**COLÉGIO JOÃO PAULO I – UNIDADE SUL**

**INTRODUÇÃO À METODOLOGIA CIENTÍFICA 2022**

**TURMA: 9ºA**

# COMO ATAQUES CIBERNÉTICOS FUNCIONAM

Aluno: Érico P. Müller
Orientador: Lucas Floriano

Porto Alegre/RS

2022

# SUMÁRIO



## 1. INTRODUÇÃO

Nos dias de hoje, vivemos com um problema que vem se tornando cada vez mais comum de acordo com o tempo, que são os ataques cibernéticos. Ninguém sabe ao certo onde surgiu o termo *hacker*, mas acredita-se que começou a ser usado em 1960, no MIT (Instituto de Tecnologia de Massachusetts) para pessoas que criavam um *hack*, que era uma solução inovadora para algum problema. Também é possível que tenha sido usado para chamar pessoas que faziam trotes e brincadeiras no MIT, entre algumas outras teorias envolvendo esses elementos. Isso não é apenas para o setor da tecnologia, e sim para qualquer outro, contudo acabou por se popularizar mais nessa área de segurança da informação.

Há uma certa visão muito errada e negativa do *hacking*, dada pela mídia e, infelizmente, por situações pessoais. Existem vários filmes mostrando hackers como vilões, como um filme de 2015 chamado *Hacker*, o qual é muito irreal, mostrando hackers como gênios, digitando em alta velocidade com terminais de letra verde fazendo coisas impossíveis, entre outras obras. Infelizmente também temos muitas reportagens sobre ataques, tais como: "*Hackers exigem $70 milhões para liberar*

*dados após ciberataque a empresa nos EUA"* (G1), ou "*Nasa foi hackeada por computador de $35 normalmente usado por crianças"* (Exame). Isso faz com que a maioria das pessoas fique com uma visão errada sobre esse termo e sobre a área de atuação de profissionais conhecidos como *hackers*. As pessoas com essa perspectiva errônea têm medo, porque acham que eles são apenas criminosos, ou têm uma ideia muito fantasiosa, por causa dos filmes, de que *hackers* são seres místicos, geniais, que digitam em terminais com fundo preto e letras verdes em alta velocidade e entram no sistema de governos em um piscar de olhos. Ambas visões estão erradas. Mas, então, o que realmente é um *hacker*?

Um *hacker* na segurança da informação pode ser classificado de várias formas, por exemplo, *white hat, black hat* e *grey hat*. O *white hat* é o *hacker* profissional, que trabalha com isso para proteger sistemas. O *black hat* é o cibercriminoso, que utiliza seus conhecimentos, para benefício próprio. O *grey hat é* difícil de definir, por vezes ele tem boas intenções, mas, para chegar ao seu objetivo, utiliza técnicas antiéticas, ou pode encontrar uma vulnerabilidade e, antes de reportar à empresa, ele a explora. Há, ainda, outras classificações, como *red team* (um time ofensivo contratado, que ataca um sistema para reportar as falhas depois) ou *blue team* (um time defensivo, cujo objetivo é proteger o sistema contra invasores), mas essas classificações estão fora do escopo da presente pesquisa.

Muitos ataques são feitos explorando vulnerabilidades criadas por um erro no código do alvo ou uma brecha na infraestrutura, mas, atualmente, com programas mais sofisticados e serviços com uma grande infraestrutura, muitas vezes, pode demorar semanas, meses ou até anos para achar uma vulnerabilidade relevante. Então, está sendo muito usada uma técnica antiga que não tem como principal alvo uma aplicação programada.

Vale ressaltar que esses cibercriminosos optam pelo elo mais frágil, o ser humano. Eles utilizam técnicas de engenharia social, que são, de forma simples, uma manipulação psicológica da vítima, induzindo-a ao erro, por exemplo: quando há exposição de informações confidenciais ou de um ato considerado incorreto. Utilizando a falha humana com conhecimentos computacionais, nenhum sistema está seguro o suficiente.

A engenharia social é usada por todos hoje em dia, conscientemente ou não. Muitos vendedores, por exemplo, estudam essas técnicas para fazer com que as pessoas comprem seus produtos. Todavia, nessa pesquisa, focaremos essas técnicas em um contexto de fraude.

Além disso, serão apresentadas técnicas de engenharia social, como elas funcionam, como se proteger delas e alguns outros ataques (que não são de engenharia social) os quais são usados em conjunto com ela.

