**Segurança de Redes**

Prof. Harley Rios

Trabalhando com o NMAP (Linux) – Prática Valor:

Aluno:

*O* ***Nmap*** *(“Network Mapper”) é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características. Embora o Nmap seja normalmente utilizado para auditorias de segurança, muitos administradores de sistemas e rede consideram-no útil para tarefas rotineiras tais como inventário de rede, gerenciamento de serviços de atualização agendados, e monitoramento de host ou disponibilidade de serviço. O* ***ZeNmap*** *(*<http://nmap.org/zenmap/>*) é uma GUI (interface gráfica) para o programa Nmap, que facilita seu uso por usuários iniciantes.* ***Fonte****:* <http://nmap.org/man/pt_BR/>

Instale o nmap (apt-get install nmap) na máquina de Internet , e execute as seguintes verificações:

**Verifique quais serviços estão ativos em seu host.**

1. Todas as portas TCP na sua máquina
2. Todas as portas TCP em algum host alvo na rede (host, roteador,etc)
3. Todas as portas UDP no seu computador
4. Todas as portas UDP em um HOST alvo da rede Interna
5. Testar a portasTCP 80 em seu host.
6. Testar as portas da faixa de endereços de sua rede de computadores.
7. Todas as portas TCP no HOST da rede Interna usando a porta **de** origem 80
8. Use o parâmetro –sS e faça uma varredura nas portas de 1 a 150 de sua rede
9. Testar a porta UDP 53 em seu host.
10. Todas as portas UDP em algum host alvo da rede Interna usando a porta de origem 53
11. Descubra todos hosts ativos na rede.
12. Teste porta UDP 53 no host [www.globo.com](http://www.globo.com/)
13. Descubra o sistema operacional utilizado em um host alvo
14. Descobrindo se a porta 161 está aberta nos host 172.17.12.0 até 172.17.12.255 utilizando um scan UDP (troque o IP por um IP de sua faixa de rede).
15. Verifique se a porta 80 de algum site à sua escolha está ativa.
16. Verifique também no mesmo site, como está a porta 22.
17. Verifique também detalhes de informação sobre um host alvo (ou site), utilizando a opção nmap –A.
18. Instale o pacote “traceroute” e logo depois execute o comando “traceroute [www.google.com.br](http://www.google.com.br)”. Descubra o endereço do roteador da rede, e logo depois verifique as portas TCP abertas neste roteador.

**Nmap com Interface Gráfica**

1. Com a interface gráfica (**sudo zenmap**), rode testes mais simples em toda a rede, como por exemplo o “ping scan”. Quantas e quais máquinas foram identificadas na rede (painel da esquerda)? Salve o gráfico da topologia observada (dica: na aba topologia, clique no botão “olho de peixe” pra facilitar a visualização)

OBS.: o comando abaixo foi gerado automaticamente pelo zenmap:

**sudo nmap** -sP -PE -PA21,23,80,3389 **192.168.0.\***

1. Ainda, com a interface gráfica (**sudo zenmap**), rode testes mais completos **em um alvo específico** (senão fica muito demorado caso rode pra toda a rede). Dentre outros, testem o “intense scan” para ver quais informações é possível obter de uma máquina em rede. Observe na aba “Portas/Máquinas” as portas dos programas comunicantes de nosso servidor. Salve novamente o gráfico da topologia observada: o que mudou?

OBS.: o comando abaixo foi gerado automaticamente pelo zenmap:

**sudo nmap** -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 **192.168.0.1**

* No ZeNmap, o painel da esquerda exibe os hosts e serviços encontrados pelo Nmap, durante o escaneamento da rede do Laboratório. Alguns deles, caso mal configurados, poderiam ser utilizados como porta de invasão do sistema? Quais?
* Pense em exemplos de **situações em que vocês utilizariam** o nmap caso fossem administradores de rede de uma grande empresa ou universidade (onde e quando esta ferramenta seria útil pra você, como profissional de segurança).

Salve o resultado da consulta num arquivo texto e envie para o e-mail harley@iftm.edu.br