wireshark

Introdução

- o Wireshark pode ser usado também pelo lado negro da força.
- Se você estiver em uma rede local, com micros ligados através de um hub ou através de uma rede wireless, outro usuário pode usá-lo para capturar todas as suas transmissões.

Introdução

- além de alguém de fora, existe a possibilidade de um dos seus próprios funcionários resolver começar a brincar de script kiddie, pregando peças nos outros e causando danos. Como vimos, isso não requer muita prática.
- Ao utilizar um hub-switch, o risco é um pouco menor, já que, por default, os pacotes são enviados apenas às portas corretas.

Introdução

- Entretanto, muitos sistemas são vulneráveis a ataques de ARP poisoning, sem falar dos ataques de MAC flooding, que permitem burlar a proteção

ARP poisoning

- No ARP poisoning, o micro do atacante envia pacotes com respostas forjadas para requisições ARP de outros micros da rede.
- O protocolo ARP é utilizado para descobrir os endereços MAC dos demais micros da rede, já que os switches não entendem endereços IP.

ARP poisoning

- Esses pacotes forjados fazem com que os outros micros passem a enviar seus pacotes para o micro do atacante, que é configurado para capturar as transmissões e retransmitir os pacotes originais para os destinatários corretos.
- A rede continua funcionando normalmente, mas agora o atacante tem chance de logar todo o tráfego, usando o Wireshark ou outro sniffer. Felizmente, o Wireshark também pode ser usado para perceber as anormalidades na rede e chegar até o espertinho.

MAC flooding

- Os ataques de MAC flooding, por sua vez, tem como alvo o switch da rede e trabalham dentro de um princípio bastante simples.
- O switch possui uma área limitada de memória para armazenar a tabela com os endereços MAC dos micros da rede, de forma que, ao receber um grande número de pacotes com endereços MAC forjados, a tabela é completamente preenchida com os endereços falsos, não deixando espaço para os verdadeiros.

MAC flooding

- Nessa situação, existem apenas duas opções: ou o switch simplesmente trava, derrubando a rede, ou abandona o uso da tabela de endereços e passa a trabalhar em modo failopen.
  - Os frames são simplesmente retransmitidos para todas as portas, da mesma forma que um hub burro, permitindo que o atacante capture todo o tráfego da rede (até que o switch seja reiniciado).

MAC flooding

- Uma das ferramentas mais usadas é o macof, um pequeno utilitário que faz parte da suíte dsniff (que roda sobre o Linux), cujo código fonte está disponível no:

  http://www.monkey.org/~dugsong/dsniff/

- O dsniff também pode ser encontrado nos repositórios de muitas distribuições, o que facilita a instalação. Nas distribuições derivadas do Debian, você pode instalá-lo via apt-get:

dsniff

- Instalação

  # apt-get install dsniff

- Uma vez que o dsniff foi instalado, usar o macof é bastante simples: basta especificar a interface de saída, usando a opção "-i", e especificar o número de pacotes forjados a serem enviados, usando a opção "-n", como em:

dsniff

- # macof -i eth0 -n 100000
- A maioria dos hub-switchs são capazes de armazenar entre 1000 e 8000 endereços MAC na memória, de forma que bombardeando o hub-switch com 100000 endereços MAC diferentes você consegue chavear qualquer aparelho vulnerável para modo failopen.

dsniff

- Basta lançar o Wireshark e passar a capturar todo o tráfego da rede.
- Note que, em alguns casos, rodar o comando vai fazer o switch travar, derrubando toda a rede até que você o reinicie manualmente, o que nos modelos mais simples é feito desconectando e reconectando o cabo de energia.

dsniff

- O dsniff inclui também um utilitário para ARP poisoning, o arpspoof.
- Ao usá-lo, você deve especificar a interface de rede local e também o endereço IP do host de destino dos pacotes que você deseja capturar.
- Especificando o endereço do gateway da rede (o uso mais comum), você pode capturar todos os pacotes destinados à Internet.

dsniff

- Para usá-lo, o primeiro passo é ativar o encaminhamento de pacotes na configuração do Kernel, o que é feito usando o comando abaixo:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

