LABORATÓRIO XII

PORTSCAN & FOOTPRINTING

Redes de Computadores – Da Teoria à Prática com Netkit

Laboratório XII – Portscan & Footprinting

Objetivos do laboratório

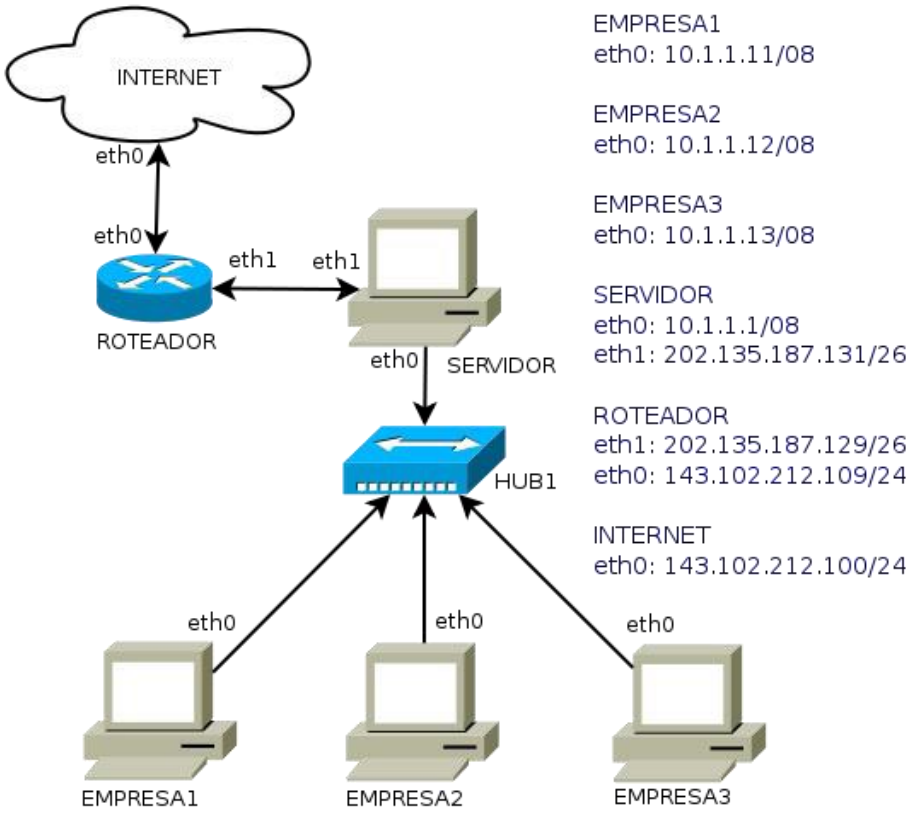
- Conhecer técnicas de footprinting
- Aprender a realizar portscans
- Relacionar portscans com firewalls

Cenário sendo reproduzido

A figura abaixo representa a topologia de rede sendo estudada, sendo a mesma que foi utilizada no laboratório de firewall, representando a infraestrutura de redes da empresa Cosmo Books.

Para o compartilhamento da internet, foi utilizado um servidor montado numa velha máquina do proprietário, um K6-II 500 MHz com 64 MB de RAM, o qual denominamos SERVIDOR. Esta máquina é ligada à internet pelo provedor Fasty. Os computadores são ligados em rede por um hub de 8 portas de 100Mbps e cabos categoria 5, devidamente dimensionados. Os possíveis usuários são **joaquim, manuel**, **maria** e **comprador.**

Em nosso laboratório virtual, o provedor é representado pelo "ROTEADOR" e os números de IPs são mostrados. Ao iniciar o laboratório virtual, SERVIDOR e INTERNET se comunicam à vontade.



Conhecimentos de segurança que você irá adquirir

Diferente do ponto de vista do laboratório de firewall, agora estamos interessados em

ataques ativos e passivos que podem ser realizados em uma rede. Uma habilidade importante para um possível atacante é conhecer o alvo. Quanto mais informações o mesmo tiver melhor.

Para levantar estas informações, o atacante poderá realizar a coleta das informações disponíveis na rede de modo passivo através de observações, ou então, realizar pequenas pesquisas de informações.

Antes de continuar, é importante lembrar que você deve ter feito a instalação do software **Wireshark** que será utilizado neste lab, portanto use os comandos apt-get install wireshark (distribuições debian) ou urpmi wireshark (mandriva) para instalar este software, caso o mesmo não esteja instalado.

Devemos lembrar que, os comandos marcados com a tag [real] deverão ser executados no console real. Os demais comandos serão executados dentro das máquinas virtuais. Sempre que exigido a instrução pedirá uma máquina virtual específica.

Execução do laboratório

Importante: Antes de executar este lab, você desejará se preparar com os seguintes requisitos: Este lab requer diversas janelas. Use um ambiente de trabalho com vários espaços, preferencialmente 4 deles. Gnome, Kde, Xfce tem quatro espaços por padrão. Use um deles ou configure seu ambiente preferido para quatro espaços.

