Quebra de senha: Ataques passivos online

Como em outros casos em que examinamos e usamos medidas passivas, os ataques às senhas são usados para obte-las sem interagir diretamente com o alvo. Estes tipos de ataques são eficazes em ser furtivos, porque eles tentam coletar senhas sem revelar muito sobre o sistema coletor. Esse tipo de ataque depende menos da maneira como uma senha é construída e mais sobre como ela é armazenada e transportada. Quaisquer problemas com essas áreas podem ser apenas o suficiente para abrir a porta para obter essas valiosas credenciais.

Packet Sniffing

Um sniffer ou analisador de pacotes é um mecanismo (normalmente um software) feito para capturar pacotes de acordo com que eles passam pela rede. Na prática, um sniffer é usado para coletar informações para diagnosticar uma rede e identificar problemas, mas os sniffers não se preocupam com o tipo de informação está passando, mas sim se eles podem ver. Você poderá usar filtros para escolher o tipo de informação que quer ver.

Por padrão, um sniffer só é capaz de capturar informações dentro de um domínio de colisão e não em outros domínios sem

Por padrão, um sniffer só será capaz de capturar informações dentro de um único domínio de colisão e não em outros domínios sem executar medidas adicionais, como ARP spoofing. Isso significa que, se houver um switch ou outro tipo de dispositivo entre você e o destino do qual você deseja obter uma senha, você não o verá sem transmitir sua presença.

É possível usar o sniffer fora de um determinado domínio de colisão comum, mesmo se um switch estiver no caminho, desde

que você use uma abordagem que é projetada para atacar e superar o switch ou bridge. No entanto, tais métodos são agressivos e ativos e, portanto, gerar uma grande quantidade de tráfego que torna a detecção muito mais fácil para o defensor.

Geralmente, um ataque sniffing é mais eficaz se for realizado em uma rede que emprega um hub entre o atacante e a vítima, ou se as duas partes estão no mesmo segmento do domínio de colisão. Muitas das ferramentas que você vai encontrar ou usar será mais eficaz no contexto de uma rede que emprega um hub. Entretanto, uma coisa que deve ser mencionada é que os hubs são raramente usados em redes hoje por causa de seus riscos de segurança.

Então, que tipos de protocolos seriam mais propensos a ser revelado através de sniffing? Basicamente, qualquer coisa que usa texto claro para transmitir credenciais vai ser vulnerável, o que na prática significa Telnet, FTP, SMTP, rlogin, SNMPv1 e protocolos similares. Se uma senha é enviada em um formato criptografado, isso não significa que você não será capaz de interceptar a senha, apenas que você não será capaz de lê-lo. Depois de reunir as credenciais, você pode usá-las para obter acesso a sistemas ou serviços.

Man-in-the-Middle

Durante este tipo de ataque, duas partes estão se comunicando entre si e um terceiro se insere na conversa e tenta alterar ou escutar as comunicações. Para ser bem sucedido, o atacante deve ser capaz de farejar o tráfego de ambas as partes ao mesmo tempo.

Existem muitos utilitários disponíveis para realizar ataques man-in-the-middle (MitM), incluindo:

- SSL Strip
- Burp Suite

- Browser Exploitation Framework (BeEF)

Os ataques Man-in-the-middle normalmente visam protocolos vulneráveis e tecnologias sem fio. Protocolos como Telnet e FTP são particularmente vulneráveis a este tipo de ataque. No entanto, tais ataques são difíceis de realizar e podem resultar em tráfego invalidado. Veja como usar o SSL Strip nesta postagem.

Replay Attack

No ataque de repetição, os pacotes são capturados usando um sniffer de pacote. Depois que as informações relevantes são capturadas e extraídas, os pacotes podem ser colocados de volta na rede. A intenção é injetar as informações capturadas – como uma senha – de volta para a rede e direcioná-las para um recurso como um servidor, com o objetivo de obter acesso. Uma vez que os pacotes são reproduzidos, as credenciais válidas fornecem acesso a um sistema, dando a um invasor a capacidade de alterar informações ou obter dados confidenciais.

Sugestões de livros: