ARTIGO CIENTÍFICO

ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

O USO DA FERRAMENTA GNS3 PARA CONSTRUÇÃO DE UM AMBIENTE VIRTUALIZADO PARA CURSOS DE CIBERNÉTICA.

1° SGT MNT COM TIAGO WASEM ZIEMBOWICZ
2° SGT MNT COM MAURO DIEGO ANDRADES DEGLIOMENI

RESUMO:Este artigo descreve o uso da ferramenta GNS3 para construção de um ambiente virtualizado para cursos de cibernética. A pesquisa foi conduzida em áreas relacionadas à prática de laboratórios virtuais em cibernética, para suporte ao ensino-aprendizado. Com base nisso, foram estudadas algumas ferramentas para construção de ambientes virtuais e escolhido o GNS3 (Graphical Network Simulator-3) para essa finalidade. Posteriormente, foi projetada uma arquitetura de rede, similar a um SOC (Security Operations Center) com diversos ativos de rede e máquinas virtuais. Esses últimos, com a finalidade de prover serviços de rede, segurança e monitoramento, foram implementados no GNS3. Após a configuração da arquitetura de rede, testes foram realizados e os resultados apresentados demonstraram a eficiência da ferramenta ao emular a arquitetura de rede proposta. Desta maneira, o ambiente virtualizado proporciona aos alunos mais oportunidade de executarem atividades práticas em cibernética, além do aumento de habilidades e conhecimentos na área.

Palavras Chaves: VIRTUALIZAÇÃO, GNS3, CIBERNÉTICA, LABORATÓRIO.

1 INTRODUÇÃO

Inúmeras são, atualmente, as ameaças à segurança das redes ao redor do mundo. Destacam-se os códigos maliciosos, comumente chamados de malware. O relatório do diretor executivo de segurança da informação da empresa de tecnologia CISCO aborda, em uma de suas seções, a preocupação com a evolução do malware (CISCO, CISO Benchmark, 2019).

Os malwares podem ter diversos objetivos, estando entre os principais a forma de expansão das “botnets”, redes de computadores infectadas utilizadas para fins maliciosos [CISCO, Relatório de Ameaças, 2019]. O combate às botnets se dá por meios de ativos de segurança de redes, como firewalls e sistemas de detecção e prevenção de intrusão, do inglês, Intrusion Detection System (IDS) e, Intrusion Prevent System (IPS).

O desenvolvimento de mecanismos para detecção constitui-se em uma atividade complexa e trabalhosa, que envolve pesquisa e experimentação. Assim, trabalhos que buscam este desenvolvimento, contribuem verdadeiramente para a evolução tecnológica dos ativos de segurança de redes, bem como para a manutenção da segurança no espaço cibernético (GÓMES CARMONA, 2017).

No entanto, implementar ativos e ferramentas para realizar o monitoramento e prevenção das ameaças cibernéticas, requer elevado investimento financeiro, conforme aponta o relatório de Cybersegurança de 2020 da empresa multinacional de tecnologia da informação Accenture.

Adquirir hardwares específicos para equipar laboratórios com o objetivo de treinamento e ensino na área de cibernética, tornou-se cada vez mais oneroso. Além da possibilidade desses hardwares tornarem-se obsoletos em um curto espaço de tempo, é necessário adquirir uma quantidade considerável de equipamentos para equipar um laboratório que atendesse satisfatoriamente a um mínimo de 10 alunos. Sendo assim, um recurso menos dispendioso, que serve ao propósito do ensino e treinamento em cursos ou estágios de cibernética, é a virtualização.

A virtualização já está bastante

consolidada em ambientes de servidores e datacenters (VMWARE, 2020). Quanto ao uso desse mecanismo em ambientes de ensino-aprendizagem na área de cibernética, é o que se pretende discutir neste trabalho.

O intuito da pesquisa será explorar a ferramenta GNS3 (Graphical Network Simulator-3), um software livre que tem por finalidade emular ambientes complexos de rede, disponibilizando ao usuário uma quantidade considerável de ativos para pesquisa e experimentação (GNS3, 2020). Neste contexto, o estudo irá concentrar-se no uso do GNS3 para emular cenários voltados ao ensino em cursos e estágios de proteção cibernética.

2 DESENVOLVIMENTO

Um dos aspectos da proteção cibernética é a segurança de uma rede, usada para garantir a conexão entre inúmeros dispositivos. Desse modo, especialistas em segurança devem, constantemente, passar por treinamentos nos vários aspectos de segurança da rede, ter uma forte base de conhecimento dos diversos serviços de rede e como podem ser protegidos frente às ameaças, na proporção que elas apareçam (CHAPMAN, 2017).

Realizar o treinamento desses especialistas, para que possam responder com eficiência às ameaças em uma rede, requer um ambiente sofisticado, atualizado e dinâmico. Posto isso, a pesquisa irá abordar o uso da virtualização dos serviços de rede, analisando as principais ferramentas destinadas a essa finalidade, suas características e demonstrar o motivo da escolha do software GNS3 para esse trabalho.

Os emuladores de rede oferecem a possibilidade de imitar uma rede sem a necessidade de alguns componentes, como cabos para conexão de dados e rede elétrica. (LANDERS, 2019). A seguir, serão apresentadas as principais ferramentas que podem emular topologias de redes, tanto de baixa como alta complexidade.

2.1 VIRTUALIZADORES DE REDE

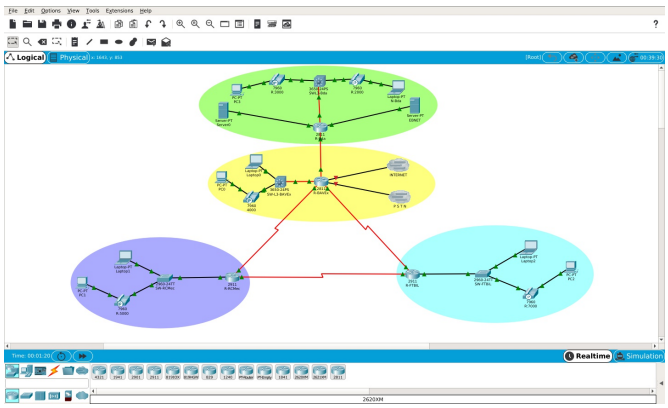
2.1.1 CISCO PACKET TRACER

O packet tracer foi desenvolvido para o ensino de redes de computadores com simulações baseadas nos níveis de conhecimento exigido para obter uma certificação cisco CCNA ou CCNP. É um programa gratuito, com interface gráfica simples e amigável, proporcionando a simulação de ativos de rede, principalmente switches e roteadores da Cisco (PACKET TRACER, 2020).

O programa pode ser utilizado em sistema operacional Windows e Linux. A versão 7.2.1 do Packet Tracer contém recursos para simular soluções de Internet das Coisas (IoT), projetos inteligentes, como cidades e casas inteligentes, com a possibilidade de utilizar Python e Java Script para programar seu comportamento (PACKET TRACER, 2020).

No entanto, o packet tracer não possibilita a integração com uma variedade de dispositivos intermediários ou finais, como soluções de firewall open source e desktop Linux. Está limitado a dispositivos da própria CISCO. A figura 1 mostra um exemplo de uma topologia de rede na interface do packet tracer 7.2.1 para Linux.

FIGURA 1: Topologia de Rede



Fonte: o autor

2.1.2 EVE-NG

O EVE-NG (Emulated Virtual Environment – Next Generation) é uma ferramenta para emulação de ambientes de

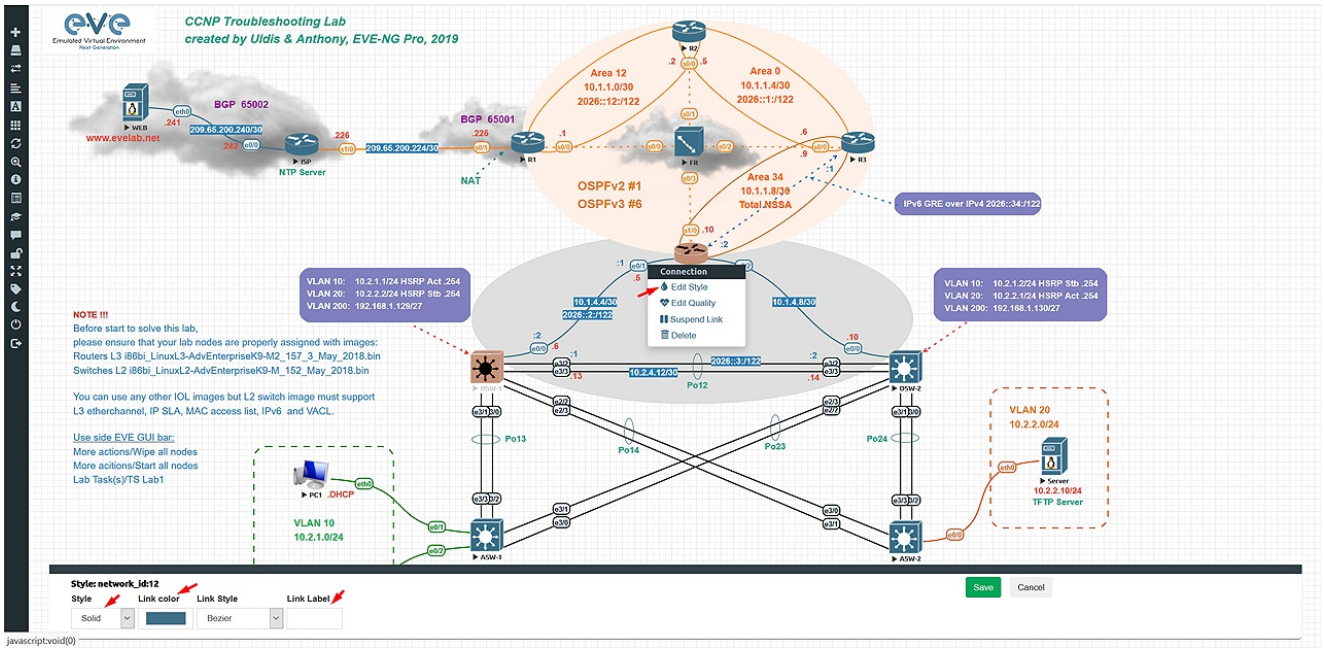
rede que vem sendo bastante aplicada em testes de vulnerabilidades de segurança, para testar novas tecnologias como as Redes Definidas por Software (SDN – Software Defined Network) ou para desenvolvedores que desejam testar seus softwares (BALYK, 2019).

Com o EVE, pode-se emular redes corporativas complexas, homologar soluções e mudanças em uma topologia antes de colocá-las em produção. Outros recursos interessantes são a construção de ambientes de POCs (Proof of Concepts) para clientes, a análise de tráfego de pacotes com o programa Wireshark e testes em soluções para problemas reais (BALYK, 2019).

Este emulador está disponível nas versões Community Edition, Professional Edition e Learning Centre Edition. A versão Community é gratuita, oferecendo menos recursos que a versão profissional, que é paga, mas, mesmo assim, a versão gratuita possibilita a criação de inúmeros cenários de rede. Deve ser instalado preferencialmente em ambiente de servidor, pois requer recursos de hardware consideráveis para um correto desempenho (EVE-NG, 2020).

Uma das vantagens do EVE-NG é a possibilidade de integração com vários tipos de dispositivos de diversos fabricantes, como Cisco, Checkpoint, Palo Alto, PfSense, Mikrotik, Dell, HP, entre outros. Através da integração com o emulador “Dynamips”, pode emular o hardware de switchs e roteadores da Cisco, e com o software livre QEMU, possibilita a execução da maioria dos sistemas operacionais como Linux, Windows, FreeBSD e outras arquiteturas suportadas (BALYK, 2019). A figura 2 exibe um exemplo de topologia de rede elaborada no EVE-NG.

FIGURA 2: Topologia de rede EVE



Fonte: www.eve-ng.net

2.1.3 GNS3

O GNS3, do inglês “Graphical Network Simulator-3” é um emulador de software de rede que permite a combinação de dispositivos virtuais e reais, usados para simular redes complexas (GNS3, 2020).

É uma ferramenta de código aberto e utiliza vários softwares emuladores como o Dynamips, Dynagen, QEMU, Docker, VirtualBox, entre outros, capazes de emular ambientes baseados em Linux e Windows, além dos diversos dispositivos de rede dos principais fabricantes do mercado (WONLY;SZOLTYSIK, 2014).