Sobre as pastas:
Em seu computador pessoal, o caminho ideal é /home/seu_nome/nklabs/
Se você está executando estas práticas em um laboratório restrito, utilize a pasta /tmp. (Lembrando que o conteúdo entre execuções será apagado ao finalizar a máquina).

1. [real] Salve o arquivo netkit_lab12.tar.gz na sua pasta de labs. (/pasta_dos_labs).

2. [real] Acesse a pasta nklabs a partir do terminal
```
[seu_nome@suamaquina ~]$ cd /pasta_dos_labs
```

3. [real] Use o comando:
```
[seu_nome@suamaquina ~]$ tar -xf netkit_lab12.tar.gz
```
Será criada a pasta lab12 dentro da sua pasta nklabs.

4. [real] Use o comando a seguir:
```
[seu_nome@suamaquina ~]$ lstart -d /pasta_dos_labs/lab12
```

As seis máquinas virtuais serão iniciadas com as interfaces de rede devidamente configuradas. A internet não está distribuída para os computadores da empresa e os serviços de rede ainda não estão inicializados.

5. [real] Organize suas janelas de modo a localizar qualquer uma delas rapidamente.É recomendável que você utilize duas áreas de trabalho, para deixar as janelas com certa largura, pois algumas linhas de saída dos comandos deste tutorial são longas.

6. O primeiro passo é colocar a rede em funcionamento. Faça os seguintes comandos para realizar o compartilhamento da internet, no SERVIDOR.
```
SERVIDOR:~$ echo 1 > /proc/sys/net/ipv4/ip_forward
SERVIDOR:~$ iptables –F
SERVIDOR:~$ iptables -F -t nat
SERVIDOR:~$ iptables -F -t mangle
SERVIDOR:~$ iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

7. Tente executar um ping de INTERNET para EMPRESA2.
```
INTERNET:~$ ping 10.1.1.12
```

   O resultado esperado é que a rede não pode ser alcançada. Lembre-se de interromper o ping com o comando Ctrl+C após algumas entradas.

8. Tente executar um ping à partir do SERVIDOR para INTERNET
```
SERVIDOR:~$ ping 143.102.212.100
```

   O resultado esperado é sucesso na comunicação

9. Tente fazer o mesmo da EMPRESA1 para a INTERNET
```
EMPRESA1:~$ ping 143.102.212.100
```

O resultado esperado é sucesso na comunicação.

Devemos lembrar que cada computador permite o acesso de 4 usuários, maria, joaquim, manuel e comprador. As senhas são 123mar, 123joa, 123man e 123com respectivamente.

10. Nos computadores EMPRESA1 acione os serviços de SSH, FTP, DNS, PROXY e HTTP com os seguintes comandos:
```
EMPRESA1:~$ cd /etc/init.d
EMPRESA1:~$ ./apache2 start
EMPRESA1:~$ ./squid start
EMPRESA1:~$ ./bind start
EMPRESA1:~$ ./proftpd start
EMPRESA1:~$ ./ssh start
```

11. Repita o procedimento anterior com os computadores EMPRESA2 e EMPRESA3.

12. Verifique os processos em execução no computador EMPRESA1 com o comando ps aux | more.
```
EMPRESA1:~$ ps aux | more
```

O comando more permite fazer pausas na saída do comando ps aux. O comando ps aux exibe uma lista de processos detalhada. Para avançar páginas sobre uma saída sendo exibida com more, utilize a barra de espaços.

13. No computador EMPRESA1, execute o seguinte comando e tome nota da saída.

