Quebra de senha: Ataques ativos online

Continuando com as opções de ataques para quebra de senha, veremos o próximo tipo de ataque é o ataque online ativo. Esses ataques usam uma forma mais agressiva de invasão que é projetada para recuperar senhas.

As técnicas, basicamente, são:

- Adivinhação de senha
- Trojans, Spyware e Keyloggers
- Injeção de Hash

Adivinhação de senha

A suposição da senha é um tipo de ataque muito bruto mas eficaz. Um invasor procura recuperar uma senha usando palavras do dicionário ou por força bruta. Este processo é geralmente realizado usando um software projetado para tentar centenas ou milhares de palavras a cada segundo. O aplicativo tenta todas as variações, incluindo alterações de maiúsculas e minúsculas, substituições, substituição de dígitos e caso inverso. É claro que um item a ser observado é que muitos sistemas empregam o bloqueio de conta, que bloqueia a conta quando ocorrem muitas tentativas ou falhas.

Para refinar essa abordagem, um invasor pode procurar informações sobre uma vítima, com a intenção de descobrir passatempos favoritos, nomes de familiares, seu time favorito, etc.

Complexidade de senha pode atrapalhar muitos desses tipos de ataques, porque torna o processo de descobrir uma senha mais lenta e muito mais difícil.

Trojans, Spyware e Keyloggers

Malware, como Trojans, spyware e keyloggers podem ser muito úteis durante um ataque, permitindo que o invasor colete informações de todos os tipos, incluindo senhas.

Uma forma é farejar o teclado ou keylogging, que intercepta uma senha quando o usuário digita ele. Esse ataque pode ser realizado quando os usuários são vítimas de software de keylogging ou se eles fazem logon em sistemas remotamente sem usar proteção.

Injeção de Hash

Este tipo de ataque baseia-se no conhecimento de hash e alguns truques. O ataque consiste nas seguintes etapas:

1. Comprometa uma estação de trabalho ou área de trabalho vulnerável;
2. Quando conectado, tente extrair os hashes do sistema de usuários de alto valor, como administradores de domínio ou de empresa;
3. Utilize o hash extraído para iniciar sessão num servidor, tal como um controlador de domínio;
4. Se o sistema serve como um controlador de domínio ou similar, tente extrair hashes do sistema com a intenção de explorar outras contas.

Sugestões de livros: