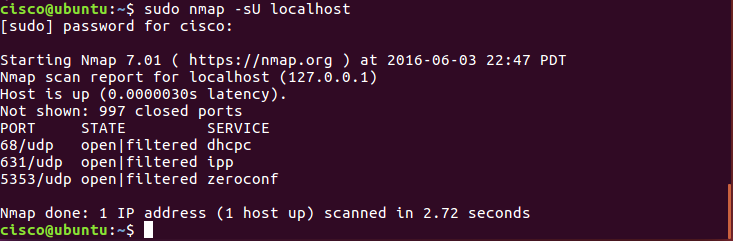
Os resultados são uma varredura das primeiras 1024 portas TCP.

Quais portas TCP estão abertas?

22/tcp – ssh e porta 23/tcp telnet

* 1. Use privilégios administrativos com Nmap.
     1. Digite o seguinte comando no terminal para varrer as portas UDP do computador (lembre-se o Ubuntu faz distinção entre maiúsculas e minúsculas) e insira a senha **password** quando solicitado:

cisco@ubuntu:~$ **sudo nmap –sU localhost**

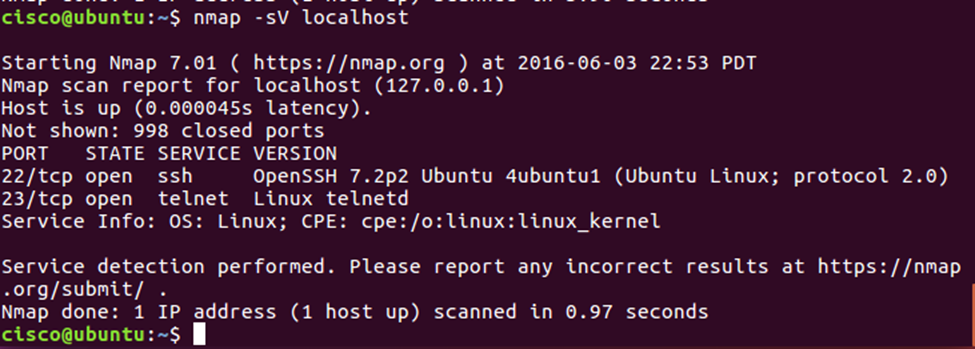


Quais portas UDP estão abertas?

Portas 68, 631 e 5353

* + 1. Digite o seguinte comando no terminal:

cisco@ubuntu:~$ **nmap –sV localhost**

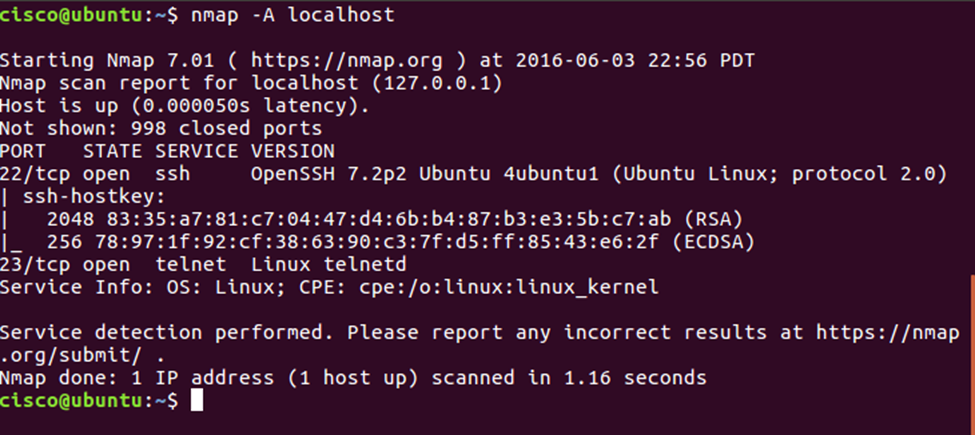


Usar a opção **–sV** com o comando **nmap** executa uma detecção de versão que pode ser usada para pesquisar vulnerabilidades.

* 1. Capturar chaves SSH.

Digite o seguinte comando no terminal para iniciar uma varredura de script:

cisco@ubuntu:~$ **nmap –A localhost**



Você capturou as chaves SSH para o sistema host. O comando executa um conjunto de scripts incorporados no Nmap para testar vulnerabilidades específicas.

**Referências**

Nmap: <https://nmap.org/>