LABORATÓRIO XVI
Detecção de Intrusão com SNORT

Redes de Computadores – Da Teoria à Prática com Netkit

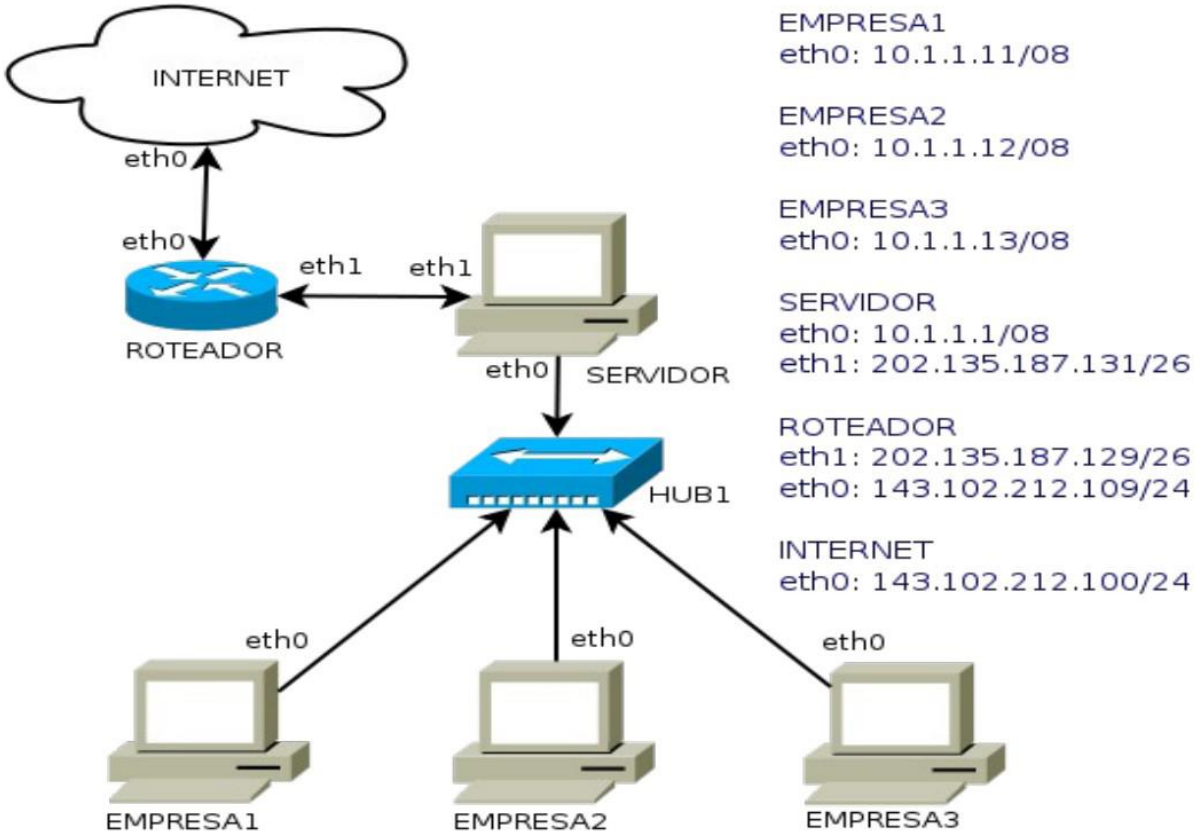
Laboratório XVI – Detecção de intrusão com snort

Objetivos do laboratório

- Compreender o funcionamento do Snort
- Aprender a configurar uma detector de intrusão

Cenário sendo reproduzido

O cenário proposto mostra uma rede já conhecida daqueles que fizeram os tutoriais anteriores. Este cenário foi escolhido pois representa satisfatoriamente um ambiente que tem a necessidade de usar .



Durante a seção **execução do laboratório**, evite fazer experimentos para que os resultados sejam equivalentes aos da saída. Situações de erros são intencionais.

Conhecimentos que você irá adquirir

Ao completar este lab você estará familiarizado com a ferramenta de detecção de intrusão **Snort**. Aprenderá que ela pode funcionar no modo sniffer, log de pacotes, ou no modo de

NIDS. Você verificará exemplos de ataques que podem ser visualizados no arquivo de alerta.