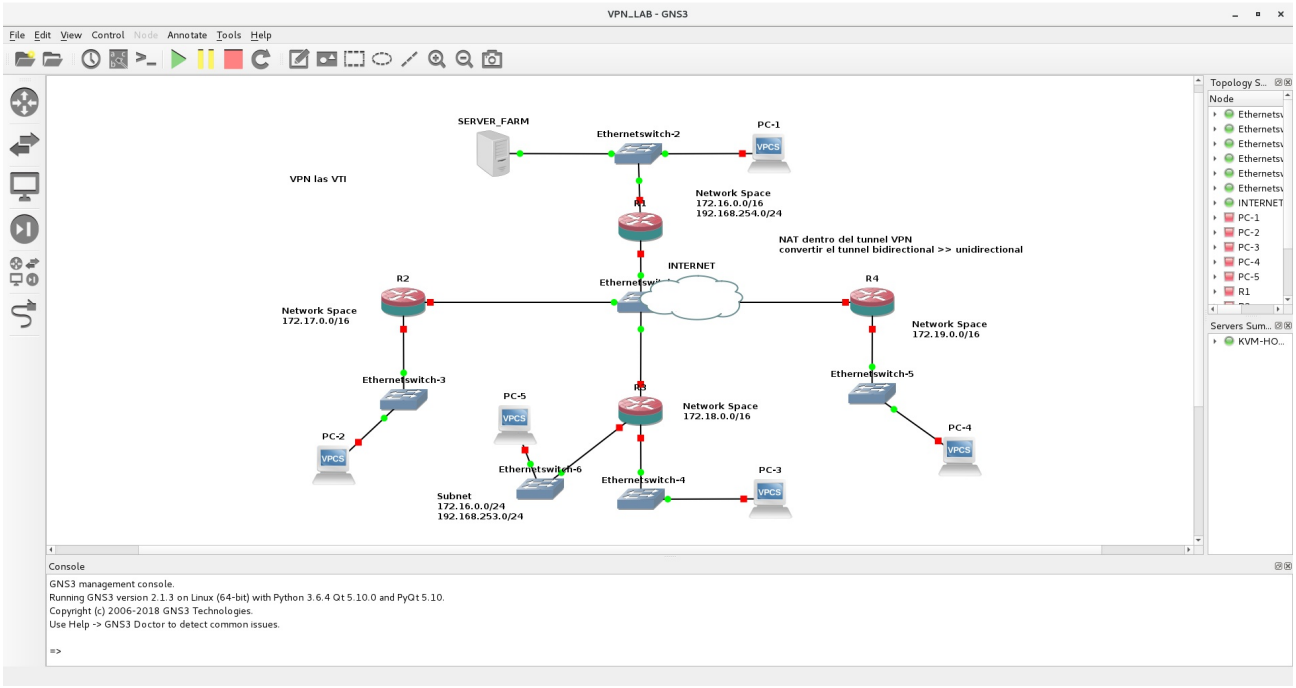
O GNS3 pode ser instalado nas plataformas Linux, Windows e MAC OS, oferecendo também um conjunto de funcionalidades ao se integrar com aplicativos terminais como Putty, VNC, Gnome Terminal,

Windows telnet client, entre outros. Realiza integração também com o Wireshark, fazendo captura e análise de pacotes, assim como em um ambiente de rede virtual (MOHTASIN, 2016).

Uma das vantagens do GNS3 é a simulação de rede em tempo real para testes de pré-implementação, sem a necessidade de hardware de rede e a criação de mapas de rede dinâmicos para a solução de problemas e teste de prova de conceito (GÓMEZ CARMONA, 2017).

A seguir, a figura 3 mostra um exemplo da interface GUI do GNS3.

FIGURA 3: Interface do GNS3



Fonte: https://gns3.com

A tabela a seguir resume as principais características e recursos das três ferramentas para virtualização de redes encontradas na homepage de cada uma delas:

TABELA1: Comparação entre virtualizadores de rede

Característica / Recurso	Ferramentas		
	Packet Tracer	EVE-NG Community	GNS3
Versão Atual	7.2.1	2.0.3-110	2.2.8
Tipo	simulador	emulador	emulador
Licença	livre	livre	livre
Custos	gratuito	gratuito	gratuito
Instalação	fácil	complexa	complexa
Processador	n/a	Core i5	Core i5
Memória	n/a	8 GB	*gb
HD	n/a	50 GB	35 GB
Virtualização	não	sim	sim
Integração	apenas cisco	vários	vários

Fonte: autores

Importante destacar que os dados compilados na tabela se referem aos requisitos mínimos para instalação. O número de instâncias virtuais que podem ser implementadas varia com a capacidade do hardware físico no qual está instalada a ferramenta.

2.2 MODELO PROPOSTO

Após uma breve análise das ferramentas, levando principalmente em consideração o objetivo da pesquisa, sobre um ambiente virtual adequado para o ensino de proteção cibernética, optou-se pela ferramenta GNS3. A principal vantagem apresentada pelo GNS3 frente as outras ferramentas, foi o fato de ser totalmente gratuito e possibilitar uma integração com um número considerável de sistemas operacionais e dispositivos de rede.

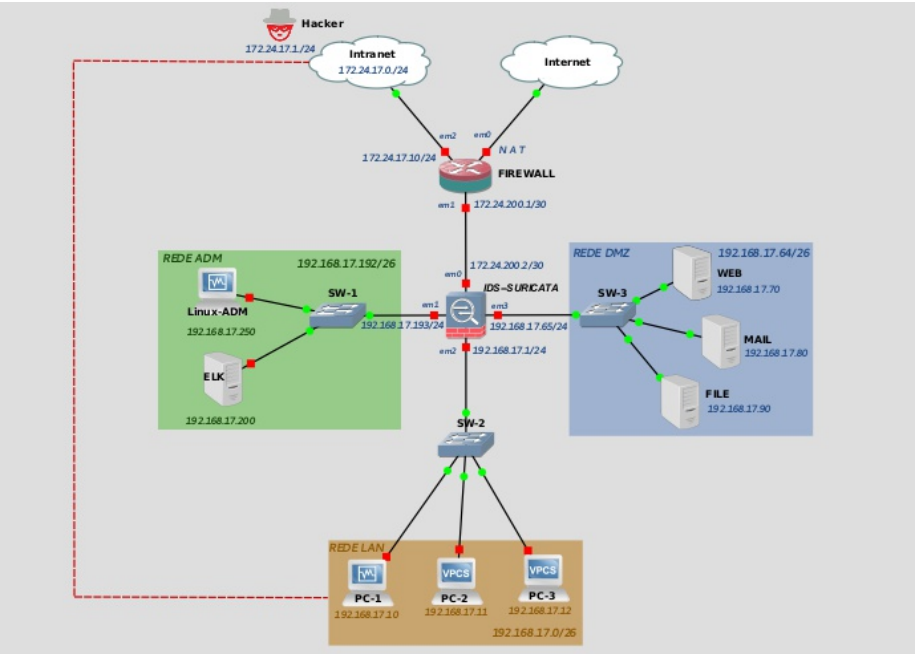
O packet tracer fica limitado apenas aos dispositivos de rede da cisco e estes não possuem os mesmos recursos disponíveis nos equipamentos reais. O EVE-NG, apesar de ser uma ferramenta excelente para o acesso remoto, em sua versão gratuita, não é integrado dinamicamente com o wireshark, recurso importante para análise de pacotes e essencial em assuntos que envolvem proteção cibernética.

Vários outros quesitos que serão tratados nas próximas seções deste artigo favoreceram a utilização do GNS3.

Diversos cenários poderiam ser implementados na abordagem de uma topologia de rede voltada à proteção cibernética. Dessa forma, a topologia proposta visa apresentar uma rede de baixa complexidade, porém voltada a explorar os serviços de rede mais visados por cibercriminosos, bem como as ferramentas necessárias para identificar e tentar reduzir possíveis ataques.

A figura 4 apresenta a topologia de rede que será trabalhada nessa pesquisa, os serviços de rede implementados e os recursos necessários para realizar a proteção da rede, ambiente totalmente virtualizado, gerenciado pelo GNS3.

FIGURA 4: Topologia GNS3



Fonte: autor

2.2.1 TOPOLOGIA DE REDE

Para cumprir o objetivo de apresentar um ambiente virtual capaz de simular uma rede voltada à proteção cibernética, resolveu-se utilizar os dispositivos de rede descritos a seguir, que representam a arquitetura mínima em um Centro Operacional de Segurança, (SOC - Security Operational Center) (DEMERTZIS, 2019):

2.2.1.1 FERRAMENTAS DE SEGURANÇA E MONITORAMENTO:

Firewall: o sistema escolhido foi o pfSense, que é uma distribuição de firewall de rede gratuita, baseada no sistema operacional FreeBSD com um kernel personalizado e incluindo pacotes de software livre de terceiros para funcionalidades adicionais (PFSENSE, 2020).

IPS/IDS: O Suricata é um mecanismo de detecção de ameaças à rede gratuito e aberto, maduro, rápido e robusto. O mecanismo Suricata é capaz de detecção de intrusão em tempo real (IDS), prevenção de intrusão em linha (IPS), monitoramento de segurança de rede (NSM) e processamento de pcap (captura de pacotes) offline. O pacote Suricata foi instalado no sistema pfSense. (SURICATA, 2020).

Servidor ELK-Stack: "ELK" é o acrônimo para três projetos open source: Elasticsearch, Logstash e Kibana. O Elasticsearch é um mecanismo de busca e análise. O Logstash é um pipeline de processamento de dados do lado do servidor que faz a ingestão de dados a partir de inúmeras fontes simultaneamente, transforma-os e envia-os para um “esconderijo” como o Elasticsearch. O Kibana permite que os usuários visualizem dados com diagramas e gráficos no Elasticsearch. A pilha ELK foi instalada em uma VM (Virtual Machine) com sistema operacional Debian9. (ELK, 2020)

2.2.1.2 SERVIÇOS DE REDE

Servidor WEB: uma VM com sistema operacional Debian 9 e com o servidor web Apache2 instalado.

Servidor MAIL: uma VM com sistema operacional Debian 9 simulando um servidor de e-mail.

Servidor FILE: uma VM com sistema operacional Debian 9 simulando um servidor de FTP.

2.2.1.3 DEMAIS ATIVOS

PC ADM: uma VM com sistema operacional Debian9 e GUI XFCE, com a finalidade de realizar a gerência dessa arquitetura.

PC1, PC2 e PC3: Vms com sistema operacional Debian 9 e GUI XFCE que representam a rede LAN nessa topologia, ou seja, o usuário final.

A topologia é completada com três switchs e duas nuvens NAT (Network Adress Translation), onde uma simula uma rede intranet e outra a internet. Todas as máquinas virtuais mencionadas são integradas ao GNS3 através do VirtualBox. O ícone representando um Hacker é uma VM com o Sistema Operacional Kali Linux, também integrado por meio do VirtualBox.

A versão do GNS3 na qual foram realizados os testes é a 2.2.5 para Linux, pois a ferramenta está instalada em um notebook com sistema operacional Debian GNU/Linux 9 (stretch) 64-bit, com 16 GB de memória RAM, processador Intel Core i5-4200U CPU de 1.60GHz × 4 (quad-core) e disco de 240 GB HD SSD. A versão do VirtualBox utilizada nos testes é a 6.0.4 para o Linux Debian.

3 CONCLUSÃO

3.1 TOPOLOGIA E CONECTIVIDADE

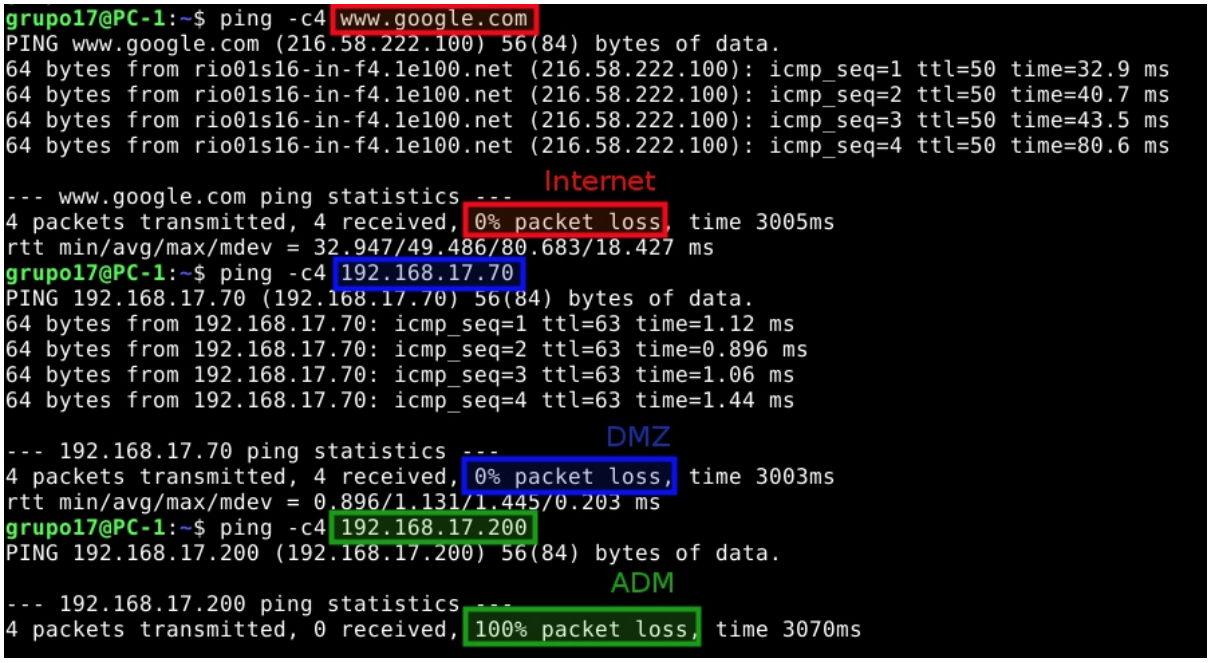
Com a finalidade de validar a topologia apresentada na seção anterior, interconectar e integrar seus elementos, foram realizados testes de conectividade entre os dispositivos.

3.1.1 CONECTIVIDADE COM A REDE LAN

A figura 5, demonstra que tomando como origem o PC-1, utilizando o comando ping obtivemos sucesso na comunicação da rede LAN com as redes externas conectadas e ele,

quais sejam, Internet e rede DMZ. A rede LAN não tem acesso para a rede ADM.

Figura 5: Conectividade com a LAN

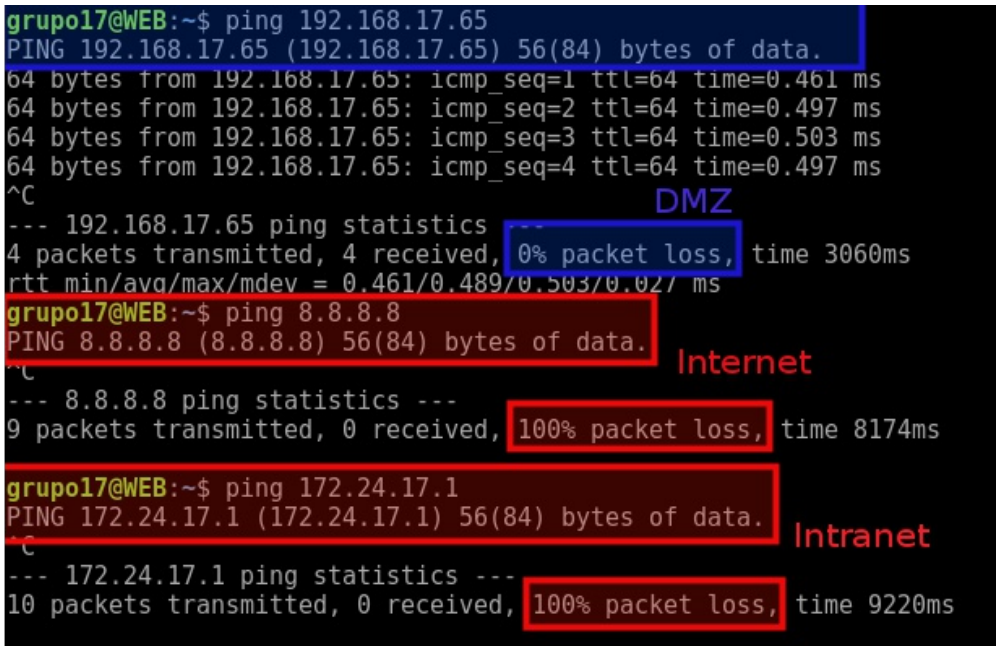


Fonte: autores.

3.1.2 CONECTIVIDADE DA REDE DMZ

A Figura 6, demonstra que utilizando como origem o Servidor WEB, obtivemos sucesso na comunicação dentro da própria DMZ, mas a mesma não se comunica com as redes intranet e internet, devido às configurações realizadas no firewall. Não foram permitidos que pacotes icmp originados da rede DMZ saíssem para a internet ou intranet, comportamento esse, padrão para uma rede DMZ.

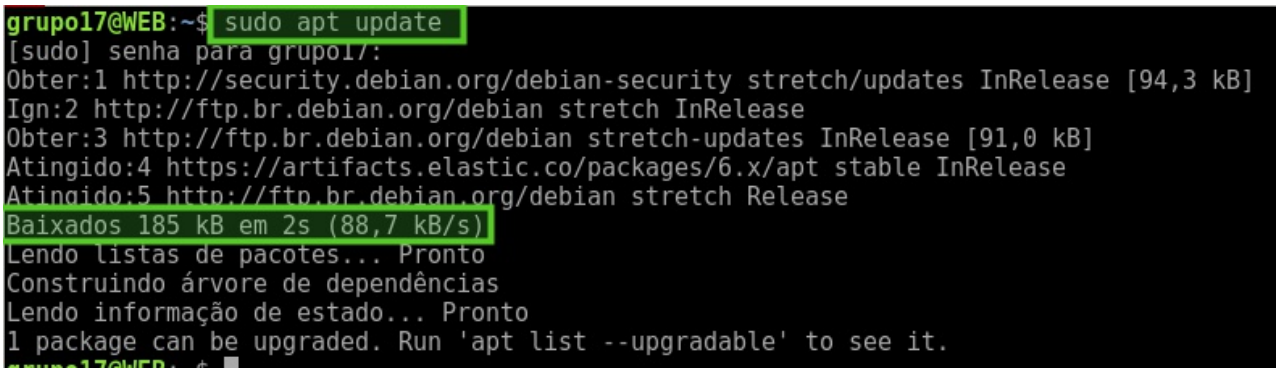
FIGURA 6: Conectividade com a DMZ



Fonte: autor.

Para comprovar que a configuração do firewall só bloqueou a saída de pacotes icmp para internet oriundos da DMZ, a figura 7 exibe o resultado de uma atualização de pacotes (comando update) realizado através do servidor WEB.

