FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

INTRUSÃO EM REDES DE COMPUTADORES

COMPUTER NETWORK INTRUSION

INTRUSIÓN EN LA RED INFORMÁTICA

Geovane Ganeo[1]

Jhemesson Santos da Silva[2]

Cleberson Eugenio Forte[3]

RESUMO

Quando falamos em segurança de informação, logo pensamos em sistemas de computadores altamente protegidos por criptografia, senhas e códigos, mas também nos questionamos se mesmo com todas essas medidas de segurança nossos sistemas ainda estão a salvo de invasões por pessoas mal intencionadas. Com o aumento no desenvolvimento de produtos inteligente que possuem acesso à internet, dispositivos como computadores, smartphones e tablets estão diariamente sujeitos a invasões criminosas por meio de falhas em seus sistemas de defesas, e essas falhas podem ocasionar situações indesejadas para as empresas tal como, roubo de dados, vazamento de informações ou até mesmo a indisponibilidade de serviços. Esse artigo apresenta as etapas seguidas pelo “hacker ético”, um profissional da segurança da informação que busca desenvolver temas como a detecção, prevenção e respostas a intrusões de redes de computadores.
Palavras-chave: Segurança. Hacker ético. Redes. Intrusão. Sistemas.

ABSTRACT

When we talk about information security, we immediately think of computer systems highly protected by encryption, passwords, and codes, but we also wonder if even with all these security measures our systems are still safe from invasions by malicious people. With the increase in the development of intelligent products that have access to the internet, devices such as computers, smartphones and tablets are daily subject to criminal invasions through flaws in their defense systems, and these flaws can cause unwanted situations for companies such as, data theft, information leakage or even unavailability of services. This article presents the steps followed by the “ethical hacker”, an information security professional who seeks to develop topics such as detection, prevention, and responses to computer network intrusions
Keywords: *Safety. Ethical hacker. Networks. Intrusion. Systems.*

INTRODUÇÃO

Os cibercrimes são infrações executadas ou que envolvam práticas ilícitas nas redes, os relatos desse tipo de crime têm aumentado consideravelmente com o passar dos anos e dentre eles os mais comuns são as violações de privacidade por meio de intrusão.

As invasões de redes de computadores são um dos principais métodos utilizado pelos *hackers* para poderem obter informações desejadas, essas entradas ilegais geralmente ocorrem por falhas humanas que resultam em brechas nos sistemas de segurança permitindo o acesso a dados sensíveis de extremo sigilo, tais como folha salarial, projetos em desenvolvimento ou até mesmo senhas de clientes, por pessoas que não possuem autorização para acessar esses dados.
Com o sancionamento da lei geral de proteção de dados em 2018 pelo governo brasileiro, as empresas estão cada vez mais buscando no mercado de trabalho por profissionais qualificados da área da segurança da informação para que possam atuar na parte de desenvolvimento de melhorias e métodos para que seus sistemas fiquem cada vez mais seguros e confiáveis.

1 O PROFISSIONAL: HACKER ÉTICO

O *hacker* ético é um profissional de segurança da informação especializado em *Offensive Security*, comumente chamado de "*red team*" pelas empresas, ou seja, atua na parte da cibersegurança focada em testes de invasão com a finalidade de identificar e corrigir vulnerabilidades existentes principalmente em redes cabeadas, redes sem fio ou aplicações web.

Para realizar um trabalho como esse é necessário que o profissional possua muito conhecimento técnico em áreas como programação e rede de computadores, além de um excelente conhecimento das tecnologias existentes no mundo da informática como um todo, isso permite que o *hacker* não atue somente no mercado de trabalho como um *pentester*, mas podendo também trabalhar como programador, administrador de redes, ser membro de um CSIRT (*Computer Security Incident Response Team*) entre outras atividades que envolvam segurança da informação.

Ainda sobre o mercado de trabalho para um *hacker*, ele pode atuar como autônomo nos programas de *Bug Bounty*, programas de recompensas de *bugs* oferecidos por muitos sites, empresas e desenvolvedores de *software* pelo qual os *hackers* são remunerados por relatar *bugs*, especialmente aqueles relativos a explorações e vulnerabilidades. Um dos maiores programas de *bug bounty* conhecidos no mundo é o do Facebook, onde recentemente em outubro de 2020, um adolescente de 14 anos chamado Andrés Alonso Bie Perez, de Nova Lima (MG), recebeu uma recompensa de 25 mil dólares (equivalente a 140 mil reais na cotação da época em que a recompensa foi paga) por relatar um bug no Instagram.

Não existe uma faculdade que empregue o título de hacker ético, porém existem certificações relacionadas a área. Uma das primeiras, que surgiu em meados de 2004/2005 é a "CEH" (*Certified Ethical Hacker*) disponibilizada pela EC-Council e considerada uma ótima opção para quem deseja iniciar na área, inclusive foi a responsável pela popularização do termo Hacker Ético. Existem outras como "*Ethical Hacking Foundation*" disponibilizada pela Exin, a *Giac Certified Penetrarion Tester* e *Giac Web APP Pen Tester* e a OSCP (*Offensive Security Certified Professional*), sendo esta última a mais "complexa" em conhecimento técnico por exigir um pouco mais de conhecimentos no desenvolvimento de *exploits* (algoritmos utilizados para a exploração de uma falha conhecida) e programação para melhorar e desenvolver ferramentas utilizadas durante o teste de penetração.

2 PERFIRS DE HACKERS

Os *white hat* são *hacker* que não utilizam os seus conhecimentos para fazer ataques ilegais, eles geralmente são consultores de segurança que são contratados por empresas para prestarem serviços como testes de invasões a fim de tentar encontrar alguma brecha nesses sistemas testados, esse tipo de hacker precisa sempre estar em constante evolução para acompanhar o crescimento das ferramentas disponíveis no mercado, pois é necessário conhecer as novas técnicas e métodos utilizados para as invasões serem feitas.

Já os *black hat* são os tipos mais conhecidos de *hackers*, eles usam as suas técnicas para invadirem computadores e infectar sistemas de forma ilegal, os white hat travam uma guerra constante contra os black hat pois enquanto eles estão sempre buscando melhorar os sistemas de segurança os outros hackers estão procurando uma forma de destruir esses sistemas.

Entre os *black hat* e os *white hat* existem os *gray hat* que são *hackers* que apesar de não utilizarem suas habilidades para obter vantagens, eles não operam dentro das leis e nas normas das empresas, os *gray hat* geralmente invadem os sistemas das empresas para demonstrar que existem falhas de segurança.

Culturalmente os *gray hat* não solicitam diretamente um valor para manter em sigilo as falhas encontradas, mas casualmente acontecem convites das empresas para esses *hackers* fazerem parte da equipe de segurança pois eles conseguem demonstrar um conhecimento amplo de seus sistemas e seus pontos fracos.

Script Kiddie é uma forma depreciativa como são conhecidos os hackers iniciantes que tem curiosidade e vontade de aprender mais sobre as técnicas de invasão, esse tipo de invasor geralmente não tem muito conhecimento sobre os métodos utilizado por profissionais mais experientes e utiliza softwares básicos baixados na internet para tentar um ataque, mas normalmente não conseguem alcançar os seus objetivos.

3 TIPOS DE ATAQUES

Segundo Lima (2018), os sistemas de defesas cibernéticas Brasileiras não exercem o seu papel principal, e deixa a deseja em inúmeros tipos de ataques ao país, não somente no plano estatal, mas também da sociedade e das corporações, o Brasil se destaca de outros países da americana latina recebendo em média milhões de tentativas de violações por dia.

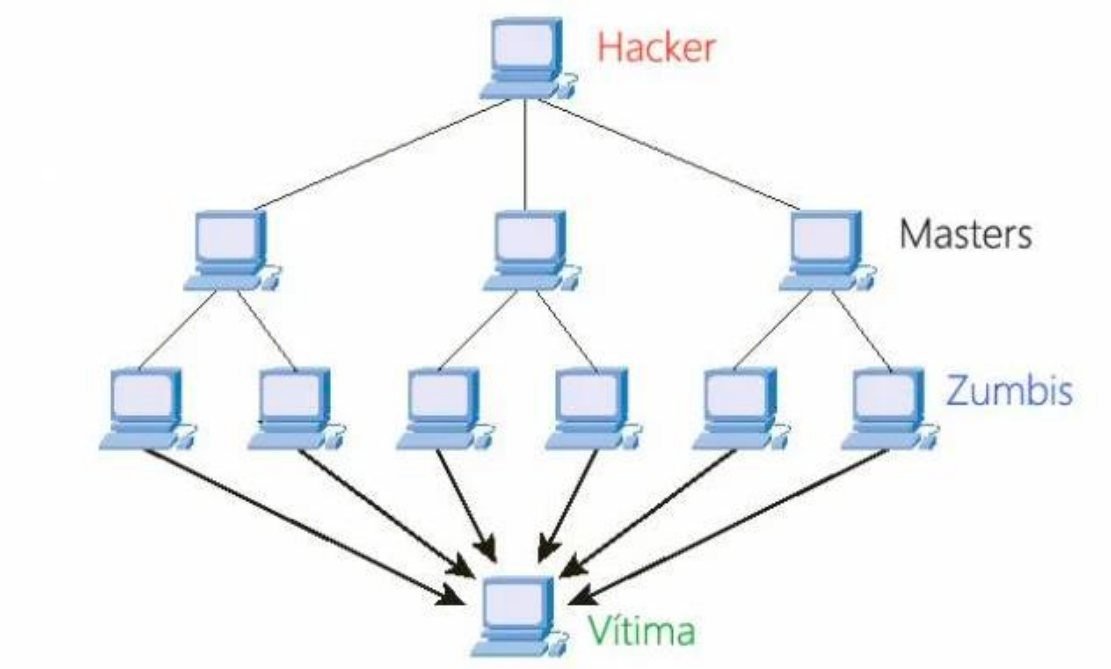
De acordo com Assunção (2014), para que possamos entender um pouco mais sobre os cibercrimes e seus reais danos, precisamos antes de tudo conhecer quais são os principais métodos de ataque utilizado pelos infratores. Também é possível encontrar listas das vulnerabilidades mais exploradas separadas por tipo e data no site *Common Vulnerabilities and Exposures* (cve).

