UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI
Curso de Graduação em Sistemas de Informação
Camila Aparecida Pereira Alves

ESTUDO SOBRE DETECÇÃO E PREVENÇÃO DE ATAQUES DE FORÇA BRUTA

Diamantina
2023

Camila Aparecida Pereira Alves

ESTUDO SOBRE DETECÇÃO E PREVENÇÃO DE ATAQUES DE FORÇA BRUTA

Trabalho de Conclusão de Curso apresentado ao Curso de Sistemas de Informação da Universidade Federal dos Vales do Jequitinhonha e Mucuri, como requisitos parcial para conclusão do curso.

Orientador: Eduardo Pelli

Diamantina
2023

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

FOLHA DE APROVAÇÃO

Camila Aparecida Pereira Alves

ESTUDO SOBRE DETECÇÃO E PREVENÇÃO DE ATAQUES DE FORÇA BRUTA

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Federal dos Vales do Jequitinhonha e Mucuri.

Aprovada em 06/02/2023

BANCA EXAMINADORA

Prof Dr. Eduardo Pelli
Faculdade de Ciências Exatas - UFVJM

Prof. Dr. Rafael Santin
Faculdade de Ciências Exatas - UFVJM

Prof. Dr. Áthila Rocha Trindade
Faculdade de Ciências Exatas - UFVJM

Documento assinado eletronicamente por **Áthila Rocha Trindade**, **Servidor (a)**, em 10/02/2023, às 15:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rafael Santin**, **Servidor (a)**, em 10/02/2023, às 19:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufvjm.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0980394** e o código CRC **48F64F31**.

Dedico este trabalho aos meus pais, Ataíde Alves e Vilma Aparecida, que nunca mediram esforços para que o mesmo fosse possível.

AGRADECIMENTOS

Primeiramente a Deus pela grande oportunidade que me proporcionou e pela força que sempre me deu todos os dias dessa trajetória. Agradeço aos meus pais, Ataíde e Vilma pelo apoio incondicional e todo o esforço que fizeram para que hoje a graduação fosse uma realidade na minha vida. Aos meus amigos que estiveram nessa caminhada comigo, principalmente Caliny e Tiago, que sempre me apoiaram e passaram por diversas situações juntamente à mim, desde obstáculos aos momentos de conquista. Por fim quero agradecer ao meu professor orientador Eduardo Pelli, por todas as vezes em que me orientou, ajudou e foi paciente comigo nessa jornada. Saibam que todos foram de extrema importância para que eu pudesse chegar nesse momento, muito obrigada!

A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos. (NAISBITT, 2020).

RESUMO

Um dos campos presentes na área de Tecnologia que mais avançaram nos últimos anos, foi a Internet. A facilidade de acesso às mais diversas informações, modos de comunicação, entre tantas outras vantagens, trouxeram grandes avanços no modo de viver das pessoas e não menos importante, na execução das atividades cotidianas de uma organização. Esse avanço tecnológico é constante, com ferramentas sempre em evolução, exigindo que as empresas se mantenham sempre atualizadas para uma utilização eficaz dos dispositivos de modo em geral. Porém é importante salientar que, da mesma maneira que todos os dias acompanhamos o crescimento tecnológico para o benefício da sociedade, também existem aprimoramentos nas tentativas de encontrar pontos falhos na troca de informações entre pessoas ou empresas, ou seja, *hackers* estão a todo momento se aperfeiçoando na realização dos ataques, exigindo que a área de Segurança da Informação esteja em constante desenvolvimento. Atualmente existem diversos tipos de ataques, sendo alguns deles de fácil realização, como por exemplo, o ataque de força bruta, que busca o acesso às informações por meio de tentativas de quebra de senhas de servidores, roteadores, sites, etc. Para tentar identificar este tipo de ataque, é importante analisar alguns pontos, dentre eles a quantidade de fluxo entre dois *hosts* e tentativas de conexões. Este trabalho busca analisar, identificar e comparar duas técnicas de identificação e/ou prevenção de ataques, em específico, o ataque de força bruta, sendo a primeira técnica por configurações de *firewall* do dispositivo, que são capazes de impedir o ataque, e a segunda com as configurações do protocolo *IPFIX* aplicado ao conjunto de ferramentas da *Elastic Stack*, e através dos dados coletados e técnicas de análises de comportamento do fluxo de rede, desenvolver um mecanismo que seja capaz de identificar um ataque de força bruta. Sob essa ótica, define-se que, a escolha de qual técnica seguir para implementação, depende de alguns fatores, dentre eles, a infraestrutura da rede.

Palavras-chave: Redes de Computadores. *Mikrotik*. *Elasticsearch*. Fluxo de Rede. Análise por Comportamento.

ABSTRACT

One of the fields present in the area of Technology that has advanced the most in recent years is the Internet. The easy access to the most diverse information, and modes of communication, among many other advantages, obtained great advances in people's dynamism and, not least, in the execution of the daily activities of an organization. This technological advancement is constant, with ever-evolving tools, requiring companies to keep up-to-date for the effective use of devices in general. However, it is important to point out that, in the same way, that we follow technological growth every day for the benefit of society, there are also improvements in attempts to find flawed points in the exchange of information between people or companies, that is, hackers are improving at all times in performing attacks, requiring that the Information Security area must be in constant development. There are currently several types of attacks, some of which are easy to perform, such as brute force attacks, which seek access to information through attempts to crack passwords on servers, routers, websites, etc. In order to identify this type of attack, it is important to analyze some points, among them the amount of flow between two hosts and connection attempts. This paper seeks to analyze, identify and compare two techniques for identifying and/or preventing attacks, in particular, the brute force attack, the first technique is based on device settings, which are capable of preventing the attack, and the second uses the IPFIX protocol settings applied to the Elastic Stack toolset, and through the collected data and analysis of network flow behavior, design a mechanism that is capable of identifying a brute force attack. From this perspective, we determine the choice of which technique to follow in the implementation depends on some factors, including the network infrastructure.

Keywords: Computer Networks. *Mikrotik*. *Elasticsearch*. Network Flows. Behavior Analysis.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACK	*Acknowledgement*
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
ELK	*Elastic Logstash Kibana*
FIN	*Finish*
FTP	*File Transfer Protocol*
HIDS	*Host Intrusion Detection System*
HTTP	*Hyper Text Transfer Protocol*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPFIX	*Internet Protocol Flow Information Export*
IPS	*Intrusion Prevention System*
LAN	*Local Area Network*
NIDS	*Network Intrusion Detection System*
SGMP	*Simple Gateway Management Protocol*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SYN	*Synchronize*
TCP	*Transmission Control Protocol*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

A internet com o passar dos anos, se tornou o maior meio de comunicação usado globalmente. Hoje em dia pessoas de diferentes partes do mundo, através da rede de computadores, se conectam e trocam dados entre si, fazendo com que a distância se minimize e questões do âmbito pessoal ou profissional que antigamente tinham a necessidade de serem resolvidas presencialmente, atualmente dispensam esse requisito, surgindo várias possibilidades que não deixam a desejar na qualidade e eficácia de suas decisões e resultados. Profissionalmente, as empresas veem seus negócios se tornarem mais rápidos, além de facilitar os seus processos.

A facilidade à esse acesso ilimitado, faz com que o número de usuários cresça rapidamente. Para se ter uma ideia, no ano de 2019, 134 milhões de brasileiros fizeram uso da internet (CETIC, 2019), ou seja, mais de 60% da população no Brasil tiveram acesso à internet, seja ele por meio de um celular, *tablet*, computador ou qualquer outro dispositivo capaz de navegar nessa rede mundial.

Pessoas utilizam a internet em busca dos mais variados benefícios, que vão desde encontrar um amigo ou familiar distante, até a realizar transações bancárias e troca de documentos confidenciais. Diante da situação, se faz necessário entender que ao aproveitar todas as vantagens de navegar em uma rede, o usuário está exposto à diversos riscos, como o furto ou perda de dados, entre vários outros perigos que podem ser minimizados e até mesmo evitados quando a utilização da internet é feita de forma segura.

Dados apresentados por Oliveira (2022) mostram que os ataques cibernéticos no Brasil, cresceram exponencialmente no ano de 2022, 94% se comparado com os números do primeiro semestre do ano, chegando a 31,5 bilhões de tentativas de invasões aos sistemas das empresas e organizações.

O Brasil é o segundo país da América Latina com mais tentativas de ataques, ficando atrás somente do México, dados estes que são influenciados pelo investimento na área de segurança, que corresponde a 10% do total investido em tecnologia (OLIVEIRA, 2022).

Com a grande utilização das redes para diferentes fins e a necessidade de segurança que muitos requerem, a evolução dos dispositivos, *software* e da infraestrutura em geral, se tornou crucial para que continuássemos a utilizar a internet de forma segura, integra e confiável, além de que, muitas dessas atualizações não vieram somente pensando na segurança, mas também no intuito de facilitar a utilização e melhorar a experiência do usuário.

Quando se navega na *web*, todos os usuários possuem um identificador que permite o rastreio da origem de devida informação ou ação no meio virtual, garantindo quem é o destinatário ou remetente, e também possibilitando que a troca de dados possa ser endereçada, garantindo a saída do dado para o destino endereçado, isso é possível graças ao IP. O protocolo IP, ou *Internet Protocol*, é o número único que cada dispositivo tem na rede, sendo que o mesmo pode ser público, atribuído pelo provedor de internet para a navegação na mesma, ou privado, que nesse caso, o próprio roteador atribui para que seja possível a identificação dentro de uma rede local.

De modo igual, é necessário a identificação dos *sites* na *web*. Sendo assim, eles também possuem um endereço IP único que os identificam, para que uma pessoa possa encontrá-lo no meio digital. Mas a procura feita através de uma determinada sequência de números tornou-se inviável com o passar dos anos, o que acarretou na criação do DNS (*Domain Name System*).

O DNS é um sistema que faz a tradução de nomes de domínios em seus endereços IP's, ou seja, um usuário pode procurar por um site, como por exemplo, o site do ecampus através do nome: ecampus.ufvjm.edu.br, sem a necessidade de procurar pelo seu endereço IP 200.128.186.66 e chegará no mesmo site. O DNS se faz presente para facilitar a identificação dos sites e páginas na web, mas vale destacar que o endereço IP é que efetivamente identifica unicamente o local do site.

Partindo da afirmação que os endereços IP's identificam os dispositivos e sites, entende-se que, muitas vezes ataques podem acontecer de forma direcionada, com o objetivo de captar informações importantes, através por exemplo, de um ataque de força bruta, que basicamente acontece quando um atacante, direciona o ataque a determinado IP, para descobrir por tentativa de usuário e senha, o acesso a determinado dispositivo ou sistema, para roubar informações sigilosas, causar danos, etc.

Cibercriminosos estão a todo momento realizando ataques dos mais diversos tipos, tendo como alvos empresas, desde às de pequeno porte, até às multinacionais e organizações de alcance mundial. Dados apresentados pela Microsoft (2022), mostram algumas tendências da última década nessa área, além de exemplificar com alguns acontecimentos, dentre eles o ataque de *ransomware* sofrido pela CNA Financial em março de 2021, que além de ter sofrido com a indisponibilidade de seus sistemas, também sofreu com a perda de dados de clientes, o que lhe causou um prejuízo de 40 milhões de dólares.

À primeira vista, o prejuízo financeiro se destaca frente aos outros que se sucedem com uma invasão cibernética, porém é sempre válido salientar que muitos são os impactos negativos, sendo eles legais, imposição de multas regulatórias ou até mesmo, mas não menos importante, os danos à reputação da organização, onde o cliente se sente inseguro de continuar o vínculo com a mesma.

Com esse cenário de ameaças sendo cada dia mais presente na *web*, principalmente nos dias atuais, onde o *home office* se tornou frequente nas empresas, e em uma casa comum na maioria das vezes não usufruir de uma infraestrutura de segurança que as instalações de uma empresa oferece, a utilização de *software* e *hardware* que ajudam a diminuir a ocorrência dessas invasões se torna essencial na prevenção de ataques, ajudando a detectá-los, mitigá-los ou impedi-los em tempo hábil.

Os Sistemas de Detecção e Prevenção de Invasão (IDS e IPS) foram desenvolvidos com a intenção de ajudar na proteção contra as invasões que os dispositivos e sistemas podem sofrer.

Ambos possuem a característica de analisar o tráfego na rede, mas sua principal diferença é que, enquanto o IDS tem como finalidade apenas analisar o tráfego de pacotes e alertar quando alguma atividade suspeita acontece, o IPS visa parar o ataque, não entregando o pacote quando alguma atividade suspeita é detectada (BERTOLLI, 2018). Sendo assim, é proposto uma análise criteriosa sobre a utilização de ferramentas para realizar o bloqueio e alerta de ataques de força bruta.

1.1 Objetivo

Realizar um ataque de Força Bruta à um roteador *Mikrotik* sob as configurações e utilização de duas ferramentas para identificação e/ou bloqueio do ataque ao qual o dispositivo será submetido.

1.1.1 Objetivos Específicos

- Identificação e análise das características de um ataque de força bruta;
- Análise do funcionamento de um ataque de força bruta;
- Configuração das ferramentas para bloqueio e identificação do ataque de força bruta;
- Execução dos ataques de força bruta;
- Estudar e analisar os dados obtidos do ELK (*Elasticsearch, Logstash, e Kibana*) que podem ter uma relação direta com as características do ataque mencionado, afim de identificá-lo no sistema;
- Análise e comparação das duas ferramentas de identificação/bloqueio do ataque de força bruta.

2 REVISÃO DE LITERATURA

A revisão de literatura do presente trabalho, que segue nas próximas seções, foi necessária para um melhor entendimento do mesmo. Sendo assim, serão dadas definições e descritos termos importantes para o embasamento teórico deste trabalho de conclusão de curso.

2.1 Rede de computadores

Uma rede de computadores é qualquer conjunto de máquinas ou dispositivos, que estão interligados com o objetivo de se comunicarem e compartilharem recursos entre si. Para Tanenbaum (2003), é um conjunto de computadores autônomos interconectados por uma única tecnologia.

Também é considerada como uma rede de computadores mundial, que interconecta milhões de equipamentos de computação em todo o mundo (KUROSE; ROSS, 2006). Essa rede, pode existir em diferentes formatos, sendo que a necessidade da empresa ou pessoa, que vai definir o tipo de rede à ser implantado.

Portanto, definimos como Rede de Computadores elementos computacionais que estão conectados com o objetivo de trocarem dados e informações entre si. Alguns desses elementos que podem ser citados são os *laptops*, computadores pessoais, servidores ou roteadores, que juntos formam essa Rede, sendo ela local, de longo alcance, etc.

> Na maioria das redes geograficamente distribuídas, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão transportam os bits entre as máquinas. Elas podem ser formadas por fio de cobre, fibras ópticas ou mesmo enlaces de rádio. Os elementos de comutação são computadores especializados que conectam três ou mais linhas de transmissão. Quando os dados chegam a uma linha de entrada, o elemento de comutação deve escolher uma linha de saída para encaminhá-los, estes elementos no passado receberam diversos nomes, porém o mais utilizado até hoje é roteador (TANENBAUM, 2003).

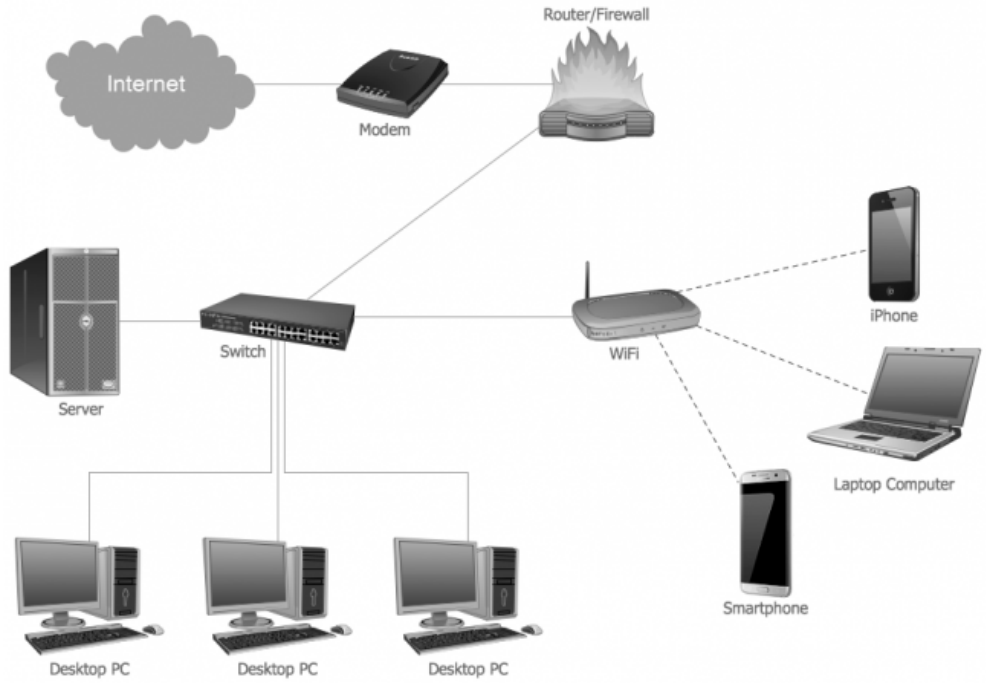
2.1.1 Redes locais

As redes locais, que também são conhecidas como *LAN's*, são redes privadas, delimitadas pela extensão de algum edifício, ou até mesmo um campus universitário (TANENBAUM, 2003).

Tanenbaum (2003) destaca que, uma organização cria redes de computadores para deixar todos os programas, equipamentos e, especialmente os dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso ou do usuário. Os dispositivos localizados na rede dedicada para alguma empresa, fazem essa troca de informações de modo mais seguro, o que não significa que não estão expostos à riscos.

Seguindo essa linha de raciocínio, Filho (2020) define as Redes Locais, também chamada de LAN, como a interconexão de dispositivos que estejam dentro de um espaço geográfico limitado, variando o tamanho de acordo com o número de elementos conectados e sendo geralmente operada apenas por uma empresa privada. Na Figura 1, observa-se uma rede local composta por dispositivos como computadores, servidor, celular, etc.

Figura 1 – Exemplo de uma infraestrutura de rede LAN



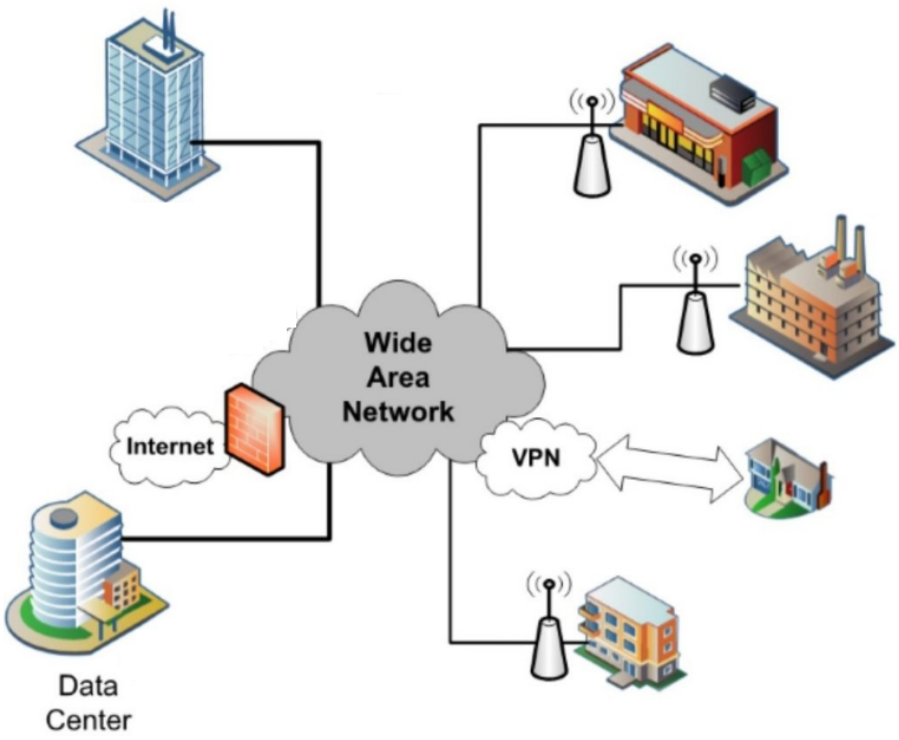
Fonte: (SCOTA, 2019)

2.1.2 Redes de longo alcance

Redes de longo alcance, são aquelas que abrangem uma área maior de distribuição na comunicação dos dispositivos, podendo ter os mesmos distribuídos em uma área do tamanho de um país. Conhecida também como WAN, essas redes são como várias sub-redes interligadas por roteadores de borda, que realizam a conexão entre vários dispositivos, levando as informações de uma origem para o seu destino.

Soares, Lemos e Colcher (1995) destacam que o surgimento destas redes veio da necessidade de realizar o compartilhamento de recursos e dados por uma maior comunidade de usuários geograficamente dispersos. Exemplifica-se na Figura 2 uma rede de longo alcance, onde tem-se os dispositivos em várias localidades mais distantes, porém dentro de uma mesma rede.

Figura 2 – Exemplo de uma infraestrutura de rede WAN



Fonte: (REHMAN, 2023)

2.1.3 Internet

A internet pode ser considerada como um dos maiores avanços tecnológicos da humanidade. Através da mesma podemos nos conectar com pessoas do outro lado do mundo a qualquer momento. Outro ponto a se destacar e que ganhou mais força devido à pandemia do corona vírus, é o trabalho à distancia, o conhecido *home office*, que nos permite exercer nossas atividades profissionais de nossa própria casa, sem a necessidade de nos locomover ao local de trabalho. Claro que essa condição não é contemplada por todas as modalidades de trabalho, porém muitas são as que se encaixaram no recente modelo.

Podemos definir a internet como a maior rede de conexões a nível mundial, que possibilita que vários dispositivos, sejam eles desde um pequeno celular a um super computador, troquem informações entre si. Dumas (2011) afirma que a internet nasceu na Guerra Fria, nos grupos militares norte-americanos, que usavam como saída para a comunicação, caso os meios tradicionais fossem destruídos.

O termo ”internet”também pode ser definido como uma rede mundial que tem como objetivo interligar computadores para fornecer ao usuário o acesso a diversas informações, sendo esse o motivo de ser chamada de rede mundial de computadores (TELECOM, 2022).

2.1.4 Gerenciamento de redes

O crescimento das redes de computadores tem sido algo exponencial no mundo de gerenciamento de redes, fazendo com que as empresas e organizações tenham que dedicar

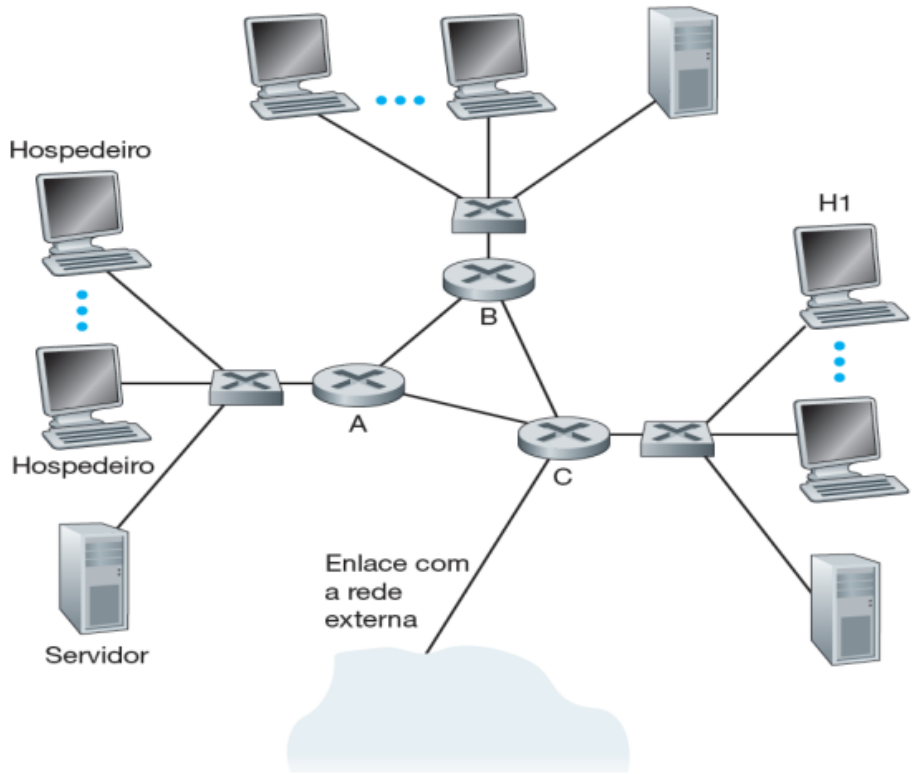
grandes esforços nesse assunto que pode ser bastante sensível para as mesmas, acarretando na necessidade de sempre estar monitorando e administrando esses recursos, para que os seus clientes tenham sempre segurança, disponibilidade e qualidade dos serviços contratados.

Menezes e Silva (1998) define o gerenciamento de redes como o processo de controlar uma rede de computadores de maneira que seja possível maximizar sua eficiência e produtividade, compreendendo um conjunto de funções que podem estar em uma máquina ou espalhados por milhares de quilômetros em dispositivos distintos. Outro ponto importante a se considerar é que, estas funções permitem controlar uma rede de computadores e seus serviços, munindo de mecanismos de análise, controle e monitoração dos dispositivos e recursos da rede (MENEZES; SILVA, 1998).

Para se ter um bom gerenciamento de uma rede, é necessário ter um amplo conhecimento sobre a mesma, saber quais equipamentos a compõem, por exemplo, *switches* e servidores, a interconexão entre eles e seus desempenhos, além da definição de métricas.

Tendo esses requisitos em mãos, pode-se garantir a qualidade da infra-estrutura da mesma, planejar o seu crescimento, analisar se há comportamentos que seguem tendências e observar se há algum padrão, além de que, caso surja algum problema, a chance de resolvê-lo com mais eficácia é maior. A Figura 3, demonstra um cenário de gerenciamento de uma rede.

Figura 3 – Cenário de gerenciamento de uma rede



Fonte: (SOUSA, 2019)

2.1.5 Arquitetura de gerenciamento de redes

A ideia apresentada por Raulino (2002) afirma que a arquitetura geral dos sistemas de gerenciamento de redes pode ser dividida em quatro componentes básicos: elementos gerenciados, que são os componentes da rede que precisam operar adequadamente para que a rede ofereça os serviços para os quais foi projetada. O segundo componente são as estações de gerência, que executa o software de protocolo de gerenciamento que solicita informações dos agentes. O terceiro componente é composto pelos Protocolos de gerenciamento, que define as mensagens utilizadas entre o agente e gerente, além de realizar funções de monitoramento e controle. Por último temos as informações de gerenciamento (MIB), que são as informações sobre os elemento s gerenciados que ficam guardadas em um banco de dados (RAULINO, 2002).

2.2 Protocolos

Baseado na ideia de que, a rede de computadores pode ser considerada como uma troca de comunicação entre dispositivos, sendo estes delimitados por uma área, caracterizando o tipo de rede, é necessário que haja um meio para que os mais diversos dispositivos se entendam, e é nessa questão que entra a definição de protocolos.

Os protocolos são necessários no meio tecnológico, pois são eles que definem o formato e a ordem das mensagens trocadas entre os dispositivos, definindo também as ações realizadas nessa comunicação (CORTEZ, 2022). Portanto, entende-se que a utilização de protocolos na internet é intensa, dos mais variados tipos, pois cada protocolo define qual tipo de informação ou ação contém naquela comunicação.

Uma definição apresentada por Souza (2009) é que, os protocolos controlam o envio e o recebimento de mensagens em uma rede de computadores. Em paralelo com a definição apresentada, Ueyama (2012) afirma que os protocolos determina a ordem de envio e chegada das mensagens, as ações que devem ser executadas na recepção e transmissão das mesmas, além de estipular o formato das mensagens.

2.2.1 Camadas de protocolos

Os protocolos podem ser diferenciados, pois cada um tem sua funcionalidade bem definida. Sendo assim, se separam em camadas e modelos de serviços, que na Figura 4 pode-se ver alguns exemplos:

Figura 4 – Pilha TCP/IP

Fonte: Imagem do autor

Essa representação é conhecida como ”Pilha TCP/IP”, que tem como finalidade facilitar a implementação de cada protocolo, já que cada camada tem sua função bem definida, além de que cada uma tem a função de prover serviços para a camada que está logo acima.

Através da imagem, concluímos que o modelo TCP/IP possui quatro camadas:

- Camada física;
- Camada da internet;
- Camada de transporte;
- Camada de aplicação

Fisher (2019) define a camada física, ou também conhecida como a camada de enlace de dados, como aquela camada que é responsável pelos quesitos físicos da troca de dados, como placas de interface de rede e *drivers* de dispositivos no computador.

A camada de internet é responsável pelo movimento de pacotes na rede (FISHER, 2019). Pode-se dizer que a camada de internet endereça os pacotes através do IP, fazendo seu roteamento e controle de envio/recepção.

Outra camada do modelo *TCP/IP* é a camada de transporte, que segundo Tanenbaum (2003) tem como objetivo fazer a transferência de dados, garantindo um serviço confiável, ou seja, uma integridade na troca de dados entre a origem e o destino, disponibilizando uma interface de alto nível às outras camadas.

Por fim, temos a camada de aplicação. Esta camada é onde ficam os protocolos de mais alto nível, como DNS, HTTP, FTP, etc..

2.2.2 Protocolo TCP

Um dos protocolos mais importantes e utilizados em redes, é o *Transmission Control Protocol*, conhecido também como protocolo TCP, sendo ele orientado à conexão e considerado um protocolo de transporte, realizando uma transferência de dados confiável e sem perdas.

É importante destacar que, devido à sua característica de ser orientado à conexão, antes que qualquer dado possa ser trocado entre o *host* origem com o *host* destino, primeiramente deve ser estabelecida entre eles uma conexão, para que assim aconteça a troca de dados.

O objetivo desse protocolo é realizar a comunicação entre aplicações, sendo que para que haja o envio do pacote TCP, primeiramente se faz necessário o estabelecimento de uma conexão (TANENBAUM, 2003). Outras características que Tanenbaum (2003) apresenta é uma entrega confiável, ou seja, há a retransmissão do pacote caso haja falha na sua entrega, além da ordenação dos mesmos em sua entrega e controle do fluxo.

O TCP garante uma transmissão confiável de pacotes através da utilização de mensagens *acknowledgements* (ACK's) e para que ocorra uma conexão entre dois dispositivos através do protocolo TCP, é realizado o *Handshake* de três vias, que basicamente é um mecanismo para estabelecimento de uma conexão TCP (FALL; STEVENS, 2012).

2.2.3 Protocolo IP

Segundo os autores Oliveira e Garcia (2014), o protocolo *IP* (*Internet Protocol*) tem a função de identificar qualquer tipo de dispositivos que estão conectados na rede de computadores transmitindo informações para outros locais.

Segundo o autor Morimoto (2006) apud Terense e Freitas (2016), o endereço *IP* possui duas divisões, onde a primeira parte faz a identificação da rede onde os *hosts* se encontram, e a segunda parte faz a identificação dos *hosts* na rede, já que , para que haja a navegação na internet, o dispositivo precisa de sua identificação única.

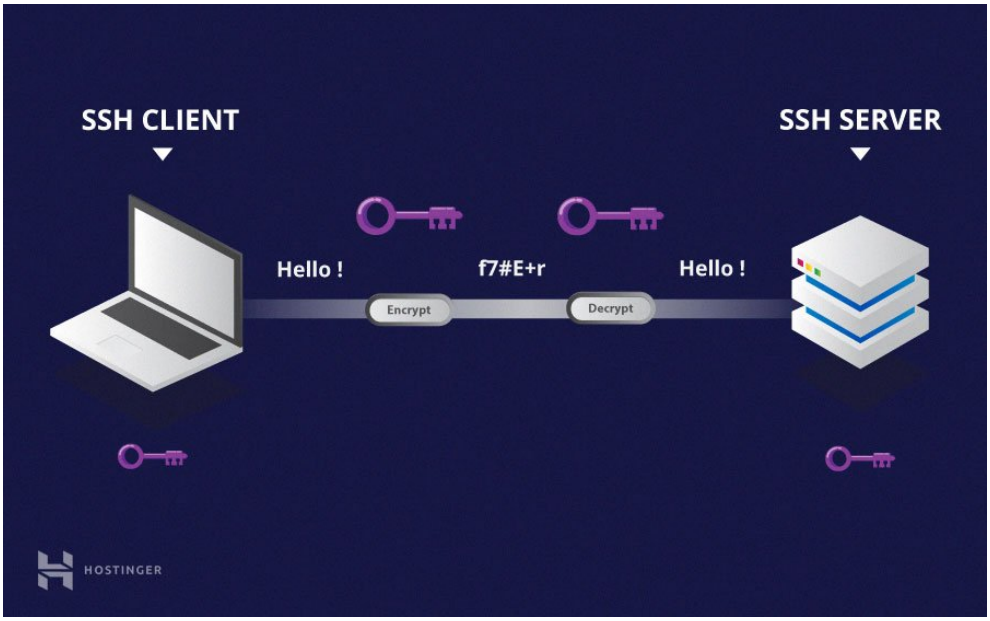
A troca de recursos, apesar de ser grande e rápida, também tem que acontecer de modo seguro, já que empresas e pessoas estão a todo momento compartilhando informações pessoais ou cruciais para o negócio, e sua perda pode ocasionar em um grande prejuízo para as partes interessadas.

2.2.4 Protocolo SSH

A definição do protocolo *Secure Socket Shell* (SSH) se dá como um protocolo de aplicação que oferece aos usuários, um modo seguro de acessar um computador em uma rede aberta (GASPAR, 2021). Isso se deve ao fato de que o mesmo faz uso da criptografia e dessa forma, garante que a comunicação entre servidores remotos aconteça de maneira segura(GASPAR, 2021).

Rios (2012) define o SSH como um protocolo que além de oferecer uma comunicação segura, faz a transferência de dados adicionais e independentes pela mesma conexão.

Figura 5 – Exemplo de conexão SSH



Fonte: (G., 2021)

Na Figura 5 podemos concluir que o SSH usa chaves públicas na troca de dados, ou seja, os *hosts* que desejam trocar informações entre si, primeiramente trocam essas chaves, uma para encriptar os dados, e outra para decifrá-los, estabelecendo a conexão entre ambos e garantindo a autenticidade dos usuários, além da segurança dos dados, já que os mesmos são criptografados (G., 2021). Através deste protocolo também é possível fazer a administração de servidores remotamente, sendo bastante utilizado para esse fim.

Segundo Comer (2001), o protocolo SSH é considerado como de aplicação, ocupando a camada 5 do modelo de referência TCP/IP, tendo como função implementar um terminal em um cliente para ele conectar-se a um servidor remoto, utilizando a porta 22 do TCP.

2.2.5 Protocolo SNMP

O *Simple Network Management Protocol* (SNMP), é um protocolo especificado pela RFC 1157, possui uma certa facilidade em sua implementação, além de utilizar o protocolo UDP nos seus envios de mensagens.

Kurose e Ross (2006) detalha que, o protocolo tem sua base formada pelo Protocolo de Monitoramento do *Gateway* Simples - *Simple Gateway Monitoring Protocol* (SGMP), sendo que o SGMP foi implementado por uma equipe de pesquisadores, usuários e administradores universitários de rede, de tal maneira que a experiência com o protocolo proporcionou que eles idealizassem e oferecessem o SNMP em poucos meses.

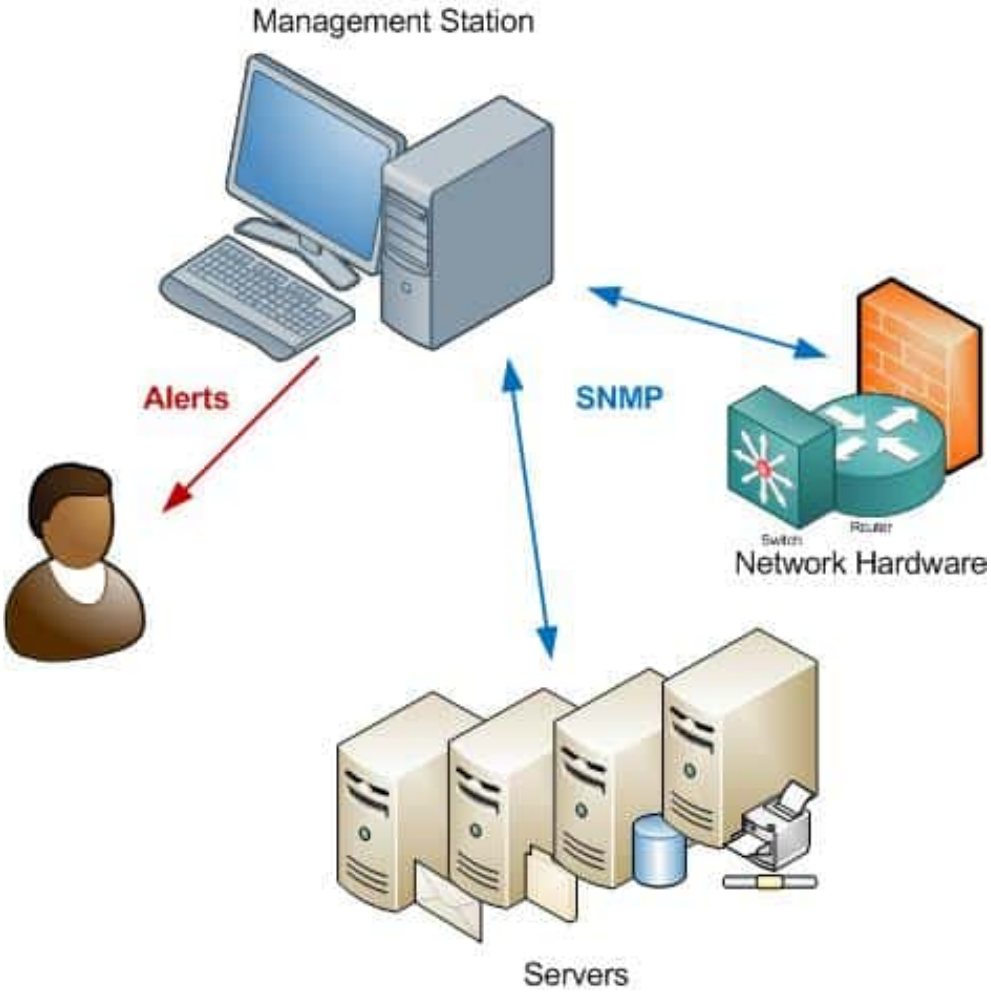
Portanto, pode-se definir o SNMP como um protocolo que trata do gerenciamento de redes, contendo um conjunto de informações sobre a gerência da mesma, dados valiosos dos mais diversos dispositivos que podem ser obtidos através desse protocolo.

Duarte (2011) afirma que o SNMP foi criado para padronizar o gerenciamento de dispositivos IP, tendo ele três componentes fundamentais: os dispositivos gerenciados, os agentes e os sistemas de gestão de redes.

> Dispositivos gerenciados constituem os nós da rede onde interfaces SNMP são implementadas para que informações relevantes ao seu gerenciamento possam ser armazenadas e transmitidas. Também conhecidos como elementos de rede, dispositivos gerenciados incluem, mas não estão limitados a: impressoras, câmeras de vídeo IP, telefones IP, servidores de acesso, roteadores e *switches*.
>
> Agentes estão presentes em cada dispositivo gerenciado e são justamente os responsáveis pela implementação da interface de comunicação SNMP. Trata-se de um software que atua como tradutor das informações de gerenciamento local e específica aos dispositivos gerenciados que os hospedam para o formato específico SNMP - tornando as informações do dispositivo gerenciado compreensíveis globalmente - e portanto, gerenciáveis.
>
> As tarefas de monitoramento e gerenciamento propriamente ditas são delegadas aos Sistemas de Gestão de Redes. Por representarem a atividade que consome de fato a maior parte dos recursos de processamento, o sistema NMS normalmente é abrigado em um ou mais computadores. (DUARTE, 2011).

Na Figura 6 pode-se ver um sistema distribuído constituído de agentes (*switch*, roteador), servidores de banco de dados, monitorados por um gerenciador que recebe alertas e permite ao administrador realizar a gerencia do mesmo.

Figura 6 – Exemplo de arquitetuta SNMP



Fonte: (LESKIW, 2022)

2.2.6 Protocolo Netflow

Realmente a criação do protocolo SNMP foi de grande valia no quesito de padronização e gerenciamento, porém com os avanços tecnológicos e a crescente quantidade de tráfego de rede nas empresas, a necessidade de um conhecimento maior sobre o fluxo de rede, obtendo mais detalhes, é algo que o SNMP não conseguia dar o devido suporte.

O protocolo *Netflow* foi criado pela Cisco para realizar a exportação de todos os fluxos dos dispositivos, criando tabelas que contém informações detalhadas, com ferramentas capazes de realizar o tratamento dos dados, dando aos administradores de redes informações úteis para a tomada de decisões.

O objetivo do *Netflow* é criar uma padronização na maneira em como os fluxos de rede são exportados, e através dos campos pré definidos no mesmo, permitir não somente o gerenciamento ou planejamento de redes, mas também detectar possíveis ataques e atividades suspeitas (CLAISE *et al.*, 2004).

Várias versões foram sendo atualizadas do protocolo, sendo que a mais recente é a V9 que possui 104 campos disponíveis e trouxe alguns benefícios em relação às versões

anteriores, dentre eles a facilidade de adição ou remoção dos campos que serão exportados (SOBRINHO, 2021).

Alguns dos campos destacados por Sobrinho (2021) são:

- TCP_FLAGS: acumulativo de todas as *flags* TCP vistas no fluxo;
- IN_BYTES: número de *bytes* de entrada associados a um fluxo;
- OUT_BYTES: número de *bytes* de saída associados a um fluxo;

2.2.7 Protocolo IPFIX

O protocolo IPFIX foi criado pelo *Internet Engineering Task Force* (IETF), e surgiu para equalizar as variadas soluções que surgiram em torno de medições de fluxos de rede, afim de padronizar e identificar os fluxos e realizar a transferência dos dados de um dispositivo para o coletor.

2.3 ELK - Elastic Stack

O *Elastic Stack* pode ser considerado como uma solução de TI que atende várias áreas dentro do universo tecnológico, desde a monitoramento do fluxo de uma determinada rede, à análises mais complexas de dados. Além disso, disponibiliza também gráficos e visualizações dos dados obtidos e até alertas de algum fluxo fora do comum dentro do monitoramento.

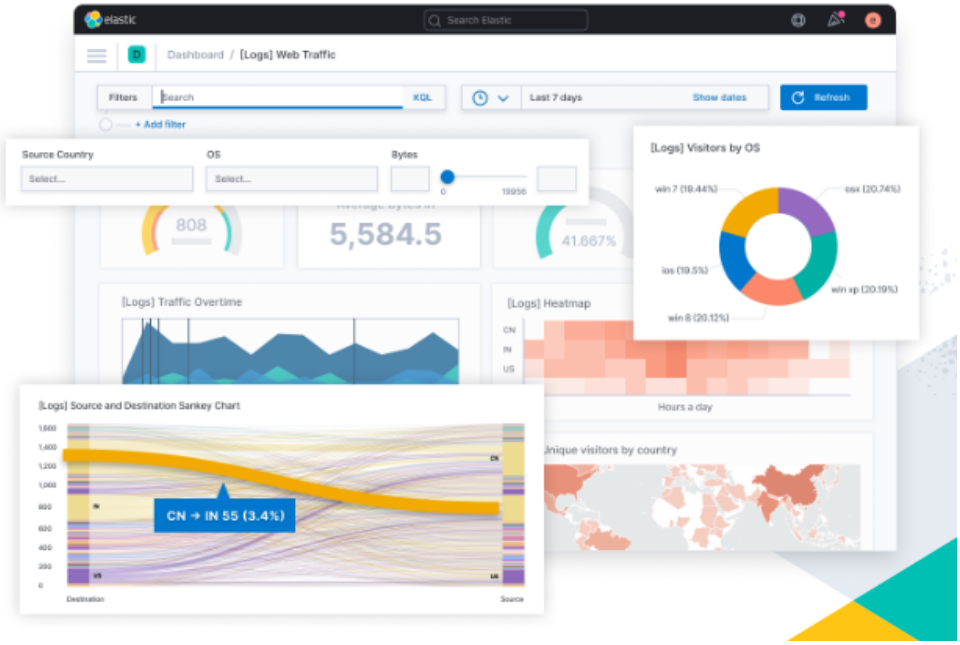
Essa solução é composta por três componentes: o *Elasticsearch*, o *Logstash* e o *Kibana*, cada qual com sua funcionalidade, mas que juntos entregam as mais diversas funcionalidades que esta pilha proporciona.

A arquitetura da "*stack*"se dá em camadas, sendo que primeiramente acontece a ingestão de dados através do *Logstash*, para posteriormente pelo *Elasticsearch* realizar a pesquisa e análise das informações coletadas, e por último, através do *Kibana*, na camada de apresentação, observar visualmente esses dados (B.V., 2022). Em resumo, a pilha realiza a indexação, análise e visualização de dados.

Röhrs (2021) descreve o funcionamento do da pilha de forma sucinta, considerando como um transito de dados provenientes de diversas fontes através do *Logstash*, que são tratados para serem indexados no *Elasticsearch*, para posteriormente habilitar aos usuários realizarem consultas complexas e recuperar informações, e por fim visualizá-las pelo *Kibana*, através de *dashboards* e painéis que apoiam no gerenciamento da rede.

Essa ferramenta disponibiliza também realizar filtros com os dados coletados e agrupá-los, descobrindo como os campos se relacionam entre si, a fim de identificar padrões e eventos anômalos. Pode-se observar na Figura 7 alguns gráficos gerados pelo Kibana, onde pode conter informações sobre os IP's que mais trocaram fluxo na rede, o protocolo mais utilizado na troca de pacotes, etc.

Figura 7 – *Exemplo de gráficos gerados pelo Kibana*



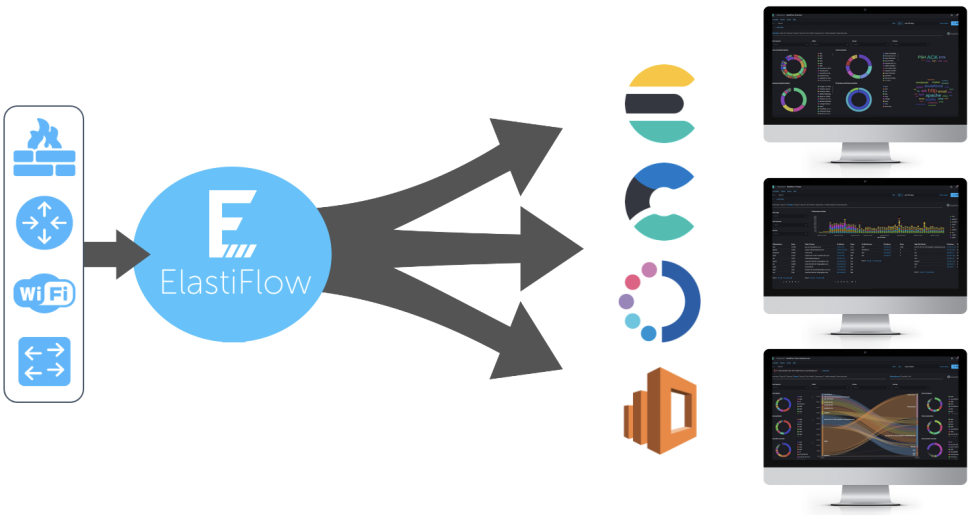
Fonte: (B.V., 2022)

2.3.1 Plugin Elastiflow

De acordo com Remontti (2017), o *Elastiflow* disponibiliza uma coleta e visualização de todos os dados dentro de um fluxo de rede utilizando o *Elastic Stack*, oferecendo suporte à utilização também do IPFIX, *Netflow* e sFlow.

A Figura 8 exemplifica algumas ferramentas com as quais o *Elastiflow* pode ser integrado.

Figura 8 – *Exemplo de integração e interface do Elastiflow*



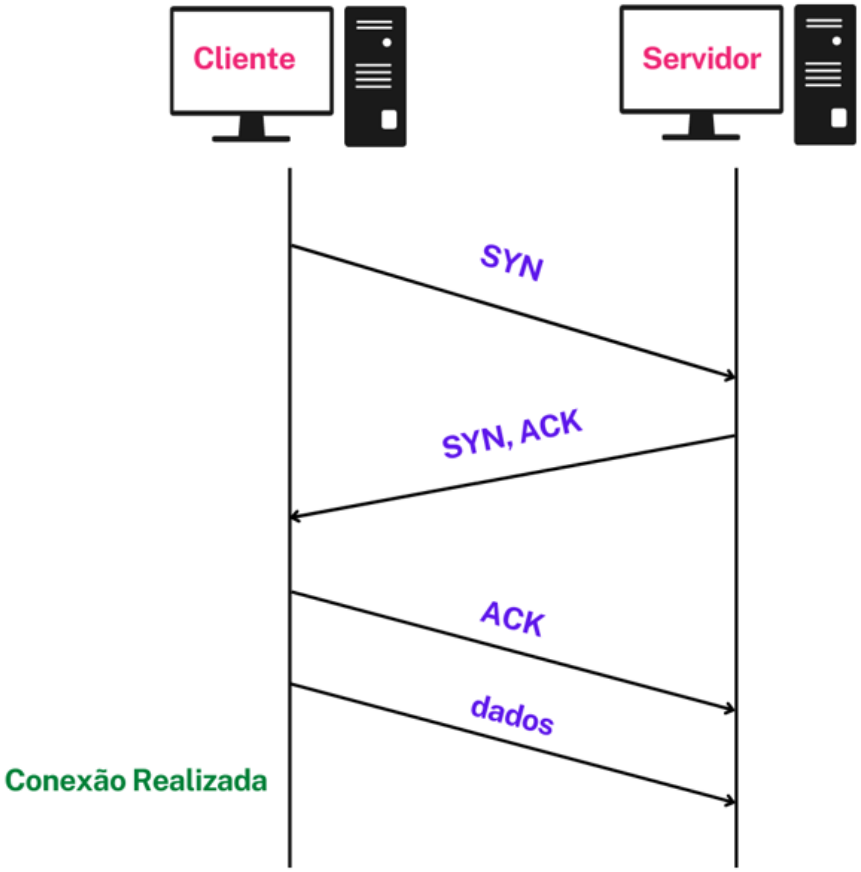
Fonte: (REMONTTI, 2017)

2.4 *Handshake* de três vias

Antes que dados possam ser trocados, é necessário estabelecer uma conexão entre duas entidades, ou seja, entre um IP origem e um IP destino (FARREL, 2005). O *handshake* de três vias, é um modelo de estabelecimento de conexão entre duas máquinas, para que as mesmas, através de um canal, possam fazer uma troca de pacotes.

Esse estabelecimento de conexão se dá basicamente em três passos. O primeiro passo para que a conexão seja estabelecida parte do cliente, que inicia enviando um pacote TCP com a *flag* SYN, possuindo também um número de sequência de 32 bits, que identifica a requisição SYN. Depois disso, como segundo passo, o servidor enviará um pacote com as *flags* SYN e ACK, gerando novamente um número de sequência e ao gerar um número de confirmação, o mesmo será igual ao primeiro número de sequencia enviado pelo cliente, acrescido de 1, para que o mesmo também consiga reconhecer a resposta. Por fim, depois de receber e identificar o pacote do servidor, o cliente enviará outro pacote com a *flag* ACK, procedendo da mesma maneira que o servidor para gerar o número de sequência, estabelecendo assim a conexão. Na Figura 9, tem-se exemplificado o estabelecimento da conexão pelo *handshake* de três vias.

Figura 9 – Exemplo de conexão pelo *handshake* de três vias



Fonte: Próprio autor

De maneira mais sucinta, Fall e Stevens (2012) explica o *handshake* de três vias como um estabelecimento de conexão após um cliente enviar um pacote com o bit da *flag* SYN

para um servidor. O mesmo responde confirmando o recebimento com um pacote com os bits da *flag* SYN e a *flag* ACK ativados. Por último, o cliente responde com um pacote com o bit da *flag* ACK para o servidor.

De modo análogo, para o encerramento de uma conexão, o cliente inicia enviando um pacote com os bits FIN e ACK. O servidor confirma o recebimento enviando um pacote com o bit ACK, além de outro pacote FIN/ACK para encerrar a conexão. Ao final, o cliente então envia um pacote ACK, para confirmar o recebimento do último pacote enviado pelo servidor (FALL; STEVENS, 2012).

2.5 Segurança da informação

O conceito de segurança da informação envolve entre outras características, a proteção dos dados, com o intuito de garantir que, somente aqueles com autorização tenha acesso aos mesmos.

Conforme definido por Beal (2005), a Segurança da Informação é proteger a informação de possíveis ameaças, mantendo sua integridade, confidencialidade e disponibilidade. Portanto, o objetivo da segurança é preservar estes três pilares.

Fontes (2006) especifica de maneira minuciosa os três pilares da segurança da informação da seguinte maneira:

- Confidencialidade: garantia de que somente as pessoas com autorização prévia tenham acesso à determinado recurso.
- Integridade: a informação não pode ser corrompida, ou seja, ela tem que se manter integra, sem nenhuma alteração.
- Disponibilidade: garantia de que a informação estará disponível sempre que for preciso.

Preservar esses três pilares consiste em proteger o ambiente físico e o ambiente virtual de uma organização. Alguns aspectos que podem ser citados são: dar acesso à determinadas áreas e informações somente àquelas pessoas que necessitam das mesmas para o cumprimento das suas tarefas, divisão da rede em externa e interna, atualização dos dispositivos físicos e virtuais em dia, utilização de protocolos que dão garantia de segurança na troca de dados, etc.

Os gastos com a segurança nunca podem ser considerados dispensáveis, pois o prejuízo com sua falta pode alcançar um tamanho exponencialmente maior, porém podemos minimizá-los se levar em consideração o que é necessário proteger. Informações confidenciais, aquelas que poucas pessoas podem ter acesso para execução de determinada tarefa, se faz necessário esforços e recursos maiores dedicados à sua segurança, o que não é necessário com informações públicas, que caso haja o vazamento, não irá afetar o negócio. Sendo assim, quanto mais crítica e sensível for a informação, considerando também o impacto que um possível vazamento cause, maior deve ser a segurança empregada na sua proteção.

Atualmente, a informação é uma das maiores vantagens competitivas no mundo corporativo, sendo de suma importância para as empresas protegê-las durante todo o seu ciclo de vida, desde quando ainda é um dado bruto, até o seu processamento, uso, armazenamento e por fim, seu descarte.

Apesar de todos os softwares e esforços empregados para a proteção dos dados, vale ressaltar que, falhas na segurança podem ocorrer, sejam elas físicas ou humanas. Mitigá-las é um grande desafio e prática constante da segurança da informação, considerando que a infraestrutura computacional está sempre submetida à riscos e ameaças, e com a tecnologia sempre em avanço, o surgimento de vulnerabilidades é inevitável.

2.5.1 Riscos

Riscos existentes em um sistema de informação são as probabilidades de que ameaças se aproveitem das vulnerabilidades, fazendo com que os ativos estejam sujeitos à quebra de sua segurança, ou seja, à quebra da confidencialidade, integridade e disponibilidade, o que pode acarretar em danos nos negócios (SêMOLA, 2003).

A definição de riscos de segurança apresentada por Fernandes (2011) diz que é um evento possível e com grandes chances de causar prejuízo para uma organização, com chances de acontecer futuramente e causar um efeito negativo considerável.

2.5.2 Ameaças

Campos (2006, p.13) considera a ameaça como um agente externo ao ativo da informação, onde se aproveita das vulnerabilidades da informação. Outra definição apresentada por Hintzbergen *et al.* (2018) é de que a ameaça é a raiz de um incidente, sendo que pode resultar no prejuízo para a organização ou em um dano ao sistema.

A ameaça à um sistema de informação pode ser definida em poucas palavras como um evento que tem grandes chances de impactar negativamente o sistema ou organização, sendo ela através de qualquer agente que explore uma vulnerabilidade.

2.5.3 Vulnerabilidades

As vulnerabilidades no ambiente tecnológico consistem em fraquezas de segurança que são deixadas na infraestrutura de TI. Essas podem ser um software mal configurado, um aplicativo desatualizado, senhas padrões que são utilizadas, dados internos expostos, etc.

Conforme definido por Abomhara e Køien (2015), as vulnerabilidades presentes em um sistema ou projeto são pontos falhos que permitem a execução de códigos maliciosos, um ataque de DDoS ou até mesmo o acesso a dados confidenciais.

É sempre válido ressaltar que não é certo afirmar que, as infraestruturas que possuem vulnerabilidades, sejam elas de software, hardware, redes e até mesmo os recursos humanos, irão resultar em algum incidente só por possuírem tal falha, pois as brechas podem existir, mas para que o incidente ocorra de fato, é necessário algum agente que aproveite da situação.

Outra correspondência ao termo apresentada por Almeida (2007) é que, vulnerabilidade é um ponto frágil no sistema que, devido a mesma, acontece uma ação não autorizada, podendo ser causada por uma falha de projeto, de implementação ou de configuração, resultando em uma invasão que pode ter vários prejuízos, como por exemplo, o roubo de recursos.

Com o aumento do uso da tecnologia nos últimos anos, considerando que muito desse uso inclui troca de dados sensíveis, a todo momento brechas são aproveitadas por hackers

e cibercriminosos para realização de ataques, dos mais variados tipos e objetivos, e uma das maneiras de conseguir impedi-los ou minimizar seus impactos, é conhecendo-os bem.

2.5.4 Ataques

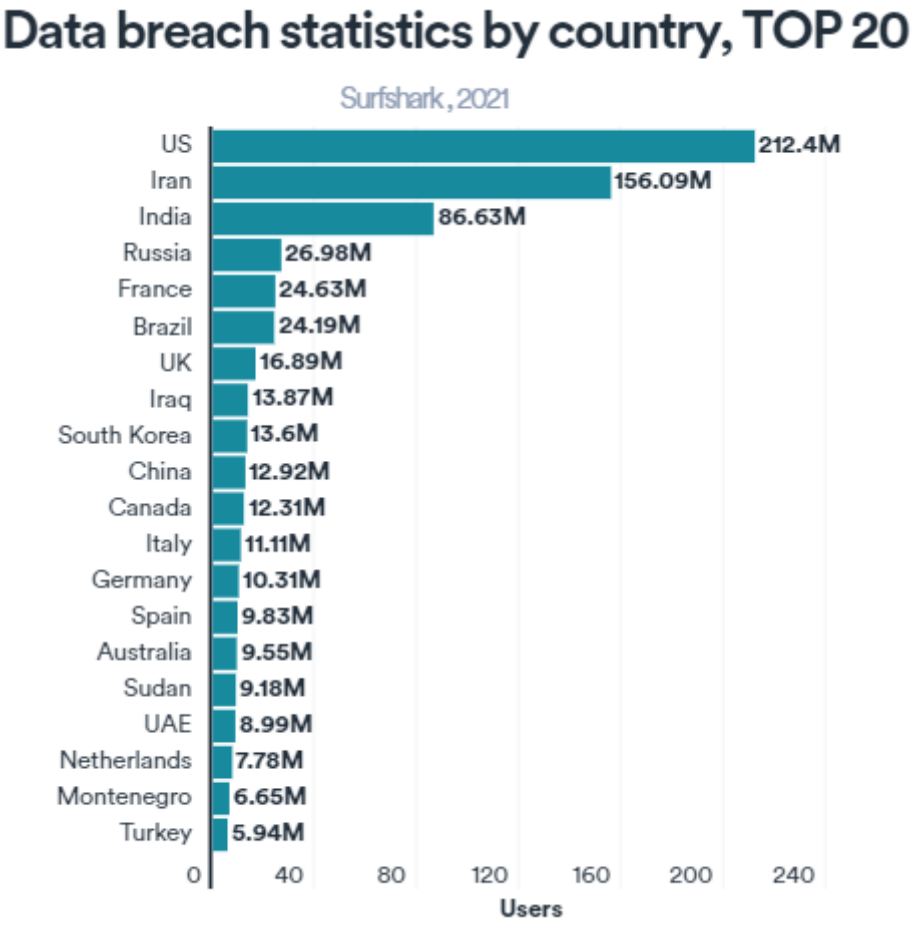
Os ataques e invasões à redes e sistemas tem se tornado cada vez mais comuns e sofisticados, capturando informações sensíveis das organizações e deixando-as em situações críticas que por muitas vezes podem ser irreversíveis.

Os danos que um ataque de redes pode causar, vão desde a um simples roubo de imagens, podendo chegar a grandes raptos de dados sensíveis de empresas e clientes ou até mesmo causar uma indisponibilidade de serviço por tempo indeterminado, até que o mesmo seja identificado para posterior interrupção.

Existem diversos motivos que podem levar à realização de um ataque. Os mesmos variam desde a uma simples curiosidade, até a objetivos mais sérios, como espionagem, venda de informações sigilosas para empresas concorrentes, e a danificação de imagem de uma pessoa ou organização Pinheiro (2007).

Segundo a empresa Surfshark (2022), o Brasil foi no ano de 2021, considerando os meses de janeiro a novembro, o sexto país em que mais ocorreu vazamento de dados no mundo, resultando num total de 24,2 milhões de pessoas atingidas, dados que podem ser vistos na Figura 10.

Figura 10 – Estatísticas de violação de dados por país, TOP 20



Fonte: (SURFSHARK, 2022)

A IBM (2021), cita algumas ameaças mais comuns no mundo cibernético, dentre elas, o *malware*, que pode ser considerado um software malicioso que causa danos a um sistema, fornecendo acesso não autorizado. Outro citado é o *ransonware*, que bloqueia e ameaça apagar dados caso um resgate não seja pago aos cibercriminosos.

Alguns desses ataques são de conhecimento mundial, que já vem sendo praticado por anos, dando às empresas e profissionais da área de Segurança da Informação certo compreendimento de seu funcionamento, além da oportunidade de desenvolver praticas e hábitos para evitá-los, e o uso de sistemas e softwares especializados para proteção de seus ativos. Entre esses ataques podemos citar o Ataque de Força Bruta, de DDoS, *spoofing*, *pishing*, etc.

2.5.4.1 Ataques de força bruta

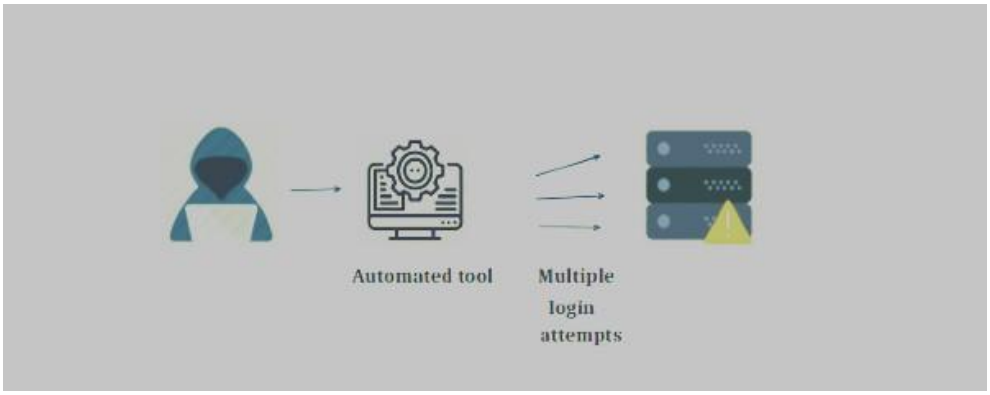
As ocorrências de ataques de segurança no âmbito tecnológico tem aumentado cada vez mais, e alguns desses ataques acontecem de maneira corriqueira na internet. Esse é o caso dos ataques de força bruta, que por tentativa e erro de usuário e senhas, cibercriminosos tentam descobrir os acessos de usuários à determinados sistemas ou dispositivos, seja para invasão de algum dispositivo ou até mesmo contra sites, buscando arruinar a reputação dos mesmos.

Nos dias atuais, várias ferramentas contemplam a execução desse tipo de ataque, sendo que a maioria delas utilizam as famosas *"words lists"*, que são listas que contém usuários e senhas que são frequentemente utilizados, como por exemplo: "admin", "12345", ou até mesmo listas personalizadas para o perfil da vítima, contendo data de aniversário, nome do animal de estimação e assim por diante, para fazer uma combinação de acessos e verificar de maneira automatizada, até encontrar o acesso correto.

Segundo a empresa ESentire (2017) apud Diorio *et al.* (2019), as tentativas de ataques de força bruta tiveram um aumento de quase 400% entre 2016 e 2017, sendo que no ranking mundial de países que mais realizaram tal ataque, o Brasil ficou em segundo lugar. Outro dado a se considerar vem da empresa Labs (2018), que segundo seus relatórios, esse tipo de ataque foi o sexto mais realizado no terceiro trimestre do ano de 2018, marcando presença entre os *"top network attacks"*.

Tem-se exemplificado na Figura 11 um ataque de força bruta, onde um atacante utiliza algum tipo de ferramenta automatizada, que irá fazer todas as combinações possíveis das listas de usuários e senhas, até encontrar um acesso que ocorra com sucesso.

Figura 11 – Ataque de Força Bruta



Fonte: Imagem da Internet

2.5.5 Tipos de detecção e prevenção de Ataques

Com o avanço das técnicas e tipos de ataques, um forte trabalho na área de segurança é feito constantemente, a fim de mitigar cada vez mais os pontos vulneráveis que são sempre buscados pelos crimes cibernéticos e também de descobrir novas formas para detectá-los previamente, antes mesmo que de fato aconteça a invasão.

Prevenir ataques envolve desde simples hábitos de uso do ambiente computacional, como remover ou alterar senhas padrão, eliminar aplicativos e softwares desnecessários e adicionar bloqueio de portas que não são utilizadas, até a utilização de grandes sistemas desenvolvidos para este fim, como *firewalls* e softwares anti-vírus. Alguns softwares e sistemas são desenvolvidos especificamente para esse fim, sendo alguns deles conhecidos como IPS e IDS.

2.5.5.1 Sistema de detecção de intrusão

Os Sistemas de Detecção de Intrusão, mais popularmente conhecidos como IDS, são aqueles sistemas em que seu principal objetivo é identificar algum ataque que possa estar acometendo a rede de computadores na qual o mesmo está configurado. Esse tipo de sistema, parte do princípio de monitorar a rede, guardando informações e analisando-as, afim de encontrar alguma anomalia, para que, caso encontre, possa alertar os responsáveis de que a anomalia identificada pode gerar um ataque. Sendo assim, em sua maioria, não agem por conta própria para interceptar o ataque, apenas monitora e alerta.

Na mesma linha apresentada, Araujo, Leite e Costa (2016) apresenta a ideia de que o IDS se baseia na monitoração do fluxo em uma rede ou sistema, buscando encontrar alguma atividade suspeita.

Outra definição apresentada por Goodrich e Tamassia (2012) que exprime a mesma ideia é de que, um IDS é basicamente um sistema que tem como objetivo a detecção de sinais que apontem alguma atividade maliciosa, podendo ser desde uma rede de computadores, até a um simples dispositivo individual.

