HACKERS E VULNERABILIDADES NAS REDES

NASCIMENTO, Gabriel Silva do[1]

GAVILAN, Júlio Cesar [2]

RESUMO

Desde os primórdios da Computação, o ataque de *hackers* criminosos no gerenciamento de segurança tem sido um grande problema na era da informação. Muitos usuários de equipamento computacionais acreditam ser um alvo pequeno para ataques de *hackers*, porém o comportamento dos cibercriminosos podem não estar de acordo com essa avaliação. Os *hackers* veêm os dados de qualquer indivíduo ou organização como algo valioso e que pode lhe dar poder. Atacar (ou invadir) o pequeno usuário também é muito atraente para o hacker pois evita a necessidade de ter de passar por *firewalls* e sistemas de segurança mais complexos. Sem a necessidade de passar por *firewalls* corporativos sofisticados ou contornar vários protocolos de segurança, a ideia de penetrar nas defesas quase inexistentes de um computador pessoal se torna muito atraente. Neste artigo, discutimos a identificação da vulnerabilidade, relatando o que significa e como melhor conduzi-la. Discutimos também novas abordagens que podem ser adotadas para identificar vulnerabilidades e os diferentes níveis de ocorrência, impacto e risco geral. Finalmente, discutimos que os usuários de equipamentos tecnológicos, de uma grande organização até o usuário de smatphone devem ficar, atentos com os possivéis ataques e invasões dos *hackers*, e como nos adequarmos as práticas de segurança cibernética, para nossas informações não serem apropriadas por cibercriminosos.

Palavras Chave: Hackers. Vulnerabilidades. Segurança. Redes.

[1] Acadêmico do Curso de Sistemas de Informação da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço –EDUVALE.

[2] Físico Computacional formada pela Universidade de São Paulo, Mestre em Ciências da Computação, pela Universidade Federal de Santa Catarina. Docente titular do Curso de Sistemas de informação da Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço –EDUVALE.

ABSTRACT

Since the dawn of computing, the attack by criminal *hackers* on security management has been a major problem in the information age. Many users of computer equipment believe they are a small target for hacker attacks, but the behavior of cybercriminals may not be in line with this assessment. *Hackers* see the data of any individual or organization as valuable and empowering. Attacking (or invading) the small user is also very attractive to the *hacker* because it avoids the need to go through firewalls and more complex security systems. Without the need to go through sophisticated corporate firewalls or bypass various security protocols, the idea of penetrating the almost nonexistent defenses of a personal computer becomes very attractive. In this article, we discuss the identification of the vulnerability, reporting what it means and how to best manage it. We also discuss new approaches that can be taken to identify vulnerabilities and the different levels of occurrence, impact and overall risk. Finally, we argue that users of technological equipment, from a large organization to the user of smatphones, should be aware of possible attacks and invasions by *hackers*, and adapt to cyber security practices, so that our information is not stolen by cyber criminals.

Keywords: Hackers. Vulnerabilities. Safety. Networks

INTRODUÇÃO

Atualmente, toda empresa precisa do ciberespaço para implementar seu negócio, porém ficam vulneráveis às tentativas de ataques em seus sistemas, e as tentativas para invadir seus sistemas são constantes nesse ambiente. Podemos dizer o mesmo dos usuários de *smartphone* ou de qualquer outro equipamento conectado na internet. Portanto, ninguém está realmente seguro e é grande a possibilidade de ser alvo de um *hacker*, bastando para isso ter um

equipamento conectado à Internet. Reagir aos ataques defendendo-os é apenas uma parte da trabalho dos profissionais de Tecnologia da Informação. É importante detectar e prevenir ataques às estações de trabalho, servidores e redes de seus usuários antes que eles causem estragos nos negócios.

Soluções de defesas personalizadas, oferecem segurança cibernética intensa, com uma plataforma especializada de proteção contra ameaças. A plataforma de proteção contra ameaças realiza monitoramento em toda a rede para detectar *malware,* comunicações maliciosas e comportamentos cibercriminosos para defesas de segurança padrão. O *malware* é uma denomiação para inúmeras classificações de vírus. (MITSHASHI, 2011)

Ter soluções de segurança, permitem que se descubra o risco, a origem e as características do ataque. Ele oferece inteligência acionável de maneira única para ajudá-lo a reprimir o ataque e corrigir a perda, permitindo ainda, adaptações e fortalecimentos de sua proteção contra novos ataques cibernéticos. (LOMILER, 2016)

Se os *hackers* obtiverem acesso ao sistema, seja ele pessoal ou de uma organização, uma série de cenários não agrádaveis podem ocorrer. Eles usam métodos sofisticados e precisos para ultizar os dados como uma forma de chantagem, permitir o apropriamento de identidade e até mesmo lançar ataques em outras redes através do seu computador. A maneira mais conhecida de combater esses criminosos cibernéticos é entender como eles realizam seus ataques. (ZOTTO, 2012)

Como nas ultimas décadas aumentaram o uso de equipamentos conectados à Internet, celulares e *smarthphones* e até mesmo computadores e notebooks, colocamos a seguinte questão: Podemos evitar a invasão de *hacker* em dispositivos conectados à Internet, disponibilizando conhecimento aos usuários, permitindo que tomêm providências para evitarem ser hackeados?

Existem dois tipos de segurança de *firewall* geralmente disponíveis no mercado - *gateways* de aplicativos e *gateways* de filtragem de pacotes. Os *gateways* de aplicativos são *proxies* e causam problemas computacionais em computadores devido ao uso intenso da CPU (LOMILER, 2016). Portanto, os dispositivos de filtragem de pacotes são mais preferidos em redes ocupadas. Instalar um *firewall* de segurança em um *gateway* não é uma solução permanente para as necessidades de segurança. Todos os *firewalls*

disponíveis no mercado hoje estão sujeitos a ataques - como notamos pelos crescentes ataques cibernéticos a cada ano. Se configurar incorretamente ou não mantiver um *firewall* de maneira adequada, será um caminho fácil para os *hackers*. (BUZZATTE, 2014). A proteção de *firewall* atua como um impedimento na infiltração de redes de computadores.

Pode-se testar as vulnerabilidades de segurança em aplicativos a partir de qualquer uma das ferramentas disponíveis. (LOMILER, 2016)

Desta forma, este artigo busca discutir e identificar vulnerabilidades, relatando o que significa, e a melhor forma de conduzí-las.

Como metodologia para este trabalho, utiliza-se recursos e métodos para investigação e aplicação de procedimentos, por meio da pesquisa exploratória de documentação e bibliográfica, de fontes primárias (teses e artigos publicados) e secundárias (revistas, jornais, portais especializados).

1 REDES

Com o passar dos anos a espécie humana foi se desenvolvendo cada vez mais, contudo a tecnologia está sendo o ápice dessas evoluções, podemos destacar nessa área que as redes de computadores têm um valor significativo para tudo que ocasionou esses avanços. (TANENBAUM, 1981)

Para Lomiler (2016, p.21) “Redes de computadores são estruturas lógicas e físicas que permite que dois ou mais computadores troquem informações entre si”. Segundo Macedo et al. (2018, p.12) “os dispositivos de uma rede de computadores podem ser computadores, *smartphones*, *smart TVs*, câmeras de segurança, ou dispositivos responsáveis pela comutação de dados”.

Com isso podemos entender que com as redes, temos a facilidade de compartilhar recursos e informações a todo momento. Ainda falando sobre redes podemos citar as redes sem fio chamadas de Wi-Fi.

> O termo Wi-Fi (Wireless Fidelity), refere-se a um padrão (IEEE 802.11) para redes sem-fio. Através da tecnologia Wi-Fi é possível realizar a interligação de dispositivos compatíveis como notebooks,

> impressoras, tablets, smartphones, entre outros. (Franciscatto et al. 2014, p.92)
> As redes sem fio tornaram-se alvo de exaustivos estudos e muitos ataques foram desenvolvidos e/ou adaptados para poderem se valer das fraquezas presentes nestas redes. Além disso, estas redes apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio protocolo. (Duarte 2003, p.26)

Para Silva (2003, p.11) "A evolução das redes de computadores identificou um importante equipamento de gerenciamento que é o servidor de redes. Sua função principal é prover serviço de comunicação, acesso e validação de usuários".

2 HACKERS

Infelizmente no ambiente das redes de computadores temos alguns inimigos, que aproveitam de algumas falhas e vulnerabilidades desse ambiente. Claro que com o avanço das tecnologias de rede, fica cada vez mais difícil de estarmos protegidos de cibercriminosos conhecidos como *Hackers*. (DUARTE, 2003)

Segundo Vilela (2006, p.13) "Comumente na mídia e em algumas populações, usa-se o termo *'hacker'* para designar *'crackers'*, ou seja, pessoas que praticam atos ilegais ou sem ética".

> Black Hat ou cracker é um especialista que usa suas habilidades de forma maliciosa e para o mal; alguns exemplos são invasões não autorizadas, furto de informações, negações de serviço etc. Gray Hat é um termo que foi criado para qualificar um tipo de hacker que, na maioria das vezes atua dentro da lei, porém alguns de seus atos podem ser qualificados como estando às margens da lei. O White Hat ou hacker ético é um profissional com conhecimento na área de segurança computacional que utiliza suas habilidades para o bem, como por exemplo, o teste de penetração. Apesar de o hacker ético utilizar as mesmas ferramentas do black hat, ele as utiliza de forma ética e somente mediante autorização. (GIAVAROTO 2015, p. 5 apud LOMILER 2016 p.17)

2.1 ATAQUES HACKERS

Quando falamos de ataques e invasões de *hackers*, não sabemos então qual a intenção do invasor. Alguns com o prazer de fazer o mal, enquanto

outros apenas procurando uma forma de aumentar o seu ego, e mostrar ser um cara altamente capaz. (SILVA, 2003)

Para Lomiller (2016, p.18) “O *hacker* precisa se sentir desafiado, instigado a prosseguir com a ação. Muitas vezes essas pessoas agem somente por agir, para perceberem que algo é possível e que eles conseguem fazer”.

Podemos citar ataques DDOS como uma forma de prejudicar uma rede de computadores.

> Ataques que agem da mesma forma que o DOS, ou seja, visam indisponibilizar serviços porém, ao contrario do DOS, em que o ataque parte de um único ponto, no DDOS o ataque é coordenado e simultâneo a partir de diversos pontos, dificultando qualquer ação de defesa, exatamente por ser distribuído. (MITSHASHI, 2011, p.31)
> Segundo MENEZES et al. (2015) consiste em um ataque que infecta vários computadores, que se tornam “zumbis”, que são comandados pelo computador “mestre”, onde acessam um serviço todos os computadores na mesma hora, fazendo com que o número limitado de usuários, que o servidor atende simultaneamente nos ‘slots’ acabem e o servidor não seja capaz de atender a mais nenhum pedido, fazendo com que haja um travamento.

Os ataques DDOS são um dos grandes desafios atuais dos administradores de servidores e uma fonte de renda para os donos de redes de zumbis e *BotNets*. (JUNQUEIRA, 2020).

Na figura 1, temos a ilustração de um ataque DDOS.

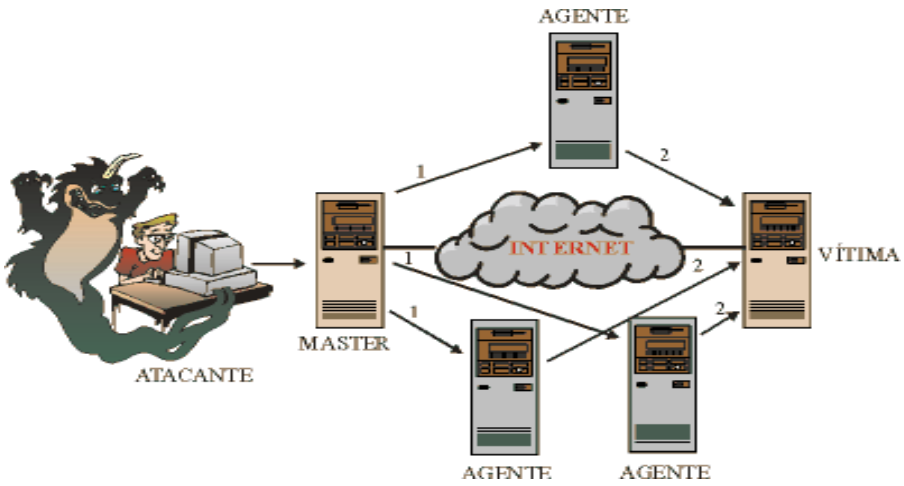

Figura 1 - Ataque DDOS(2020)

Fonte: https://memoria.rnp.br/newsgen/0003/ddos.html

Atacante: Quem está coordena o ataque.

Master: Máquina que recebe as instruções para o ataque e comanda os agentes.

Agente: Efetivamente concretiza o ataque contra uma ou mais vítimas, conforme for especificado pelo atacante.

Vítima: Alvo do ataque. Máquina que é completamente infectada por um volume enorme de pacotes, ocasionando um extremo congestionamento da rede e resultando na paralização dos serviços oferecidos por ela. (SOLHA; TEIXEIRA; PICCOLINI, 2020).

3 ATAQUES EM CELULARES E SMARTHFONES

O cibercrime tem se modernizado e atingido cada vez mais alvos em todo o mundo. Os dispositivos móveis passaram a estar na mira desses ataques e muitos usuários ainda não conhecem as falhas de proteção de seus *smartphones*. Dispositivos móveis, celulares e *tablets* estão tornando-se alvos de muitos ataques e, em grande parte, pelo fato de muitos usuários não terem muita consciência do que estão sendo expostos. (REDAÇÃO, 2019).

Os cibercriminosos têm diversas técnicas para conseguir ter acesso indevido a um celular e ter acesso remoto a contas de aplicativos instalados no aparelho. E o *WhatsApp* e o *Telegram* têm sido alvos constantes desses ataques virtuais. (REDAÇÃO, 2019).

Frequentemente, aplicativos e sistemas operacionais trazem falhas de código que se exploradas por *hackers*, podem permitir o acesso a dados sigilosos de seus usuários, acarretando a integridade de dados de seus usuários. (FABRO, 2020)

> Ao acessar redes Wi-Fi públicas, um invasor pode se colocar entre o seu celular e o roteador e capturar todos os dados transmitidos. Geralmente, os hackers são atraídos pelas mesmas facilidades que atraem o público em geral: o acesso a uma rede sem necessidade de autenticação. Isso cria uma oportunidade para que pessoas mal intencionadas tenham acesso aos dispositivos desprotegidos na rede. (REDAÇÃO,2019).

Continuando com palavras do mesmo autor:

> Outra hipótese é um ataque direcionado. Recentemente, surgiram uma série de relatos de ataques a computadores e smartphones que sequer dependem de interação do usuário para que a infecção com um malware aconteça. O ataque também pode ser feito por meio de links falsos enviado por e-mail, por exemplo. E um dos objetivos desse tipo de ataque é dar acesso para que o hacker controle o dispositivo remotamente, para obter as informações desejadas. Outro objetivo é ficar de olho em senhas e outras informações sensíveis digitadas para utilização posterior. (REDAÇÃO, 2019).

Para evitar invasões ou furto de informações pessoais, temos alguns métodos de prevenção na parte de dispositivos móveis, sendo que o usuário tende a ter uma educação digital. Manter seu dispositivo sempre atualizado, cuidado com o que você publica nas redes sociais, mude as senhas periodicamente, Cuidado com sites que pedem muitas informações, atenção nas compras online e evite uso de redes *wi-fi* públicos. (REDAÇÃO, 2019)

4 VULNERABILIDADES

“Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém”. (SOARES; LEMOS e COLCHER,1995, p.448 apud ZOTTO, 2012 p.17).

> Técnicas utilizadas para invadir sistemas computacionais não autorizados, os invasores testam as possibilidades de falhas de segurança (vulnerabilidades) nos sistemas, para isso utilizam algumas técnicas, como por exemplo, tentativas de invasão para conhecer os meios de segurança dos sistemas a serem invadidos e nisto suas possíveis falhas para uma invasão efetiva. (MITSHASHI, 2011, p.28)

Assim podemos entender vulnerabilidade como um fator que quando não devidamente identificado e reparado pode comprometer a integridade de seu sistema. (MITSHASHI, 2011)

“As ameaças e as vulnerabilidades podem mudar rapidamente, pois uma vulnerabilidade não causa prejuízo sozinha, necessita que haja uma ameaça capaz de explorá-la”. (BUZZATE, 2014, p.16).

Segundo ABREU (2011): Existem sites na internet que disponibilizam listas de vulnerabilidades em softwares de sistemas operacionais. Os fabricantes também costumam informar em páginas na internet com algumas

informações específicas a respeito de possíveis vulnerabilidades em seus softwares.

Ao longo dos anos, pesquisadores e fornecedores de segurança procuraram tornar o processo de identificação de vulnerabilidades o mais simples e rápido possível. Isso foi possível devido ao desenvolvimento e contribuição a projetos como o projeto *Kali Linux*, que envolve a integração de várias ferramentas de segurança em um sistema operacional de segurança (NETO, 2004).

4.1 NESSUS

O Nessus é da Tenable Security's é um dos *scaners* de vulnerabilidades mais usados comercialmente, apesar de vários fornecedores fornecerem produtos comparáveis. (MACÊDO, 2016)

Como exemplo para utilização de ferramentas para auxiliar no controle de vulnerabilidades irei citar o *NESSUS.* O Nessus tem sua versão *free* e também tem sua versão por assinatura, e pode ser encontrado em seu site http://www.nessus.org, está disponível para qualquer usuário que tenha conhecimento ou interesse sobre vulnerabilidades.

O Nessus é executado em interface web, através de um nome de domínio e porta. (MACÊDO, 2016)

> Funciona em diversas plataformas como, Windows, FreeBSD, Linux e Mac OS, composto por uma arquitetura cliente/servidor, sendo o servidor responsável pela varredura da rede e detecção de falhas de segurança, e o cliente prover a interface ao usuário, permitindo o mesmo analisar as vulnerabilidades. (Buzzatte 2014, p.30)
> Segundo Buzzatte (2014, p.31) O Nessus oferece uma descrição detalhada da(s) vulnerabilidade(s) detectada(s) e o(s) passos a ser seguido para eliminá-la(s), através de relatórios em HTML, XML, LaTeX e texto simples. A exibição desses relatórios pode ser feita de diferentes maneiras, ou seja: remedições sugeridas – Nessus resume as ações a serem tomadas para o endereço com a maior quantia de vulnerabilidades na rede; vulnerabilidades agrupadas por plugin – lista cada vulnerabilidade encontrada durante o escaneamento dos hosts afetados; vulnerabilidades agrupadas por host – lista cada host encontrado durante o escaneamento e suas vulnerabilidades associadas.

Na figura 2 temos uma interface do sistema NESSUS:

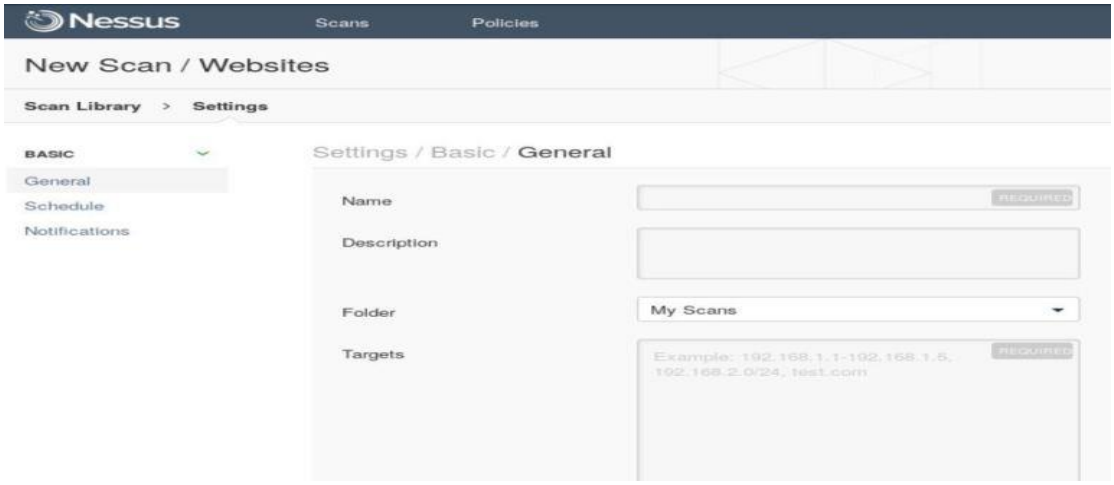

Figura 2 – NESSUS
Fonte: (MACÊDO, 2016)

5 SEGURANÇA NAS REDES

“Técnicas de contra-medidas de invasão tornam-se ineficazes muito rapidamente. Novas técnicas de invasão são descobertas diariamente, tornando se impossível manter redes de computadores 100% seguras”. (SILVA, 2003, p.12)

Ninguém, literalmente ninguém está 100% seguro de invasões e furto de informações, começando por redes convencionais mais comuns até rede de grandes organizações que investem muito dinheiro para manter suas valiosas informações em segurança. (FERNANDES et al. 2015)

> A política de segurança é um documento organizado com informações cada vez mais detalhadas sobre procedimentos, práticas e padrões a serem aplicados em determinadas circunstâncias, sistemas ou recursos. Sua implantação deve ocorrer formalmente, podendo ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares.(BUZZATTE, 2014, p.19)

A segurança em rede de computadores é o resguardo dos dados mantidos na rede, ou seja, na segurança das informações que estão sendo armazenadas em um determinado local (ZOTTO, 2012 apud LOMILER, 2016, p.16).

5.1 Firewall e Proxy de Rede

“A abordagem de segurança de rede inclui **firewalls** para proteger os sistemas internos e redes, usando um sistema de autenticação forte e encriptação para proteger dados particularmente importantes que transitam na rede”. (MITSHASHI, 2011, p.5)

Segundo Zotto (2012, p.23) “O *Firewall* é uma ferramenta extremamente importante na proteção das redes corporativas, visto que ele é o responsável por filtrar os pacotes que entram e saem da rede, bem como ajuda no bloqueio das portas de uso comum nos ataques de intrusos”.

O *Firewall* pode ser em *hardware* ou *software* e controla e monitora o trafego de dados na rede que consiste em bloquear tráfegos específicos conforme suas regras de segurança. (ZOTTO, 2012)

“Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de e-mail, *cavalos de tróia* e outros tipos de *malware*, antes mesmo que os antivírus entrem em ação”. (ABREU, 2011, p.28)

Existem 3 tipos de *firewall,* sendo que cada um tem uma função específica a exercer.

Packet filtering: Oferece um excelente nível de filtragem, mas possui uma metodologia simples, tem a função básica de analisar uma lista de regras configuradas pelo desenvolvedor e faz a verificação de quais informações são compatíveis. O sistema se divide em dois tipos: o estático e o dinâmico.

Proxy services: Funciona como um intermediário entre um computador e outra rede, como a internet, os *proxyes* são geralmente instalados em servidores robustos, pelo fato de trabalharem com grande número de solicitações. É um firewall muito bom, oferece uma excelente opção de segurança por impedir a comunicação direta entre origem e o destino.

Stateful inspection: Realiza uma espécie de comparação entre o que está acontecendo e o que possivelmente espera que aconteça. Funciona de forma que o dispositivo executa essa ação conforme análise do tráfego de dados, em busca de padrões aceitáveis pelas diretrizes, que seriam utilizadas para manter a comunicação. O *firewall* utiliza esses dados armazenados, como

parâmetro para tráfegos subsequentes. Assim, quando a entrada e saída das informações ocorrer por uma porta não mencionada, o firewall irá ver isso como uma anormalidade, e realizará o bloqueio do processo.

Sendo que o estático analisa os dados com base nas diretrizes configuradas. E o dinâmico permite que as regras sejam adaptadas de acordo com a situação, corrigindo as limitações dos filtros estáticos. (PIZZOLATO, 2020)

O *proxy* é um servidor que atua como intermediário entre o usuário e um outro servidor, seu uso comum é para segurança, balanceamento de carga, *caching* de dados com o intuito de diminuir a exigência de largura de banda e filtragem. (ABREU, 2011)

> Os proxies também são ferramentas de grande ajuda na proteção da rede,seu intuito é limitar o acesso dos usuários da rede para o mundo externo, ou seja,proxies bloqueiam o acesso dos usuários da rede interna para a internet, sites impróprios, downloads, execução de complementos, programas de downloadscomo: P2P, torrents entre outros. O uso de Proxies é muito recomendado visto quegrande parte das vulnerabilidades da rede ocorre devido ao mau uso da internet porparte dos usuários. (ZOTTO, 2012, p.23)

Na figura 3 podemos observar a atividade de um *firewall.*

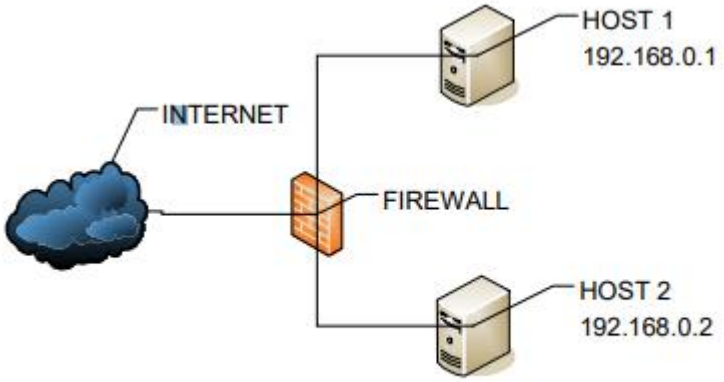

Figura 3 - Ilustração Firewall
Fonte: (MITSHASHI, 2011)

Temos 2 redes *HOST 1* (192.168.0.1) e *HOST 2* (192.168.0.2) em intermediário com a internet temos um *firewall*.

Vemos a figura 3 com os HOST 1 e o HOST 2, solicitam um pacote de dados para a internet, e até mesmo pode haver troca de arquivos entre eles.

O *firewall* vai filtrar o trafego de informações nessa rede, e irá tomar uma decisão se essas informações são de segurança. Caso as informações sejam de segurança, o *firewall* não irá interferir nessa troca de informações. Mas caso ele intenda que essas informações não sejam de segurança ele irá bloquear essa troca de informação. (MITSHASHI, 2011)

5.2 FERRAMENTAS ANTI-VIRUS E ANTI-MALWARES

Um dos maiores problemas que a segurança da informação enfrenta, são os *malwares* e os vírus. Ter um anti-virus a seu favor não quer dizer que estará completamente seguro aos ataques, mas essas ferramentas são de grande ajuda para a proteção de softwares e hardwares.