Antes de continuar, é importante 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.

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

1. [real] Salve o arquivo netkit_lab16.tar.gz na sua pasta de labs. (/home/seu_nome/nklabs).

2. [real] Use o comando:
```
[seu_nome@suamaquina ~]$ tar -xf netkit_lab16.tar.gz
```
Ele irá criar a pasta lab16 dentro da sua pasta nklabs.

3. [real] Use o comando a seguir:
```
[seu_nome@suamaquina ~]$ lstart -d /home/seu_nome/nklabs/lab16
```

4. No computador da EMPRESA3, inicie o serviço e FTP:
```
EMPRESA3:~# /etc/init.d/proftpd start
```

5. Acione o tcpdump na máquina EMPRESA1, criando o arquivo com o nome lab16logs.pcap.
```
EMPRESA1:~# tcpdump -i eth0 -s 1024 -w /hosthome/lab16_ftp.pcap
```

6. Faça a configuração do Firewall no servidor, redirecionando o serviço de FTP para o computador EMPRESA3. Se precisar de instruções para este procedimento, consulte o tutorial de Firewall.

7. A partir dos computadores EMPRESA2 e INTERNET, efetue um portscan do tipo xmas no SERVIDOR. Lembre-se de usar o IP externo e interno conforme aplicáveis. Compare as saídas.
```
EMPRESA2:~# nmap -sX -A -v 10.1.1.1
... aguarde concluir ....
INTERNET:~# nmap -sX -A -v 202.135.187.131
```

8. Efetue a conexão, através do computador INTERNET, no serviço de FTP do computador EMPRESA3. Verifique que o conteúdo acessado seja mesmo o do computador correto (empresa3) por meio da existência do arquivo local_EMPRESA3.txt na pasta do usuário. (Usuário joaquim, senha 123joa)

9. Utilize o comando quit para encerrar o ftp.
```
ftp> quit
```

As instruções a seguir solicitam que você faça alterações nos arquivos de configuração. Ao final deste tutorial, algumas instruções sobre edição de arquivo podem ser encontradas, de modo a tornar o processo de edição mais fácil.

10. A pasta /root do SERVIDOR contém dois modelos de arquivos de configuração: o padrão do debian e o arquivo preparado para o laboratório. Copie o arquivo do laboratório sobrescrevendo o arquivo snort.conf de /etc/snort/. Confirme se perguntar para sobrescrever.
```
SERVIDOR:~# cp /root/snort_lab.conf /etc/snort/snort.conf
```

    Abra o arquivo snort.conf no editor de sua preferência e estude brevemente seu conteúdo, observando atentamente cada uma das seções.

11. Altere o arquivo /etc/snort/snort.conf do computador SERVIDOR, para que o início seja modificado da seguinte forma (o restante do arquivo deverá permanecer igual:

```
#Configurações da rede
######################################
var HOME_NET any
var EXTERNAL_NET any
######################################
```

12. Inicie o snort com o seguinte comando:
```
SERVIDOR:~# snort –vde
```

    O comando snort simples, não carrega arquivo de regras e opera no modo sniffer, como o tcpdump. Várias informações aparecerão na tela, e a carga estará concluída quando aparecer:

```
 ,,_   -*> Snort! <*
o" )~ Version 2.7.0 (Build 35)
''''  By Martin Roesch & The Snort Team:
      http://www.snort.org/team.html
      (C) Copyright 1998-2007 Sourcefire Inc., et al.
```

13. Refaça os portscans e observe as informações detectadas.

14. Use Ctrl+C no snort para interrompê-lo. Se o snort não interromper por algum problema na virtualização, ou bug, será necessário um evento adicional para destravá-lo. Um ping de qualquer computador ao servidor deve resolver.
```
EMPRESA2:~# ping 10.1.1.1
```

15. Execute agora o snort no modo NIDS, com a seguinte instrução:
```
SERVIDOR:~# snort -A full -c /etc/snort/snort.conf
```

16. Refaça os portscans de ambas as fontes (EMPRESA2 e INTERNET).

17. Após concluir os portscans, verifique os arquivos de log da pasta /var/log/snort.
```
SERVIDOR:~# cat /var/log/snort/alert
```

18. Faça o ataque man in the middle utilizando o Ethercap (tutorial 11), sendo o atacante o computador EMPRESA2, e as vítimas o SERVIDOR e o computador EMPRESA1.

