

**ATAQUES A CONTAS DE SERVIÇOS ONLINE**

SÃO CAETANO DO SUL/SP

2019

**ANTONIO DUARTE DIAS NETO**

**IGOR VINÍCIUS MOREIRA**

**MARCOS GONÇALVES SIQUEIRA**

**MIKAEL AKIRA SHISHITO MATOS**

**VITOR KIOMASSA KINA**

**YAN MOURA VIRGINIO**

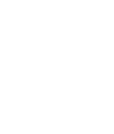
**ATAQUES A CONTAS DE SERVIÇOS ONLINE**

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação do Professor Dr. Jacinto Carlos Ascêncio Cansado, como requisito parcial para a obtenção do diploma de Graduação no curso de Segurança da Informação.

SÃO CAETANO DO SUL/SP

2019

**SUMÁRIO**

[Introdução………………………………………………………………………………….](#_30j0zll) 4

1 Contas e Autenticação…………………………………………………………………. 9

2 Tipos de ataques…………………………………………………………………….... 12

3 Prevenção de ataques………………………………………………………………... 17

Considerações finais……………………………………………………………………. 21

Referências……………………………………………………………………………….22

**INTRODUÇÃO**

As pessoas estão cada vez mais dependentes da tecnologia, seja para o trabalho ou apenas para uso pessoal, e muitos dos sites acessados necessitam criar uma conta de usuário, seja para uma rede social, um *streaming* de filmes ou um de música, tornando essencial ter uma senha que seja forte e segura para que dificulte o acesso de alguém não autorizado. Portanto é necessário saber como é possível prevenir ou diminuir as possibilidades de comprometimento da conta, para isso é preciso tomar medidas de segurança essenciais, como usar senhas diferentes em sites diferentes, usar senhas longas e com caracteres especiais.

As aplicações *web* são o principal alvo quando falamos sobre autenticação de contas utilizando e-mail, usuário ou senhas, isso ocorre devido ao alto nível de acesso a informações pessoais quando existe o sucesso ao ingresso a uma conta pessoal, podendo render lucro para o invasor de diversas formas e prejudicar o proprietário da conta acessada, tanto em termos de privacidade quanto financeiros. De acordo com o ramo do site alvo, os invasores podem conseguir dados de cartões de crédito, informações pessoais e outros dados sensíveis que podem compor um cenário de ataque e causar impactos significantes. As páginas *web* podem estar vulneráveis por muitas razões, em função, por exemplo do desenvolvedor da página não usar comandos e precauções necessárias para manter o site confiável e seguro. Segundo a Open Web Application Security Project (OWASP, 2019) em 2017 os ataques mais críticos em aplicações *web* foram a injeção de Structured Query Language (SQL), que tem como objeto aproveitar de falhas de bancos de dados através a injeção de comandos SQL, o segundo ataque mais crítico é a quebra de autenticação, onde a autenticação e gerenciamento de sessão são implementadas incorretamente.

É importante para as empresas terem formas de mitigar os impactos de um ataque a uma aplicação *web*, segundo Gênesis Rivas (2018), as etapas importantes para a proteção de aplicações *web* são o uso de criptografia e configurar o servidor *web* para redirecionar para uma página *web* com criptografia, desenvolver um sistema de redefinição de senha segura, realizar uma avaliação de risco e uma ferramenta de segurança de aplicativos da *web*.

**Justificativa**

O estudo do comprometimento de contas é importante pois muitos usam o mesmo *e-mail* como palavra chave (password) e a mesma senha em diversos sites, se sujeitando à possibilidade de terem seus dados privados descobertos por indivíduos “mal intencionados” que tenham acesso a um único site. Isso pode ser analisado segundo Glazier W. e Dhiman em Automation Attacks at Scale - Credential Exploitation (2017), onde na grande maioria dos dados que foi analisado, tinham sido usados em grandes sites famosos que tiveram seus dados vazados.

É importante ressaltar que esse tipo de ataque pode se tornar grave uma vez que pode atingir milhares de pessoas, tudo depende da segurança do site alvo e dos dados de usuário que as pessoas usam no site em questão. Por isso é recomendado por diversos especialistas que a sua senha não seja usada em mais de um site e que ela seja uma senha complexa, porém a complexidade da senha tem estado em discussão em detrimento do tamanho ou do uso de variações de caracteres.

Hoje em dia muitos sites ainda colocam a autenticação baseada em *e-mail* e senhas, por esse fator e através dos programas corretos, como o SentryMBA é possível acontecer o que foi demonstrado por Glazier W. e Dhiman (2017), em que houve a manipulação de dados de outros sites para acesso de contas ao site alvo, também foi verificado que mesmo os acessos legítimos constavam em outros sites, mas a quantidade desses dados em outros sites era bem menor em relação aos acessos tentados pelo programa em questão.