Tendo em vista que esse tipo de sistema monitora e recolhe informações do fluxo em um sistema ou rede, as mesmas são de suma importância uma medida reativa com o intuito de proteger o alvo e mitigar a vulnerabilidade, servindo também como uma base de conhecimento.

Vários são os tipos de IDS, e o que vai definir qual a escolha a ser feita para a implementação do mesmo será o tipo de infraestrutura ao qual se quer proteger, os tipos de ataques que são mais propensos a acontecer naquela infraestrutura, entre vários outros fatores, que em conjunto levará a definição do IDS mais eficaz para a situação.

Basicamente temos os seguintes tipos de IDS:

- Sistemas de detecção de intrusão baseados em *host* (HIDS)
- Sistemas de detecção de intrusão baseados em redes (NIDS)
- Sistemas de detecção de intrusão híbridos

> Sistemas de detecção de intrusão baseados em *Host* monitora e analisa informações coletadas de um único *host* (Máquina). Não observa o tráfego que passa pela rede, seu uso volta-se a verificação de informações relativas aos eventos e registros de *logs* e sistema de arquivos (permissão, alteração, etc.). São instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor e os usuários não precisam ser monitorados. Também é aplicada em redes onde a velocidade de transmissão é muito alta como em redes *"Gigabit Ethernet"* ou quando não se confia na segurança corporativa da rede em que o servidor está instalado (SANTOS, 2010).

Já os NIDS, são definidos por Santos (2010) como objetivo a monitoração e análise dos pacotes e fluxo de uma rede em sua totalidade, identificando atividades maliciosas na mesma, afim de detectar uma intrusão em seu sistema, ou mal uso da mesma.

Por fim, temos os Sistemas de Detecção de Intrusão Híbridos que é a junção dos dois anteriores, para controle e monitoração de todo o ambiente, com o objetivo de garantir a segurança do mesmo.

2.5.5.2 Sistema de prevenção de intrusão

Diferentemente do IDS, o *IPS* possui uma característica mais ativa, pois o mesmos além de identificar o possíveis ataques, é capaz de agir por si só para impedi-los de causar danos ao alvo. Sendo assim podemos considerar que os Sistemas de Prevenção de Intrusão funcionam como uma junção da capacidade do IDS de analisar o possível ataque com a capacidade de bloquear de um *firewall*.

A definição de IPS dada por Goodrich e Tamassia (2012), afirma que os IPS's são sistemas reativos atuando juntamente com dispositivos de rede, para que haja a redução e prevenção de ações maliciosas.

Os sistemas de prevenção de intrusão (IPS) possuem funcionamento de maneira parecida ao IDS no que diz respeito análise de pacotes, diferenciando-se na capacidade de bloquear as requisições fora das regras pré estabelecidas no mesmo. Lembrando que é importante se considerar a chance de bloqueio de requisições que são classificadas como anômalas mas que são reais, gerando um falso-positivo.

Ashoor e Gore (2012) afirma que os Sistemas de Prevenção de Intrusão além de detectar os pacotes maliciosos, também realiza ações para impedir que os mesmos completem seu objetivo, ou seja, causem prejuízos, por exemplo, financeiro ou moral, aos administradores da infraestrutura em questão. Segundo Maia e Rehem (2005), um IPS pode realizar várias medidas para interceptar um ataque, como adicionar regras aos roteadores e também bloquear portas no *switch*.

Outra definição apresentada por Endorf, Schultz e Mellander (2004) que especifica mais a fundo um IPS, é de que o mesmo é constituído por quatro componentes principais, que seriam o modelador de tráfego, responsável pelo gerenciamento do fluxo de pacotes, o *scanner* de serviço, que classifica as informações a partir de uma tabela de referencia. O terceiro componente seria a máquina de detecção, que através da tabela de referencia seleciona uma resposta adequada, e por último o normalizador de tráfego, que analisa e reestrutura os pacotes, executando ações de bloqueio.

2.5.5.3 Análises de ataques por comportamento

Ao longos dos anos, vários estudos e técnicas foram surgindo no ramo do combate aos cibercrimes, levando em consideração as características que cada tipo de ataque possui, se o mesmo acontece através da exploração de portas abertas, se sobrecarrega sistemas e sites para torná-los indisponíveis ou realiza o envio de *emails* e mensagens para direcionar os usuários para sites maliciosos, dentre tantas outras maneiras de explorar as falhas dos sistemas e causar prejuízos às vítimas.

Uma maneira que vem sendo utilizada pelas empresas para detecção e prevenção de ameaças, é a realização do comportamento de utilização da rede, podendo ser focada em

determinado usuário, como é explicado por Gomes (2020) que, a análise de comportamento de determinado usuário na rede empresarial, deve ser feita de maneira comparativa em relação ao perfil do restante da equipe e dos funcionários, onde caso os dados coletados fujam do padrão da equipe, um alarme deve ser gerado. Outro foco que a análise pode ter, é ser feita de modo geral, ou seja, não dando foco à apenas um usuário, mas olhando os usuários e dispositivos como um todo no fluxo de dados.

Segundo a Cisco (2020), a detecção de um comportamento atípico em uma rede, acontece quando se tem um conhecimento prévio de como é o comportamento normal, ou seja, quando se tem uma amostra da rede quando a mesma não está sob ataques, para que, com esses dados, possa ser feita uma comparação de atividades que se destacam perante um comportamento padrão da rede.

Durante a realização de alguns tipos de ataques, os mesmos costumam deixar rastros característicos, que dificilmente são encontrados em outros tipos de invasão, ou ao se comparar com os aspectos de um ambiente computacional em seu estado de perfeição, essas características também irão se destacar, indicando que ali pode estar ocorrendo um crime cibernético.

Através das analises dos fluxos em uma rede de computadores, as organizações podem concluir se está acontecendo algum comportamento malicioso, incomuns em um tráfego ”normal”de dados. Essas análises são extremamente importantes para as empresas, que podem conseguir prever as invasões antes que as mesmas ocorram de fato, além de servir como uma base de conhecimento para identificar ataques parecidos.

2.6 Trabalhos Relacionados

O projeto desenvolvido por Peres (2017), faz-se a utilização de ferramentas como o *Snort*, que é um IDS baseado em redes, ou seja, um software que analisa o tráfego de pacotes, examinando o comportamento dos mesmos e fornece dados para que o sistema identifique se aqueles dados possuem características maliciosas. Outra ferramenta utilizada é o IPFW, que basicamente pode ser definido como um filtro de pacotes que alguns sistemas operacionais possuem, com a função de filtrar pacotes, aceitando-os ou bloqueando-os com base nas regras pré-estabelecidas. Após a configuração da infraestrutura e das simulações dos ataques, Peres (2017) concluiu que, aplicando-se apenas um tipo de prevenção, a eficácia fica comprometida, pois alguns funcionarão apenas como um alarme, enquanto outros conseguem barrar a invasão.

A pilha ELK é mencionada e utilizada na execução do trabalho de Rodrigues (2017). É feita uma indexação, armazenamento e visualização de todos os dados trafegados na rede simulada, porém nesse caso, o ELK é utilizado somente com o intuito de fazer uma análise e inspeção profunda dos dados, não sendo usado para alertar possíveis ataques ou barrá-los.

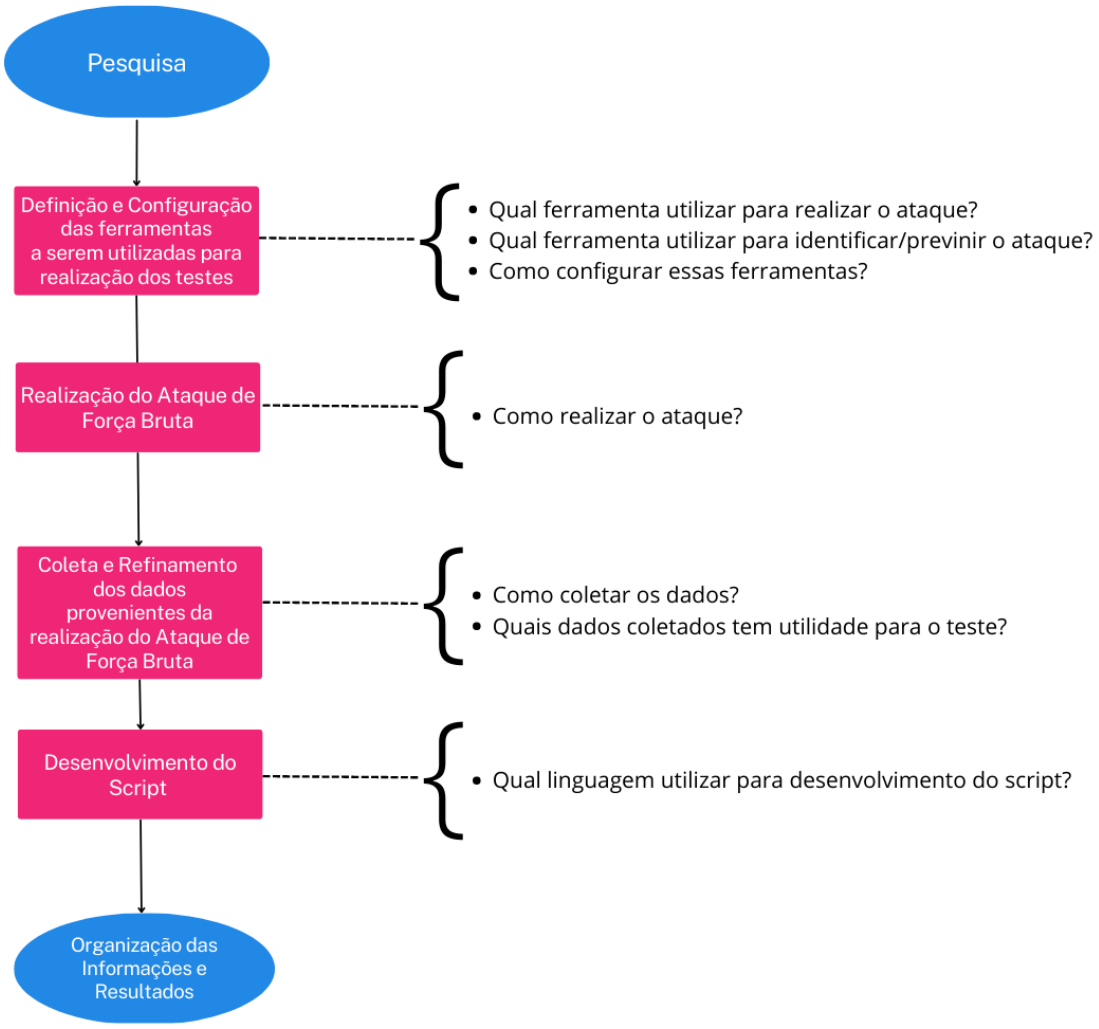
No artigo apresentado por Neto, Almeida e Lucas (2014), tem-se a simulação de um ataque de negação de serviço originado por um ataque de força bruta, em uma infraestrutura configurada com as ferramentas *IDS/IPS Fail2ban*, que conseguem realizar a identificação dos *IP's* atacantes, enviando-os para a ferramenta utilizada em conjunto, *Firewall Netfilter/Iptables*,

que tem a função de realizar o bloqueio dos IP’s, obtendo sucesso ao conseguiram evitar e bloquear as máquinas atacantes.

3 MATERIAIS E MÉTODOS

Para que fosse possível a realização do ataque e posteriormente sua identificação ou prevenção, e até mesmo a análise dos dados do fluxo de rede enquanto o mesmo ocorria, alguns passos foram seguidos, conforme visto no fluxograma presente na Figura 12.

Figura 12 – Fluxograma das etapas do desenvolvimento do Trabalho



Fonte: imagem do autor

3.1 Definição e configuração das ferramentas

As ferramentas a serem utilizadas e configuradas para a realização dos testes foram as seguintes:

- ELK, ferramenta de monitoramento e análise, instalada em uma máquina virtual (*Ubuntu* 18.04), no servidor *PowerEdge* r730 Dell, do provedor de internet Faxt Telecomunicações LTDA na cidade de Diamantina;
- Computador DELL, Sistema Ubuntu/Linux (Ip: 177.124.72.16);
- ELK com o *plugin Elastiflow*;
- Roteador *Mikrotik* com IP público 177.124.77.45;

- Medusa - Ferramenta de realização do ataque;
- *Notebook* DELL, Windows 10, 8GB;
- *Jupyter Notebook*;

Todos os testes foram realizados tendo como *host* atacante a máquina DELL com sistema Ubuntu (Ip: 177.124.72.16), e como *host* vítima o *Mikrotik* (Ip: 177.124.77.45).

3.1.1 Monitoração e coleta de dados com ELK

O ELK foi utilizado para fazer a monitoração e coleta dos dados tanto para simulações de ataques quanto para simulações de navegação na rede sem ataques. No caso das simulações de ataque foram coletados todos os dados obtidos do fluxo do roteador junto com os dados do ataque.

Segue no Anexo A, um tutorial de como fazer a instalação do ELK e configuração do *plugin elastiflow* em uma máquina com sistema *Debian*.

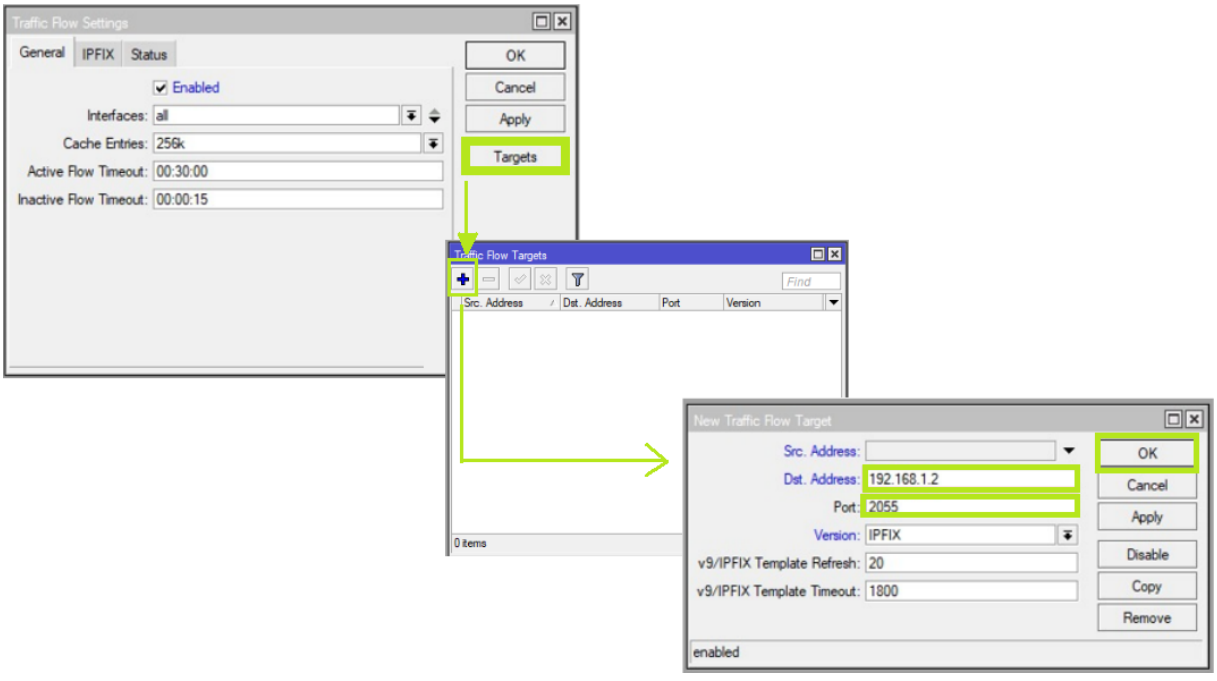
3.1.2 Mikrotik

O roteador *Mikrotik* recebeu duas configurações em diferentes momentos. Em um primeiro momento, o roteador foi configurado com o IPFIX, para trabalhar juntamente ao ELK para receber o ataque. Em um segundo momento, sem as configurações do IPFIX, o roteador foi novamente configurado com regras de *firewall* para interceptar o ataque.

3.1.2.1 Configuração do Mikrotik para coleta de dados com ELK

No roteador *Mikrotik*, foram realizadas as configurações de adição do IPFIX, que podem ser vistas na Figura 13.