### Justificativa

83% das empresas americanas alegam ter sido alvo de ataques cibernéticos, principalmente de fraude, em 2021, segundo relatório divulgado pela KPMG. Na América Latina, houve um aumento de mais de 700% de ataques cibernéticos por conta da pandemia, segundo a ESET. O Brasil também teve uma alta de 200% em ataques de engenharia social só no ano de 2020. Qualquer tipo de organização que preza por suas informações, deve cuidar da sua segurança tecnológica, e isso precisa incluir os funcionários e os participantes da organização. Essas pessoas devem ser treinadas e instruídas em relação a esses ataques para que, dessa forma, a segurança seja alcançada no ambiente digital.

### Objetivo

Essa pesquisa tem como objetivos: compreender como ataques cibernéticos, que visam ao acesso a informações de organizações por meio de um membro, funcionam, instruir o leitor a se prevenir desse tipo de ataque e entender o papel de profissionais de segurança da informação na proteção de sistemas.

## 2. METODOLOGIA

Essa pesquisa será feita a partir da leitura de livros e de artigos científicos disponibilizados dentro da plataforma Google Acadêmico, utilizando palavras-chave,

como: *hacking, hacker,* invasão*,* engenharia social, ataque cibernético*, osint*. Também haverá estudo por meio de vídeos e conteúdos de sites e reportagens sobre o assunto. Esses materiais poderão ser em português e inglês.

# 3. RESULTADOS

Há basicamente dois tipos de ataques, os direcionados e os em massa. Além disso, raramente se utiliza apenas uma técnica; na maioria das vezes, combinam-se múltiplas delas.

Os ataques direcionados são geralmente os mais perigosos, antes do hacker praticar o delito, é feita uma longa pesquisa sobre o alvo por ele. O hacker faz inicialmente uma coleta de informações de forma passiva, também conhecida como *footprinting*, utilizando-se de *OSINT* (Open Source Intelligence). Essas informações são coletadas por meio de múltiplas fontes, mas uma das mais perigosas são as redes sociais. Atualmente se expõe muita informação pessoal nesses locais. No caso de um ataque direcionado a uma pessoa, pode-se coletar algo diretamente nas redes sociais, já no caso das empresas pode-se coletar informações dos funcionários, e, assim, usá-los como acesso. Algumas outras fontes podem ser: o próprio Google (e outros buscadores), usando o *Google Dorks* para uma busca avançada visando a conhecimentos mais sensíveis do alvo, reportagens/artigos, imagens públicas, número de telefone, documentos públicos, vazamentos de dados, nomes, e-mails, vídeos, domínios etc. Além dessas fontes, durante a pesquisa pode ser usada também algumas ferramentas que automatizam esse processo, algumas delas são mais especializadas em um tipo de dado ou fonte, e outras são mais gerais. Muitas dessas ferramentas e fontes podem ser encontradas no website OSINT Framework.

Após essa extensa coleta de dados, o hacker procura fazer uma análise, procurando quais dados são relevantes para o crime, além de ir mapeando cada um. Com isso, ele consegue modelar e projetar um ataque específico para o alvo. Digamos que o hacker quer acesso ao Instagram da vítima, se ele já não achou as

credenciais de acesso à conta dela, poderia enviar um e-mail ou uma mensagem se passando por outra pessoa ou por uma empresa. Levando em consideração que ele estudou o alvo, todas as informações que dão credibilidade na mensagem, ele utiliza. Esse e-mail ou mensagem pode solicitar alguma determinada informação a qual é possível acessar a conta da vítima. Além das credenciais de acesso de alguma conta, o hacker pode querer outras informações, como: localização, imagens da câmera, algum dispositivo eletrônico etc. Para obtê-las, é possível utilizar programas, como Seeker (utilizado para descobrir a localização), Saycheese (utilizado para conseguir informações da câmera), Msvenom, da Metasploit, ou AndroRAT (para conseguir acesso a um dispositivo).

Ataques em massa não têm um alvo particular, no máximo um nicho específico de pessoas em que não é necessária uma busca extensiva de dados, apenas uma análise de alguns dependendo do acesso utilizado, como a interface de um determinado site para copiá-la. Um ataque muito comum é chamado de *phishing*, que, na maioria das vezes, é uma página solicitando suas credenciais de acesso a algo seja ela criada, seja ela copiada de outro site, como: Facebook, Instagram, Twitter. Com isso, é possível unir mais outras técnicas, como *domain look-alike*, comprando um domínio semelhante ao do site copiado, por exemplo: em vez de *discord.com,* o site estará com o domínio *discocrd.com*; *facebook.com* com *facebok.com*, *instagram.com* com *instagrarn.com*, *amazon.com* com *amazn.co*, ou seja, existem infinitas possibilidades. Ademais, existe um site feito para adivinhar o domínio correto, além de treinar seus olhos para não cair nesse tipo de golpe.