19. Interrompa novamente o snort com um Ctrl + C. Pode ser necessário novamente efetuar o ping:
EMPRESA2:~# **ping 10.1.1.1.**

20. Altere novamente o arquivo snort.conf, com o seguinte conteúdo inicial.

```
#Configurações da rede
#####################################
var HOME_NET 10.0.0.0/8
var EXTERNAL_NET !HOME_NET
#####################################
```

21. Reative o snort no modo NIDS e refaça os portscans. Observe o arquivo de alertas.

    Até este momento, você aprendeu a configurar o snort e a executá-lo. Toda vez que efetuar um portscan deverá encontrar algum tipo de alerta no arquivo alerts da pasta /var/log/snort/alerts:

22. Altere o arquivo /etc/snort/rules/local.rules adicionando as seguintes regras (cuidado com as áspas ao copiar e colar, certifique-se de não serem as áspas francesas):

```
alert tcp any any -> $HOME_NET 21 \
(content:"anonymous"; msg: "Login FTP (anonimo) invalido!";)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 \
(msg: "Login de FTP externo";)
```

23. Execute novamente o snort no modo IDS e verifique se as novas regras estão sendo aplicadas corretamente.

24. Encerre o laboratório com **halt** em cada máquina virtual. Caso precise repetir, é interessante apagar os arquivos .disk da pasta do laboratório ou da pasta tmp.

Exercícios

Lembrando a especificação da rede, com seus atuais conhecimentos de rede, tente explicar:

1. Pesquise sobre a opção inline do snort. Escreva uma regra para bloquear conexões ftp anônimas.
2. Além do snort, que outras ferramentas de detecção de intrusão poderiam ser utilizadas? Aborde os tipos HIDS, NIDS e NIPS.
3. Porque um honeypot não pode ser caracterizado como um IDS?

Instruções adicionais sobre o Linux

Ao trabalhar com arquivos de configuração, tome cuidado com as permissões dos arquivos. Você pode utilizar o "vim" ou então um editor de interface gráfica de sua preferência, como o gedit. Caso utilize este método, ao final, verifique as permissões do arquivo e sua propriedade. Utilize os seguintes comandos:

```
COMPUTADOR:~# ls -l /etc/destino/
COMPUTADOR:~# cp /hosthome/alice/arquivocopiado /etc/destino/arquivocopiado
COMPUTADOR:~# chown root:root /etc/destino/arquivocopiado
COMPUTADOR:~# chmod 644 /etc/destino/arquivocopiado
```

Como você viu no laboratório anterior, caso tenha feito, a permissão exigida pode ser diferente da permissão 644. Antes de editar o arquivo você pode verificar a permissão com o comando ls -l.

```
COMPUTADOR:~# cd /pasta/arquivo/desejado
COMPUTADOR:~# ls –l
-rwxr-xr--usuariodono grupousuario arquivodesejado
```

Os 10 caracteres iniciais representam a permissão. O primeiro traço indica se é um link simbólico ou diretório. Os próximos 3 grupos de 3 indicam as permissões de leitura, escrita e execução para o usuário proprietário, grupo proprietário ou demais usuários. Os números representam as permissões da seguinte forma:

Permissão	Binário	Decimal
---	000	0
--x	001	1
-w-	010	2
-wx	011	3
r--	100	4
r-x	101	5
Rw-	110	6
rwx	111	7

Caso tenha dificuldades com este processo, você ainda pode utilizar os editores **vim** ou **nano** direto na janela das máquinas virtuais. Para o **vim**, os comandos são:

```
COMPUTADOR:~# vim /etc/destino/arquivoeditado
Dentro do vi:
<i> para o modo de edição (inserção – tecla i minúscula)
<ESC> para sair do modo de edição (tecla ESC)
Fora do modo de edição, a tecla ":" inicia um commando
:q! <ENTER> Para sair sem salvar
:w <ENTER> Para escrever as alterações
:wq <ENTER> Salva e sai do vi
```