```
EMPRESA1:~$ netstat -nap
```

Observe a saída atentamente.

14. Execute o comando a seguir no SERVIDOR para ativar a captura de pacotes. Atenção para não executá-lo duas vezes.
```
SERVIDOR:~$ tcpdump -i eth1 -w /hosthome/lab12.pcap &
```

Atenção ao & comercial no final do comando que irá permitir que o tcpdump execute em background. Ao executar o comando, será necessário pressionar ENTER uma vez mais para que o *"prompt de comando"* seja devolvido.

Devido a configuração da sua rede, por estar feito NAT, não há possibilidade de atingir os computadores atrás da sua rede. Será necessário fazer redirecionamento de portas para que eles possam ser acessíveis.

Antes de realizar o redirecionamento de portas propriamente dito no entanto, vamos verificar quais portas estão ativas no servidor, no momento, a partir da INTERNET.

15. No computador INTERNET, use o seguinte comando (atenção as maiúsculas, e o parametro é uma letra "Oh" maiúscula, não um dígito zero):
```
INTERNET:~$ nmap -sS -O 202.135.187.131
```

Este comando fará uma investigação das portas abertas no servidor. Atenção as portas abertas e informações retornadas pelo comando. Agora, vamos fazer os serviços dos computadores internos da rede funcionar.

16. Agora, redirecione a porta 1122 do SERVIDOR, para a porta 22 do computador EMPRESA1. (O comando deve ser digitado sem quebra de linhas):
```
SERVIDOR:~$ iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 1122 -j DNAT --to-dest 10.1.1.11:22
SERVIDOR:~$ iptables -A FORWARD -p tcp -i eth1 --dport 1122 -d 10.1.1.11 -j ACCEPT
```

17. Inicie o SSH no servidor de firewall com o seguinte comando:
```
SERVIDOR:~$ /etc/init.d/ssh start
```

18. Conecte por SSH, a partir do computador chamado INTERNET, no computador SERVIDOR com o seguinte comando:
```
INTERNET:~$ ssh joaquim@202.135.187.131
```

Ao pedir a senha, lembre-se que é **123joa**.

19. Verifique o conteúdo da pasta acessada com o comando ls:
```
joaquim@SERVIDOR:~$ ls
```

Deixamos um arquivo com o local especialmente para que você verifique que de fato está no computador SERVIDOR, mas o "prompt de comando" já era uma pista aceitável.

20. Para encerrar a conexão, use o comando **exit**:
```
joaquim@SERVIDOR:~$ exit
```

21. Conecte por SSH novamente, a partir do computador INTERNET, no computador SERVIDOR com o novo comando:
INTERNET:~$ ssh joaquim@202.135.187.131 -p 1122

Observe que agora, ao invés de acessar o conteúdo do computador SERVIDOR, está acessando o conteúdo do computador EMPRESA1, embora tenha usado o endereço do servidor.

22. Faça o redirecionamento das demais portas, usando as duas instruções do iptables, de acordo com a tabela a seguir. Atenção para não errar os ip's e portas.

Obviamente, toda a configuração deverá ser feita no SERVIDOR.

Serviço	Computador	IP de Destino	Porta de destino	Porta de Origem
FTP	EMPRESA1	10.1.1.11	21	1121
HTTP	EMPRESA1	10.1.1.11	80	1180
SSH	EMPRESA2	10.1.1.12	22	1222
FTP	EMPRESA2	10.1.1.12	21	1221
HTTP	EMPRESA2	10.1.1.12	80	1280
SSH	EMPRESA3	10.1.1.13	22	1322
FTP	EMPRESA3	10.1.1.13	21	1321
HTTP	EMPRESA3	10.1.1.13	80	1380

23. Ao terminar o redirecionamento, repita o port-scan realizado no passo **15**, com o seguinte comando modificado para escanear portas adicionais (não somente as primeiras 1024 que é o padrão).
INTERNET:~$ **nmap -p 1-1500 -sS -O 202.135.187.131**

Descobrir informações sobre serviços

Uma vez que sabemos as portas abertas, podemos descobrir informações interessantes, utilizando ferramentas simples.

24. Na máquina INTERNET, utilize o seguinte comando para descobrir a versão do SSH. Digite quit e tecle enter para finalizar a conexão.
INTERNET:~$ **telnet 202.135.187.131 22**

25. O comando a seguir traz um pouco mais de informações de depuração.
INTERNET:~$ **ssh -vN 202.135.187.131**

26. Conecte-se via telnet ao servidor apache na porta 1180 com o comando:
INTERNET:~$ **telnet 202.135.187.131 1180**

27. Use o seguinte comando HTTP para trazer informações sobre o servidor Apache. (Serão necessários dois toques na tecla ENTER). Observe que a saída pode incluir versão de PHP, de OpenSSL e de outros módulos

carregados no Apache.
```
HEAD / HTTP/1.0
```

28. Estude atenciosamente o pacote no wireshark. Para interromper sua captura, no computador SERVIDOR utilize o comando abaixo e em seguida, pressione Ctrl + C. Após isso o arquivo lab12.pcap estará na sua pasta de usuário.
```
SERVIDOR:~$ fg tcpdump
```

29. [real] Use o comando a seguir para encerrar a execução do laboratório:
```
[seu_nome@suamaquina ~]$ lhalt -d /pasta_dos_labs/lab12
```

30. [real] Use o comando a seguir para apagar os enormes arquivos.disk:
```
[seu_nome@suamaquina ~]$ lclean -d /pasta_dos_labs/lab12
```

Formule as teorias

Lembrando seus conhecimentos sobre NAT, Firewall e segurança.

1. Explique o funcionamento dos comandos de redirecionamento de portas.
2. Pesquise comandos interessantes para se utilizar com o iptables e outras opções de uso da ferramenta nmap.
3. Pesquise outras formas de levantar informações sobre o computador de uma possível vítima.
4. Pesquise possíveis configurações de firewall para bloquear port-scans. Porque elas não são muito efetivas? Quais as melhores formas de realizar essa proteção?
5. Pesquise sobre scanners de rede. Utilize o laboratório 4 com o zebra ativo e, se possível, tente usar o scanner neste laboratório.