O que favorece um ataque Hacker?

12
jan,2016

0 (https://www.auzac.com.br/o-que-favorece-um-ataque-hacker/)

(https://www.auzac.com.br/o-que-favorece-um-ataque-hacker/)
(https://www.auzac.com.br/o-que-favorece-um-ataque-hacker/)

(https://www.auzac.com.br/o-que-favorece-um-ataque-hacker/)

(https://www.auzac.com.br/author/admin/) por admin

(https://www.auzac.com.br/author/admin/)

Ataque hacker (https://www.auzac.com.br/tag/ataque-hacker/), Vulnerabilidades (https://www.auzac.com.br/tag/vulnerabilidades/)

O que favorece um ataque Hacker? (https://www.auzac.com.br/o-que-favorece-um-ataque-hacker/)

Todo computador, seja ele um servidor web, um notebook ou até mesmo um smartphone, que esteja conectado à internet, está sujeito a sofrer ataque ***hacker***. Dados pessoais, senhas de contas bancárias, arquivos confidenciais ou pessoais podem para nas mãos desses invasores.

Esse tipo de ataque pode vir de fontes diferentes: desde um malware vindo de um email, uma tentativa direta de invasão pela internet ou por uma brecha na segurança que permitiu a entrada de um estranho que conseguiu plugar um pendrive no servidor da empresa.

Existem vários fatores que favorecem um ataque hacker, seja ele através de portas abertas nos servidores sendo utilizadas por softwares desatualizados, esquecidos e em funcionamento ou através de engenharia social, aqueles famosos emails do tipo “você foi nosso visitante nº 10.000, clique para pegar seu prêmio”.

Abaixo segue uma lista (não necessariamente em ordem de prioridade) das principais causas de vulnerabilidades que favorecem um ataque hacker bem sucedido:

O Fator Humano (Social Engineering)

O fator humano sempre estará presente na maioria das vulnerabilidades das aplicações e servidores, neste caso, na vunerablidade em conseguir informações. Social Engineering (engenharia social (http://www.auzac.com.br/ataques-de-engenharia-social/)) é um tipo de ataque hacker onde o atacante faz uso da persuasão, quase que se aproveitando da ingenuidade ou confiança do usuário, seja através de falsos telefonemas da área de TI da empresa ou através de emails com links para sites maliciosos, para conseguir acesso não autorizado à rede de computadores ou a informações confidenciais.

Falha de Implementação nas Aplicações Web (Sql Injections e XSS)

Em aplicações web, o backend (código que roda no lado do servidor) precisa ser bem estruturado e bem analisado, pois receberá todo tipo de informação vinda de formulários e requisições dos usuários. Sem o devido tratamento dessas informações, toda uma rede de computadores com firewalls e proxys pode ser invadida através de um ataque hacker utilizando a URL do site. Abaixo, dois tipos de ataques bem comuns voltados à aplicações web.

Sql Injection (injeção de sql): se aproveita de brechas de segurança nas consultas ao banco de dados onde o sql recebe um parâmetro direto da requisição sem o devido tratamento podendo assim 'injetar' comando sql através de uma simples requisição de uma página ou formulário de login, por exemplo.

XSS (cross-site scripting): parecido com o parceiro dele acima, o atacante (como usuário de uma aplicação web) faz uso dos formulários para gravar códigos javascripts maliciosos que serão executados por outros usuários, já que esse código persiste na aplicação.

Má Configuração de Servidores (Exploits)

Servidores web, ftp, dns, firewalls, proxys ou até mesmo controladores de domínio, todos eles precisam de uma determinada configuração para tornarem-se 'seguros', mas essas configurações nem sempre são genéricas, muitas dependem das regras de negócio da empresa o que muitas vezes fazem com que elas se tornem fracas caso não sejam bem estabelecidas.

Exploits são códigos criados para 'explorar' vulnerabilidades em computadores, através de um determinado serviço por meio de suas configurações, e, geralmente, esses exploits ao serem bem sucedidos, executam um segundo código que na maioria das vezes abrem uma conexão shell com o servidor alvo.

Softwares Piratas e a Falta de Atualização (Vírus e Malwares)

A falsa segurança ao pensarmos que a utilização de softwares piratas á algo inofensivo nos faz cair em dois erros: o da ilegalidade e o da ingenuidade. Ilegalidade pois existem lei de direitos autorais e intelectuais protegendo as fabricantes desses softwares, e ingenuidade ao pensarmos que, quem 'desbloqueou' e disponibilizou o software pirata não injetou nada de malicioso nele, apenas queria ser legal com as pessoas.

Sem o suporte fornecido pelos fabricantes, os softwares piratas não recebem as atualizações de segurança advindas de um contrato ao comprarmos a licensa de uso do mesmo, sendo assim, estamos literalmente com portas abertas para invasores através de virus e malwares injetados nos mesmos.

Senhas de Usuários (Brute Force)

A internet conta com uma gama de serviços variados: emails, blogs, fórums, redes sociais, repositórios e backups virtuais. Com isso os usuários acabam utilizando diferentes contas com nomes de usuários que divergem entre si: com

ou sem ‘underscore’, com ou sem ‘ponto’ ou até mesmo o próprio email. Já as senhas variam entre diferentes regras, senhas numéricas, tamanho, maíusculas e minúsculas, com ou sem caracteres especiais, etc.

Para evitar que caiam no esquecimento, muitos usuários costumam utilizar de uma mesma senha para a maioria dos serviços utilizados na internet, ou quiçá todos eles, e na mairoia dos casos são senhas de fácil assimilação: sequências numéricas, palavras conhecidas com sufixos/prefixos simples.

Aí entra o ataque hacker Brute Force (força bruta), tentativas constantes de adivinhação por meio de listas de palavras (listas grandes!!) até mesmo personalizadas com conceitos comuns ao usuários, como locais, cidades, times de futebol e até nomes de familiares.

Sobre o Autor

admin
administrator

Deixe uma resposta