Figura 13 – Configuração do *Mikrotik* com IPFIX



Fonte: imagem do autor

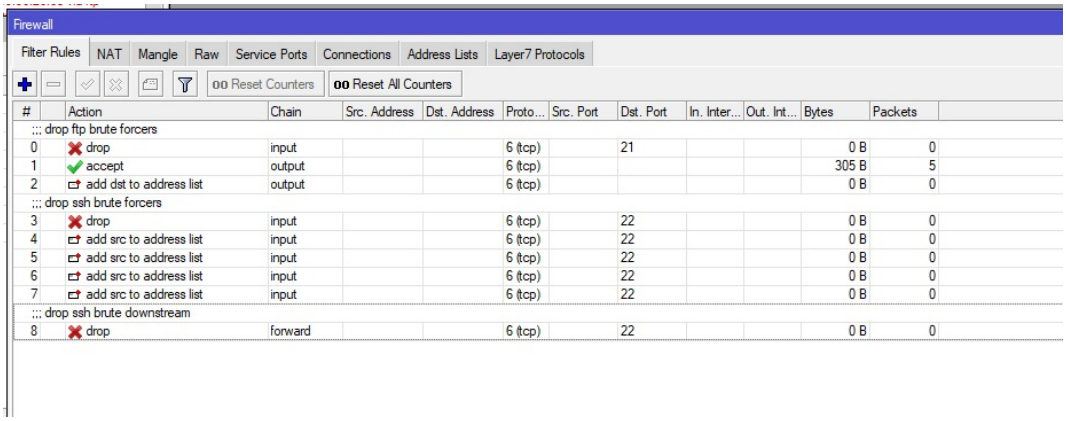
3.1.2.2 Configuração do firewall do Mikrotik para interceptar ataque

O roteador *Mikrotik* permite adicionar nele regras de *firewall* que ajudam a interceptar um ataque de força bruta. Adicionando essas configurações e posteriormente realizando os ataques, o próprio roteador intercepta o ataque, e adiciona o IP do *host* atacante à uma *black list*, ou seja, uma lista de IP's proibidos de trocarem informações com o roteador. Assim, da próxima vez que o mesmo tentar realizar algum ataque, o roteador faz a verificação se o IP consta nessa *black list*, para permitir ou barrar a entrada do IP no roteador.

Segue abaixo a adição das regras de *firewall* no terminal do roteador e sua interface correspondente na Figura 14.

- add chain=input protocol=tcp dst-port=21 src-address-list=ssh_blacklist action=drop
- add chain=output action=accept protocol=tcp content="530 Login incorreto" dstlimit=1/1m, 9,dst-address 1m
- add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorreto" address-list=ssh_blacklist address-list-timeout=3h

Figura 14 – Interface do *mikrotik* após configuração do *firewall*



Fonte: imagem do autor

3.1.3 Medusa

O medusa é uma ferramenta nativa de sistemas *Linux/Ubuntu*, que efetua os ataques via SSH, SMB, HTTP, entre outros, visando quebrar sistemas que utilizem senhas fracas. Sendo assim sua instalação não foi necessária. O Medusa permite que seja utilizado uma lista de possíveis usuários e uma lista de possíveis senhas, descartando a necessidade de saber previamente o *user* do roteador *Mikrotik*, o que não acontece com algumas outras ferramentas que existem, como por exemplo o *MKBRUTUS*, que só permite receber uma lista de senhas, porém o usuário é fixo. A verificação e tentativa de descoberta de usuário e senha no Medusa acontece da seguinte maneira: para cada usuário da lista, a ferramenta faz a verificação de todas as senhas, após fazer a verificação, ele prossegue para o segundo usuário da lista e assim sucessivamente.

Portanto, uma lista de usuários(user.txt) e uma lista de senhas(password.txt) foram criadas para a realização do ataque, lembrando que nessas listas, para o presente trabalho, conter

ou não os verdadeiros *user* e *password* é indiferente, pois o objetivo não é a obtenção do sucesso do ataque.

3.1.4 Configuração do jupyter notebook

Após a realização dos ataques e coleta dos dados capturados pelo ELK, para a análise dos mesmos, foi utilizado o *jupyter notebook*, uma ferramenta de código aberto disponibilizada pela Anaconda, que facilita na criação e compartilhamento de código, podendo ser utilizada com as mais variadas linguagens de programação, trabalhos estatísticos e *machine learning*.

O Hardware utilizado para realizar as análises foi o *notebook* com o Sistema *Windows 10*, sendo assim, a instalação do *Jupyter Notebook* pode ocorrer de duas maneiras: através do site oficial da ferramenta ou através do pip (Gerenciador de pacotes do *python*). No presente trabalho foi utilizado a segunda opção, tendo como pré-requisito a instalação do *python* no computador. Caso não tenha o *python* instalado, o download do mesmo pode ser feito no site oficial, que se encontra o link no Anexo B do presente Trabalho.

Após a instalação do *python*, pode-se utilizar o comando abaixo através do terminal do computador, para que todos os pacotes e dependências sejam baixados para a utilização do *jupyter notebook*.

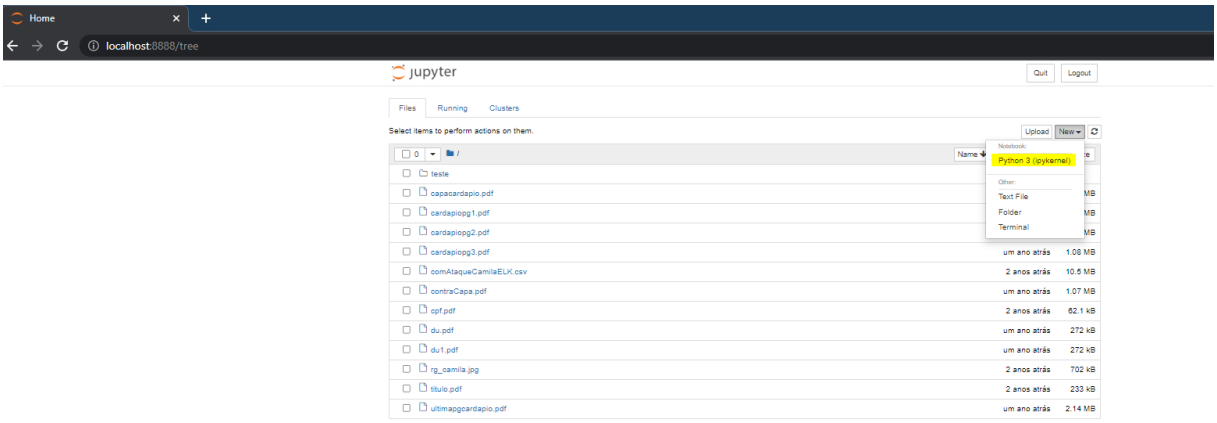
- pip install jupyter

Para inciar o *jupyter notebook*, a linha de comando abaixo foi utilizada no terminal do computador.

- jupyter notebook

O ferramenta é aberta no navegador padrão do *host*, porém funcionando local. A interface de entrada possui muitas funcionalidades, dando acesso às pastas no nosso computador, permitindo abrir projetos criados anteriormente ou criar novos projetos. Para o presente trabalho, um novo Notebook foi criado com o *python* 3 como linguagem de programação configurada. Tem-se na Figura 15 a interface inicial do *jupyter notebook*.

Figura 15 – Interface Inicial do *Jupyter Notebook*

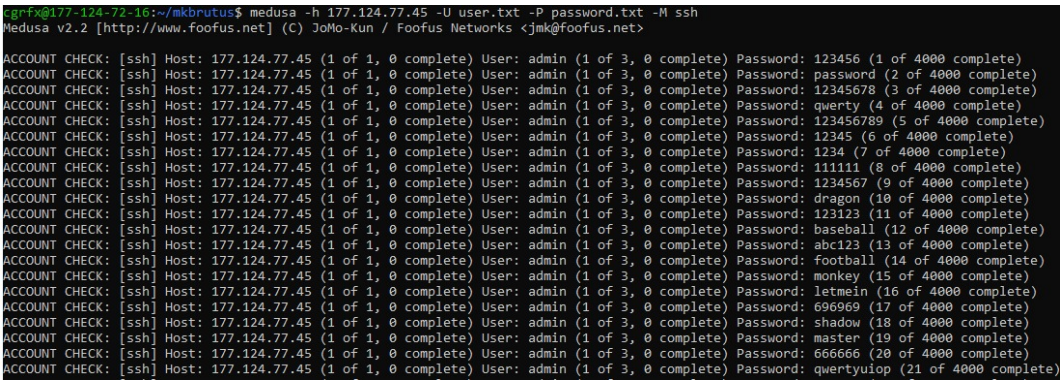


Fonte: imagem do autor

3.2 Realização do ataque

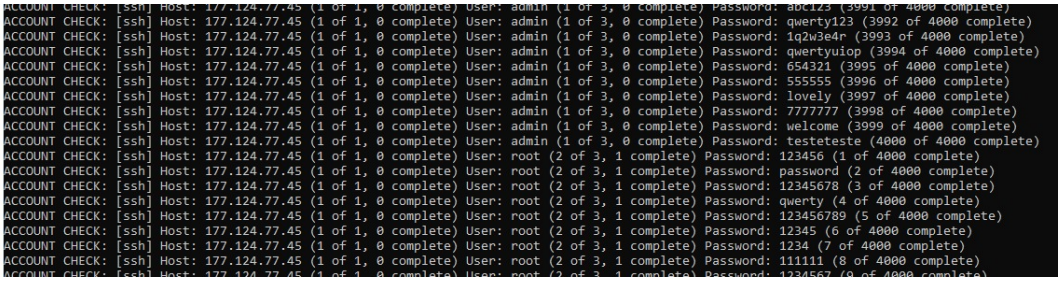
O ataque de força bruta, foi realizado em dois momentos, o primeiro com as configurações somente do *Mikrotik* para que houvesse a adição do IP atacante na *black list*, e o segundo, após a retirada das primeiras configurações feitas no *Mikrotik*, e realizadas as configurações do IPFIX no *Mikrotik*. Porém, vale destacar que o ataque foi feito da mesma maneira para os dois procedimentos descritos. Na Figura 16, pode-se observar o início do ataque de força bruta, através do comando: *medusa -h 177.124.77.45 -U user.txt -P password.txt -M ssh*. Nas Figuras 17, 18 e 19, tem-se a verificação de todas as senhas do arquivo *password.txt* para cada usuário do arquivo *user.txt*.

Figura 16 – Comando para início de ataque de Força Bruta



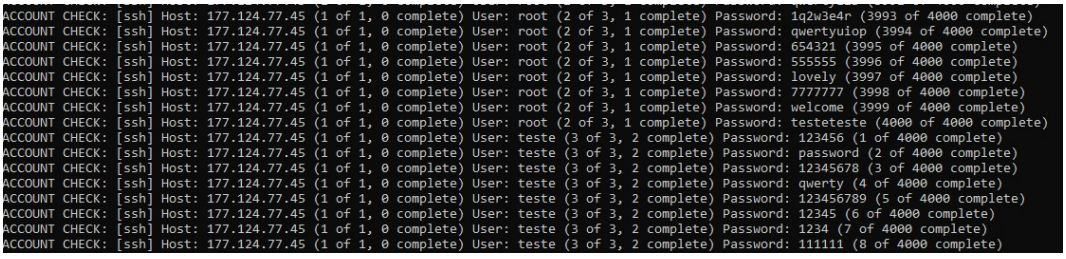
Fonte: imagem do autor

Figura 17 – Ataque de Força Bruta acontecendo, com a verificação pelo segundo usuário da lista



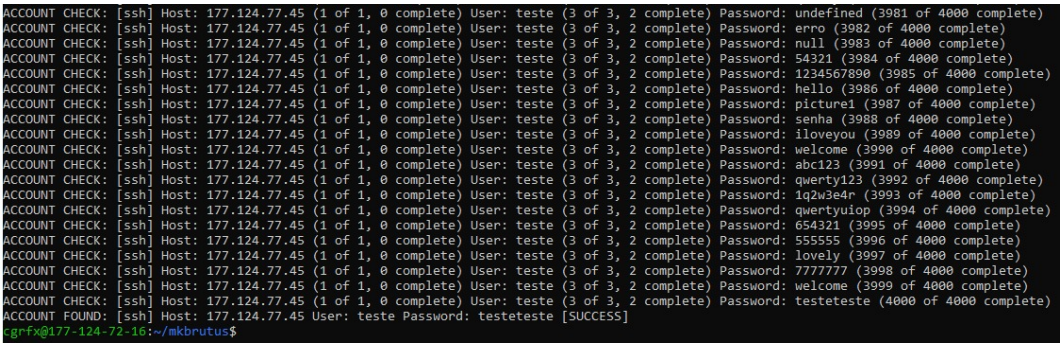
Fonte: imagem do autor

Figura 18 – Ataque de Força Bruta acontecendo, com a verificação pelo terceiro usuário da lista



Fonte: imagem do autor

Figura 19 – Fim do ataque de Força Bruta



Fonte: imagem do autor

3.3 Dados Coletados

Os dados coletados pelo ELK, *plugin elastiflow* e IPFIX em conjunto, são recuperados através da própria interface do *Kibana*, permitindo colocar um intervalo de tempo, que no caso seria o intervalo de tempo de realização do ataque, que foi de aproximadamente 15 minutos. Também foi coletado dados em um intervalo de tempo de 15 minutos onde não ocorria o ataque, com o fluxo de rede em condições ”normais”para observação do comportamento do fluxo.

Muitos são os dados que são coletados pelo software, porém alguns que não possuíam relevância para os estudos, foram descartados a fim de otimizar as análises. Na Figura 20 pode-se observar todos os tipos de dados que foram coletados pelo ELK.

Figura 20 – Dados coletados do fluxo de rede

Dados Coletados do Fluxo					
@timestamp	@version	_id	_index	_score	_type
agent.hostname	agent.id	agent.name	agent.type	agent.version	as.organization.name
client.as.number	client.as.organization.name	client.bytes	client.domain	client.geo.city_name	client.geo.country_iso_code
client.geo.country_name	client.geo.location	client.ip	client.packets	destination.as.number	destination.as.organization.name
destination.domain	destination.geo.city_name	destination.geo.country_iso_code	destination.geo.country_name	destination.geo.location	destination.ip
destination.mac	destination.nat.ip	destination.nat.port	destination.port	ecs.version	event.category
event.dataset	event.kind	event.module	event.severity	event.type	flow.direction
flow.dst_mask_len	flow.dst_port_name	flow.dst_rep_tags	flow.input_ifname	flow.input_snmp	flow.next_hop
flow.output_ifname	flow.output_snmp	flow.rep_tags	flow.sampling_interval	flow.server_rep_tags	flow.service_name
flow.service_port	flow.src_mask_len	flow.src_port_name	flow.src_rep_tags	flow.tcp_flags	flow.tos
flow.traffic_locality	geo.city_name	geo.country_iso_code	geo.country_name	host.ip	host.name
ipfix.flowEndSysUpTime	ipfix.flowStartSysUpTime	ipfix.flowset_id	ipfix.icmpCodeIPv4	ipfix.icmpTypeIPv4	ipfix.igmpType
ipfix.ipHeaderLength	ipfix.ipTTL	ipfix.ipTotalLength	ipfix.isMulticast	ipfix.octetDeltaCount	ipfix.packetDeltaCount
ipfix.postSourceMacAddress	ipfix.tcpAcknowledgementNumber	ipfix.tcpSequenceNumber	ipfix.tcpWindowSize	ipfix.udpMessageLength	ipfix.version
log.level	message	network.bytes	network.iana_number	network.packets	network.transport
network.type	server.as.number	server.as.organization.name	server.bytes	server.domain	server.geo.city_name
server.geo.country_iso_code	server.geo.country_name	server.geo.location	server.ip	server.packets	source.as.number
source.as.organization.name	source.bytes	source.domain	source.geo.city_name	source.geo.country_iso_code	source.geo.country_name
source.geo.location	source.ip	source.nat.ip	source.nat.port	source.packets	source.port
tags					

Fonte: imagem do autor

O arquivo CSV gerado através do ELK com todos os dados do fluxo, pode ser encontrado no Apêndice A deste trabalho.

3.3.1 Coeficiente de correlação de Pearson

Antes que seja feito o detalhamento do desenvolvimento do *script*, vale destacar que, um estudo com os dados coletados foi feito afim de encontrar um padrão entre os mesmos, ou seja, encontrar características nos dados coletados sob o ataque, que poderiam seguir algum padrão entre os mesmos.

O coeficiente de correlação de *Pearson* foi utilizado para descobrir se, entre os dados coletados, dois a dois, poderia ser encontrado alguma correlação. Ou seja, dado duas variáveis, pode-se definir através do cálculo do coeficiente o quão elas se relacionam linearmente, sendo o resultado dentro de uma escala de -1 a 1, onde quanto mais perto 1 tem-se uma relação positiva que se a variável A cresce, a B também cresce, ou quanto mais perto de -1 tem-se uma relação negativa, onde quando uma variável cresce, a outra decresce. Por fim, quanto mais perto de 0, indica que não há correlação entre as variáveis (COLOSIMO, 2019).

O cálculo do coeficiente foi realizado na ferramenta *Jupyter Notebook*, utilizando a linguagem *python*, através do comando *nomeDoDataframe.corr()*, e pode ser encontrado no Apêndice A do presente Trabalho. Na Figura 21, pode-se observar uma amostra da correlação da variável *"destination.as.number"* calculada para todas as outras variáveis do *dataframe*.

Figura 21 – Amostra da correlação de uma variável sendo calculada em relação às outras variáveis do *dataframe*

```
In [48]: tabelaCorrelacao = baseForcaBrutaCA.corr()

In [49]: tabelaCorrelacao
```

Out[49]:

	destination.as.number
destination.as.number	1.000000
destination.nat.port	0.209367
destination.port	0.209367
flow.input_snmp	-0.098916
flow.output_snmp	-0.048114
flow.service_port	0.077760
ipfix.flowEndSysUpTime	0.020359
ipfix.flowStartSysUpTime	0.021506
ipfix.ipTTL	0.012895
ipfix.ipTotalLength	-0.365314
ipfix.tcpAcknowledgementNumber	0.092054

Fonte: imagem do autor

Após essa análise e o cálculo associando todas os campos, dois a dois, para encontrar alguma relação entre si, percebe-se que a maioria dos resultados se aproximaram de zero, indicando que não há uma correlação forte entre as variáveis. Algumas correlações calculadas se aproximaram de um, porém ao analisá-las, percebe-se que isso acontece quando o método compara a variável com ela mesma, ou com uma outra variável de significado similar ou igual. Sendo assim, a técnica de análise por comportamento foi utilizada, analisando o comportamento da rede sob o ataque, e sob condições normais.

3.4 Desenvolvimento do *Script*

Primeiramente, foi feito um filtro para identificar quantas conexões ou tentativas de conexões entre IP's origem existiam com o IP destino do *host Mikrotik*. Em condições normais de

rede, o IP do *Mikrotik* costuma receber algumas ou até mesmo nenhuma conexão do IP atacante, como mostrado na Figura 22.

Figura 22 – IP's que tentaram conexão com o *Mikrotik* e número de tentativas - fluxo normal

```
listaCombinadaIpOcorrenciasSA = list(zip(listaIPSA, listaNumeroOcorrenciasSA))
listaCombinadaIpOcorrenciasSA
```

```
Out[70]: [('1.182.188.139', 1),
          ('103.56.116.214', 1),
          ('106.13.231.243', 1),
          ('115.164.114.48', 1),
          ('120.79.20.228', 1),
          ('125.136.249.155', 3),
          ('125.74.59.27', 1),
          ('139.215.251.87', 1),
          ('14.204.139.106', 1),
          ('146.88.240.4', 2),
          ('157.185.149.55', 1),
          ('162.142.125.161', 1),
          ('162.142.125.167', 1),
          ('162.142.125.68', 1),
          ('163.171.179.72', 1),
          ('165.22.227.240', 1),
          ('167.248.133.21', 1),
          ('167.248.133.68', 1),
          ('167.248.133.70', 1),
          ('167.99.128.242', 1),
          ('176.65.3.109', 1),
          ('177.124.0.214', 1),
          ('177.124.167.182', 1),
          ('177.124.184.11', 10),
          ('177.124.230.210', 2),
          ('177.124.231.118', 3),
          ('177.124.3.70', 11),
          ('177.124.48.235', 1),
          ('177.124.51.80', 11),
          ('177.124.57.238', 10),
          ('177.124.61.98', 1),
          ('177.124.75.224', 1),
          ('177.223.78.2', 1),
          ('179.43.134.190', 1),
          ('183.136.225.42', 1),
          ('185.142.239.16', 1),
          ('188.166.172.189', 1),
          ('192.168.0.75', 1),
          ('192.241.206.146', 1),
          ('194.61.25.194', 1),
          ('195.133.40.141', 1),
          ('209.141.46.141', 1),
          ('217.128.255.47', 1),
          ('218.7.198.189', 1),
          ('23.90.145.36', 1),
          ('27.148.141.213', 1),
          ('3.97.211.227', 1),
          ('31.13.74.53', 1),
          ('45.143.203.12', 1),
          ('45.146.164.196', 8),
          ('45.146.164.211', 1),
          ('45.155.205.129', 7),
          ('46.101.160.136', 1),
          ('47.94.227.170', 1),
          ('60.249.188.117', 1),
          ('61.164.210.103', 1),
          ('69.235.184.27', 2),
          ('69.235.184.29', 2),
          ('71.6.147.254', 1),
          ('74.82.47.9', 1),
          ('82.130.221.222', 1),
          ('89.163.225.137', 1),
          ('92.118.161.49', 1),
          ('93.174.95.106', 1)]
```

Fonte: imagem do autor

Já analisando o fluxo de rede para o mesmo IP, porém estando sob as condições de um ataque de força bruta, esse número aumenta exponencialmente, como mostrado na Figura 23, que para o IP atacante 177.124.72.16, houve 1060 tentativas de conexão com o IP do *mikrotik*. Mas somente esse parâmetro não garante a ocorrência de um ataque. Podemos exemplificar a situação com uma chamada de vídeo, onde há uma grande troca de dados entre os IP's origem e destino, aumentando assim significativamente a quantidade de conexões, porém não há ocorrência do ataque.

Figura 23 – IP's que tentaram conexão com o *Mikrotik* e número de tentativas - fluxo com ataque

```
listaCombinadaIpOcorrenciasCA = list(zip(listaIPAtacanteCA, listaNumeroOcorrenciasCA))
listaCombinadaIpOcorrenciasCA
```

```
Out[17]: [('104.140.188.26', 1),
          ('121.12.165.214', 1),
          ('122.225.28.226', 1),
          ('124.236.70.192', 1),
          ('125.124.13.108', 1),
          ('143.198.167.43', 1),
          ('143.198.65.86', 1),
          ('146.88.240.4', 1),
          ('158.101.149.76', 1),
          ('162.142.125.21', 1),
          ('162.142.125.71', 1),
          ('162.142.125.80', 1),
          ('165.227.4.237', 1),
          ('167.248.133.78', 1),
          ('172.105.219.236', 1),
          ('177.124.184.11', 10),
          ('177.124.3.70', 1),
          ('177.124.48.245', 2),
          ('177.124.61.98', 10),
          ('177.124.72.16', 1060),
          ('184.105.139.126', 1),
          ('185.191.34.207', 1),
          ('187.153.118.43', 1),
          ('188.166.87.18', 1),
          ('188.92.77.235', 1),
          ('189.148.90.114', 1),
          ('190.210.166.140', 1),
          ('192.241.195.158', 1),
          ('193.107.216.203', 1),
          ('193.46.255.123', 1),
          ('205.185.114.54', 1),
          ('220.134.27.69', 1),
          ('3.10.234.97', 1),
          ('45.145.66.90', 1),
          ('45.146.164.196', 4),
          ('45.155.205.129', 5),
          ('45.83.64.182', 1),
          ('46.234.125.89', 1),
          ('62.169.203.69', 1),
          ('68.183.80.7', 1),
          ('74.120.14.20', 1),
          ('74.120.14.89', 1),
          ('74.82.47.10', 1)]
```

Fonte: imagem do autor

Como descrito anteriormente, não é possível identificar o ataque somente com o número de tentativas de conexões entre o IP origem e o IP destino, mas é um índice que podemos considerar na hora de identificar e filtrar IP's ao qual devemos analisar mais profundamente essas conexões.

Portanto, um outro parâmetro foi considerado para identificar o ataque, o "flow.tcp_flags", que captura as *flags* trocadas para estabelecimento de uma conexão TCP entre dois IP's, ou seja, através desse parâmetro podemos concluir se uma conexão foi inicializada, se de fato

ela se estabeleceu, e para os casos negativos, quantas tentativas de conexões ocorreram de um mesmo IP origem, para um mesmo IP destino.

Nas Figuras 24 e 25, tem-se exemplificado as *flags* trocadas existentes no fluxo entre o IP atacante e o IP vítima.

Figura 24 – *Flags* enviadas pelo IP atacante

	source.nat.ip	destination.nat.ip	flow.tcp_flags
0	177.124.72.16	177.124.77.45	["SYN"]
2	177.124.72.16	177.124.77.45	["SYN"]
8	177.124.72.16	177.124.77.45	["SYN"]
15	177.124.72.16	177.124.77.45	["SYN"]
17	177.124.72.16	177.124.77.45	["SYN"]
...	...	...	...
9411	177.124.72.16	177.124.77.45	["SYN"]
9427	177.124.72.16	177.124.77.45	["SYN"]
9428	177.124.72.16	177.124.77.45	["SYN"]
9433	177.124.72.16	177.124.77.45	["SYN"]
9434	177.124.72.16	177.124.77.45	["SYN"]

Fonte: imagem do autor

Figura 25 – *Flags* enviadas pelo IP vítima

Out[12]:

	source.nat.ip	destination.nat.ip	flow.tcp_flags
1	177.124.77.45	177.124.72.16	["SYN","ACK"]
3	177.124.77.45	177.124.72.16	["SYN","ACK"]
13	177.124.77.45	177.124.72.16	["SYN","ACK"]
14	177.124.77.45	177.124.72.16	["SYN","ACK"]
16	177.124.77.45	177.124.72.16	["SYN","ACK"]
...	...	...	...
9387	177.124.77.45	177.124.72.16	["SYN","ACK"]
9397	177.124.77.45	177.124.72.16	["SYN","ACK"]
9412	177.124.77.45	177.124.72.16	["SYN","ACK"]
9419	177.124.77.45	177.124.72.16	["SYN","ACK"]
9432	177.124.77.45	177.124.72.16	["SYN","ACK"]

Fonte: imagem do autor

Identificados quais os parâmetros seriam utilizados para a análise, um *script* foi desenvolvido em *python* 3, que é uma linguagem que permite trabalhar de maneira eficaz com grandes volumes de dados e realizar análises estatísticas, utilizando a ferramenta Jupyter Notebook, para que ao receber esses dados, fosse possível concluir se havia um possível ataque acontecendo entre IP's origens e IP's destinos.

Os seguintes passos foram executados no desenvolvimento do *script*:

- Importação de bibliotecas necessárias para desenvolvimento do *script*;

```
    %matplotlib inline
    import pandas as pd

```

- Conversão do arquivo CSV gerado pelo ELK sob o ataque de Força Bruta em *dataframe*;

```
    baseForcaBrutaCA = pd.read_csv("C:/Users/camil/Downloads/
    camilaServidorComAt.csv")

```

- Extração de uma lista ordenada de IP's destino de todos os fluxos retornados no *Dataframe*;

```
    listaIpDestinoSemOrdenacao = baseForcaBrutaCA['destination.nat.
    ip'].values
    listaIpDestinoOrdenado = sorted(listaIpDestinoSemOrdenacao)

```

- Criação de uma nova lista de IP's destino retirando as repetições;

```
    cont = 0

listaIpsDestino = [] #lista com ip's que tentaram conex o
rep = 0
#itera  o para salvar nas listas os ip's com seus respectivos
    n meros de tentativas
for k in range(0,len(listaIpDestinoOrdenado)-1):
    if(listaIpDestinoOrdenado[k] == listaIpDestinoOrdenado[k+1]):
        rep += 1
        if (k == len(listaIpDestinoOrdenado)-2):
            listaIpsDestino.insert(k, listaIpDestinoOrdenado[k])
    else:
        listaIpsDestino.insert(k, listaIpDestinoOrdenado[k])
        rep = 0

```

- Iteração sobre todos os IP's que receberam algum fluxo, ou seja, por algum momento foram IP's destino;

```
    for cont in range(len(listaIpsDestino)):

```

- Criar um novo *dataframe* a partir do original, filtrando somente pelos valores de determinado IP destino que possa estar sofrendo um ataque;

```
    #Mascara e filtro para obter dados do dataframe relacionados somente a determinado ip quando est  sofrendo um suposto ataque de for a bruta, por fim salvando em um novo dataframe
    baseForcaBrutaCA_mask=baseForcaBrutaCA['destination.nat.ip']==listaIpsDestino[cont]
    filtered_baseForcaBrutaCA = baseForcaBrutaCA[baseForcaBrutaCA_mask]
    baseForcaBrutaCA_FluxoAtacanteVitima = filtered_baseForcaBrutaCA [['source.nat.ip' ,'destination.nat.ip', 'flow.tcp_flags']]
    baseForcaBrutaCA_FluxoAtacanteVitima

```

- Listar as *flags* que saíram dos IP's origem do suposto ataque;

```
    #Salvando em um vetor as flags que chegaram ao ip destino
    vetorFlagsAtacanteToVitima = baseForcaBrutaCA_FluxoAtacanteVitima['flow.tcp_flags'].values

```

- Listar todos os IP's origens que tentaram conexão com determinado IP's destino;

```
    #Salvando em um vetor os ip's que tentaram uma conex o com o ip destino
    vetorCA = baseForcaBrutaCA_FluxoAtacanteVitima['source.nat.ip'].values

```

- Lista ordenada dos IP's que tentaram conexão com determinado IP destino;

```
    #Ordenando todos os ip's que tentaram conex o com o ip destino
    vetorCAOrdenado = sorted(vetorCA)

```

- Listagem dos IP's origem e seus respectivos números de tentativas de conexão com o IP destino;

```
    listaIPAtacanteCA = [] #lista com ip's que tentaram conex o
    listaNumeroOcorrenciasCA = [] #lista com o n mero de tentativas de conex o de cada ip origem com o ip destino
    rep = 0
    #itera  o para salvar nas listas os ip's com seus respectivos n meros de tentativas
    for k in range(0,len(vetorCAOrdenado)-1):
        if(vetorCAOrdenado[k] == vetorCAOrdenado[k+1]):
            rep += 1
            if (k == len(vetorCAOrdenado)-2):
                listaIPAtacanteCA.insert(k, vetorCAOrdenado[k])
                listaNumeroOcorrenciasCA.insert(k, rep+1)
        else:
            listaIPAtacanteCA.insert(k, vetorCAOrdenado[k])
```

```
13              listaNumeroOcorrenciasCA.insert(k, rep+1)
14              rep = 0
15
```

- Filtrar o numero de tentativas de conexão de cada IP origem com determinado IP destino, e depois selecionar somente aqueles que tiveram um número de tentativas maior que 10, que seria o mesmo número de tentativas falhas do *firewall* do *mikrotik*;

```
1     listaIpsFluxoMaiorDez = [] #Lista dos ip's origem que tentaram
    por mais de 10 vezes uma conex o com o ip destino
2     i = 0
3     #itera  o para salvar na lista os ip's que tentaram por mais
    de 10 vezes uma conex o com o ip destino
4     for i in range(len(listaNumeroOcorrenciasCA)):
5         if listaNumeroOcorrenciasCA[i] > 10:
6             listaIpsFluxoMaiorDez.insert (i, listaIPAtacanteCA[i])
7
```

- Verificar sequencialmente as *flags* enviadas de determinado IP origem para determinado IP destino, se houveram somente *flags* ”SYN”sequencialmente, por mais de 10 vezes, podemos considerar como um ataque.

```
1     i = 0
2     ip = 0
3     aux = 0
4     #itera  o para verificar a sequencia de flags enviadas pelo
    ip origem, sendo que se o mesmo enviou o flag "SYN"
    sequencialmente, sem ter qualquer outro flag, podemos concluir
    que o mesmo est  tentando uma conex o sem sucesso, o que pode
    identificar um ataque
5     for ip in range(len(listaIpsFluxoMaiorDez)):
6         for i in range(len(listaNumeroOcorrenciasCA)):
7             if vetorCA[i] == listaIpsFluxoMaiorDez[ip]:
8                 if vetorFlagsAtacanteToVitima[i] == '["SYN"]':
9                     aux = aux + 1
10                    if aux > 10:
11                        print ("Poss vel ataque ocorrendo do Ip
    Origem ", vetorCA[i], " para o Ip Destino ", listaIpsDestino[
    cont])
12                        break
13                else:
14                    aux = 0
15
```

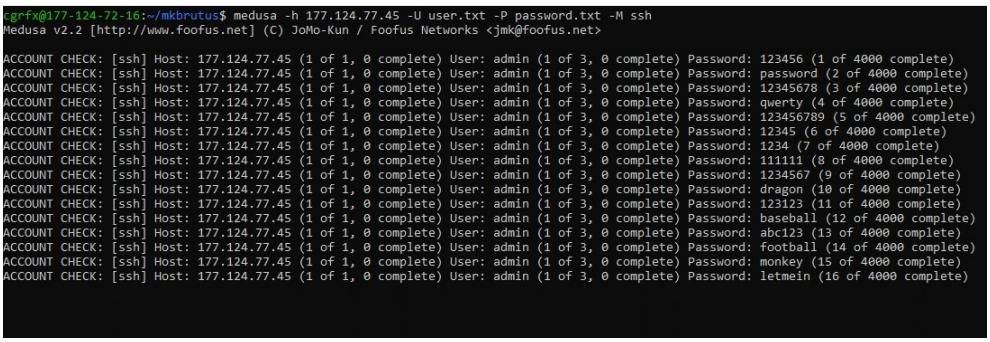
4 RESULTADOS E DISCUSSÃO

Após a realização dos ataques e observação dos mesmos sob as técnicas apresentadas, alguns resultados foram concluídos com êxito, cada qual com suas características e eficácia, considerando pontos importantes, como infraestrutura de rede, adaptabilidade de dispositivo, etc.

