LABORATÓRIO XV
IPSEC

Redes de Computadores – Da Teoria à Prática com Netkit

Laboratório XV – IPSec

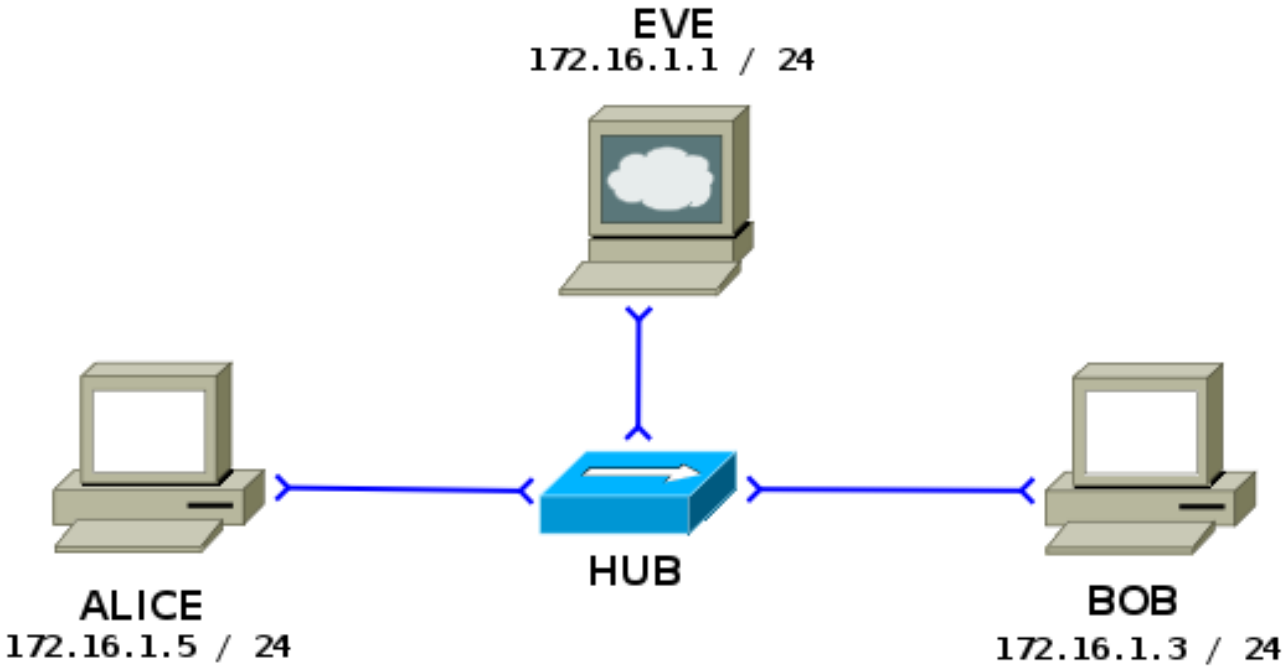
Objetivos do laboratório

- Compreender o funcionamento do IPSec
- Aprender a configurar uma rede básica com IPSec

Este laboratório requer as versões personalizadas do sistema de arquivos, bem como a versão do kernel disponível no site, não sendo garantido seu funcionamento na versão oficial do Netkit.

Cenário sendo reproduzido

O cenário proposto mostra uma rede local, com três computadores. Os computadores ALICE e BOB, e o computador EVE que deseja ouvir a comunicação entre os dois interlocutores. Com ajustes nos endereços, o experimento apresentado poderia ser aplicado em uma rede com IPs reais ao invés dos Ips privados, porém, eles foram utilizados para viabilizar a captura de informações pelo computador EVE.



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

Este tutorial foi baseado na documentação do Debian a respeito da ferramenta Racoon e adaptado para a forma de um experimento que utiliza o Netkit. Ao completar este lab você estará familiarizado com a configuração básica de um sistema de IPSEC, através da ferramenta racoon. Existem outras formas de implementar IPSec em uma rede, mas esta é uma das mais simples de obter sucesso e já é um modo consolidado há tempos no mundo Linux.

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_lab15.tar.gz na sua pasta de labs. (/home/seu_nome/nklabs).

2. [real] Use o comando:
```
[seu_nome@suamaquina ~]$ tar -xf netkit_lab15.tar.gz
```
Ele irá criar a pasta lab15 dentro da sua pasta nklabs.