3.1 Ddos

Um dos principais e mais conhecidos tipos de ataque, o DDoS (*Distributed Denial of Service*) é um método que utiliza a negação de serviços onde seu principal objetivo é o envio de inúmeros pedidos de pacotes para sua vítima afim de causar uma sobrecarga nos servidores resultando em lentidões ou até mesmo indisponibilidade de acesso ao serviço desejado.

É comum em um ataque DDoS um computador principal coordenar diversos outros computadores para acessar o servidor alvo ao mesmo tempo, transformando assim os computadores em espécies de zumbis seguindo ordens superiores, o que chamamos de *botnet* como demonstrado na figura 1.

Figura 1 – Método DDoS retratado



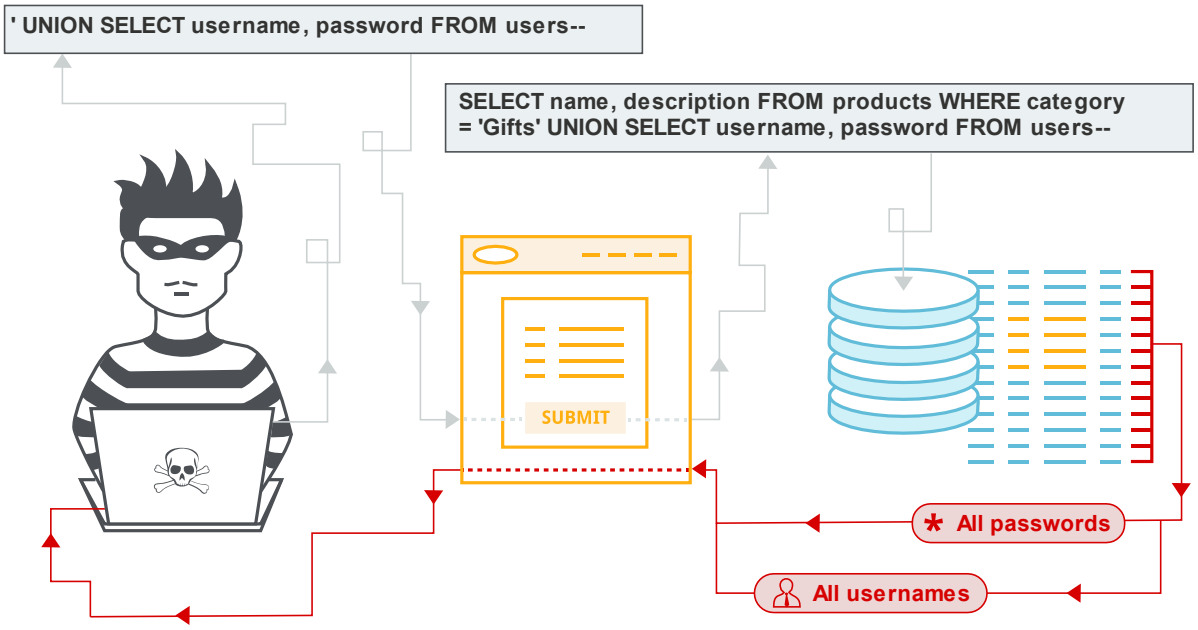
Fonte: https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/

3.2 Sql injection

Sql injection é uma técnica fundamentada na manipulação de uma linguagem utilizada para fazer a troca de informações entre aplicativos e bancos de dados relacionais, a linguagem SQL (*Standard Query Language*).

Como descrito por Moreno (2017), essa técnica consiste em trocar ou inserir consultas que a aplicação requisita diretamente do banco de dados conforme o exemplo da figura 2, o ataque tem como alvo a obtenção de informações sigilosas, burlando telas de login para conseguir acesso não autorizado ou até mesmo a destruição de dados.

Figura 2 – Demonstração de um ataque sql



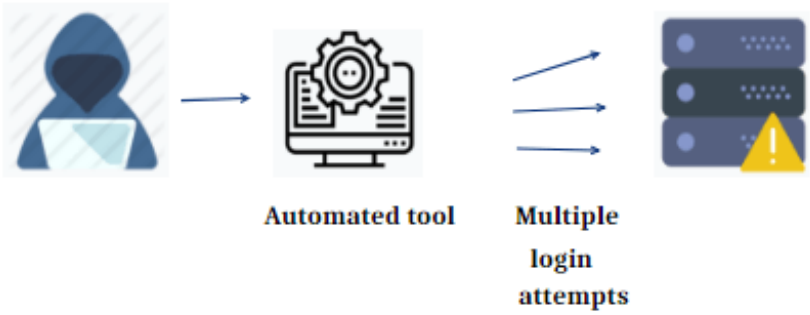
Fonte: https://portswigger.net/web-security/sql-injection

3.3 Brute force

Para Doiro (2019), no meio de diversos ataques de segurança realizados na internet, os ataques de força bruta dependem de os atacantes conseguirem adivinhar, logins e senhas de acesso de usuários legítimos por meio de tentativa e erro, exemplificado na figura 3.