FIGURA 7: Atualização de pacotes

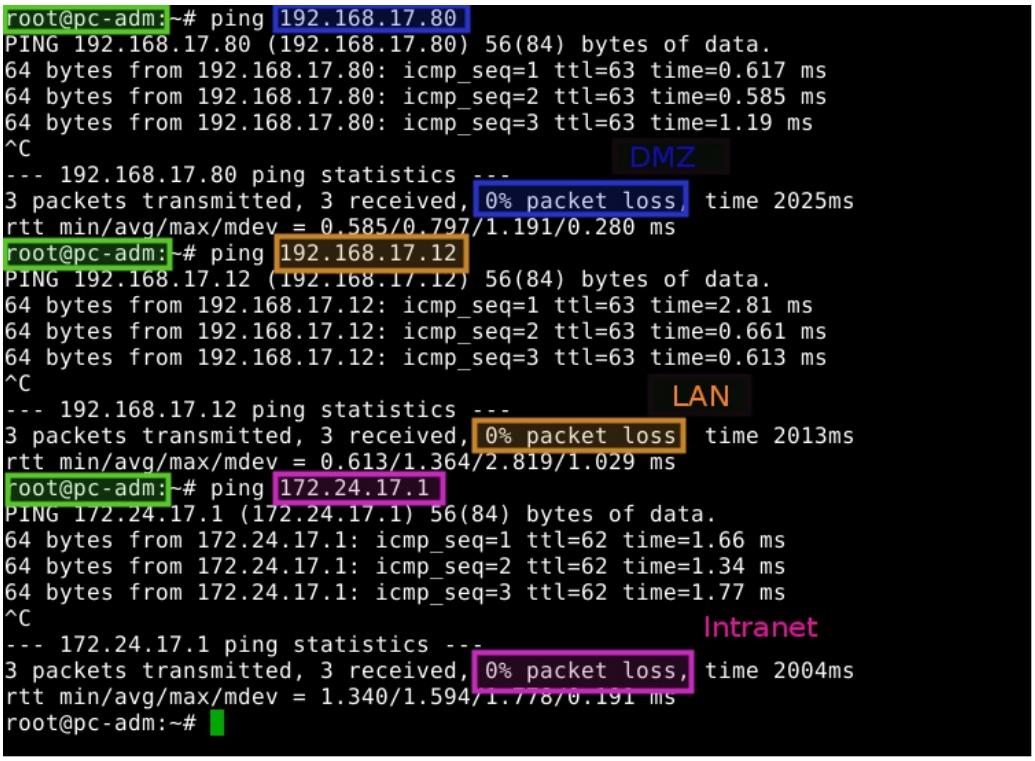


Fonte: autor.

3.1.3 CONECTIVIDADE DA REDE ADM

A figura 8, exibe a comunicação originando do PC-ADM para a rede DMZ, LAN e Intranet, através do comando ping. O host PC-ADM deve ter conectividade com todas as redes pois é o host responsável pela gerência da rede.

FIGURA 8: Conectitidade com a rede ADM



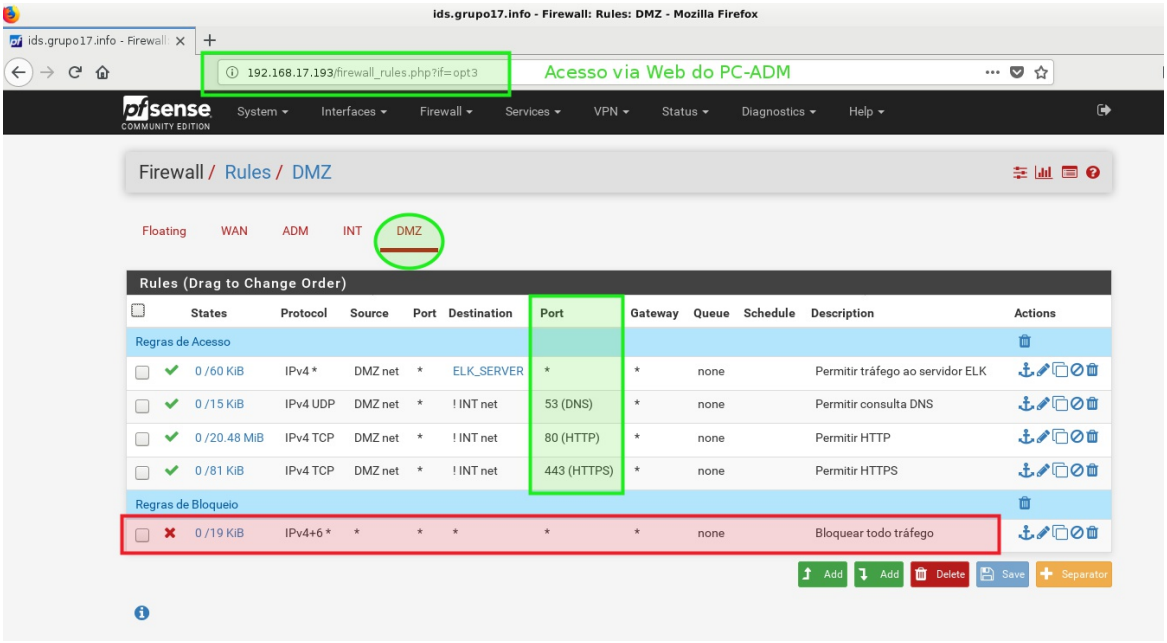
Fonte: autor.

Os testes de conectividade demostraram que o GNS3 consegue realizar a gerência das interfaces de rede das Vms do VirtualBox, o que comprova a integração bem sucedida entre as ferramentas.

3.2 REGRAS DE FIREWALL

Os resultados obtidos nos testes de conectividade apresentados na subseção anterior, principalmente aqueles referentes à rede DMZ com saída para internet e intranet, foram fruto das configurações realizadas no firewall. As regras de firewall da rede DMZ estão descritas na figura 9.

FIGURA 9: Regras de Firewall



Fonte: autor.

Através da imagem, verificamos que as regras foram configuradas no firewall pfSense em sua interface web via PC-ADM. Essa configuração comprova que a topologia de rede no GNS3 se comporta como se fosse uma arquitetura real. O usuário ou aluno que utiliza esses recursos dificilmente observará alguma diferença, proporcionando assim, habilidades práticas elevadas que auxiliam consideravelmente na construção do seu conhecimento.

3.3 GERAÇÃO DE TRÁFEGO TCP

Com a finalidade de realizar mais testes no ambiente virtual, esta subseção está dedicada à geração de tráfego TCP. A geração desse tráfego possibilita testar a integração do GNS3 com o aplicativo de captura de tráfego wireshark (WIRESHARK, 2020), com o auxílio do programa “Iperf”, que tem por finalidade testar a largura de banda em uma conexão, utilizando protocolos como TCP, UDP, FTP e outros (IPERF, 2020).

As figuras 10 e 11, mostram respectivamente a geração do tráfego TCP via iperf de um host cliente (Kali Linux), situado na rede intranet para o servidor WEB hospedado na DMZ.

FIGURA 10: Tráfego TCP cliente

```
root@twz-debian:/home/tiagowz# iperf -c 192.168.17.70
------------------------------------------------------------
Client connecting to 192.168.17.70, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 172.24.17.1 port 48944 connected with 192.168.17.70 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  84.2 MBytes  70.3 Mbits/sec
```

Fonte: autor.

FIGURA 11: Tráfego TCP servidor

```
grupo17@WEB:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.17.70 port 5001 connected with 172.24.17.1 port 48944
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.1 sec  84.2 MBytes  69.8 Mbits/sec
```

Fonte: autores.