3. [real] Use o comando a seguir:
```
[seu_nome@suamaquina ~]$ lstart -d /home/seu_nome/nklabs/lab15
```

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

5. Acione o tcpdump na máquina EVE, criando o arquivo com o nome lab15_ftp.pcap.
```
EVE:~# tcpdump -i eth0 -s 1024 -w /hosthome/lab15_ftp.pcap
```

6. Através da máquina ALICE, faça um FTP na máquina de BOB, com o seguinte comando:
```
ALICE:~# ftp 172.16.1.3
```

7. Ao conectar no ftp, utilize o usuário “maria” e a senha “123mar”

8. Utilize o comando ls para verificar o conteúdo do computador remoto.
```
ftp> ls
```

9. Utilize o comando quit para encerrar o ftp.

```
ftp> quit
```

Agora você precisará trabalhar com uma série de arquivos de configuração. Uma dica para trabalhar com os vários arquivos é editá-los em sua hosthome em pastas chamadas Alice e Bob e depois copiar através de um comando de cópia. Neste caso, não esqueça de adicionar uma quebra de linha extra no final da última linha do arquivo.

Caso utilize este método, ao final, verifique as permissões do arquivo e sua propriedade. Utilize os seguintes comandos:

```
ALICE:~# cp /hosthome/alice/arquivocopiado /etc/destino/arquivocopiado
ALICE:~# chown root:root/etc/destino/arquivocopiado
ALICE:~# chmod 644 /etc/destino/arquivocopiado
```

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

```
ALICE:~# 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
```

Antes de prosseguir com a edição dos arquivos de configuração, vamos identificar alguns requisitos, pois é muito fácil se confundir com os diversos IPs que vão aparecer.
Para montar o IPSEC, você deverá definir os IPs e endereços de redes virtuais, e montar as rotas, acrescentando um novo IP, o ip seguro, a cada adaptador de rede.

Vamos supor que você acrescente os seguintes IPs para Alice e Bob, chamando-os de IPSecs.
IPSEC Alice: 172.20.1.1/24
IPSEC Bob: 192.168.10.1/24

Vamos chamar os IPs originais de IPOs (de IP Original, criativos não?). Quando nos referimos aos endereços de rede dos IPSECs, vamos usar a abreviatura IPSNET. Chamaremos também os endereços da máquina sendo configurada de próprio, e o da máquina destino, de outro. Desta forma, montamos uma espécie de cola, ou esquema, para você seguir nos arquivos de configuração que serão descritos. Nos próximos passos esta colinha fará sentido.

```
remote IPSEC_Outro
sainfo remote IPSNET_Propria any IPSNET_Outro

spdadd IPSNET_Propria IPSNET_Outra any -P out ipsec
          esp/tunnel/IPO_Proprio-IPO_Outro/require;

spdadd IPSNET_Outra IPSNET_Propria any -P in ipsec
          esp/tunnel/IPO_Outro-IPO_Proprio/require;
```

Na configuração spdadd, se precisar de um mnemônico para decorar, a configuração OUT, o OUTRA aparece a direita, mais perto do out. Na linha “in”, o OUT está mais longe, e fica o propr”in”o mais próximo. É ruim, sabemos, mas esperamos que ajude você a se lembrar. É fácil errar essa configuração.

10. Altere o arquivo /etc/racoon/racoon.conf do computador da Alice, para que o mesmo tenha o seguinte conteúdo (não há margem esquerda ou linhas anteriores ou posteriores):

```
#Configuracao Racoon IPSEC - Alice
path pre_shared_key "/etc/racoon/psk.txt";

remote 172.16.1.3 { #endereço real do BOB
      exchange_mode main,aggressive;
      proposal {
            encryption_algorithm 3des;
            hash_algorithm sha1;
            authentication_method pre_shared_key;
            dh_group 2;
      }
}

# address IPSNET_Alice any address IPSNET_Bob
sainfo address 172.20.1.0/24 any address 192.168.10.0/24 any {
      pfs_group 2;
      lifetime time 1 hour ;
      encryption_algorithm 3des, blowfish 448, rijndael ;
      authentication_algorithm hmac_sha1, hmac_md5 ;
      compression_algorithm deflate ;
}
#Fim da Configuracao
```

11. Altere o arquivo /etc/racoon/psk.txt do computador da Alice, para que o mesmo tenha o seguinte conteúdo:

```
# Arquivo de chaves
172.16.1.3 0a1b2a3c4a5d6a7b8a90
# Fim do arquivo de chaves
```

12. Altere o arquivo /etc/ipsec-tools.conf do computador da Alice, para que o mesmo tenha o seguinte conteúdo. Pode desconsiderar os comentários:

```
flush;
spdflush;

#IPSNET_Alice - IPSNET_Bob esp/IPOAlice IPOBob/
spdadd 172.20.1.0/24 192.168.10.0/24 any -P out ipsec
       esp/tunnel/172.16.1.5-172.16.1.3/require;

#IPSNET_Bob - IPSNET_Alice esp/IPOBob IPOAlice/
spdadd 192.168.10.0/24 172.20.1.0/24 any -P in ipsec
       esp/tunnel/172.16.1.3-172.16.1.5/require;
```

Os três arquivos anteriores foram salvos para a Alice. Agora você fará arquivos similares, para o **Bob**. Basicamente, os IPs envolvidos serão modificados.