Esse tipo de ataque pode ser feito de forma manual preenchendo os campos de login e senhas e realizando as tentativas de entrada ou de forma automática, onde um software executa uma lista de palavras chaves salvas em um arquivo.

Figura 3 – Funcionamento de um ataque brute force



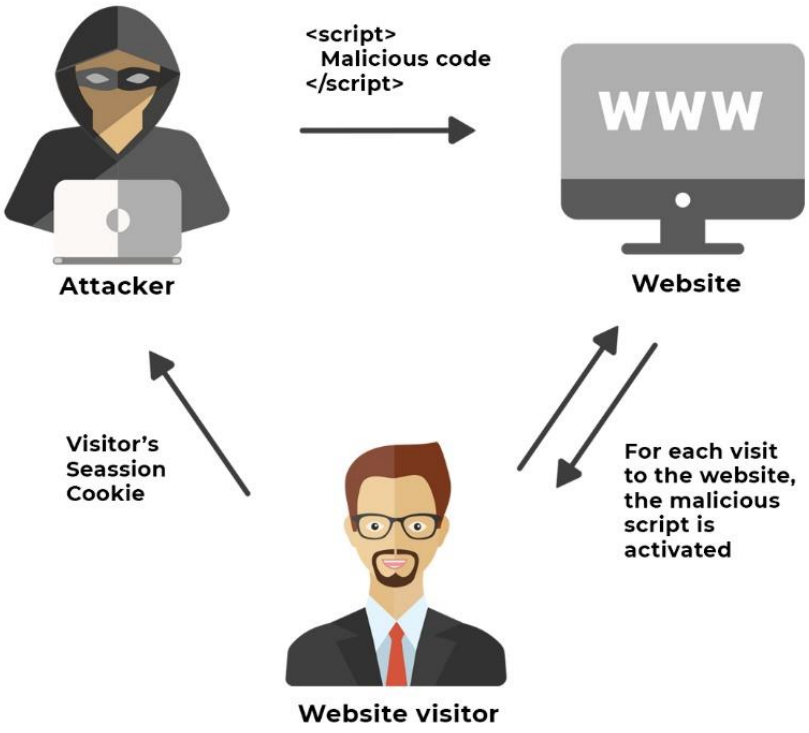
Fonte: https://www.manageengine.com/log-management/cyber-security-attacks/what-is-brute-force-attack.html

3.4 Cross-site scripting

O *Cross-Site Scripting* (XSS) é uma vulnerabilidade que geralmente ocorre nas aplicações web em que possibilita o atacante inserir códigos que na maioria das vezes são *java script* sem nenhum tipo de verificação ou tratamento para obter privilégios sobre a sua vítima, como ilustrado na figura 4.

Para explorar esse tipo de vulnerabilidade o atacante precisa de algum "formulário" que permita a interação como por exemplo os campos de inserção de comentário de algum fórum, campos de busca ou até mesmo como no caso da vulnerabilidade reportada pelo hacker ético e pesquisador de vulnerabilidades em aplicações web Gabriel Pato, elaborador da palestra de título "Cross-site Scripting continua sexy" que ocorreu em novembro de 2018 em um dos maiores eventos mundiais de segurança da informação (Roadsec), o próprio calendário do outlook.

Figura 4 – execução de um ataque xxs



Fonte: https://digitalartsagency.com/?blog-posts=cross-site-scripting-vulnerability

4 PRINCIPAIS VUNERABILIDADES

A maior preocupação de empresas que tem informações importantes armazenadas, é sua capacidade de garantir a integridade e confidencialidade desses dados, e mesmo com esse cenário os incidentes que acontecem nas empresas geralmente são provocados por causas parecidas.

Por se tratar uma área de prevenção e não trazer um retorno imediato, é muito comum em empresas a falta de investimento na área de segurança de TI (Tecnologia de informação), e essa falta de capital podem causar sérios riscos a seguridade dos dados, pois softwares desatualizados são sempre um grande alvo os para os atacantes.

O treinamento dos funcionários é essencial para que eles possam ter pleno conhecimento das medidas básicas de proteção, tendo em vista que a maioria dos malwares aparentam ser inofensivos e seu real perigo só é revelado quando alcançam seus objetivos.

Um outro motivo para a falta de segurança é a carência de restrições de acesso, os sistemas de uma empresa devem ter limitações do alcance pelos usuários conforme as suas necessidades, é indispensável que um funcionário só possa acessar informações que são necessárias para ele e que não ter livre acesso por toda rede.