Para Macedo et al. (2018, p.157) “as ferramentas *anti-malware* são aqueles softwares capazes de detectar, anular (colocar em quarentena) ou remover códigos maliciosos de um computador”.

“São programas que fazem uma constante varredura em busca de vírus presentes na memória da máquina, e-mails, CDs, entre outros. É muito importante manter esse software sempre atualizado e executando regularmente”. (FERNANDES et al. 2015, p.5).

5.3 BACKUP (CÓPIA DE SEGURANÇA)

Como não temos a total garantia de segurança em nossas redes, temos sempre que pensar em um segundo plano. Segundo Abreu (2011, p.29) Cópias de segurança dos dados armazenados em um computador são importantes, não só para se recuperar de eventuais falhas, mas também das consequências de uma possível infecção por vírus, ou de uma invasão. (MORAES, 2019)

Para Macedo et al. (2018, p.157) “backup propicia que dados sejam recuperados em situações como falha de disco, atualização malsucedida do sistema operacional, exclusão acidental de arquivos, ação de vírus, furto/perda de dispositivos, entre outros”.

6 CONSIDERAÇÕES FINAIS

Neste artigo, discutimos sobre as redes de computadores, ataques e vulnerabilidades. A identificação de vulnerabilidades é um importante exercício de segurança que ajuda a proteger seu ambiente.

Sem a identificação da vulnerabilidade, não seria possível determinar quais vulnerabilidades existem em uma rede. Ser paranóico com a possibilidade de existir uma vulnerabilidade em sua rede é muito importante. Salienta-se que a identificação de vulnerabilidades de forma contínua, busca eliminar o período de espera por essas vulnerabilidades, ou seja, configura-se um sistema para que possa sair varrendo sua rede na frequência que se escolher.

Configurar para ser executado semanalmente, mensalmente, diretamente pode ser uma boa opção, após uma correção - o que fizer mais sentido para a organização. Normalmente, as ferramentas que monitoram tais vulnerabilidades, compilam os resultados de cada varredura em um relatório que prioriza as vulnerabilidades por risco e fornece etapas acionáveis para eliminar todos os problemas detectados

A segurança corporativa e até mesmo a segurança pessoal de cada usuário que utilza as redes é de grande importância no mundo de hoje, já que todos entendem perfeitamente como medidas inadequadas podem dificultar suas operações diárias. A melhor coisa que se pode fazer para manter os *hackers* fora da rede é educar-se, entender a configuração de segurança do *software* e do sistema operacional que se usa e ter extremo cuidado quando estiver *online*.

Para proteger os ativos contra ataques cibernéticos, deve-se ter um conhecimento completo das primeiras indicações de uma violação de segurança. Este artigo, evidencia que a segurança gerenciados sob medida oferece métodos de análise e monitoramento de segurança proativos e sistematizados para descobrir sinais de penetração no tráfego da rede e nos logs de segurança, o que o ajuda a ficar alerta contra ataques. Identifica-se e elimina lacunas, pontos fracos e áreas de vulnerabilidade nas redes.

Desta forma esse artigo responde o questionamento inicial, mostrando a ferramenta NESSUS, onde o usuário pode verificar o status da sua rede e verificar se esta suscetível ao ataque *hacker*, no entanto vendo suas possíveis vulnerabilidades, pode-se tomar uma decisão de como configurar sua rede, de possíveis invasões e ou até roubo de dados. E também abordamos alguns métodos de segurança para proteger seus dispositivos que estão conectados a uma rede.

REFERÊNCIAS

ABREU, L. (2011). **A Segurança da Informação nas Redes Sociais**. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf> Acesso em: 12 out. 2020.

BUZZATTE, P. (2014). ANÁLISE DE VULNERABILIDADES ATRAVÉS DE SCANNERS DETECTORES. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2019/05/2014-TCC_Final_Patricia.pdf Acesso em: 12 out. 2020.

DUARTE, L. (2003). **Análise de Vulnerabilidades e Ataques Inerentes a Rede sem Fio 802.11x**. Disponível em: <http://smeduquedecaxias.rj.gov.br/nead/Biblioteca/Forma%C3%A7%C3%A3o%20Continuada/Tecnologia/cursos/seguranca/ataques%20e%20vulnerabilidades%20em%20redes%20sem%20fio.pdf> Acesso em: 16 nov. 2020.