13. Altere o arquivo /etc/racoon/racoon.conf do computador do BOB, para que o mesmo tenha o seguinte conteúdo (não há margem esquerda ou linhas anteriores ou posteriores). Os IPs estão zerados para que você complete com os corretos:

```
#Configuracao Racoon IPSEC - Bob
path pre_shared_key "/etc/racoon/psk.txt";

remote 0.0.0.0 {
      exchange_mode main,aggressive;
      proposal {
            encryption_algorithm 3des;
            hash_algorithm sha1;
            authentication_method pre_shared_key;
            dh_group 2;
      }
}

sainfo 0.0.0.0/24 any address 0.0.0.0/24 any {
      pfs_group 2;
      lifetime time 1 hour ;
      encryption_algorithm 3des, blowfish 448, rijndael ;
      authentication_algorithm hmac_sha1, hmac_md5 ;
      compression_algorithm deflate ;
}
#Fim da Configuracao
```

14. Altere o arquivo /etc/racoon/psk.txt do computador do Bob, para que o mesmo tenha o seguinte conteúdo:

```
# Arquivo de chaves
172.16.1.5 0a1b2a3c4a5d6a7b8a90
# Fim do arquivo de chaves
```

15. Altere o arquivo /etc/ipsec-tools.conf do computador **do Bob** para que o mesmo tenha o seguinte conteúdo: Não esqueça de conferir os IPs

```
flush;
spdflush;

spdadd 192.168.10.0/24 172.20.1.0/24 any -P out ipsec
       esp/tunnel/172.16.1.3-172.16.1.5/require;

spdadd 172.20.1.0/24 192.168.10.0/24 any -P in ipsec
       esp/tunnel/172.16.1.5-172.16.1.3/require;
```

16. Nos computadores da Alice, execute os seguintes comandos para reinicializar a ferramenta racoon e o serviço de chaves:

```
ALICE:~# /etc/init.d/setkey restart
ALICE:~# /etc/init.d/racoon restart
```

Caso as instruções acima acusem parsing error do arquivo de configuração, consultar o arquivo /var/log/syslog do computador que mostrou o erro poderá fornecer uma pista sobre o que está errado.
Dica: compare o arquivo racoon.conf do Bob, com o racoon.conf da Alice.

17. Repita o passo anterior para o computador do Bob.

Até aqui, a ferramenta racoon deve estar em funcionamento. O próximo passo é garantir as rotas dos IP's para os túneis IPSec.

18. No computador EVE, interrompa a captura do tcpdump e faça uma cópia do arquivo, para não correr o risco de sobrescrevê-lo (sua quantidade de pacotes provavelmente diferirá da minha):

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture
size 1024 bytes
<pressione Ctrl+C>
120 packets captured
120 packets received by filter
0 packets dropped by kernel
EVE:~$ cp /hosthome/lab15_ftp.pcap /hosthome/lab15_ftp_desp.pcap
```

19. Ative novamente a captura de pacotes na máquina EVE, preferencialmente com um novo nome de arquivo. Faremos também os pacotes maiores:

```
EVE:~# tcpdump -i eth0 -s 4096 -w /hosthome/lab15_ipsec.pcap
```

20. Usando o pacote ip, acrescente um endereço ip na interface eth0 do computador da Alice, com a seguinte instrução:

```
ALICE:~# ip addr add 172.20.1.1/24 dev eth0
```

21. Acrescente agora uma rota para o novo IP:

```
ALICE:~# ip route add to 192.168.10.0/24 via 172.20.1.1 src 172.20.1.1
```

22. Faça o mesmo com o computador do Bob, novo IP e rota.

```
BOB:~# ip addr add 192.168.10.1/24 dev eth0
BOB:~# ip route add to 172.20.1.0/24 via 192.168.10.1 src 192.168.10.1
```

23. Verifique o funcionamento através de um ping, de Alice para Bob:

```
ALICE:~# ping 192.168.10.1
```

24. Caso o passo anterior não retorne saídas, revise os arquivos de configuração. É comum digitar endereços incorretos impedindo o funcionamento adequado. Ao alterar um arquivo de configuração o passo 16 precisará ser efetuado (reinicialização dos serviços setkey e racoon)

25. Repita a sequencia de comandos de ftp, utilizando o IPSec do Bob. (Passos 6, 7, 8 e 9).

26. Interrompa a captura de pacotes do computador EVE.

27. Observe, no wireshark, o conteúdo do arquivo lab15_ftp_desp.pcap e como

o conteúdo do ftp é legível.

28. Repita o processo para o arquivo lab15_ipsec.pcap (ou lab15_ftp se você esqueceu de trocar o comando).

29. 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. Outra ferramenta, baseada no KAME e no firewall shorewall, pode ser utilizada para montar redes baseadas em IPSec. Compare as vantagens e desvantagens de cada abordagem.
2. Pesquise brevemente e descreva o processo que seria utilizado para configurar IPSec através do shorewall e do patch Kame.
3. Descreva em linhas gerais a configuração de IPSec em IPv6.