Uma ferramenta muito conhecida no meio da segurança da informação e da engenharia social é o SET (*social engineering toolkit*), um kit de ferramentas que automatiza alguns processos do uso de uma técnica. Por exemplo, com essa ferramenta, é possível clonar um site, infectar o clone e já criar um QR Code para ele, ou seja, um atacante pode espalhar o QR Code nas ruas, num cartaz falando sobre um sorteio, um desconto, um prêmio; ao utilizá-lo, a pessoa que o leu será levada para uma página falsa solicitando dados para receber o que está escrito no cartaz.

É importante ter cuidado para não se deixar levar por esses ataques, verificar a fonte das mensagens, pensar antes de passar alguma informação, principalmente

se, de alguma forma, isso envolver dados sigilosos. Além disso, cuidar quando sites e aplicativos pedem autorizações e baixar aplicativos direto da fonte oficial são meios de evitar possíveis incômodos. Mesmo que o antivírus não seja perfeito, ele dará uma camada de proteção aos dados pessoais do usuário. Ademais, a utilização de múltiplas senhas em diferentes lugares, sempre uma sequência forte (para isso, deve conter letras maiúsculas e minúsculas, números e caracteres especiais de forma aleatória), é mais uma barreira contra os ataques. Vale ressaltar que, para organizar essas senhas, existem gerenciadores delas, assim não é preciso ficar lembrando uma sequência muito complexa a cada uso de algum site ou aplicativo, por exemplo. Por fim, não se expor muito nas redes sociais, de preferência mantendo a conta privada, apenas com conhecidos, é mais um reforço para a segurança virtual, visto que informações do que se gosta, de onde se está, de amigos, de familiares são perigosas se deixadas expostas para qualquer um.

## 4. CONCLUSÃO

Conclui-se, então, que um ataque, em geral, funciona com os seguintes passos: coleta de dados, análise de dados, modelagem do ataque e a execução. Como se pode ver, são bem planejados e é indispensável ter cuidado ao gerenciar dados.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

ARIMURA, Mayumi. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros**. E-GOV. 2016. Disponível em:

<https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros> Acesso em: 11 de abril de 2022.

BAZZELL, Michel. **Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information**. 2016. Createspace Independent Publishing Platform, 5ª Edição.

ESET. **ESET issues its Q4 2020 Threat Report recording a massive increase in RDP attack attempts since Q1**. 2021. Disponível em: <https://www.eset.com/us/about/newsroom/press-releases/eset-issues-its-q4-2020-threat-report-recording-a-massive-increase-in-rdp-attack-attempts-since-q1-1/> Acesso em: 29 de junho de 2022.

KALI. **Kali Tools**. Disponível em: <https://www.kali.org/tools/> Acesso em: 21 de agosto de 2022.

LABS, MalwareBytes. **White hat, black hat, grey hat hackers: What's the difference?**, 2021. Disponível em: <https://blog.malwarebytes.com/101/2021/06/white-hat-black-hat-grey-hat-hackers-whats-the-difference/> Acesso em: 11 de abril de 2022.

MORENO, Daniel. **Introdução ao Pentest**. 2015. Novatec Editora, 1ª Edição.

TECH, Noomis FEBRABAN. **Ataque cibernético afeta 83% das empresas nas Américas nos últimos 12 meses**. 2022. Disponível em: <https://noomis.febraban.org.br/blog/ataque-cibernetico-afeta-83-das-empresas-nas-americas-nos-ultimos-12-meses> Acesso em: 11 de abril de 2022.

TECH, Noomis FEBRABAN. **Brasil tem alta de 200% nos ataques de engenharia social em 2020**. 2021. Disponível em: <https://noomis.febraban.org.br/temas/seguranca/brasil-tem-alta-de-200-nos-ataques-de-engenharia-social-em-2020> Acesso em: 11 de abril de 2022.

TOOLKIT, The Social-Engineer. (SET). **Trustedsec**. Disponível em: <https://github.com/trustedsec/social-engineer-toolkit> Acesso em: 21 de agosto de 2022.

WEB, Jamie. **Lookalike Domain Names Test**. Disponível em: <https://www.jamieweb.net/apps/lookalike-domains-test/> Acesso em: 21 de agosto de 2022.