VULNERABILIDADE DE SENHAS E REQUISITOS NECESSÁRIOS PARA ATAQUE DE FORÇA BRUTA

Marcelo Machado Pereira[1], Ivan Leal Morales[2]

[1]Aluno da Graduação de Ciência da Computação - Faculdades Integradas de Bauru - FIB - lobo.death@gmail.com

[2]Orientador e Professor Especialista - Faculdades Integradas de Bauru - FIB - ilmoralesbr@hotmail.com

INTRODUÇÃO

Este trabalho visa demonstrar, por meio da teoria, o estudo de diferentes autores, e da prática, com a criação de arquivos "wordlist", que os Ataques de Força Bruta efetuados por Hackers ou Crackers são dependentes das Vulnerabilidades de Senhas e Sistemas de Autenticação desprovidos de ferramentas IDS e IPS.
De acordo com FERREIRA e ARAÚJO(2008), a maioria dos programas de computador dispõem de sistemas de autenticação, onde o processo de logon é usado para obter acesso aos dados e aplicativos em um sistema informatizado. Os sistemas de autenticação são uma combinação de hardware, software, políticas e procedimentos que permitem o acesso de usuários aos recursos computacionais. Definem ainda que, **deve ser inibida, de todas as formas, qualquer oportunidade de uso compartilhado de senhas.**

Usuários sempre serão usuários e impedir que usuários acrescentem software não autorizado em seus computadores de mesa ou notebooks se tornou uma preocupação comum entre gestores de TI e de Segurança da Informação. Para dificultar a tarefa de um invasor, recomenda-se limitar o número de tentativas incorretas de acesso *(logon)*, bloqueando a conta do usuário ao alcançar um número limite. Os colaboradores devem manter suas **senhas como informação confidencial,** segundo FERREIRA e ARAÚJO(2008).

Segundo CARUSO e STEFFEN(2013), no mundo todo essa expansão da micro informática envolve muitos usuários descomprometidos com a segurança, sem uma prévia cultura de TI. Devido à arquitetura aberta das plataformas do tipo PC e similares, esses equipamentos e seus softwares ainda são essencialmente inseguros. Os computadores portáteis, com discos de grande capacidade, encorajam os usuários a

manter seus arquivos armazenados localmente. O risco de perda, furto ou roubo cresce vertiginosamente. Segundo FERREIRA e ARAÚJO(2008), vulnerabilidade é uma fraqueza que pode ser acidentalmente utilizada ou intencionalmente explorada. Ameaça é a possibilidade de um invasor ou evento inesperado explorar uma vulnerabilidade de forma eficaz. O estudo visa demonstrar que as ameaças e o roubo de informações estão presentes em qualquer área da organização e passa pela área de tecnologia adotar métodos e controles para assegurar a guarda correta dos dados da empresa.

MATERIAL E MÉTODOS

A metodologia utilizada foi a Pesquisa Bibliográfica, utilizando-se a opinião de outros autores, conforme (CERVO, BERVIAN & SILVA - 2007) além de explicar um problema a partir de referências teóricas publicadas em artigos, livros, dissertações e teses, pode ser realizada independentemente ou como parte da pesquisa descritiva ou experimental. Em ambos os casos, busca-se conhecer e analisar as contribuições culturais ou científicas do passado sobre determinado assunto, tema ou problema.

RESULTADOS E DISCUSSÕES

Um software que promove ataques de Força Bruta, como o Caim (http://www.oxid.it/), necessita apenas de um arquivo ou arquivos com uma lista ou listas variadas de palavras ou códigos, chamados arquivos de wordlist, que lhe forneçam uma boa quantidade de possibilidades para explorar vulnerabilidades e invadir o sistema em questão. Um arquivo de wordlist pode ser criado em formato texto ou qualquer outra extensão, gerado de forma automatizada através de programa de computador, escrito em Linguagem C ou outra qualquer. O programa irá gerar a lista de forma ordenada, para que o programa possa posteriormente ler o arquivo de forma sequencial, combinando usuários prédefinidos (admin, master, root, administrador, guest, etc) com as palavras geradas no arquivo pelo programa. Um arquivo de senhas numéricas, com 4 caracteres gerados à partir do 1000 até a quantidade de 6 caracteres, até o 999.999 irá possuir quase 1 milhão de senhas, das quais todas as combinações possíveis serão geradas. Dependendo das configurações do computador, o programa que gera o arquivo de

wordlist pode demorar de 2 até 3 horas para criar todas as senhas numéricas possíveis entre o intervalo citado, mas o programa Cain pode levar até 10x mais tempo para conseguir o login desejado, caso o usuário não seja um dos padrões previamente configurados no software. Senhas numéricas são mais simples de serem descobertas, principalmente as iniciadas entre 0 à 4 e o recomendável é que além de usar caracteres alfanuméricos, na criação de uma senha também sejam utilizados símbolos para aumentar a complexidade da senha. Alguns programas geram senhas através de funções matemáticas como o número fatorial ou a análise combinatória. Essas ferramentas da matemática podem não só nos proporcionar formas de gerar senhas mais complexas como também nos informar da quantidade que é possível gerar para cada situação.

CONCLUSÕES

Quanto mais complexa for a senha, melhor, pois mais difícil será descobrí-la. Uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar, segundo FERREIRA e ARAÚJO(2008). Um ponto importante a ser destacado é a utilização de sistemas Case Sensitive, que no caso dos caracteres alfanuméricos fazem distinção entre maiúsculas e minúsculas, aumentando assim a complexidade da senha e dificultando ainda mais a descoberta por programas que lêem arquivos de wordlist e promovem ataques de força bruta. Um outro recurso que também pode ser utilizado, principalmente em sistemas Web, é o recurso do Captcha. Este recurso consiste em gerar um código em uma imagem que testa se o usuário é ele mesmo ou se é um robô que está realizando as tentativas de login. Alguns sistemas possuem um contador Flag, que ao atingir um determinado valor, cancelam a sessão do usuário por determinado período de tempo, impossibilitando assim, que o robô que executa o ataque de força bruta, obtenha sucesso em descobrir as credenciais de logon do sistema. Ferramentas de detecção de intrusão que agem de forma a detectar comportamentos estranhos que estão sendo executados no sistema também são ferramentas úteis para mitigar esses problemas de ataques Hacker. Por fim, o usuário ainda é o elo principal que mantém um sistema informático seguro ou não e uma boa política de segurança pode ser um primeiro passo para gerar um sentimento de conscientização para que senhas não sejam compartilhadas, que os

usuários não criem e utilizem senhas simples demais e que o mesmo não deixe anotado as senhas em locais de fácil acesso de outros usuários.

REFERÊNCIAS

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** 4ª edição São Paulo: Editora Senac, 2013.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA; Roberto da. **Metodologia Científica**. 6ª edição São Paulo: Pearson Prentice Hall, 2007.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação.** 2ª edição Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.