Com um ponto de vista da área da segurança, é sempre necessário estar atualizado aos meios de proteção atuais e buscar uma evolução constante, pois os ataques sempre estão evoluindo. De acordo com Glazier W. e Dhiman em Automation Attacks at Scale - Credential Exploitation (2017), uma tática de defesa ideal é aquela em que não alerte a presença da defesa para os atacantes e que não seja apenas um bloqueio, pois apenas isso pode fazer com que os atacantes criem técnicas para ultrapassar a segurança.

Para Feldmeier, D. e Kam (1990), as senhas são talvez os métodos mais utilizados de autenticação do usuário. Embora haja mais segurança em mecanismos de autenticação, por exemplo: *token de hardware*, autenticação baseada em impressão digital ou certificação, a autenticação baseada em senha continua a ser o mecanismo amplamente utilizado devido ao seu baixo custo e conveniência. Como senhas devem ser memorizadas, elas são geralmente escolhidas de um pequeno domínio, que permite a montagem de um ataque de dicionário em sistemas baseados em senha e outras formas de ataque. Baseado nesta informação, este trabalho de graduação, propõe a seguinte reflexão: é possível demonstrar proteção total do sistema de autenticação do usuário de acordo com os métodos de ataque tratados no trabalho?

**Objetivo**

O trabalho tem como objetivo explicar passo-a-passo como contas de serviços *online* podem ser invadidas e as formas que podem prevenir isso, tanto da empresa quanto do usuário. O presente trabalho demonstra a importância das partes entenderem e se conscientizarem sobre esse assunto, pois um problema como esse pode causar um grande impacto para a organização e também para o consumidor daquele serviço.

Este trabalho aborda mais profundamente o processo em que existe o acesso aos dados das contas de usuários e por que é imprescindível existir a conscientização sobre esse tema, tanto para informar o usuário do serviço quanto para que as empresas consigam desenvolver novas técnicas para defender seus dados e barras acessos não autorizados.

Contribuir com desenvolvedores de forma geral, de modo que os conhecimentos que estarão disponíveis neste trabalho de graduação ajudem no desenvolvimento de sites, ou outros tipos de plataformas de serviços, e buscar esses resultados através de uma descrição detalhada das diversas maneiras de se obter acesso às contas privadas de usuários nos diversos tipos de serviços disponibilizados via internet, bem como a maneira recomendada de mitigação.

**Metodologia**

Neste trabalho de graduação, exploramos o tema proposto através de um cenário prático para demonstração dos métodos de invasão, e explicamos como prevenir tais métodos falados anteriormente, junto com o cenário, utilizando como base pesquisas bibliográficas em artigos, livros, sites acadêmicos e corporativos.

Este documento é composto de quatro capítulos, sendo o primeiro utilizado para a compreensão do funcionamento da autenticação em contas , o segundo irá focar nas ferramentas utilizadas, o terceiro será em um cenário prático do projeto e o último tratará das formas de mitigação.

**1. Contas e autenticação**

As contas na internet podem ser classificadas como uma forma de identificação, para que assim o sistema saiba quem você realmente é e consiga salvar seus dados e informações, além de protegê-los. Para podermos analisar essa ação de uma forma mais clara, usamos a analogia de uma blitz policial, quando existe a solicitação de seus documentos por parte do policial, é como se o site, programa ou aplicativo em questão estivesse requisitando seus dados para verificar que você é quem diz ser, após o fornecimento desses dados, uma checagem interna é feita em ambos os casos. No caso real, é verificado no sistema governamental se o documento é válido, enquanto no caso de contas virtuais essa verificação pode ser feita de algumas formas diferentes, mas todas com o mesmo princípio: checar se os dados que você forneceu conferem com os dados necessários para acessar ou validar informações. De acordo com Renaud (2004, p. 2) “Todos os sistemas de segurança vão perguntar para a pessoa se identificar“.

Nessa verificação de identidade virtual, o modo mais comum é o que utiliza um e-mail ou usuário e também uma senha, isso significa que para ter acesso aos dados, é necessário possuir no mínimo duas informações, onde a senha é sempre extremamente pessoal e que só o proprietário daquela conta deveria possuir a informação, porém, em muitos casos como Felten e Gaw (2006, p.1)relata: “Quando as pessoas utilizam as mesmas senhas em várias contas, elas aumentam sua vulnerabilidade; o comprometimento de uma senha pode ajudar um atacante a assumir várias contas.”, isso faz com que a segurança de suas contas esteja em risco, mais adiante isso será abordado profundamente neste trabalho. Segundo Cristofaro et al (2013, p. 1), 20% das senhas são cobertas em uma lista com apenas 5,000 senhas. Por conta desse hábito dos usuários, passaram a existir alguns fatores extras para aumentar a segurança das contas, dentre eles, podemos citar a autenticação de dois fatores.

