Sniffers são programas que capturam pacotes de rede. Seu propósito legal é analisar tráfego de rede e identificar áreas potenciais de preocupação. Por exemplo, suponha que um segmento de sua rede esteja executando precariamente: a entrega de pacotes parece incrivelmente lenta ou as máquinas inexplicavelmente bloqueiam em uma inicialização de rede. Você utiliza um sniffer para determinar a causa precisa.

Sniffers variam significamente em funcionalidade e projeto. Alguns analisam somente um protocolo, enquanto outros podem analisar centenas. Como uma regra geral, sniffers mais modernos analisarão pelo menos os seguintes protocolos:

- Ethernet padrão
- TCP/IP
- IPX
- DECNet

Os sniffers capturam pacotes de rede colocando a interface de rede Ethernet por exemplo, em modo promíscuo.

Em redes locais os dados trafegam de uma máquina para outra ao longo do cabo em pequenas unidades chamadas frames. Esses frames são divididos em seções que carregam informações específicas. Os sniffers impõem um risco de segurança por causa da forma como os frames são transportados e entregues.

Cada estação de trabalho em uma rede local tem seu próprio endereço de hardware. Esse endereço identifica de maneira exclusiva essa máquina em relação a todos os outros na rede. Quando você envia uma mensagem através da rede local, seus pacotes são enviados para todas as máquinas disponíveis (broadcast).

Sob circunstâncias normais, todas as máquinas na rede podem “ouvir” esse tráfego, mas somente responderão aos dados endereçados especificamente a elas. (Em outras palavras, a estaçãoa de trabalho A não irá capturar dados destinados à estação de trabalho B. Em vez disso, a estação de trabalho A simplesmente ignora esses dados.)

Se uma interface de rede da estação de trabalho está em modo promíscuo, entretanto, ela pode capturar todos os pacotes e frames na rede. Uma estação de trabalho configurada dessa forma (e o software sobre ela) é um sniffer.

Os sniffers representam um alto nível de risco, porque:

- Os sniffers podem capturar senhas
- Os sniffers podem capturar informações confidenciais
- Os sniffers podem ser utilizados para abrir brechas na segurança de redes vizinhas ou ganhar acessos de alto nível.

De fato, a existência de um sniffer não autorizado em sua rede pode indicar que seu sistema já está comprometido.

Os sniffers capturarão todos os pacotes na rede, mas na prática, um atacante tem de ser altamente seletivo. Um ataque de sniffer não é tão fácil quanto parece. Ele requer algum conhecimento de rede. Simplesmente configurar um sniffer e deixá-lo trabalhando levará a problemas porque mesmo uma rede de cinco estações transmite milhares de pacotes por hora. Dentro de um breve tempo, o arquivo de saída de um sniffer pode facilmente encher uma unidade de disco rígido (se você capturar todos os pacotes).

Para superar esse problema, os crackers geralmente farejam somente os primeiros 200-300 bytes de cada pacote. O nome de usuário e senha estão contidos dentro dessa parte, o que é realmente tudo que a maioria de crackers querem.

A tecnologia de segurança desenvolveu-se consideravelmente. Alguns sistemas operacionais agora empregam criptografia no nível de pacote e, portanto, mesmo se um ataque de sniffer consiguir obter dados valiosos,

esses dados são criptografados. Isso representa um obstáculo adicional a ser ultrapassado somente por aqueles com conhecimento mais profundo de segurança, criptografia e rede.

Veja abaixo alguns dos sniffers mais famosos disponíveis sob licença de uso de software freeware e shareware:

Plataforma: UNIX/Linux

- Esniff
http://www.asmodeus.com/archive/IP_toolz/ESNIFF.C

- LinSniff
http://www.rootshell.com/archive-1d8dkslxlxja/199804/linsniff.c

- linux_sniffer
http://www.rootshell.com/archive-1d8dkslxlxja/199707/linux_sniffer.c

- sniffit
http://reptile.rug.ac.be/~coder/sniffit/sniffit.html

Plataforma: MS-DOS/Windows

- Gobbler
http://www.cse.rmit.edu.au/~rdssc/courses/ds738/watt/other/gobbler.zip

Na parte prática do curso você aprenderá a utilizar o Sniffit.

Derrotar ataques de sniffers não é fácil. Você pode adotar duas abordagens:

- Detectar e eliminar os sniffers
- Proteger seus dados contra sniffers

Os sniffers são extremamente difícies de detectar porque são programas passivos. Eles não geram uma trilha de auditoria e a menos que seu dono seja muito estúpido (farejando todo tráfego em vez dos primeiros bytes significativos por conexão), eles consomem poucos recursos de rede.

É possível localizar um sniffer em uma máquina usando o MD5, desde que tenha um banco de dados decente dos arquivos originais da instalação. Você precisa obter o script md5check que automatiza o processo.

http://wsspinfo.cern.ch/sec/cert/tools/md5check/md5check

Certamente, pesquisar por soma de verificação em uma única máquina é bastante eficaz. Entretanto, localizar um sniffer em uma rede grande é difícil. Há algumas ferramentas que podem ajudar:

Nitwit
Detecta sniffers mesmo se a interface de rede não estiver no modo promíscuo.
http://www.7thsphere.com/hpvac/files/hacking/nitwit.c

Suponha que alguém entra em um escritório vazio, desconecta uma máquina da rede e conecta um laptop com o mesmo IP. Eles utilizam isto como um sniffer. Isso é difícil de detectar a menos que você esteja utilizando mapas de topologia de rede (ferramentas que marcam qualquer alteração na topologia) e os verifica diariamente.

Se você acredita verdadeiramente que alguém grampeou sua rede, você pode obter ferramentas para verificar isso. A ferramenta que você precisa chama-se TDR (time domain reflectometer). Os TDRs medem a propagação ou flutuação de ondas eletromagnéticas. Um TDR anexado à sua rede local revelará partes não autorizadas sugando dados de sua rede.

No final das contas, entretanto, soluções preventivas são difíceis e dispendiosas. Em vez disso, você deve adotar uma abordagem mais defensiva. Há duas defesas importantes contra sniffers:

- Topologia segmentada
- Sessões criptografadas

Os sniffers somente podem capturar os dados no mesmo segmento de rede. Isso significa que quanto mais você segmenta sua rede, menos informações um sniffer pode coletar. Há três interfaces de rede que um sniffer não pode cruzar:

- Switches
- Roteadores
- Bridges

As sessões criptografadas fornecem um solução diferente. Em vez de preocupar-se com dados sofrendo sniffing, você simplesmente os adultera até um ponto que estejam além do reconhecimento. O SSH (Secure Shell é um exemplo de programa que fornece comunicação criptografada, substituindo o velho Telnet. Você pode adquirir uma versão livre para Linux em:

http://www.cs.hut.fi/ssh/

Bibliografia:

The Sniffer FAQ
http://www.netsys.com/firewalls/firewalls-9502/0320.html

Maximum Security
Anonymous