Ferramentas sniffers

Nós vimos alguns dos conceitos básicos sobre o uso do sniffer na postagem anterior, mas agora vamos nos aprofundar um pouco mais. Estão disponíveis alguns pacotes de software sniffer que executam funções quase idênticas. A vantagem real de um sobre o outro é a robustez da funcionalidade em como o sniffer exibem os dados e que opções estão disponíveis para ajudá-lo a digerir e dissecá-lo.

Em termos de Interceptação Legal (Lawful Interception – LI), tipicamente o processo de sniffing tem três componentes. O primeiro componente é um ponto de acesso de interceptação (intercept access point – IAP) que reúne informações para a LI. O segundo componente é um dispositivo de mediação fornecido por um terceiro que lida com a maior parte do processamento da informação. O terceiro componente é uma função de coleta que armazena e processa informações interceptadas pela terceira parte.

Ferramentas de Sniffing

Ferramentas de sniffing são aplicações extremamente comuns. Alguns delas estão listadas aqui:

- **Wireshark** – Um dos sniffers de pacotes mais conhecidos e usados. Oferece um grande número de recursos projetados para auxiliar na dissecação e análise do tráfego.
- **Tcpdump** – Um analisador de pacotes de linha de comando bem conhecido. Fornece a capacidade de interceptar e observar TCP/IP e outros pacotes durante a transmissão através da rede. Disponível em www.tcpdump.org.
- **WinDump** – Uma versão Windows do sniffer de pacotes Linux popular tcpdump, que é uma ferramenta de linha de comando que é ótimo para exibir informações de cabeçalho.
- **OmniPeek** – Fabricado por WildPackets, OmniPeek é um

produto comercial que é a evolução do produto EtherPeek.

- **Dsniff** – Um conjunto de ferramentas projetadas para realizar sniffing com diferentes protocolos com a intenção de interceptar e revelar senhas. Dsniff é projetado para plataformas Unix e Linux e não tem um equivalente na plataforma Windows.
- **EtherApe** – Uma ferramenta Linux / Unix projetada para exibir graficamente conexões de entrada e saída.
- **MSN Sniffer** – Um utilitário sniffing projetado especificamente para tráfego gerado pelo aplicativo MSN Messenger.
- **NetWitness NextGen** – Inclui um sniffer baseado em hardware, juntamente com outros recursos, projetados para monitorar e analisar todo o tráfego em uma rede; A ferramenta é popular e usada pelo FBI e outras agências da lei.

Usar o sniffer em uma rede de uma forma efetiva e discreta, é uma habilidade que um ethical hacker deve ter. Configurar uma conexão da forma correta e capturar o tráfego com sucesso é extremamente importante, mas como um hacker, você deve também ser capaz de se aprofundar e entender os pacotes capturados.

Sugestões de livros: