ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DR. SOLON TAVARES
CURSO TÉCNICO EM REDES DE COMPUTADORES

Pedro Henrique Pereira

ÉTICA HACKER E COMO UM PENTEST PODE AUXILIAR NO ESCANEAMENTO DE VULNERABILIDADES

Guaíba, RS
2021/1
Pedro Henrique Pereira

ÉTICA HACKER E COMO UM PENTEST PODE AUXILIAR NO ESCANEAMENTO DE VULNERABILIDADES

Trabalho de Conclusão de Curso apresentado à Escola Estadual de Educação Profissional Dr. Solon Tavares como requisito parcial para a obtenção do título de Técnico em Redes de Computadores.

Orientador: Profª. Aline Teresinha Velloso

Co orientadora: Profª. Ingrid Silva dos Santos

Guaíba, RS

2021/1

Pedro Henrique Pereira

ÉTICA HACKER E COMO UM PENTEST PODE AUXILIAR NO ESCANEAMENTO DE VULNERABILIDADES

Trabalho de Conclusão apresentado à Escola Estadual de Educação Profissional Dr. Solon Tavares como requisito parcial para obtenção do título de **Técnico em Redes de Computadores**

Aprovado em _____/_____/_____

BANCA EXAMINADORA

_____

Prof.ª Projeto Técnico: Ingrid Silva dos Santos. Licenciatura em Computação. FACOS

_____

Prof. Orientadora: Aline Teresinha Velloso. Pós Graduada em Sistemas de Segurança da Informação. Unisul

_____

Prof. Avaliador: Robson Arndt Salvadori. Mestre em Letras. Universidade Feevale

Dedico aos meus pais, por todo apoio e incentivo no término deste trabalho. Sou muito grato a coragem me dada para não desistir.

AGRADECIMENTOS

Agradeço principalmente aos meus professores, em especial a minha professora orientadora Aline Teresinha Velloso e a professora de projeto técnico Ingrid Silva dos Santos,

pelo apoio e as instruções durante o desenvolvimento do trabalho.

Não menos importante, aos meus pais e meu irmão, que sempre foram atenciosos sobre o meu tempo dedicado ao trabalho, e os incentivos dados pelos mesmos, o que acarretou para a conclusão deste curso.

"Os gênios vivem apenas uma história de loucura"

Arthur Schopenhauer

RESUMO

Por meio de pesquisas e de uma enquete online, foi organizado um gráfico que certifica que muitas pessoas, mesmo possuindo meios de pesquisa, ainda desconhecem o real significado da palavra hacker e a ética por trás da profissão, além de consequentemente não ter o conhecimento da função exercida pelo profissional e as etapas de seu trabalho em análise de vulnerabilidades. Tendo em vista o cenário atual, onde a tecnologia evolui cada vez mais, o uso de computadores tende a aumentar, e possibilitando invasões a redes por pessoas não autorizadas, um profissional em pentest é o indivíduo que neste cenário tecnológico, poderá evitar invasões aos sistemas, além de fortalecer a rede local. A fim de mostrar a importância que tem um profissional em hacking em nossa sociedade, é necessário ter em mente a função que ele exerce, de acordo com a própria ética de conduta, assim como o funcionamento de uma varredura de vulnerabilidades, e suas etapas. Diante disso, possuir um conhecimento maior sobre este assunto poderá abrir portas não somente para o profissional em pentest, mas também para si mesmo, na nossa sociedade moderna, a necessidade de uma rede segura e robusta é de suma importância para manter nossas informações longe de indivíduos com má índole.

Palavras-chave: Ética hacker. Análise de vulnerabilidades. Segurança da informação. Proteção.

ABSTRACT

Through surveys and an online poll, a graphic was organized that certifies that many people, even with the means of research, still unaware of the real meaning of the word hacker and the ethics behind the profession, in addition to consequently not having knowledge of the function performed by the professional and the stages of their work in vulnerability analysis. Given the current scenario, where technology is evolving more and more, the use of computers tends to increase, and allowing intrusions to networks by unauthorized people, a professional in pentest is the individual who in this technological scenario, can prevent system

invasions, in addition to strengthening the local network. In order to show the importance of a hacking professional in our society, it is necessary to keep in mind the role he plays, according to his own ethics of conduct, as well as the functioning of a vulnerability scan, and its steps. That said, having a greater knowledge of this subject may open doors not only for the professional in pentest, but also for themselves. In our modern society, the need for a secure and robust network is of paramount importance to keep our information away from bad-natured individuals.

Key words: hacker ethics. Vulnerability analysis. Information security. Protection.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

No cenário atual, com a tecnologia evoluindo a cada dia, o uso de computadores tanto em ambientes domésticos como em ambientes empresariais tornou-se algo fundamental,

e com isso, há uma crescente nas ameaças virtuais nomeadas de “hackers”. Os hackers são indivíduos maldosos que vazam, adulteram ou corrompem alguma informação ou sistema para sua própria diversão ou por má fé, prejudicando assim mais de uma pessoa, uma rede, além de também, marginalizar a imagem de um hacker vista pela sociedade.

Os ataques hackers expõem, comprometem e danificam várias informações sigilosas de empresas, das quais não tem um sistema de proteção ou um profissional da área de informática capacitado para reconhecer e evitar esses tipos de ataques, por amadorismo ou ingenuidade essas empresas não investem na prevenção destes sinistros, justamente pelas ideias conservadoras que todo hacker é maligno. Atualmente a maioria das empresas dispõem de proteção que evita tais problemas através de uma análise de vulnerabilidades em uma rede, isso é chamado de *Pentest*, é um hacker ético, ele faz o oposto de hacker maligno. Um pentester protege a informação e evita invasões no sistema, prevenindo, modificando e principalmente melhorando a segurança da rede.

O objetivo deste trabalho é desmistificar a visão marginalizada de um hacker, mostrando que seu trabalho é de extrema importância para evitar o vazamento de dados devido às vulnerabilidades na rede, algo que deve ser protegida a todo custo, e que um hacker ético é um benfeitor que busca a segurança da informação e age dentro das leis.

O trabalho foi desenvolvido através de uma pesquisa em campo, perguntando para várias pessoas o que elas pensam sobre um hacker, além de mostrar o trabalho de um pentester através de ferramentas de análise de vulnerabilidades com o “Nessus Professional”.

O relatório foi dividido em capítulos, sendo o primeiro o Referencial Teórico, seguido da Metodologia e finalizando com Ética Hacker e seus trabalhos.

Por fim, com esse trabalho espera-se conseguir mostrar que o que é um hacker ético e acabar com o mito que todo hacker é mau, além disso, espera-se esclarecer ao leitor a importância de uma análise de vulnerabilidades da rede para a segurança de suas informações.

2 REFERENCIAL TEÓRICO

Este capítulo irá abordar o conceito da ética hacker, mostrando um pouco a visão distorcida que a sociedade tem sobre a palavra hacker, juntamente com o funcionamento de uma varredura de sistemas, seus meios e programas utilizados para funcionar corretamente.

2.1 FUNDAMENTAÇÃO TEÓRICA

A ética hacker tem como objetivo controlar o comportamento das ações de hackers, ditando o que é certo ou errado de maneira ética, para conseguir entender de forma ideal esses termos, é necessário compreender o significado dessas duas palavras: Ética e Hacker.

O hacker é a pessoa que descobre a falha de segurança em um sistema, informa a falha e desenvolve a correção para a falha encontrada para que a mesma não seja identificada por pessoas de má índole que tenham em mente realizar ataques no sistema. Com base nos fatos apresentados por PEREIRA (2015) é importante implementar e melhorar a segurança a fim de garantir a integridade dos dados que são transmitidos através de uma rede de computadores, pois um invasor, um vírus instalados ou propagando-se pela rede podem causar uma série de vulnerabilidades na rede e ter dados roubados, perdidos ou criptografados. Um hacker que segue à risca a ética hacker é devidamente preparado para evitar tais transtornos, invadindo o próprio sistema da empresa e corrigindo suas falhas identificadas. Por fim, o termo "hacker" surgiu, sendo utilizado para nomear pessoas que desvendam certos enigmas, mas hoje, esse termo é usado inadequadamente e está, na maior parte das vezes, ligado a ataques e roubos cibernéticos. Já a "Ética", assume diferentes significados, conforme o contexto em que os agentes estão envolvidos. Uma definição de NASH (2001) diz que "Ética nos negócios é o estudo da forma pela qual normas morais pessoais se aplicam às atividades e aos objetivos da empresa comercial", portanto, ética é o conjunto de valores morais de um grupo ou indivíduo.

Uma vulnerabilidade em uma rede são geralmente falhas de segurança na rede ou da informação no armazenamento de dados, ataques DDoS, má gestão de software, interceptação de dados, vulnerabilidades em servidores e uso de softwares inseguros para comunicação, esses são os mais comuns encontrados, e são resolvidos com medidas de segurança ou por programas usados por hackers éticos, como Nexpose Community e Nessus Vulnerability Scanner. O escaneamento de vulnerabilidades está totalmente relacionada a segurança da informação, como dito, essa segurança é a

defesa de dados, detalhes e afins para assegurar que eles estejam acessíveis somente aos seus responsáveis de direito ou as pessoas a quais foram enviadas, caso essas informações sejam vazadas ou enviadas incorretamente, o dano causado para a pessoa ou empresa pode ser irreparável, por isso que ter uma segurança da informação forte é importante para a estabilidade de tudo ao seu entorno.

Diferentemente como a maioria pensa a respeito da palavra hacker, que os leva a crer que tal indivíduo é um criminoso, mas a pessoa que tem tal conhecimento no ramo de segurança da informação e usa para vandalizar sistemas é nomeado de Cracker, como MORIMOTO (2005) descreve que o indivíduo que explora a deficiência na segurança de um sistema computacional ou produto sem qualquer intenção perversa, com intuito de chamar a atenção dos desenvolvedores, é chamado de Cracker, que é a pessoa que utiliza seu conhecimento de segurança da informação para realizar invasões em sistemas, quebrar senha, roubar informações, em suma, é um vândalo virtual.

A informação assume, nos dias de hoje, uma importância crescente. Ela se torna fundamental na empresa, tanto na descoberta e introdução de novas tecnologias, como na exploração das oportunidades de investimento e, ainda, na planificação de toda a atividade industrial. Na verdade, existem muitas e variadas definições de informação, que se diferem em complexidade. Segundo ZORRINHO (1995, p. 32) , informação "é um processo que visa o conhecimento, ou, mais simplesmente, informação é tudo o que reduz a incerteza. (...) Um instrumento de compreensão do mundo e da ação sobre ele". Já segundo FERREIRA (1995, pg. 170) "Informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza". Em todavia, conseguimos ver claramente que a informação tornou-se uma necessidade crescente, e por isso, se deve ter cautela com sua proteção, evitando possíveis vazamentos por falhas em sua rede, já que a

informação é indispensável para qualquer setor da atividade humana, mesmo que sua procura não seja ordenada ou sistemática, mas resultante apenas de determinações casuais e/ou intuitivas.

2.2 FUNDAMENTAÇÃO TECNOLÓGICA

Para um devido funcionamento de uma análise de rede é necessário:

● **Endereço IP (Internet Protocol):** Assim como os computadores, para conectar os objetos a rede é necessário que possuam uma identificação que os distinguirá de todos os outros em todo mundo, ou seja, é necessário que possuam um endereçamento IP, para assim podermos distingui los dos demais;

● **Scanners de vulnerabilidades:** São ferramentas de segurança da informação que são indispensáveis, já que tem como função achar e relatar falhas e brechas encontradas no sistema, como por exemplo DoS (Denial Of Service) e DDoS (Distributed Denial Of Service). Dessa forma a empresa podem identificar, consertar e mitigar riscos, protegendo seus usuários e suas informações sigilosas, além de claro, aprimorar sua infraestrutura ao decorrer do tempo com as vulnerabilidades encontradas e corrigidas, com isso vemos a necessidade de se ter uma rede segura, longe de problemas quase irreparáveis;

● **Rede:** Consiste em diversos processadores interligados e que compartilham recursos entre si, TCP/IP fazem parte da rede, localizando o IP correto na rede e garantindo o envio pelo TCP em uma outra rede. Antes, essas redes existiam principalmente dentro de escritórios (Rede local), porém, conforme a evolução, ela passou a aumentar a importância no quesito de transferir ou trocar informações, dando vez a vários tipos de rede, eles são: LAN, MAN, WAN, WLAN, WMAN, WWAN, SAN e PAN.

● **TCP (Transmission Control Protocol):** TCP tem como objetivo garantir que os dados sejam integralmente transmitidos, na sequência de envio, para os hosts de destino corretos. Os dados enviados são quebrados em blocos menores de informação, os datagramas, e recompostos no host de destino. Ele também é responsável pelo reenvio da transmissão, no caso de impossibilidade de recuperação do pacote e dados, portanto, o TCP é de extrema importância numa rede, já que o mesmo é responsável pela transmissão e envio de dados;

● **Host:** É qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes;

● **DoS (Denial Of Service):** Também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Para isso, o

invasor utiliza meios para enviar diversos pedidos de pacotes para o alvo, com a finalidade de que este fique tão sobrecarregado que não consiga mais responder a nenhuma requisição. Assim, os utilizadores não conseguem mais acessar dados do computador, por ele estar indisponível e não conseguir responder a novos pedidos. Achamos esse ataque através de uma varredura de sistema usando scanners/programas para tal feito;

- **DDoS (Distributed Denial of Service):** O ataque acontece de forma similar ao DoS, porém, ele ganha algumas camadas extras. Nele, um computador mestre pode gerenciar uma série de outros computadores, que são chamados de zumbis. Por meio do DDoS, o hacker ou cracker invade um computador mestre e este, por sua vez, escraviza várias máquinas, fazendo com que elas passem a acessar um determinado recurso em um servidor todos ao mesmo tempo. Assim, todos os zumbis acessam juntamente e de maneira ininterrupta o mesmo recurso de um servidor, tentando sobrecarregá-lo. Novamente para identificarmos o ataque, utilizamos ferramentas, scanners ou programas para encontrar e evitar problemas maiores as máquinas.

Visando o grande número de dispositivos e equipamentos com acesso à Internet e a falta de segurança principalmente em ambientes corporativos, o número de ataques de invasores e até mesmo de vírus implantados em uma máquina que se propaga através da rede possibilitando uma possível invasão. Outro fator importante para o entendimento desse conteúdo é saber o que é a Internet, suas partes, sua rede, entre outros fatores que devem ser levados em consideração em uma varredura de sistemas feitas por hackers éticos, de acordo com Kevin Kelly, “as redes interconectadas por todo o mundo é que ditam o ritmo das tecnologias que temos hoje” (2016, in OfuturodasCoisas.com).

3 METODOLOGIA

Este capítulo apresentará as maneiras utilizadas para o decorrer deste trabalho. Irá mostrar o levantamento de dados efetuados através de pesquisa, assim como a análise do gráfico elaborado através desta.

3.1 ANÁLISE DO PROBLEMA

Com o avanço da tecnologia, surgem também problemas os quais podem ou são

extremamente prejudiciais para o funcionamento de um computador ou até mesmo de um vazamento de alguma informação sigilosa que pode prejudicar os lucros ou a imagem da empresa ou o indivíduo, ambos não possuem um profissional qualificado e de confiança para evitar esses problemas, tanto por ignorância ou por não ter um devido conhecimento sobre, e por isso, tem em mente um preconceito quando as soluções para seus variados problemas vem da palavra “hacker” que para elas possui um significado distorcido.

Uma enquete on-line foi realizada durante o período de 10/04/2021 à 30/04/2021, e foi respondida por 80 pessoas de diferentes idades, a maioria era adulto, possuindo uma idade de 18 à 60 anos. Na enquete on-line, ás 80 pessoas tiveram a opção de escolher 3 alternativas que as convém, elas eram:

1) Hacker é um criminoso;

2) Existe um hacker bom e um hacker maligno;

3) Não tenho certeza ou não sei responder.

Com os indivíduos respondendo uma destas três perguntas, chegou ao resultado de 76% das pessoas acham que um hacker é um criminoso virtual, 19% das pessoas sabem que há hackers bons e hackers malignos, e por fim, 5% das pessoas não souberam responder ou ficaram com dúvida quanto as outras alternativas anteriores, isso é mostrado conforme o gráfico abaixo:

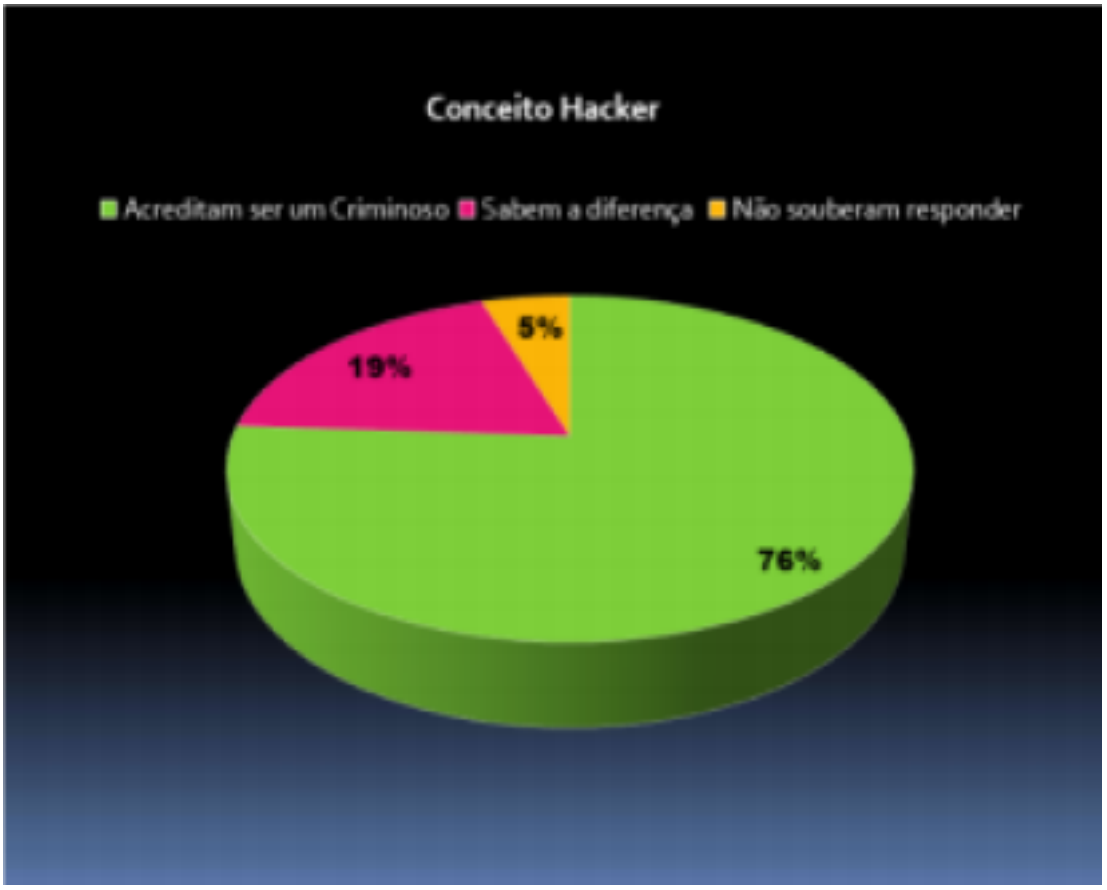

Figura 1 - Conceito hacker Fonte: Próprio autor

3.2 SOLUÇÃO DO PROBLEMA

Ter uma segurança reforçada em uma rede é essencial, tanto para evitar vazamentos de informações que possam ser prejudiciais em diversos aspectos, quanto para evitar furtos através da própria rede, ocasionando prejuízo financeiro. Portanto, tendo em mente a diferença entre um hacker ético e um hacker maligno, assim como, saber a devida importância que deve-se dar a rede, pode tanto controlar como resolver de vez os problemas citados, através do profissional em hacking ético, as vulnerabilidades encontradas na rede, por ele serão reparadas e isso irá fortalecer a segurança do sistema em questão. Além disso, ter em mente o funcionamento de uma análise de vulnerabilidades de uma rede, permitirá saber o que o profissional estará exercendo e evitando possíveis imprevistos.

3.3 MÉTODO DE FUNCIONAMENTO

A pesquisa irá funcionar da seguinte maneira, nela será abordado temas sobre ética e sobre o funcionamento de um *pentest*, que é uma varredura em uma rede de computadores, com exemplos de ética hacker, programas/ferramentas utilizadas em uma varredura de uma rede e destacando cada parte de como é realizado a varredura, além dos problemas que podem ser identificados pelo profissional.

3.4 APLICAÇÃO

O intuito deste trabalho é mostrar para Diretores de empresas, indústrias e até mesmo estudantes que existe sim um hacker que trabalha de maneira correta, e não sendo um criminoso. Por fim, sendo usado este conhecimento para os envolvidos neste ramo ganharem mais confiança entre as empresas, podendo reparar e melhorar a segurança do sistema e da rede, eliminando vulnerabilidades identificadas.

3.5 CARACTERÍSTICAS DO PROJETO

A principal característica desta pesquisa é mostrar o aumento de segurança que uma rede pode ter ao identificar vulnerabilidades e corrigi-las, melhorando gradativamente a proteção dos dados da rede, assim como a segurança do sistema. Outra característica fundamental desta pesquisa é a desmistificação da palavra hacker, mostrando a diferença entre um hacker mal-intencionado e um profissional que segue a ética hacker à risca.

3.6 CUSTO BENEFÍCIO

O custo benefício de uma análise de vulnerabilidades em uma rede de computadores é imediato e a longo prazo, porque ao fazer uma análise de vulnerabilidades, o profissional em

hacking irá identificar ameaças na rede por meio de programas/ferramentas e irá corrigi-las para assim manter a rede mais segura de imediato e continuando a longo prazo, apenas fazendo uma inspeção no servidor em alguns intervalos de tempo durante uma semana ou até um mês.

3.7 RESULTADOS ESPERADOS

O aumento da segurança é algo essencial nos dias de hoje, assim como ter confiança nos profissionais que exercem uma função que tem como finalidade a segurança de uma rede. Portanto, os resultados esperados é que o leitor saiba que existem profissionais em hacking que trabalham dentro da lei, e usuários maliciosos com más índoles, e por fim, que entendam como é realizado uma análise de vulnerabilidades para terem ciência do que o profissional está fazendo e com que ele está lidando, assim aumentando tanto a confiança sobre o indivíduo quanto a segurança da rede ou sistema.

4 ÉTICA DE UM HACKER E SEUS TRABALHOS

Este capítulo irá apresentar a Ética Hacker, assim como as funcionalidades de uma análise de vulnerabilidades em uma rede de computadores, suas etapas detalhadas e a importância da mesma.

4.1 ÉTICA HACKER

Em nossa sociedade moderna, a ética é algo que deve-se cumprir à risca, ainda mais quando o assunto é segurança de informações que podem levar a fins catastróficos. Nesta era rodeada por tecnologias inovadoras e as quais precisam de proteção em sua rede, seja qual for o problema, seja uma invasão, vírus ou vulnerabilidades na mesma. Um hacker é a pessoa para resolver esses problemas e evitar outros futuros, entretanto, sua figura é marginalizada, sendo visto como apenas um criminoso, sem um lado bom, um indivíduo no qual utiliza seus conhecimentos avançados em sistemas para roubar, extorquir, vandalizar ou vazar informações sigilosas. Entretanto, a imagem criada e transmitida pelas mídias são de sua maioria, informações falsas, pelo fato de que um Hacker não é necessariamente um criminoso

virtual, existem Hackers os quais trabalham para resolverem os problemas criados por indivíduos mal-intencionados. O verdadeiro hacker saberá seguir os princípios e com certeza se tornará um profissional exemplar, com um vasto conhecimento, pois irá seguir o código de ética. A ética hacker possui 8 princípios, os quais são:

1. Nunca apague intencionalmente ou danifique um arquivo em um computador que você tenha invadido;
2. Trate os sistemas que você invade como você trataria seu próprio computador; 3. Notifique os administradores de sistemas sobre qualquer brecha de segurança que você encontrar;
4. Não invada para roubar dinheiro;
5. Não invada para roubar informações;
6. Não distribua ou colecione software pirateado;
7. Nunca corra riscos estúpidos – tenha consciência da sua habilidade;

8. Sempre esteja disposto a compartilhar e repassar seu conhecimento e os métodos que utiliza;

Há uma divergência no que diz respeito a um hacker, tal divergência possui três categorias como abordado por Brayan Poloni (2021), a primeira categoria é a *White Hat Hackers*, são hackers éticos que agem de forma legal e trabalham para aumentar a segurança da rede e sistema. A segunda categoria é a *Black Hat Hackers*, esses são os hackers que invadem sistemas, vandalizam, roubam informações para fins beneficentes para si mesmos. E por fim, a terceira categoria *Gray Hat Hackers*, esta categoria se refere aos usuários que invadem sistemas sem permissão, mas diferentes da categoria anterior, não roubam, vandalizam o sistema para fins beneficentes para si mesmos, e sim para alertar a empresa de suas falhas ou apenas pela emoção de invadir um sistema. Podemos classificar essas categorias como bons, hackers que seguem os princípios éticos, neutros, são os que agem de forma ilegal, mas não roubam informações, e os maus, que são os usuários que vandalizam e vazam informações sigilosas.

Figura 2: Tipos de Hackers Fonte: João Vilar | Tecnologia

4.2 FUNCIONAMENTO DAANÁLISE DE VULNERABILIDADES

Uma análise de vulnerabilidades é o ponto de atenção dos gestores de qualquer negócio. Afinal, a cibersegurança é uma prioridade, e essa análise é uma ferramenta que trabalha em prol da proteção da informação e consequentemente na redução de riscos. Tal ferramenta funciona a partir de um processo de reconhecimento, análise e classificação de falhas que estão relacionadas à segurança da infraestrutura de tecnologia. Neste processo, o

profissional em pentest, nome dado aos hackers éticos, o indivíduo irá identificar os pontos enfraquecidos na cibersegurança, e assim, o profissional poderá adotar medidas corretivas para tais fragilidades da rede. Por fim, este método irá fortalecer a segurança, não só do ambiente de TI, mas de toda a empresa. Tendo ciência do aumento de ataques cibernéticos, o profissional em pentest deve frequentemente realizar a análise de vulnerabilidades para identificar as fragilidades existentes e efetuar as correções necessárias. Além de que é preciso considerar as ocorrências de falhas humanas e falhas no desenvolvimento de sistemas como vulnerabilidades que podem ser também identificadas na análise.

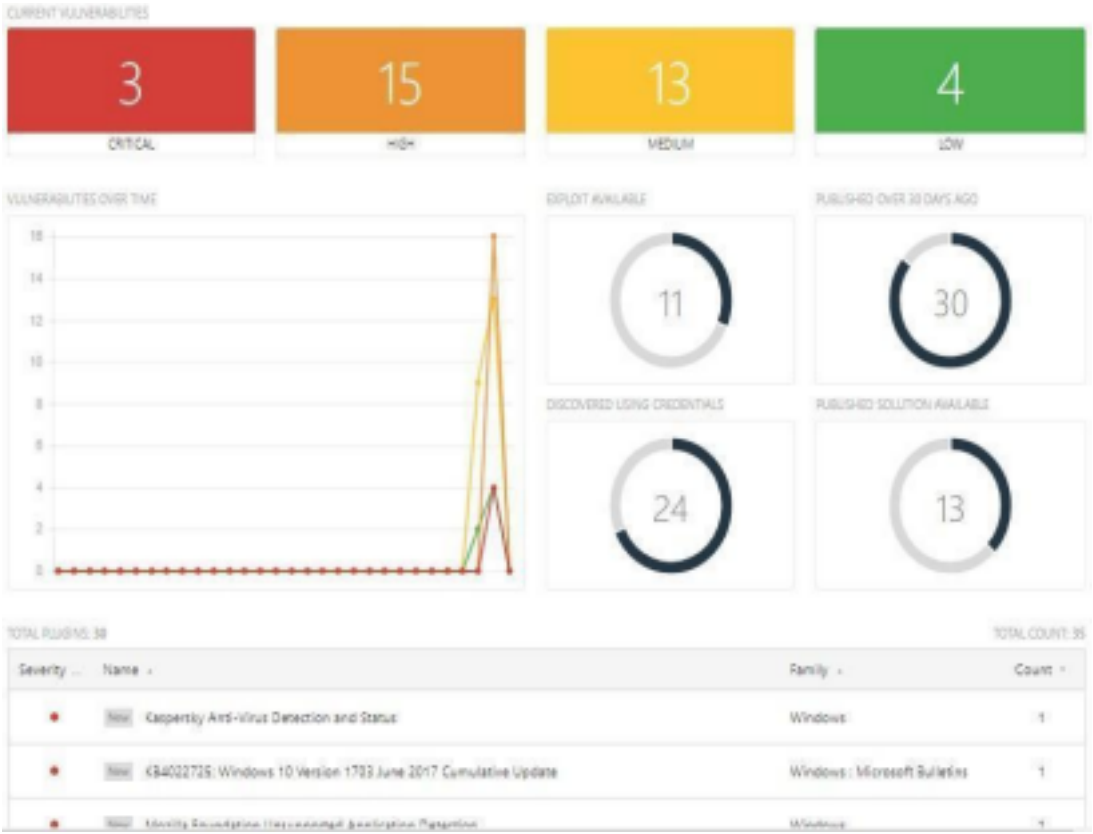

Figura 3: Análise e Gerenciamento de vulnerabilidades
Fonte: Perallis

Este é um exemplo feito por um programa chamado *Perallis Security*, onde apresenta os dados de cada vulnerabilidade encontrada com suas devidas classificações: Critica, Alta, Média e Baixa. Abaixo do gráfico é mostrado também, informações que correspondem às falhas encontradas, marcadas por cores que representam sua classificação.

4.3 IMPORTÂNCIA DAANÁLISE DE VULNERABILIDADES

A importância neste quesito é ter uma segurança robusta e sem falhas, identificar e corrigir tais falhas nessa segurança, isto tornará a rede menos propícia a acabar sendo invadida, podendo perder arquivos, informações ou dinheiro por falta de atenção à proteção da rede, além disso, aumentará também o desempenho do sistema. Em suma, a análise de vulnerabilidades é importante porque garante a melhoria da infraestrutura da empresa. Em diversos aspectos vemos isso, pois a análise tem algumas práticas importantes como:

- Monitorar continuamente os sistemas, com inspeções regulares para acompanhar e

identificar possíveis falhas;

- Reduzir a incidência de problemas com ransomwares, contas inativas, sistemas desatualizados e senhas fracas;
- Proteger os ativos empresariais contra ataques cibernéticos, evitando prejuízos financeiros e de imagem à organização;
- Aumentar a conformidade com a LGPD, demonstrando a boa prática na gestão das vulnerabilidades.

Podemos notar sua importância também em suas etapas em destaque, as quais são: avaliação de risco e de vulnerabilidades, e o tratamento do risco.

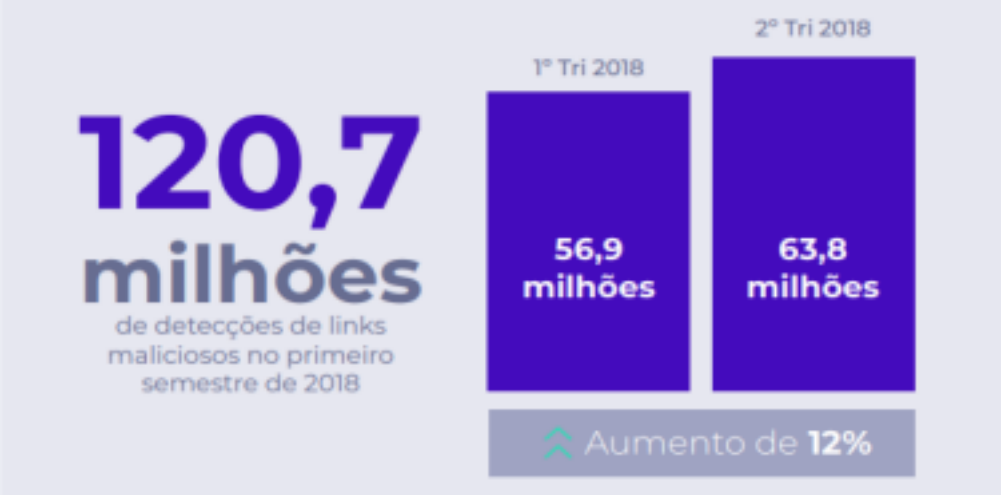

Figura 4: Porcentagem de ataques cibernéticos Fonte: CanalTech[1]

1 Fonte: https://canaltech.com.br

4.4 AVALIAÇÃO DE RISCOS

A avaliação de riscos é a primeira etapa da análise de vulnerabilidades. Antes de ser efetuada, o profissional responsável deve entender e identificar o funcionamento do negócio.

Na avaliação de riscos, o profissional deve localizar e classificar os ativos empresariais. Servidores, dispositivos móveis, estações de trabalho. Qualquer tipo de mídia que pode ser alvo de ataque cibernético deve ser listado e classificado quanto a tipo de informação. Quanto a essa classificação, o mais comum é utilizar uma escala de 1 a 5, desta forma:

1. Informações públicas sobre a organização;
2. Dados internos não confidenciais;
3. Informações sensíveis (Planos de negócios, por exemplo);
4. Dados que só podem ser vistos por funcionários determinados, como planilha salarial;
5. Informações confidenciais

Com esta etapa concluída, passamos para a Avaliação de

Vulnerabilidades. 4.5 AVALIAÇÃO DE VULNERABILIDADES

A avaliação de vulnerabilidades é a segunda grande etapa da análise de vulnerabilidades. Com as informações adquiridas na etapa anterior, o profissional irá criar um modelo das principais ameaças aos ativos organizacionais. Para tanto, ele pode utilizar-se de métodos tradicionais e conhecidos como o STRIDE (Microsoft). Cada letra corresponde a uma ameaça, elas são:

- S (*Spoofing of identity*): Roubo de identidade ou falsificação;
- T (*Tampering with data*): Violação ou adulteração de dados;
- R (*Repudiation of transaction*): Repúdio de transação;

- I (*Information disclosure*): Divulgação não autorizada de informação;
- D (*Denial of service*): Ataques de negação de serviço;
- E (*Elevation of privilege*): Elevação de privilégio.

Um modelo comum é criar uma planilha relacionada aos ativos da categoria STRIDE de ameaça.

4.6 TRATAMENTO DE RISCO

Por último, não menos importante, a última etapa da análise de vulnerabilidades, o tratamento do risco. As falhas e vulnerabilidades já foram avaliadas, por isso já temos ciência da localização das maiores brechas no sistema. Agora, é o momento de mitigá-las. Com a planilha em mãos, o profissional saberá a porcentagem de sistemas sob risco, em maior ou menor grau. Assim, deve priorizar aqueles que estão sob maior ameaça de ataques, balanceando-o com a importância do sistema. As vulnerabilidades nos controles existentes, por exemplo, devem ser corrigidas rapidamente. Neste momento de tratamento, é necessário sempre ter em mente que o negócio corre riscos que podem ser evitados, por isso, a melhor forma de resolver tais riscos é encontrar ferramentas mais eficazes para a correção e evitar problemas no futuro.

5 CONSIDERAÇÕES FINAIS

Com este trabalho, é possível concluir que diversas pessoas não sabem diferenciar um hacker ético de um cracker ou hacker maligno, além de não terem muita noção sobre o serviço prestado pelo profissional em pentest. Mesmo pesquisando na rede, a palavra hacker ainda aparece como um criminoso virtual, ou seja, tanto na rede quanto na mídia, a imagem de um hacker é marginalizada. Esta pesquisa foi elaborada para trazer um pouco de esclarecimento sobre esse fato, além da função exercida pelo profissional em hacking, e por fim, instigar as pessoas a se interessarem mais sobre o assunto, fazendo com que pesquisem mais a fundo sobre um hacker, não deixando-se levar pela primeira informação encontrada.

É muito importante que todos saibam o benefício que um hacker ético pode proporcionar, tanto em segurança de suas informações, quanto evitando possíveis problemas por falhas identificadas em meio a rede e sistemas locais. Com o nosso mundo evoluindo cada dia mais na área de tecnologia, a chance de invasões a rede de empresas tem um aumento significativo, ainda mais se esta empresa não possuir um profissional qualificado para exercer a proteção.

Portanto, tendo em vista que o conhecimento sobre o hacking ético e também conhecendo o seu trabalho, suas etapas e suas normas, conclui-se ser necessário uma divulgação ligeiramente maior tanto nas mídias como nos canais de televisão, quanto em sites

de informações, que não passam o verdadeiro significado da palavra hacker. Pois querendo ou não, o serviço de um hacker ético deve-se levar a sério e futuramente poderá ser de extrema importância por causa do avanço gigantesco da tecnologia nos dias atuais e nos próximos anos, assim, mantendo sua rede segura de invasões. Definitivamente será o melhor caminho e o que terá mais frutos a se colher.

REFERÊNCIAS BIBLIOGRÁFICAS

DELFINO, Pedro. *TOP 10 – Melhores Sistemas Operacionais Para Hacking Ético E Teste De Vulnerabilidade* In: Profissionais Linux. Disponível em: https://e-tinet.com/linux/sistemas-operacionais-para-hacking-etico/ Acessado: 15/maio/2021

FARIAS, Adriana. *Apostila de Ética* In: CRC CE. Disponível em: https://www.crc-ce.org.br/crcnovo/download/apost_eticacrc.pdf Acessado: 11 /maio/ 2021

FLOWTI. *Análise de vulnerabilidade: o que é e qual é a sua importância?* In: Flowti, segurança da informação. Disponível em: https://flowti.com.br/blog/analise-de-vulnerabilidade-o-que-e-e-qual-e-a-sua-importan cia/ Acessado: 11 /maio/ 2021

MOCELIN, Daniel Gustavo. *A ética hacker do trabalho: rompendo com a jaula de ferro?* In: SciELO Brasil. Disponível em: https://www.scielo.br/j/soc/a/VF6yzJJNmpQ9rMcVxNgshWB/?lang=pt# Acessado: 10 /maio/ 2021

NEGROMONTE, Emanuel. *Conheça a ética Hacker!* In: SempreUpdate. Disponível em: https://sempreupdate.com.br/conheca-etica-hacker/ Acessado: 30/maio/2021

OSTEC. *Análise de vulnerabilidade: 5 ferramentas para profissionais de tecnologia* In: OSTEC Segurança digital de resultados. Disponível em: https://ostec.blog/geral/analise-de-vulnerabilidade-5-ferramentas/ Acessado: 11 /maio/ 2021

POLONI, Brayan. *Ethical Hacking: O que preciso saber sobre tipos de hackers?* In: Introduce, tecnologia para crescer. Disponível em: https://introduceti.com.br/blog/ethical-hacking-o-que-preciso-saber-sobre-tipos-de-hackers/ Acessado: 31/maio/2021

VILAR, Joao. *Os 3 tipos de chapéus que diferencia os hackers* In: Joao Vilar | Technology. Disponível em:https://jvilar.wordpress.com/2017/03/11/os-3-tipos-de-chapeus-que-diferencia-os-hackers/ Acessado: 31/maio/2021