A autenticação de dois fatores consiste em uma segunda etapa além do padrão exigido de e-mail ou usuário e senha, essa etapa também consiste em validar o acesso à conta através de algo que somente o proprietário deveria ter acesso e pode ocorrer de modos distintos e pode ser realizada de duas formas diferentes, segundo Osório e Heinen (2004, p.2), conforme citado por Abbas (1994). Online e offline conforme explicado abaixo:

Na autenticação off-line, a assinatura é feita pelo usuário em uma folha de papel, que é posteriormente digitalizada e enviada para o sistema que realiza a autenticação. Na autenticação online, a assinatura é feita diretamente sobre um dispositivo de hardware, como uma mesa digitalizadora ou um tablet. Além destes dispositivos, podem ser utilizados para a autenticação on-line de assinaturas computadores do tipo Handheld, que permitem a escrita diretamente sobre uma tela sensível. O reconhecimento on-line de assinaturas permite que sejam utilizadas diversas informações temporais e dinâmicas relativas à assinatura, como a velocidade da caneta e a trajetória, que permitem que se obtenham melhores resultados no processo de autenticação.

Os dois modos mais populares e que pode ser verificados em diversos sites nos dias de hoje, são validações via um código que é recebido pelo proprietário. Ele recebe esse código, geralmente composto por números ou letras, em algum dispositivo confiável, podendo ser através de um SMS em seu número de telefone cadastrado no site ou em programa de terceiros que gere esse código, como o Google *Authenticator* faz. Como Cristofaro et al (2013, p. 1) menciona, “Autenticação em dois passos foca em melhorar a resiliência da autenticação baseada em senha solicitando que os usuários providenciem um passo adicional de verificação, por exemplo, um código gerado por um token de segurança”.

2. Explorando vulnerabilidades em contas

Entendendo como funciona autenticação nas contas de serviços online, como explicado no capítulo anterior, no decorrer deste capítulo demonstra-se como essa autenticação pode ser violada. Pensando que uma conta é autenticada através de usuário e senha, a proposta é usar um banco de dados para que essa senha seja descoberta.

2.1 Banco de Dados

Um banco de dados pode ser um arquivo com milhares de informações armazenadas, segundo Korth um banco de dados “é uma coleção de dados inter-relacionados, representando informações sobre um domínio especifico”, ou seja, sempre que for possível agrupar informações que se relacionam e tratam do mesmo assunto, podemos dizer que temos um banco de dados. No caso deste trabalho será utilizado um arquivo com milhares de possibilidades de usuário e senha, um agente mal intencionado pode utilizar facilmente de um banco de dados roubado/vazado para conseguir acesso a uma conta online, tendo em vista que isso é algo ilegal, neste trabalho utiliza um banco de dados criado para demonstração de como esse ataque ocorreria em um cenário real.

Paragrafo Hashcat

2.2 SentryMBA

Esse banco de dados poderá ser usado em um software, que neste caso será o SentryMBA, onde serão efetuados vários pedidos de autenticação de conta ao site com milhares de possibilidades de usuários e senhas do banco de dados até que o acesso ao site seja autenticado com a possibilidade certa.  
O SentryMBA funciona com uma pré-configuração, ou seja, você precisa configurá-lo para atacar um site específico, pois cada site pode possuir uma característica própria no momento da autenticação. Para saber exatamente como o site gera essa autenticação, é necessário utilizar um rastreador de pacotes.

Depois de configurado, o SentryMBA necessita de uma wordlist (arquivo de texto com campo de usuário e senha, com milhões de combinações) para tentar obter acesso as contas. Neste trabalho wordlist será gerada manualmente, porém é possível obter wordlists facilmente na internet.

Inserir Fiddler (Rastreador de Pacotes) no paragrafo.

Rastreador de pacotes

Um rastreador de pacotes monitora o tráfego da rede, conseguindo capturar qualquer informação que esteja passando por ela. Com essa ferramenta, é possível capturar as informações de como é feita a autenticação no nosso alvo.

3. Soluções de segurança

**CONSIDERAÇÕES FINAIS**

Ao longo do trabalho, verificamos possibilidade de um sistema mais seguro. Para isso, realizamos tentativas de ataque em um ambiente real, onde invadimos contas e verificamos as etapas de segurança que envolvem este processo. A partir disso, exploramos os métodos que são utilizados para realizar a proteção dessas contas.

