Atacantes

Roteiros e tópicos para estudo por

Vinícius da Silveira Serafim
professor@serafim.eti.br
http://professor.serafim.eti.br

Palavras-chave: hacker, cracker, script kid, e lammer

Atacantes

Três fatores são necessários para que um ataque se consuma: (PFLEEGER, 2006, p.8)

- Método
- Oportunidade
- Motivo

Basta subtrair qualquer um desses fatores e o ataque não se consumará.

Método

Compreende as habilidades, conhecimentos e ferramentas que o atacante deve possuir para conseguir realizar o ataque. (PFLEEGER, 2006, p. 8)

Oportunidade

A oportunidade pode ser definida como a combinação de tempo e acesso. (PFLEEGER, 2006, p. 8) O tempo se refere à disponibilidade do atacante para se preparar e executar o ataque. Já o acesso compreende:

- Obter contato físico ou lógico (via rede) ao ativo a ser atacado;
- Existência de uma vulnerabilidade no ativo ou no seu ambiente para ser explorada;
- Em alguns casos, credenciais de acesso ao ativo

Os ativos mais fáceis de serem atacados são aqueles que se encontram desatualizados (abandonados), pois as chances de já existir um bom número de vulnerabilidades conhecidas é bastante razoável.

Não só ativos desatualizados, mas ativos mal projetados e implementados são alvos interessantes. Um sistema mal projetado e implementado, por exemplo, pode conter graves vulnerabilidades a serem exploradas pelo atacante.

Motivo

Todo atacante tem uma razão, um motivo, para realizar um determinado ataque. Listo a seguir alguns possíveis motivos:

- Vingança: funcionário descontente por te sido demitido ou não ter recebido uma promoção, fornecedor que teve seu contrato cancelado, etc.;
- O ativo é fácil de ser atacado: nesse caso o atacante não se preocupa em atacar um ativo de uma empresa específica, mas qualquer ativo de qualquer empresa que esteja vulnerável;
- Notoriedade: nesses casos o atacante se identifica publicamente por algum pseudônimo a fim de ter os créditos da "proeza";
- Investigação legal: a própria polícia utiliza recursos como captura (interceptação) de tráfego de rede, por exemplo, nos seus processos de investigação;
- Lucro: nesse caso o atacante busca algum retorno financeiro direto ou indireto. Um retorno financeiro direto é obtido, por exemplo, pela venda de informações sensíveis de uma empresa ao seu concorrente no mercado. Já o retorno financeiro indireto pode ser obtido por um empresa que sabota os ativos da empresa concorrente (ex.: provoca indisponibilidade); e
- Guerra: cyberwar (ou guerra cibernética) já é uma realidade, países estão atacando a infraestrutura de TI de seus inimigos (ex.: EUA e Israel). Pesquisem na internet sobre o *Flame*.

Quem são os atacantes?

É muito importante ter em mente que os atacantes não estão apenas na Internet, é comum que haja atacantes dentro da própria empresa.

Eis alguns exemplos de atacantes, tanto internos quanto externos:

- Estudantes
- (ex)Estagiários
- (ex)Funcionários
- (ex)Prestadores de serviço
- Criminosos (crime organizado)
- Espiões
- Polícias e exércitos
- Agências de inteligência

Classes

Não há um acordo entre autores e pesquisadores da área sobre uma classificação formal e definitiva. Então aqui apresento uma simplificada e que serve perfeitamente bem para a compreensão do assunto.

A primeira classificação leva em conta o nível de conhecimento:

- Hacker ou Cracker: encontram vulnerabilidades inéditas e desenvolvem as ferramentas visando explorá-las. A essas ferramentas damos o nome de *exploits*.

- Lammer ou script kid: não possuem conhecimento aprofundado, são incapazes de descobrir novas vulnerabilidades e desenvolverem ferramentas. Utilizam os métodos já criados por hackers ou crackers e, para conseguirem realizar seus ataques, fazem uso de “how-tos” e scripts (receitas passo-a-passo) disponíveis na Internet ou publicados em revistas.

A segunda classificação pode ser feita com relação à intenção:

- Cracker: têm propósitos maliciosos; invadem sistemas computacionais para os quais não possuem qualquer autorização, seja esta de acesso regular ou mesmo permitindo o teste de invasão. (PFLEEGER, 2006, p. 22)

- Hacker: não possuem propósitos maliciosos; assim como os crackers, procuram quebrar a segurança de sistemas, porém em ambiente controlado, não utilizando ativos alheios sem a devida autorização.

Fora da área da segurança da informação, o termo hacker é utilizado tanto para indicar usuários com propósitos maliciosos (crackers) ou não.

Bibliografia

PFLEEGER, C. P. Security in Computing. 4a edição. Prentice Hall, 23 de outubro de 2006. 880 pág.