As empresas devem sempre ter um plano de contingência para minimizar os danos caso seus sistemas sejam comprometidos, o backup é a forma mais segura de garantir uma cópia das informações em casos de perdas, é importante que se estabeleça uma rotina de *backup* e que os profissionais assegurem o cumprimento dela.

5 TIPOS DE PENETRATION TEST

Existem três tipos de serviços de *pentest* que podem ser realizados para identificar as vulnerabilidades em qualquer empresa, sendo eles o *black box, white box e gray box.*

5.1 Black box

Recomendado para empresas que já possuem um nível de segurança mais trabalhado, com políticas de segurança desenvolvidas e uma equipe sólida de TI, este é o teste de maior custo, porém que mais se aproxima da realidade de um ataque externo.

Em um ataque real, o *hacker* inicialmente não possui muitas informações sobre a infraestrutura de TI do alvo, portanto na contratação de um *black box* não são reveladas ao *pentester* nenhuma informação como faixa de endereçamento ip, procedimentos internos da empresa, arquitetura de *software* ou qualquer outra informação que necessite conhecimento interno.

Dessa maneira o *black box* também é o teste que mais demanda tempo para ser realizado, e vai dar a quem contrata uma visão de como um atacante enxergaria a empresa, colocando em teste as medidas de segurança já existente, expondo as falhas e vulnerabilidades para que possam ser continuamente aprimoradas.

5.2 Gray box

Esse tipo de teste é um meio termo entre o *white box e o black box*, com o intuito de mostrar até onde um funcionário de determinado departamento conseguiria chegar caso tivesse intenções negativas por exemplo, são fornecidas ao pentester informações parciais sobre a rede e infraestrutura de TI, como por exemplo faixa de endereços IPs utilizadas na sub-rede, endereço IP do *Gateway* e do servidor DNS.

Com essas informações em mãos, a equipe ou o profissional que vai executar o teste vai ter um tempo e dificuldade menor quando comparado ao *black box*, porém ainda um pouco mais demorado e com mais obstáculos que durante um *white box.*

5.3 White box

Recomendado para empresas que ainda estão desenvolvendo sua estrutura de TI, o *white box* é o completo oposto do *black box.*

Nesse tipo de teste é fornecido ao profissional que vai realizar o trabalho total conhecimento da infraestrutura de TI da empresa, desde equipamentos de rede até sistemas operacionais utilizados e endereçamentos, podendo se comparar aos conhecimentos que um administrador da rede que trabalha internamente teria.

Naturalmente pela quantidade de informações fornecidas no início do trabalho, o *white box* pode ser realizado em um período muito menor quando comparado ao *black box.*

6 FASES DE UM PENTEST

As fases de um pentest são o passo a passo técnico que o profissional percorre, e os mesmos que um invasor percorreria ao tentar conseguir acesso a um sistema de maneira indevida e sem nenhuma autorização.

É importante ressaltar que antes de se iniciar o processo na prática, é necessário que ambas as partes, ou seja, tanto o profissional ou equipe que vai realizar o teste quanto o cliente se reúnam para decidir além do tipo de serviço contratado (*black box, white box ou gray box*), o escopo dos testes que será realizado.

Este deve conter informações como quais áreas, departamentos, equipamentos, softwares irão ser testados, os dias e horário em que os testes serão realizados e os limites que o cliente deseja impor para o profissional, como por exemplo caso encontre uma falha que possa o levar a ter acesso a algum conteúdo confidencial e a utilização ou não de técnicas de engenharia social.

O cliente também deve estar ciente do risco de eventuais imprevistos que podem ocorrer, como a indisponibilidade de algum serviço durante uma tentativa de DDOS por exemplo, e o profissional que está realizando o teste deve sempre ter um contato da empresa a quem recorrer quando algum desses imprevistos acontecerem. Isso tudo deve ser conversado, acordado e firmado em contrato que deve ser validado por alguém do departamento jurídico da empresa contratada, garantindo que nenhum crime digital está sendo cometido.

Para (ASSUNÇÃO 2015) o cronograma para a realização de um teste viária de acordo com os fatores: quantidade de tarefas que necessitam ser realizadas, a quantidade de ativos da empresa que será testado e a carga horaria diária para a realização completa do teste.

6.1 Footprinting

Para Engebretson (2013), *footprinting* é o primeiro passo de um *pentest*, é aqui que através de técnicas como por exemplo *google hacking* e pesquisas a bancos de dados *whois* o profissional vai levantar o máximo de informações possível para se construir uma base, que juntamente com as etapas seguintes irão direcionar o rumo dos testes.

Normalmente boa parte do tempo total de duração do *pentest* é gasto nessas fases iniciais, já que são essas informações que vão ajudar a garantir uma boa qualidade de todo o processo.

6.2 Varredura

Como demonstrado por Moreno (2019), nessa segunda etapa serão utilizadas ferramentas de mapeamento de rede como por exemplo o nmap, e pacotes ICMP (ping) para se descobrir o máximo sobre os componentes da rede. Como dispositivos e sistemas operacionais utilizados por eles, portas abertas, serviços rodando e até mesmo a versão desses componentes para verificar a existência de alguma falha conhecida em versões obsoletas.

É juntando o resultado dessas duas primeiras etapas que a invasão passa a ter uma forma e tomar caminhos mais específicos que vão depender desses resultados.

6.3 Análise de vulnerabilidade

Depois de feita a coleta inicial de informações nas duas primeiras etapas, o *hacker* vai enumerar e analisar tudo o que foi coletado para começar a traçar um plano de ataque.

Começando pela procura por falhas e problemas observando os sistemas operacionais utilizados, serviços e suas versões. Também são utilizadas algumas ferramentas como *scanners* de vulnerabilidades para facilitar e agilizar o procedimento.

Depois de separar as possíveis falhas o profissional começa a se preocupar em como burlar os mecanismos de defesa como por exemplo *firewalls*, antivírus ou IDS's (*Intrusion detection System* ou Sistema de detecção de Intrusão).

6.4 Exploração de falhas

Depois de escolher o tipo de ataque e a falha a ser explorada, o profissional vai efetivamente explorá-la para conseguir ganhar o acesso ao sistema, se nenhuma falha seja encontrada, também é possível se explorar configurações fracas ou até mesmo se pensar em um ataque de negação de serviço para derrubar o sistema.

Caso esteja dentro do escopo, também é possível a utilização de técnicas de engenharia social como o *phishing*, para instalação de *trojans*, *keyloogers* ou outras ferramentas como demonstrado por Weidman (2014) no livro Testes de Invasão: uma Introdução Prática ao Hacking. Além disso em casos em que há a existência de redes públicas não criptografadas, existe a possibilidade de se obter informações com a utilização de *sniffers* (analisadores de pacote) para se realizar um ataque de MITM (*man-in-the-middle*), como citado por Moreno (2016) no livro Pentest em redes sem fio.

6.5 Mantendo o acesso

Após o hacker ter conseguido o acesso ao sistema e cumprido o objetivo principal, é hora de garantir que caso necessário seja possível retomá-lo mais tarde. Isso pode ser feito de diversas maneiras, sendo a mais comum com a instalação de uma porta dos fundos (*backdoor*).

6.6 Cobrindo os rastos

Na penúltima etapa do teste o hacker vai se preocupar em apagar as evidências de que ele esteve no sistema. Isso envolve vários aspectos que vão desde esconder o IP de origem com a utilização de redes tor ou servidores próprios até a exclusão de logs e a utilização de *rootkits* (programas utilizados para esconder a existência de alguns processos ou serviços que estão rodando, como por exemplo um possível backdoor instalado pelo *hacker*, de métodos comuns de detecção).

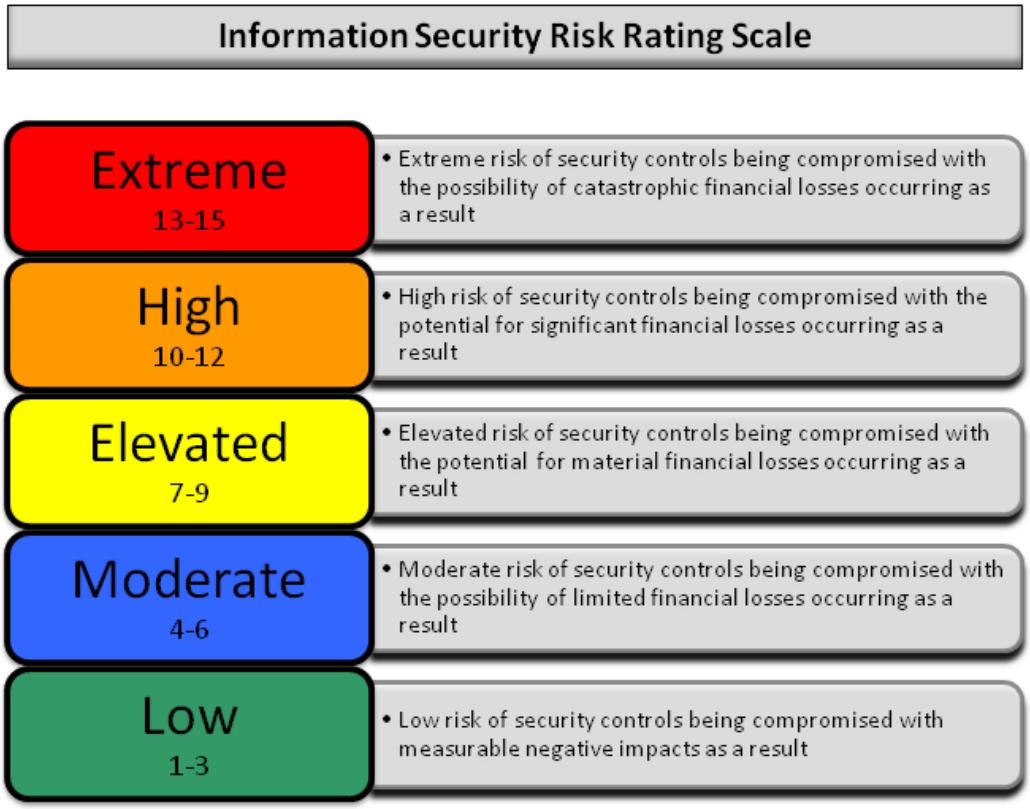
6.7 Evidência e Report

Nesta etapa final, é onde o profissional vai apresentar os resultados de todo o trabalho. Isso é feito através da entrega de dois documentos distintos, um laudo técnico e um sumário executivo.

