Entendendo os Sniffers

Sniffers são utilitários que você, pode usar para capturar e escanear tráfego movendo-se através de uma rede. Sniffers são uma categoria ampla que engloba qualquer utilitário que tenha a capacidade de executar uma função de captura de pacotes. Independentemente da construção, os sniffers executam sua função de captura de tráfego, ativando o modo promíscuo na interface de rede conectada, permitindo assim a captura de todo o tráfego, quer este tráfego seja ou não destinados a eles. Uma vez que uma interface entra no modo promíscuo, ela não discrimina entre o tráfego que é destinado ao seu endereço; Ele pega todo o tráfego na linha, permitindo que você capture e investigue cada pacote.

Sniffing pode ser ativo ou passivo. Tipicamente, o sniffing passivo é considerado ser todo o tipo de sniffing onde o tráfego é olhado mas não alterado em nenhuma maneira. Essencialmente, o sniffer passivo significa apenas ouvir. No sniffing ativo, não só o tráfego é monitorado, mas também pode ser alterado de alguma forma, como determinado pelo atacante.

Quando em uma rede comutada, sua captura de tráfego é limitada ao segmento que você está conectado, independentemente do modo de sua placa de interface. Basta lembrar que para que seu sniffer seja eficaz, sua placa de interface deve estar em modo promíscuo.

A maioria dos sniffers tem opções básicas que são bastante consistentes em toda a gama de versões. Essa consistência é válida independentemente de ser um utilitário baseado em Linux ou uma versão do Windows. Nós vamos mais a fundo nos tipos e especificidades mais tarde, mas primeiro vamos olhar para as semelhanças. Na maioria dos sniffers um painel principal exibe os pacotes de entrada e destaca ou lista-os de acordo. É geralmente linear na sua lista, a menos que especifique o contrário através de filtros ou outras opções. Além disso,

há geralmente um sub painel que permite uma visão em profundidade do pacote selecionado. É importante estar familiarizado com o seu sniffer, porque vai lhe poupar muito tempo e frustração a longo prazo. Além disso, ter uma boa compreensão das funções básicas de um sniffer permitirá que você use muitos sniffers diferentes sem muitos problemas. Assim, a partir daqui, um sniffer geralmente tem uma interface de seleção ou opção de ativação que inicia a fase de captura.

Um exemplo de software que faz captura de tráfego em uma rede é o Wireshark.

Depois de escolher o botão de captura, você deve ver os pacotes preenchendo o painel de captura; Caso contrário, verifique a seleção da interface de rede. Todos os sniffers lhe dão a capacidade de selecionar de todas as interfaces disponíveis em seu computador. Você pode facilmente escolher uma interface desconectada e sentir-se irritado porque seu sniffer não está funcionando. Apenas verifique novamente e você será felizmente recompensado com o tráfego em tempo real!

Use essa função de salvar a captura! Captura e análise em tempo real é impressionante e chamativa, mas também é uma dor de cabeça!

Lembre-se que um sniffer não é apenas um utilitário burro que permite que você visualize apenas o tráfego de streaming. Um sniffer é um conjunto robusto de ferramentas que podem lhe dar uma visão extremamente detalhada e granular do que sua rede está fazendo de dentro para fora. Dito isto, se você realmente deseja extrapolar a análise em cada pacote, salve a captura e reveja quando tiver mais tempo. Simplifique as coisas para você; Seu alvo não vai a lugar algum tão rápido.

Antes de ir muito a fundo em sniffers, é importante mencionar que existem também analisadores de protocolo de hardware. Esses dispositivos se conectam na rede ao nível do hardware e podem monitorar o tráfego sem manipulá-lo. Normalmente, esses

dispositivos de hardware não são facilmente acessíveis para a maioria dos hackers éticos devido ao seu enorme custo em muitos casos (alguns dispositivos têm etiquetas de preço na faixa de seis dígitos).

Agências da Lei e Sniffing

A intercepção legal (LI) é definida como o acesso legalmente sancionado aos dados da rede de comunicações, tais como chamadas telefônicas ou mensagens de correio eletrônico. LI deve sempre ser em conformidade com uma autoridade legal para fins de análise ou evidência. Portanto, LI é um processo de segurança em que um operador de rede ou prestador de serviços dá permissão aos agentes da lei de acesso a comunicações privadas de indivíduos ou organizações. Quase todos os países elaboraram e promulgaram leis para regular os procedimentos legais de interceptação; Os grupos de normalização estão criando especificações para tecnologias de LI. Normalmente, as atividades da LI são tomadas com a finalidade de proteção de infra-estrutura e segurança cibernética. No entanto, os operadores de infra-estruturas de rede privada podem manter as capacidades de LI dentro das suas próprias redes como um direito inerente, salvo proibição ao contrário. LI era anteriormente conhecido como escutas telefônicas e existe desde o início das comunicações eletrônicas.

O sucesso do processo de sniffing depende da insegurança relativa e inerente de determinados protocolos de rede. Protocolos como o TCP/IP nunca foram projetados com segurança em mente e, portanto, não oferecem muito nesta área. Vários protocolos se prestam a sniffing fácil:

- **Telnet/rlogin** – Teclas pressionadas, tais como aqueles que incluem nomes de usuário e senhas, podem ser facilmente capturadas.
- **HTTP** – Projetado para enviar informações em claro sem qualquer proteção e, portanto, um bom alvo para

sniffing.

- **Simple Mail Transfer Protocol (SMTP) –** Comumente usado na transferência de e-mail, este protocolo é eficiente, mas não inclui qualquer proteção contra sniffing.
- **Network News Transfer Protocol (NNTP) –** Todas as comunicações, incluindo senhas e dados, são enviadas de forma clara.
- **Post Office Protocol (POP) –** Projetado para recuperar e-mails de servidores, este protocolo não inclui proteção contra sniffing porque senhas e nomes de usuário podem ser interceptados.
- **File Transfer Protocol (FTP)** – Um protocolo criado para enviar e receber arquivos; Todas as transmissões são feitas em claro.
- **Internet Message Access Protocol (IMAP) –** Similar ao SMTP em função e falta de proteção.

Sugestões de livros: