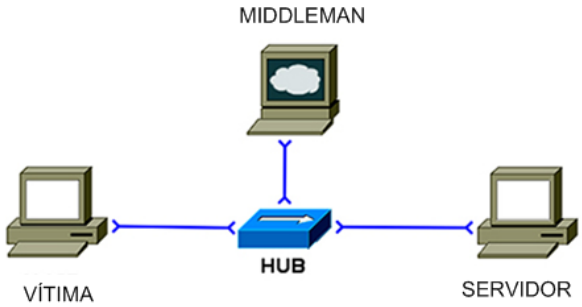

EXECUÇÃO DO LABORATÓRIO

1. [real] Salve o arquivo netkit_lab11.tar.gz na sua pasta de labs. (`/home/seu_nome/nklabs`).

2. [real] Acesse a pasta nklabs a partir do terminal.

3. [real] Use o comando:

```
[seu_nome@suamaquina ~]$ tar -xf netkit_lab11.tar.gz
```

Será criada a pasta lab11 dentro da sua pasta nklabs.

4. [real] Use o comando a seguir:

```
[seu_nome@suamaquina ~]$ lstart -d /home/seu_nome/nklabs/lab11
```

Serão iniciadas 03 máquinas virtuais, com os nomes SERVIDOR, VITIMA e MIDDLEMAN. As interfaces de rede já estão configuradas com os ips mostrados no diagrama.

5. Em cada uma das três máquinas, use o comando ip addr show dev eth0 e anote o endereço MAC da interface de rede (seu endereço mac poderá ser diferente do mostrado abaixo):

```
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
link/ether d6:e3:8e:e7:1c:e2 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.51/24 brd 192.168.1.255 scope global eth0
inet6 fe80::d4e3:8eff:fee7:1ce2/64 scope link
valid_lft forever preferred_lft forever
```

6. No computador SERVIDOR, use o comando a seguir para iniciar a captura de pacotes:

```
SERVIDOR@~# tcpdump -i eth0 -w /hosthome/lab11serv.pcap &
```

Atenção ao caractere “&” no final do comando que não pode ser esquecido. Este comando irá permitir que o tcpdump rode em background realizando as capturas.

7. Repita o passo acima para o computador VITIMA. O nome sugerido para o arquivo de pacote é lab11vitima.pcap.

8. Execute um ping entre servidor e vítima com o comando.

```
VITIMA@~# ping -c 1 servidor
```

9. Use o comando arp para conferir a tabela arp da vítima.

```
VITIMA@~# arp
```

A saída é:

```
Address HWtype HWaddress Flags Mask Iface
servidor.lazy.net ether d2:c7:a6:a7:14:d4 C eth0
```

10. Vá até o computador MIDDLEMAN. Inicie o programa ettercap com o seguinte comando:

```
MIDDLEMAN@~# ettercap –C
```

A flag -C iniciará uma interface de modo texto chamada “curses”. O “modo curses” é mais avançado que o modo texto utilizado, por exemplo, em labs como o zebra, pois fornece algum feedback visual, embora ainda estejamos trabalhando em modo texto. Você vai descobrir, dependendo da distribuição de Linux utilizada, que o mouse poderá ser utilizado.

Dica: *Numa máquina Linux com interface gráfica, é possível utilizar ettercap -G para ativar uma interface GTK*

Para navegar entre diferentes “janelas” curses, utilize a tecla <TAB>. As setas e tecla ENTER também apoiam na navegação. Cuidado, entretanto, com outras teclas, pois cada tecla pode ter um comando especial associado.

11. No menu file, procure a opção “Dump to File”.

12. Na caixa output file, preencha com o nome mitm.pcap e pressione <ENTER>.

13. Use tab se necessário, vá para o menu Sniff, e escolha a opção Unified Sniff.

14. Selecione a interface de rede eth0.

15. Selecione o menu Start e depois a opção Start Sniffing.

16. Use a combinação de teclas Ctrl+S para ativar a opção hosts → scan for hosts. Deverá aparecer a seguinte saída:

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts
2 hosts added to the hosts list
```

17. Use TAB para acessar o menu Hosts, e depois a opção Hosts list.

18. Selecione o computador com o ip 192.168.1.1 e pressione a tecla espaço. Aparecerá um menu de apoio com os comandos desejados.

19. Pressione ENTER para fechar o menu, e depois use a tecla 1 para que o computador SERVIDOR (192.168.1.1) vá para a lista TARGET1.

20. Adicione o computador VITIMA (192.168.1.2) para a lista de target2.

21. Com o mouse, clique no menu Targets e depois na opção Current targets.

22. Selecione o computador da vítima em target2 com as setas ou com o mouse e pressione a tecla espaço para ver as opções.

Veja que é possível adicionar os ips nesta lista manualmente. O ettercap se encarregaria de descobrir os macs para fazer as substituições posteriormente, mas você poderia acrescentar um ip inexistente.

23. Vá ao menu Mitm e ative a opção “ARP Poisoning...”. Veja que esta é uma das técnicas possíveis para o ataque de homem do meio.

24. Deixe a caixa parameters em branco e pressione ENTER.

25. O ataque será iniciado. Tecle s para que a janela de estatísticas apareça.

26. Execute um ping no servidor a partir da vítima com o comando:

```
VITIMA@~# ping -c 1 servidor
```

27. Use o comando arp para conferir a tabela arp da vítima.