6.8 Sumário executivo

Esse documento como evidenciado na figura 5 será entregue para o setor tático/estratégico da empresa, como por exemplo o *CEO* que contratou o *pentest*, portanto não será composto com foco nas especificações técnicas das falhas encontradas e sim em mostrar de forma mais visual, com gráficos e tabelas as informações sobre os problemas encontrados classificados por impacto e o risco que podem causar (como por exemplo baixo, moderado, extremo) e sugestões para corrigi-los.

Figura 5 – Exemplo de sumário executivo



Fonte: http://www.pentest-standard.org/index.php/Reporting

6.9 Laudo Técnico

Diferente do sumário executivo, o laudo técnico vai ser entregue para a equipe te TI da empresa, portanto contém descrições completamente detalhadas e técnicas sobre todas as falhas encontradas, bem como o caminho seguido desde o levantamento de informações até os passos que levaram a exploração efetiva da falha (incluindo capturas de tela, comandos e ferramentas utilizadas) e sugestões de correção e melhorias.

7 PRINCIPAIS MOTIVADORES DO ATACANTE

Mesmo com o fato de as falhas de segurança geralmente serem parecidas, os motivadores para um atacante realizar suas violações são diversos, sendo desde razões pessoais ou até mesmo por causas ideológicas.

Não conseguimos precisar ao certo o número de motivações existente porque a maioria dos ataques hackers não são reportados e nem divulgados, mas conseguimos listar as principais e mais populares causas desses ataques.

7.1 Curiosidade

Conhecida como a porta de entrada para esse universo, a curiosidade é provavelmente o principal motivador dos hackers iniciantes, o *hacker* vê a necessidade de testar seus limites dedicando muitas horas do seu dia para poder praticar as suas técnicas e descobrir se é possível conseguir seus objetivos.

A curiosidade de um *hacker* também é responsável por fazer que ele estude novas linguagens de programação e aprenda cada vez mais técnicas avançadas de ataques, possibilitando que seus conhecimentos na área avancem explorando novas falhas e brechas.

7.2 Razões financeiras

Talvez o motivo mais popularmente conhecido, muitos *hackers* fazem ataques direcionados com a intenção de pagamentos ou recompensas financeiras, esses ataques geralmente são feitos em empresas, bancos ou até mesmo contra pessoas físicas.

Contra as empresas é muito comum o ataque de *ransomware* que consiste na execução de um *malware* (software malicioso) por meio de *links* em *e-mails*, downloads ou até mesmo portas UBS, esse *software* contamina a rede da empresa e criptografa os dados armazenados em seus sistemas, possibilitando que os atacantes exijam pagamento de regaste para poder liberar as empresas a terem acesso aos seus dados novamente.

7.3 Liberdade

A censura da internet não é novidade em diversos locais do mundo, é muito comum em países em que se há restrições de internet o surgimento de grupos de *hackers* buscando a liberdade de expressão e o livre acesos a rede.

Essa censura de alguns países normalmente é feita pelo fato de os governos controlarem o que pode ser acessado ou não pela população e por eles terem o monopólio dos provedores de internet, em alguns locais até se tem a possibilidade de acessar outros sites que não são os indicados pelo governo, mas os valores cobrados para ser feito esse acesso geralmente acabam sendo inviáveis e abusivos.

7.4 Vingança

Uma prática que não é muito comum em empresas, mas pode ser muito perigosa quando realizada é a retaliação profissional, normalmente esse tipo de quebra de regras acontece quando um funcionário se sente desrespeitado por seus contratantes e acaba colocando a integridade dos dados da empresa em risco.

Normalmente esse tipo de motivação ocorre após uma demissão em que o colaborador se sente injustiçado ou até mesmo uma promoção de cargo que foi dada para outro funcionário, desencadeando um ataque que pode comprometer os sistemas da empresa dependendo no nível de acesso desse funcionário.

7.5 Hacktivismo

Criado pela junção das palavras *hackers* e ativismo, o hacktivismo é um novo modo de protestar criado nos anos 90 que busca o objetivo de uma sociedade onde as informações nas redes possam ser confiáveis e disponíveis, os hacktivistas são conhecidos por sempre lutarem por justiça e divulgarem muitos dos seus ideais pela internet.

O hacktivismo ganhou muitos apoiadores com os surgimentos de novas ferramentas, com a facilidade de apenas baixar e executar um *software* ou até mesmo somente acessar uma página web e já estar ajudando, esse movimento conseguir derrubar sites de agencias importantes como, a Agência Nacional de Telecomunicações (ANATEL), Agência de Segurança Nacional (NASA) ou até mesmo instituições financeiras como mostrado na figura 6.