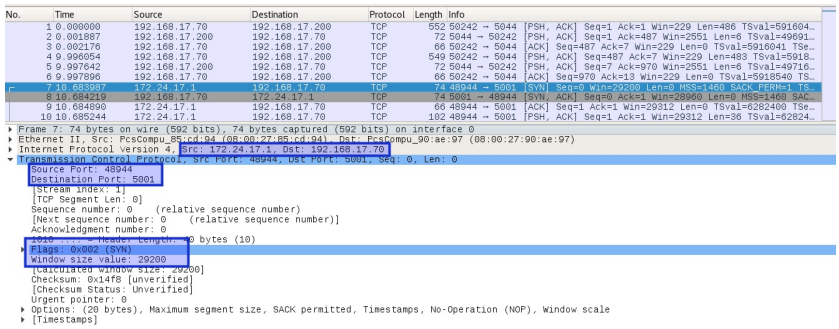
Importante destacar que, antes de se iniciar o programa iperf, foi realizada a captura de tráfego via wireshark no GNS3, na conexão entre o servidor Web e o switch 3. O tráfego foi originado da Intranet (HostOnly) no VirtualBox, por isso o endereço que origina a conexão analisada por meio do wireshark é o endereço IP do firewall (172.24.17.1:48944) gateway da rede intranet. O destino da conexão é o host WEB (192.168.17.70:5001). Nesse host, o Iperf está rodando em modo servidor. Na análise do tráfego TCP, figura 12, podemos observar o seguinte:

Antes do início da comunicação entre o cliente na Intranet e o Servidor WEB, acontece o processo de handshake TCP. O cliente envia o pacote SYN (pacote de sincronismo que é o primeiro passo para iniciar qualquer conexão numa rede TCP/IP) ao servidor, esse responde ao cliente com um pacote SYN/ACK. O processo de handshake do TCP termina quando o cliente envia o pacote ACK confirmando ao servidor que recebeu o SYN/ACK e a comunicação pode começar.

A comunicação do cliente é realizada na porta 48944 e o servidor recebe a conexão na porta TCP padrão que o Iperf trabalha, a porta 5001.

Ao final do fluxo de TCP entre cliente e servidor (quando o Iperf termina o fluxo) as mensagens trocadas entre servidor e cliente são o [FIN,ACK], onde o servidor informa que não tem mais nada a transmitir e o cliente responde ao servidor com o [ACK] e depois envia um [FIN,ACK] ao servidor que responde a finaliza a comunicação com um [ACK].

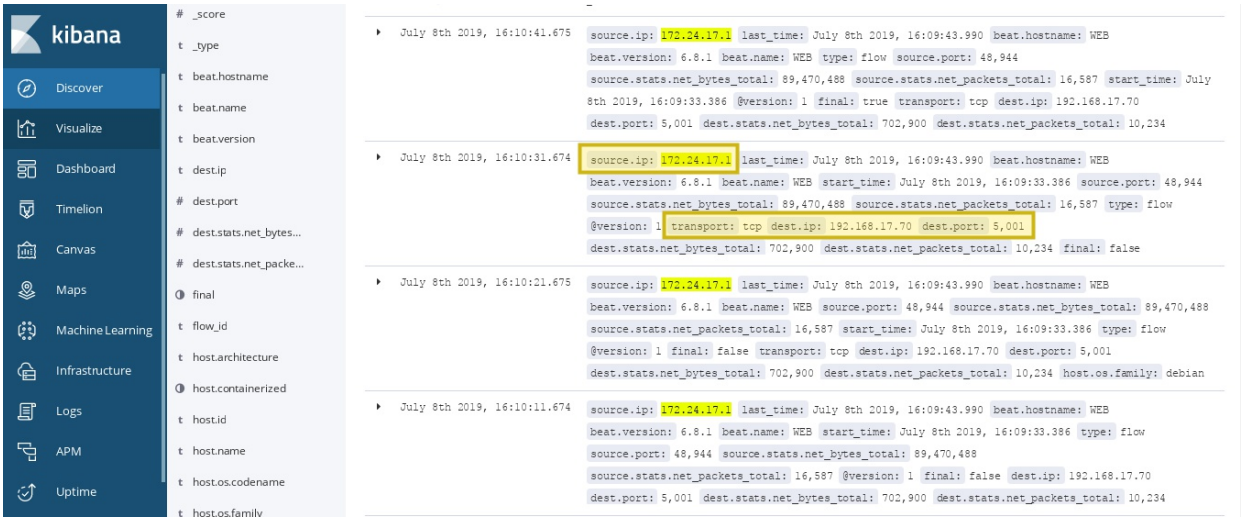
FIGURA 12: Captura wireshark



Fonte: autor

Para finalizar os testes desta seção, serão apresentados os logs do tráfego TCP gerado via iperf. Os logs são exibidos do servidor ELK da rede ADM, conforme representados na figura 13:

FIGURA 13: Visualização de logs no Kibana



Fonte: autor.

Ao implementar uma busca simples, com o endereço IP da Intranet (172.24.17.1), observamos que os logs do tráfego gerados via Iperf foram enviados com sucesso. Nesse log, identifica-se o endereço IP de origem (172.24.17.1), porta de origem (48944), endereço IP de destino (192.168.17.70), porta de destino (5001) e o tipo de protocolo da camada de transporte (TCP). Ao verificar que os logs estão sendo gerados, certifica-se que a infraestrutura de rede montada está funcional, e o servidor ELK funcionando de forma correta para analisar os logs do tráfego gerados para teste.

3.4 AVALIAÇÃO

Os resultados apresentados nessa seção puderam mostrar a eficiência do GNS3 quanto à criação de um laboratório virtual para trabalhar em cursos de cibernética. Vale destacar a importância da integração com o VirtualBox, tornando o laboratório muito flexível com a execução de inúmeras tarefas de rede, idênticas ao mundo real. O ambiente do laboratório é um bom campo de testes para estudantes em cibernética antes de começar trabalhando com equipamentos reais, onde erros podem causar falhas catastróficas (MOHTASIN, 2016).

Vale destacar que o laboratório virtual é ideal para alunos que tentam aprender como instalar, configurar e testar os dispositivos de rede, bem como arquiteturas e topologias de rede voltadas à proteção cibernética. Não é adequado para testar o desempenho dos dispositivos de rede, pois o resultado não pode ser comparado com um ambiente real.

O número de instâncias virtuais que são adicionadas em um laboratório é limitado à capacidade do hardware físico subjacente. Para criar um laboratório com mais recursos, ativos de rede e máquinas virtuais, precisa-se de mais capacidade de hardware na máquina física.