```
VITIMA@~# arp
```

28. Use o comando arp para conferir a tabela arp do servidor.

```
SERVIDOR@~# arp
```

Aqui é importante observar a possível presença dos ips com macs duplicados na tabela ARP. Note caso isso não aconteça que de qualquer modo o endereço MAC referente ao ip destino na vítima foi modificado;

29. No ettercap, interrompa o ataque no menu Mitm, Stop Mitm attack(s).

Veja que é possível iniciar mais de um tipo de ataque simultaneamente. Agora iremos preparar um ataque um pouco mais sofisticado e será fechar o ettercap momentaneamente.

30. Use o menu Start, selecione a opção Stop Sniffing.

31. Use o menu Start e a opção Exit.

O próximo ataque será um ataque de filtragem, onde o conteúdo entre as máquinas será modificado enquanto passa pelo homem do meio.

32. Crie o arquivo /root/pftp_filter.src com o seguinte conteúdo:

```
#Modifica o nome do servidor FTP
if (tcp.src == 21 && search(DATA.data, “ProFTPD”)) {
replace(“ProFTPD”, “ProFTP Hacked!”);
}
```

33. Agora, compile este arquivo com o comando:

```
MIDDLEMAN@~# etterfilter /root/pftp_filter.src -o
/root/pftp_filter.fil
```

34. Ative o ettercap novamente, com o flag da interface curses.

```
MIDDLEMAN@~# ettercap -C
```

Nós iremos refazer a preparação do ataque homem do meio, atenção ao arquivo pcap que deverá ter outro nome para não ser sobrescrito.

35. No menu file, procure a opção “Dump to File”.

36. Na caixa output file, preencha com o nome mitm_filter.pcap e pressione <ENTER>.

37. Repita os passos 13 a 22.

38. Vá ao menu Filters e use a opção “Load a Filter...”

39. Localize o arquivo pftp_filter.fil e pressione ENTER para carregá-lo.

40. Vá ao menu Mitm e ative a opção “ARP Poisoning...”.

Vamos preparar rapidamente o servidor para acessar o serviço de FTP e ver o ataque funcionando.

41. No servidor, vamos iniciar o daemon ProFTPD:

```
SERVIDOR@~# /etc/init.d/proftpd start
```

42. Na vítima, vamos acessar o serviço de FTP:

```
VITIMA@~# ftp servidor
Connected to servidor.lazy.net.
220 ProFTP Hacked! 1.3.1 Server (Debian) [::ffff:192.168.1.1]
Name (servidor:root):
```

43. Pressione ENTER duas vezes, até poder entrar o comando quit para encerrar o ftp.

44. Use o comando abaixo para trazer o tcpdump para o primeiro plano no computador vítima:

```
VITIMA@~# fg tcpdump
```

45. Pressione Ctrl+C para interromper a captura.

46. Faça o mesmo com o tcpdump que está no computador SERVIDOR.

47. Copie os arquivos mitm.pcap e mitm_filter.pcap para a pasta /hosthome.

```
MIDDLEMAN@~# cp /root/*.pcap /hosthome;
```

48. [real] Use o comando a seguir para encerrar a execução do laboratório:

```
[seu_nome@suamaquina ~]$ lhalt -d /home/seu_nome/nklabs/lab11
```

49. [real] Use o comando a seguir para apagar os enormes arquivos.disk:

```
[seu_nome@suamaquina ~]$ lclean -d /home/seu_nome/nklabs/lab11
```

50. [real] Use o comando a seguir para apagar os enormes arquivos.disk restantes:

```
[seu_nome@suamaquina ~]$ rm /tmp/*.disk
```

51. [real] Estude a captura do tcpdump no wireshark. Você poderá usar a opção follow tcp stream para ver conteúdos inteiros.

Questões

1. Através da observação do conteúdo do wireshark, explique o funcionamento do ataque do homem do meio.

2. Explique a estratégia que você, como gerente da rede, pode tomar para detectar e combater este tipo de ataque em sua rede interna.

3. Que outros ataques poderiam ser conjugados com o ataque de homem do meio além da filtragem para modificação de dados? Explique brevemente dois deles!

Referência:

P. Gurgel, K. R. L. C. Branco, L. H. C. Branco, F. E. Barbosa, and M. M. Teixeira. Redes de Computadores Da teoria à prática com Netkit. Elsevier, 1ed, 2015.