Figura 6 – Site hsbc derrubado por hacktivistas

Fonte: https://www.plantaonerd.com/blog/2012/02/02/site-do-hsbc-e-derrubado-por-hackers/

8 EXEMPLOS DE AÇÕES PREVENTIVAS

Por menor que seja uma tentativa de invasão sofrida por uma empresa, é sempre indispensável que ela tenha métodos para evitar vazamentos de dados ou indisponibilidades de serviços, e se manter segura contra os diversos tipos de ataques utilizados pelos cibercriminosos.

É essencial para uma empresa ter uma política de segurança sempre atualizada e que cumpra todas as suas necessidades abordando todos os departamentos, os softwares devem estar sempre em sua última versão para evitar que *hackers* utilizem de falhas corrigidas nas atualizações e assim conseguirem comprometer a segurança dos dados.

Um sistema de autenticação de dois fatores é indispensável para funcionários com mais privilégios de acesso, esse sistema garante que os funcionários tenham as suas senhas pessoais e uma segunda senha gerada automaticamente e que tenha uma validade predeterminada podendo variar de segundos a um dia completo.

É necessária uma limitação de acesso por meio horários e dias sendo personalizado para cada funcionário conforme sua jornada de trabalho e uma limitação de computadores que ele pode utilizar, para evitar que alguém faça o login com as suas credenciais em horários fora de serviço ou até mesmo em departamentos diferentes da empresa, isso garante uma segurança para os sistemas e até mesmo para o funcionário.

9 CONCLUSÕES

Esse artigo buscou abordar um tema em total ascensão, trazendo informações relevantes sobre o profissional da área de segurança da informação e a sua realidade, conclui-se que com a evolução digital e a necessidade crescente em segurança de dados, o profissional dessa área se torna cada dia mais indispensável para as empresas.

É necessária uma visão diferente por parte das empresas quando falamos de segurança da informação, é preciso encarar o capital aplicado nos setores de segurança como investimos para se manterem seguros e não ver como um gasto.

Ainda temos uma grande necessidade de conhecimento para que o mercado de cibersegurança brasileiro se torne mais forte, mas com a divulgação de temas como esse apresentado trazemos uma visão diferente do profissional de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSUNÇÃO, Marcos F. **Segredos do Hacker Ético**. 5. Florianópolis: Visual Books, 2014.

ASSUNÇÃO, Marcos Flávio Araújo. **Análise de eficiência na detecção de vulnerabilidades em ambientes web com o uso de ferramentas de código aberto**. 2014. Dissertação (Mestrado em Sistemas de Informação) - Universidade Fumec, [S. l.], 2014.

DIORIO, Rafael Fernando; SERAFIM, Edivaldo; ALVES, Karlan Ricomini; MEIRA, Matheus Carvalho. **Ataques de Força Bruta: Um Estudo Prático**. Disponível em: <http://lcv.fee.unicamp.br/images/BTSym-19/Papers/040.pdf>. Acesso em: 20 out. 2020.

ENGEBRETSON, Patrick. **Introdução ao Hacking e aos Testes de Invasão**. São Paulo: Novatec, 2013.

LIMA, Victor Hugo. **Hacktivismo e a Defesa Cibernética do Brasil**. Disponível em: <http://www.ebrevistas.eb.mil.br/index.php/CEEExAE/article/view/1576/1343>. Acesso em: 22 out. 2020.

MORENO, Daniel. **Introdução ao Pentest**. 2. São Paulo: Novatec, 2019.

MORENO, Daniel. **Pentest em Aplicações web**. 1. São Paulo: Novatec, 2017.

MORENO, Daniel. **Pentest em Redes sem fio**. 1. São Paulo: Novatec, 2016.

WEIDMAN, Georgia. **Testes de Invasão: uma Introdução Prática ao Hacking**. 1. São Paulo: Novatec, 2014.

REPORTING. **Pentest-standard,** 2020. Disponível em: <http://www.pentest-standard.org/index.php/Reporting>. Acesso em: 19 de out. de 2020.

VULNERABILITY by type. **cve details**, 2020. Disponívelem: <https://www.cvedetails.com/vulnerabilities-by-types.php>. Acesso em: 19 de out. de 2020.

Faculdade de Tecnologia de Americana

Geovane Ganeo

Jhemesson Santos da Silva

INTRUSÃO EM REDES DE COMPUTADORES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.

Área de concentração: Segurança da informação

Americana, 14 de dezembro de 2020.

Banca Examinadora:

_____

Cleberson Eugenio Forte (Presidente)

Doutor

Faculdade de Tecnologia de Americana

_____

Renato Kraide Soffner (Membro)

Doutor

Faculdade de Tecnologia de Americana

_____

Maria Elizete Luz Saes (Membro)

Mestre

Faculdade de Tecnologia de Americana