O ambiente virtual proposto é usado em máquina local, apesar do GNS3 permitir a execução de laboratórios de forma remota, o estudo foca na criação de laboratório local hospedado em sistema operacional Linux. A vantagem de usar o GNS3 em SO Linux é a

possibilidade de utilizar a integração de recursos como Docker, máquinas virtuais QEMU, sem a necessidade de uma máquina virtual GNS3, conhecida como GNS3 VM, necessária quando instalado em sistema operacional Windows. O próprio kernel do Linux se encarrega de disponibilizar esses recursos, economizando recursos de hardware do hospedeiro (GNS3, 2020).

Assim, se implementado com sucesso, este laboratório pode ser usado como recurso essencial para que os alunos realizem práticas de rede e cibernética. Além disso, o ambiente do laboratório é totalmente escalável, podendo ser replicado e implementado em outro computador. Os alunos devem ser capazes de implementar facilmente instâncias de dispositivos de rede da vida real, fornecendo uma maneira acessível e de baixo custo para executarem práticas de rede e cibernética.

3.5 CONSIDERAÇÕES FINAIS

O principal objetivo deste artigo foi apresentar a ferramenta GNS3 como solução para elaboração de ambientes virtuais para a prática de atividades em cursos de proteção cibernética. Criar um laboratório virtual, ajuda a superar os problemas existentes de hardware e acessibilidades limitadas. O ambiente apresentado permite configurar, gerenciar e testar diversos dispositivos de rede e máquinas virtuais, proporcionando a aquisição de habilidades práticas aos alunos.

No campo da cibernética integram-se diferentes tipos de hardware, software e ambientes de telecomunicações. Existe uma quantidade significativa de conhecimento e desenvolvimento de habilidades necessárias para trabalhar na área cibernética. De acordo com Tegliacane et al (2016), no geral, os alunos precisam de oportunidades em alternadas soluções de laboratório para que possam desenvolver os conhecimentos necessários. Desta maneira, poderão construir e manter sistemas computadorizados e em rede, mesmo quando o acesso ao treinamento físico do hardware é limitado.

Além disso, uma pesquisa realizada em 2019 mostrou que alunos com oportunidade de realizarem atividades práticas (laboratórios) na área de TI tem desempenho superior na aquisição de habilidades em comparação àqueles que possuem apenas hardwares físicos (limitados a execução de testes) para executarem exercícios práticos (LANDERS, 2019).

À vista disso, os simuladores de habilidades em tecnologia da informação (TI) podem ser usados para complementar ou substituir hardware caro para o ensino e aprendizagem em computadores e habilidades de software, redes e segurança cibernética (DEWEY & SHAFFER, 2016; GERCEK, SALEEM, & STEEL, 2016). Segundo Ghani (2015), os avanços tecnológicos tornaram possível que objetivos previamente alcançados apenas com a realização de atividades práticas, hoje pudessem ser atingidos usando simulações.

Nesse sentido, este artigo propôs o uso do GNS3 como ambiente virtual para prática de atividades nos cursos de cibernética, proporcionando aos alunos, criarem, testarem e analisarem seus próprios laboratórios em um ambiente praticamente livre de custos.

REFERÊNCIAS

BALYK, Nadiia et al. Designing of Virtual Cloud Labs for the Learning Cisco CyberSecurity Operations Course. 2019.

CHAPMAN, Samuel et al. Can a network attack be simulated in an emulated environment for network security training?. Journal of Sensor and Actuator Networks, v. 6, n. 3, p. 16, 2017.

DEMERTZIS, Konstantinos et al. A próxima geração do centro de operações de segurança cognitiva: arquitetura lambda analítica adaptativa para defesa eficiente contra-ataques adversários. Big Data e computação cognitiva , v. 3, n. 1, p. 6, 2019.

GHANI, Usman. Efeito de mecanismos de feedback no aprendizado dos alunos no uso de treinamento baseado em simulação em um

programa de engenharia da computação. In: Conferência de Líderes de Engenharia 2014 sobre Educação em Engenharia. Imprensa da Universidade Hamad bin Khalifa (HBKU Press), 2015. p. 59

GÓMEZ CARMONA, Joaquín. Proposta de manual de práticas de laboratório de redes usando o emulador GNS3. 2017. Tese de Doutorado. Universidade Central "Marta Abreu" de Las Villas, Faculdade de Engenharia Elétrica, Departamento de Eletrônica e Telecomunicações.

LANDERS, Kathy Michelle. Usando simulações para se preparar para faculdades e carreiras em tecnologia da informação. 2019.

MOHTASIN, R. et al. Desenvolvimento de um laboratório de rede virtualizado usando as estações de trabalho GNS3 e VMware. In: Conferência Internacional de 2016 sobre comunicações sem fio, processamento de sinais e redes (WiSPNET) . IEEE, 2016. p. 603-609.

SILVA, Isaias Batista da et al. Gnsmood: um aplicativo web integrado ao ambiente virtual de aprendizado que permite a comunicação de dispositivos de rede com o servidor de simulação gns3. 2018.

WOLNY, Wiesław; SZOŁTYSIK, Mateusz. Visão geral da virtualização de ambientes de redes de computadores existentes para aprendizado de redes de computadores. Studia Ekonomiczne , v. 188, p. 250-264, 2014.

ACCENTURE, Ratório de Cybersegurança 2020. Disponível em https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf. Acesso realizado em 08 de maio de 2020.

CISCO, Cybersecurity Series 2019 - CISO Benchmark. Disponível em:< https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/ciso-benchmark-optimized.pdf?.>. Acesso em: 28 abr de 2020.

CISCO, Cybersecurity Series 2019 - Threat. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/cybersecurityseries-threat.pdf?.> Acesso em: 28 abr de 2020.

ELK, 2020. Disponível em:< https://www.elastic.co/pt/what-is/elk-stack.> Acesso em: 14 de abr de 2020.

EVE-NG, 2020. Disponível em https://www.eve-ng.net/index.php/documentation/. Acesso realizao em 26 de abril de 2020.

GNS3, Software, 2020. Disponível em https://gns3.com/software. Acesso realizado em 24 de abril de 2020.

IPERF, 2020. Disponível em https://iperf.fr/. Acesso realizado em 07 de maio de 2020.

PACKET TRACER, 2020. Disponívelm em https://www.netacad.com/pt-br/courses/packet-tracer. Acesso realizado em 26 de abril de 2020.

PFSENSE, 2020. Disponível em https://www.pfsense.org/. Acesso realizado em 14 de abril de 2020.

VMWARE, Virtualização, 2020. Disponível em https://www.vmware.com/br/solutions/virtualization.html. Acesso realizado em 24 de abril de 2020.

WIRESHARK, 2020. Disponível em https://www.wireshark.org/. Acesso realizado em 02 de maio de 2020.