FABRO, Clara (18/04/2020**). Seis formas em que aplicativos podem vigiar e expor dados pessoais**. Disponível em: <https://www.techtudo.com.br/listas/2020/04/seis-formas-em-que-aplicativos-podem-vigiar-e-expor-dados-pessoais.ghtml> Acesso em: 16 nov. 2020.

FERNANDES, G., PINHO, J., SIQUEIRA, T., GONCALVEZ, G., & CRITOVAO, A. (16 de 10 de 2015). **A IMPORTÂNCIA DA SEGURANÇA DE REDES NO CENÁRIO ATUAL: ESTUDO COM O MÉTODO DELPHI**. Disponível em: <http://www.abepro.org.br/biblioteca/TN_STO_213_262_27211.pdf> Acesso em: 12 nov. 2020.

FRANCISCATTO, R., CRISTO, F., & PERLIN, T. (2014). **Redes de Computadores.** Disponível em: <http://roberto.cfw.ufsm.br/images/uploads/redes_computadores.pdf> Acesso em: 16 nov. 2020.

JUNQUEIRA, D. (03 de 10 de 2020). **Confira 5 dos maiores ataques DDoS dos últimos anos**: Disponível em: Olhar Digital.

<https://olhardigital.com.br/fique_seguro/noticia/ataques-de-ddos-aumentam-em-quantidade-e-em-escala/107977> Acesso em: 16 nov. 2020.

LOMILER, J. (2016). **DETECÇÃO DE VULNERABILIDADES E FALHAS DE SEGURANÇA EM REDES DE COMPUTADORES**. Disponível em: <https://cepein.femanet.com.br/BDigital/arqTccs/1311420268.pdf> Acesso em: 15 nov. 2020.

MACÊDO, D. (06 de 07 de 2016). **Introdução ao Nessus: Encontrando e analisando vulnerabilidades**. Disponível em: <https://www.diegomacedo.com.br/introducao-ao-nessus-encontrando-e-analisando-vulnerabilidades/> Acesso em: 15 nov. 2020.

MACEDO, R., FRANCISCATTO, R., CUNHA, G., & BERTOLINI, C. (2018). **REDES DE COMPUTADORES**. Santa Maria | RS: UAB/NTE/UFSM. Acesso em: 16 nov. 2020.

MENEZES, P., CARDOSO, L., & ROCHA, F. (06 de 2015). **SEGURANÇA EM REDES DE COMPUTADORES UMA VISÃO**. Disponível em: <https://periodicos.set.edu.br/exatas/article/download/2258/1296> Acesso em: 16 nov. 2020.

MITSHASHI, R. (2011). **Segurança de Redes**. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0017.pdf Acesso em: 16 nov. 2020.

MORAES, D. (01 de 01 de 2019). **O que é backup e como fazer a cópia de segurança das suas informações** - rockcontent.com - Disponível em: <https://rockcontent.com/br/blog/backup/> Acesso em: 18 nov. 2020.

NETO, U. (s.d.). **DOMINANDO LINUX FIREWALL E IPTABLES**. Rio de Janeiro, Editora Ciência Moderna Ltda, 2004.

PIZZOLATO, R. (Fevereiro de 2020). **O Guia Definitivo sobre Firewall**: Disponível em: <starti.com.br. https://blog.starti.com.br/firewall/> Acesso em: 17 nov. 2020.

REDAÇÃO (08/07/2020). **Ataques virtuais: conheça modalidades e veja como proteger seu celular**; Disponível em: <https://conectaja.proteste.org.br/ataques-virtuais-modalidades-e-protecao/> Acesso em: 17 nov. 2020

REDAÇÃO (08/07/2020). **10 formas de proteger seus dados pessoais na internet**; Disponível em: <https://conectaja.proteste.org.br/ataques-virtuais-modalidades-e-protecao/> Acesso em: 17 nov. 2020

SILVA, Paulo M. **POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES** (2003) Florianópolis - SC Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/84739/198174.pdf?sequence=1&isAllowed=y> Acesso em: 18 out. 2020

SOLHA, Liliana; TEIXEIRA, Renata; PICCOLINI, Jacomo (2020). **Tudo que você precisa saber sobre os ataques DDoS**; Disponível em <https://memoria.rnp.br/newsgen/0003/ddos.html> Acesso em: 18 nov.2020

TANENBAUM, Andrew S. (1981). **Computer Networks**. Amsterdam, Holanda, Tradução: Vandenberg D. de Souza, Editora Campus.

ZOTTO, F. (2012). **SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA PARA SEGURANÇA DE REDES EM PEQUENAS E MÉDIAS EMPRESAS**. Disponível em: <https://docero.com.br/doc/ce8evs> Acesso em: 13 nov. 2020.