dsniff

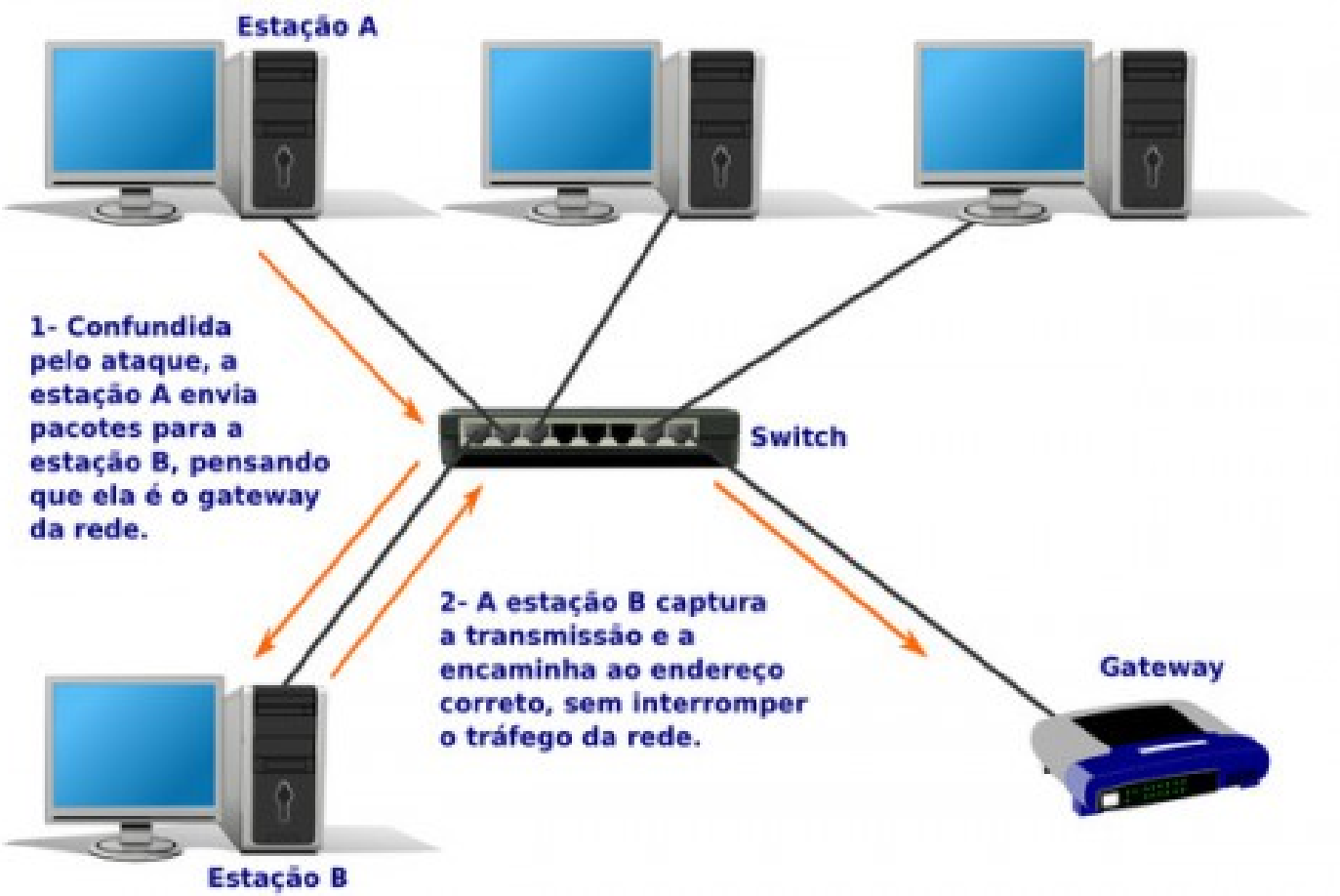
- A partir daí, você pode ativar o arpspoof, especificando o endereço de destino dos pacotes que deseja capturar, como em:

  # arpspoof -i eth0 192.168.1.1

- O arpspoof passará a enviar pacotes de broadcast para toda a rede, avisando todos os micros que o novo endereço MAC do "192.168.1.1" é o endereço da sua máquina.
- Isso fará com que ela passe a receber o tráfego destinado a ele, permitindo que você o capture usando o Wireshark.

dsniff

- O tráfego não poderia simplesmente ser desviado para a sua máquina, caso contrário, os pacotes deixariam de ir até o gateway da rede e os micros não conseguiriam mais acessar a Internet.
- Para evitar isso, o arpspoof reencaminha automaticamente todos os pacotes recebidos ao endereço correto (justamente por isso precisamos ativar o ip_forward no Kernel), fazendo com que, apesar do "desvio", o tráfego continue fluindo, como se nada estivesse acontecendo:


Estação A
1- Confundida pelo ataque, a estação A envia pacotes para a estação B, pensando que ela é o gateway da rede.
Switch
2- A estação B captura a transmissão e a encaminha ao endereço correto, sem interromper o tráfego da rede.
Gateway
Estação B

- Além de permitir escutar o tráfego, o ARP poisoning pode ser usado para alterar os dados transmitidos e também para impersonar outros hosts, de forma a obter senhas de acesso e outros dados.

- a estação A (cujos pacotes estão sendo capturados e retransmitidos pela estação B) deseja acessar o servidor A.
- Em vez de encaminhar a transmissão, como faria normalmente, a estação B responde como se fosse o servidor, pedindo o login e senha de acesso.
- O usuário na estação A, sem desconfiar do ataque, faz login e recebe de volta uma mensagem de "servidor em manutenção, espere 30 minutos e tente novamente" ou algo similar. De posse da senha, o atacante pode então se logar no servidor verdadeiro, usando a senha roubada.

- É possível detectar ataques de ARP poisoning usando o arpwatch (também disponível via apt-get).
- Ele monitora os endereços ARP usados pelas estações e gera um log com as mudanças (com a opção de enviar relatórios por e-mail), permitindo que você detecte anomalias.

- Outra possibilidade seria rodar o Wireshark na máquina que compartilha a conexão, assim você poderá observar os pacotes vindos de todas as máquinas da rede.
- Alguns modelos de switches gerenciáveis podem ser programados para direcionar todo o tráfego da rede para uma determinada porta, onde você poderia plugar um notebook para ter acesso a todo o tráfego.