**REFERÊNCIAS**

ABBAS, R. **Backpropagation Networks Prototype for Offline Signature Verification.** RMIT, 1994. Disponível em: <https://s3.amazonaws.com/academia.edu.documents/31072265/10.1.1.48.921.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1558706518&Signature=ZWOQz5FMPnwC2d%2FddMavQnWKdLk%3D&response-content-disposition=inline%3B%20filename%3DBackpropagation\_Networks\_prototype\_for\_o.pdf>. Acesso em: 19 de maio de 2019.

BONNEAU, J et al. **The Quest to Replace Passwords:** A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 IEEE Symposium on Security and Privacy, 2012. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234436>. Acesso em: 16 de maio de 2019.

BOYD, S.W.; KEROMYTIS, A. D. **SQLrand:** Preventing SQL Injection Attacks. Columbia University, 2004. Disponível em: <http://web1.cs.columbia.edu/~angelos/Papers/sqlrand.pdf>. Acesso em: 15 de abril de 2019.

BRASSARD, G. **Advances in Cryptology** - CRYPTO'89. Heidelberg: LNCS, 1995. volume 435.

CRISTOFARO, E et al. **A Comparative Usability Study of Two-Factor Authentication**. Cornell University, 2013. Disponível em: <https://arxiv.org/pdf/1309.5344.pdf>. Acesso em: 20 de maio de 2019.

DHIMAN, M.; GLAZIER, W. **Automation Attacks at Scale -** Credential Exploitation. Stealth Security, Inc, 2017. Disponível em: <https://grehack.fr/data/2017/slides/GreHack17\_Automation\_Attacks\_at\_Scale\_paper.pdf>. Acesso em: 10 de abril de 2019.

FELTEN, E et al. **Password Management Strategies for Online Accounts**.Princeton University, 2006. Disponível em: <http://www.dphu.org/uploads/attachements/books/books\_3522\_0.pdf>. Acesso em: 17 de maio de 2019.

HALFOND, W. G. J.; ORSO, A.; VIEGAS, J. **A Classification of SQL Injection Attacks and Countermeasures**. Georgia Institute of Technology, 2006. Disponível em: <https://pdfs.semanticscholar.org/81a5/02b52485e52713ccab6d260f15871c2acdcb.pdf>. Acesso em: 19 de abril de 2019.

HEINEN, M et al. **Biometria Comportamental:** Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas. Universidade Vale do Rio dos Sinos, 2004. Disponível em: <http://infocomp.dcc.ufla.br/index.php/INFOCOMP/article/view/72>. Acesso em: 18 de maio de 2019.

LAMPORT, L. **Password Authentication with Insecure Communication**. SRI International. Communications of the ACM, 1981. Disponível em: <http://merlot.usc.edu/cs530-s07/papers/Lamport81a.pdf>. Acesso em: 16 de maio de 2019.

LANGHEINRICH, M. **Privacy Invasions in Ubiquitous Computing**. Swiss Federal Institute of Technology, 2004. Disponível em: <https://uc.inf.usi.ch/wp-content/cache/mendeley-file-cache/fe35ed36-3d2c-3d85-9722-d956f47b96b7.pdf>. Acesso em: 18 de abril de 2019.

MORRIS, R; THOMPSON, K. **Password Security:** A Case History. Communications of the ACM, 2002. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.1635&rep=rep1&type=pdf>. Acesso em: 17 de maio de 2019.

OWASP. **The Ten Most Critical Web Application Security Risks**. 2017. Disponível em: <https://www.owasp.org/images/7/72/OWASP\_Top\_10-2017\_%28en%29.pdf.pdf>. Acesso em: 31 de março de 2019.

PESSOA, M. **Segurança em PHP**. Editora Novatec, 2007. Disponível em: <http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/254879.pdf>. Acesso em: 18 de março de 2019.

RENAUD, K. **Quantifying the quality of web authentication mechanisms**: a usability perspective, 2004. Disponível em: <<https://www.riverpublishers.com/journal/journal\_articles/RP\_Journal\_1540-9589\_322.pdf> Acesso em: 17 de maio de 2019.

RIVAS, G. **Web Application Security:** 7 Best Practices You Need to Know. GBadvisors, 2018. Disponível em: <https://www.gb-advisors.com/web-application-security-5-best-practices/>. Acesso em: 1 de abril de 2019.

SCHNEIER, B. **Customers, passwords, and Web sites**. IEEE Security & Privacy, Volume: 2, Edição: 4, 2004. Disponível em: <https://ieeexplore.ieee.org/document/1324609>. Acesso em: 17 de abril de 2019.

WEIDMAN, G. **Testes de Invasão:** Uma Introdução Prática ao Hacking. Santa Terezinha. Editora Novatec, 2014.