4.1 Ataque realizado configurações do *firewall* do *Mikrotik*

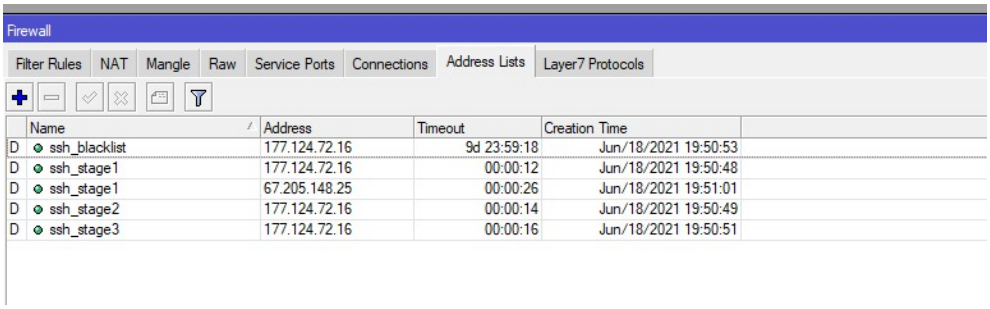
As configurações do *Mikrotik* são específicas para barrar o mesmo IP de realizar tentativas consecutivas sem sucesso. Logo no início do ataque, após iniciar com o comando de ataque, pode-se constatar que após algumas tentativas, as configurações feitas no *Mikrotik* obtiveram sucesso, e o roteador conseguiu interceptá-lo da maneira esperada, não gerando mais *logs* no terminal e adicionando o IP do *host* atacante à *black list* do roteador, como pode ser observado nas Figuras 26, 27 e 28.

Figura 26 – Ataque pelo medusa interceptado



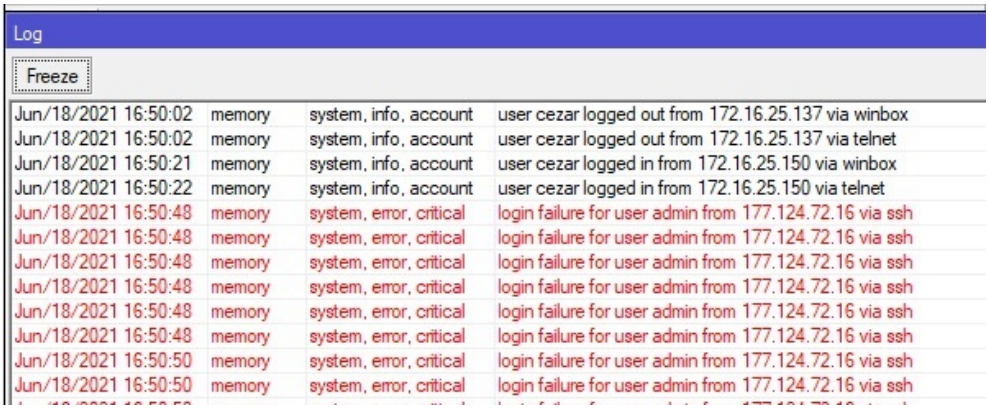
Fonte: imagem do autor

Figura 27 – Ip atacante adicionado à *black list*



Fonte: imagem do autor

Figura 28 – Tentativa de ataque bloqueada para o IP adicionado na *black list*



Fonte: imagem do autor

É importante salientar que, todos os próximos ataques de força bruta com origem desse IP, serão interceptados, pois uma vez adicionado à *black list*, o IP não é removido da mesma sem uma intervenção manual.

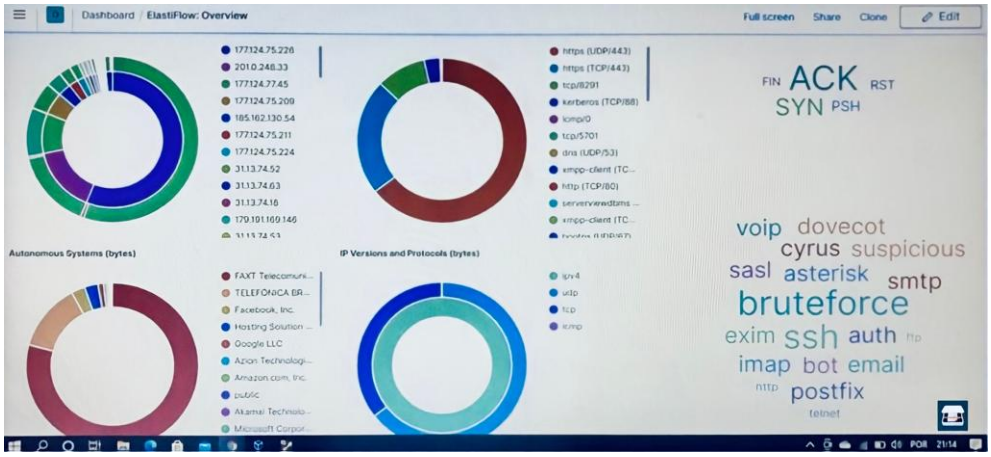
À nível de equipamento, a configuração do *Mikrotik* se mostra bastante eficiente no que diz respeito à bloquear o ataque de força bruta, não deixando chances para que o mesmo ocorra novamente, sob as condições de que um mesmo IP origem tente novamente realizar uma invasão.

4.2 Ataque realizado com monitoramento do ELK

O ELK disponibiliza um arquivo csv com os dados coletados pelo monitoramento do *host*. Sendo assim, foram coletados os dados do período de tempo em que houve o ataque de força bruta, nesse caso, aproximadamente 10 minutos. Também foram coletados os dados com o mesmo intervalo de tempo para o *host* sem estar sofrendo o ataque, possibilizando assim realizar uma análise do comportamento da rede quando ela está sofrendo um ataque, e quando ela está em condições normais, ou seja, com ausência de ataque.

Na Figura 29, tem-se o *dashboard* do *Kibana* no momento de realização do ataque, com os protocolos mais utilizados no fluxo, os IP's que mais enviaram e receberam pacotes, etc.:

Figura 29 – *Dashboard Kibana durante realização do ataque*



Fonte: imagem do autor

Após a coleta dos dados provenientes do ELK, e a execução do *script*, obteve-se a seguinte saída:

```
Possivel ataque ocorrendo do Ip Origem  177.124.72.16  para o Ip
   Destino  177.124.77.45
```

Depois de todo o processo e análise do ataque sob observação do ELK, percebe-se que a pilha *Elasticsearch, Logstash e Kibana* aliados ao *plugin elastiflow* e IPFIX, abrange uma escala maior de ataques devido à grande quantidade de parâmetros que o mesmo coleta, sendo possível identificar pelas características dos ataques, quais parâmetros de redes coletados podem ser afetados pelo mesmo, cruzando dados e analisando-os. Outro ponto a se destacar é que, o ELK é capaz de monitorar vários dispositivos conectados na rede de uma vez só, sendo configurado exclusivamente para um dispositivo ou não.

O trabalho apresentado por Neto, Almeida e Lucas (2014), faz-se a utilização de ferramentas para bloquear o ataque de força bruta, dentre elas, a *Fail2ban*, que é um software que analisa *logs* de sistemas para indicar atividades maliciosas, sendo que é possível adicionar regras para alertar administradores das possíveis falhas (NETO; ALMEIDA; LUCAS, 2014). Essa característica se assemelha com o funcionamento do ELK, que analisa o fluxo de rede a todo momento, oferendo a possibilidade de adição de scripts, como o que foi feito no presente trabalho, para gerar alertas de possíveis invasões.

Outra solução que se assemelha com o ELK, é o *Open Source Security Information Management*(OSSIM), ferramenta opensource que foi utilizada por Silva e Rodrigues (2019) para detectar um ataque de força bruta. A ferramenta realiza o monitoramento da rede, auxiliando nas tomadas de decisões, ou seja, alertar sobre comportamentos maliciosos em tempo real (SILVA; RODRIGUES, 2019).

O ELK possui excelentes interfaces para geração de gráficos, que são de grande importância na tomada de decisões, deixando explícito o significado dos dados gerados. Outra vantagem a se destacar é que, uma grande variedade de grafos podem ser instalados, a fim de

facilitar e definir a relação que há entre os campos. Não menos importante, vale ressaltar que o ELK, configurado da maneira correta, é capaz de detectar vários outros tipos de ataques.

5 CONCLUSÃO

Após a execução dos ataques e análises dos mesmos, percebe-se alguns pontos que diferem os dois mecanismos de identificação e bloqueio do ataque, onde cada um possui uma vantagem ou desvantagem em relação ao outro, que cabe ao usuário definir qual a melhor solução para o seu sistema levando em consideração as características do mesmo.

A configuração do roteador *Mikrotik* para que o mesmo consiga fazer a detecção e posteriormente o bloqueio do ataque de força bruta, no que diz respeito ao dispositivo, é um método de prevenção eficaz, resolvendo tentativas de ataques relacionadas a *IP's* que queiram realizar um ataque de Força Bruta no roteador, ou seja, para aquele determinado IP do roteador, já que a configuração está limitada apenas ao roteador.

Se tratando do ELK, podemos fazer a inserção desse *script* desenvolvido no mesmo, conseguindo detectar o ataque. Além disso, o ELK consegue monitorar vários IP's que estejam na mesma rede, ou seja, pensando em uma empresa de Tecnologia, onde se tem vários IP's que podem servir de entrada para esses ataques, é necessário alguma ferramenta que monitore a atividade de todos os IP's. Nesse quesito, o ELK leva uma grande vantagem, conseguindo monitorar vários IP's através de uma configuração única, além de que, a monitoração do *Mikrotik*, se aplica a roteadores *Mikrotik*, não se aplicando à outros *hosts* e dispositivos, o que o ELK não faz diferenciação.

Sendo assim, conclui-se que em larga escala, o ELK é mais eficiente em alertar um possível ataque, sendo ele de Força Bruta ou outros tipos. Ele também não faz diferenciação no tipo de *host*, além de conseguir monitorar muitos IP's que estão conectados à rede a qual o ELK foi configurado. Ou seja, para uma empresa de tecnologia que conta com uma grande variedade de dispositivos, o ELK seria mais eficaz.

Como trabalhos futuros, tem-se a possibilidade de associar o ELK à uma ferramenta de prevenção de ataques (IPS), enviando o alerta para a mesma conseguir interceptar o ataque. Outro ponto seria realizar uma análise mais profunda sobre os dados e campos coletados pelo ELK, e tentar encontrar através de outras técnicas algum ponto peculiar que acontece quando o fluxo está sob o ataque.

REFERÊNCIAS

ABOMHARA, M.; KøIEN, G. M. **Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks**. 2015. Disponível em: ⟨https://journals.riverpublishers.com/index.php/JCSANDM/article/download/6087/4525/⟩. Acesso em: 07 nov. 2022.

ALMEIDA, M. B. **Aplicação de ontologias em segurança da informação**. 2007. Disponível em: ⟨https://mba.eci.ufmg.br/downloads/aplicacaodeontologias.pdf⟩. Acesso em: 07 nov. 2022.

ARAUJO, A. S. de; LEITE, L. S.; COSTA, L. M. M. da. **Sistemas de Detecção de Intrusão**. 2016. Disponível em: ⟨https://www.gta.ufrj.br/grad/12_1/ids/apresentacao.pdf⟩. Acesso em: 05 nov. 2022.

ASHOOR, A. S.; GORE, S. **Intrusion Detection System (IDS) Intrusion Prevention System (IPS): Case Study**. 2012. Disponível em: ⟨https://www.researchgate.net/profile/Sharad-Gore/publication/266232983_Intrusion_Detection_System_IDS_Case_Study/links/543c0de80cf204cab1db65a3/Intrusion-Detection-System-IDS-Case-Study.pdf⟩. Acesso em: 06 nov. 2022.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. [S.l.]: Atlas, 2005. ISBN 9788522440856.

BERTOLLI, E. **IDS vs. IPS: qual a diferença?** 2018. Disponível em: ⟨https://www.varonis.com/pt-br/blog/ids-vs-ips-qual-a-diferenca/⟩. Acesso em: 21 jan. 2023.

B.V., E. **O que é o ELK Stack?** 2022. Disponível em: ⟨https://www.elastic.co/pt/what-is/elk-stack⟩. Acesso em: 02 fev. 2022.

CETIC. **Acesso e uso das TIC nos domicílios e por indivíduos**. 2019. Disponível em: ⟨https://cetic.br/pt/pesquisa/domicilios/⟩. Acesso em: 10 dez. 2020.

CISCO. **O que é segurança de rede?** 2020. Disponível em: ⟨https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html⟩. Acesso em: 21 nov. 2022.

CLAISE, B.; SADASIVAN, G.; VALLURI, V.; DJERNAES, M. **Cisco Systems NetFlow Services Export Version 9**. 2004. Disponível em: ⟨https://www.ietf.org/rfc/rfc3954.txt⟩. Acesso em: 21 nov. 2022.

COLOSIMO, E. A. **Estatítica II - Correlação e Regressão Linear Simples**. 2019. Disponível em: ⟨http://www.est.ufmg.br/~enricoc/pdf/EstatisticaII/aula9-10_corr-reg.pdf⟩. Acesso em: 09 fev. 2023.

CORTEZ, M. **Aula 01 - Conceitos de redes de computadores**. 2022. Disponível em: ⟨https://docente.ifrn.edu.br/moisessouto/disciplinas/infraestrutura-de-redes-de-computadores/slides/slides/aula-01-conceitos-de-redes-de-computadores/view⟩. Acesso em: 02 fev. 2022.

DIORIO, R. F.; SERAFIM, E.; ALVES, K. R.; MEIRA, M. C. **Ataques de Força Bruta: Um Estudo Prático**. 2019. Disponível em: ⟨https://lcv.fee.unicamp.br/images/BTSym-19/Papers/040.pdf⟩. Acesso em: 02 fev. 2022.

DUARTE, O. C. M. B. **Simple Network Management Protocol (SNMP)**. 2011. Disponível em: ⟨https://www.gta.ufrj.br/grad/11_1/snmp/index.html⟩. Acesso em: 21 nov. 2022.

DUMAS, V. **A Origem da Internet**. 2011. Disponível em: ⟨http://revistahistorien.blogspot.com/2011/08/origem-da-internet.html⟩. Acesso em: 02 fev. 2022.

ENDORF, C.; SCHULTZ, G.; MELLANDER, J. **Intrusion Detection and Prevention**. [S.l.]: McGraw-Hill, 2004.

FALL, K. R.; STEVENS, W. R. **TCP/IP Illustrated, Volume 1: The Protocols**. [S.l.]: Addison-Wesley, 2012.

FARREL, A. **A internet e seus protocolos – Uma análise comparativa**. Editora Campos, 2005. Disponível em: ⟨https://vdoc.pub/documents/a-internet-e-seus-protocolos-uma-analise-comparativa-78u2ebcf8c90⟩. Acesso em: 23/12/2020.

FERNANDES, J. H. C. **Introdução à gestão de riscos de Segurança da Informação**. 2011. Disponível em: ⟨https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf⟩. Acesso em: 20 nov. 2022.

FILHO, J. G. P. **Redes de Computadores**. 2020. Disponível em: ⟨http://www.inf.ufes.br/~zegonc/material/Redes_de_Computadores/Classificacao%20de%20Redes.pdf⟩. Acesso em: 21 nov. 2022.

FISHER, S. **O que é um TCP/IP e como ele funciona?** 2019. Disponível em: ⟨https://www.avast.com/pt-br/c-what-is-tcp-ip⟩. Acesso em: 20 dez. 2020.

FONTES, E. L. G. **Segurança da Informação - o Usuário Faz a Diferença**. [S.l.]: Saraiva, 2006.

G., A. **Como funciona o SSH**. 2021. Disponível em: ⟨https://www.hostinger.com.br/tutoriais/como-funciona-o-ssh⟩. Acesso em: 20 jan. 2022.

GASPAR, L. **Protocolo SSH: o que é e como funciona**. 2021. Disponível em: ⟨https://www.hostgator.com.br/blog/o-que-e-protocolo-ssh/#h-o-que-protocolo-ssh⟩. Acesso em: 02 fev. 2022.

GOMES, W. **O que a análise de comportamento do usuário revela para a segurança**. 2020. Disponível em: ⟨https://olhardigital.com.br/2020/08/25/pro/o-que-a-analise-de-comportamento-do-usuario-revela-para-a-seguranca/⟩. Acesso em: 21 nov. 2022.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à Segurança de Computadores**. [S.l.]: Bookman, 2012.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. [S.l.]: Brasport, 2018.

IBM. **O que é segurança cibernética?** 2021. Disponível em: ⟨https://www.ibm.com/br-pt/topics/cybersecurity⟩. Acesso em: 05 nov. 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: uma abordagem top-down**. São Paulo, SP: Person Addison Wesley, 2006.

LABS, M. **McAfee Labs Threats Report**. 2018. Disponível em: ⟨https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf⟩. Acesso em: 02 fev. 2022.

LESKIW, A. **Aprenda instalar o ElastiFlow, uma poderosa ferramenta para análise de tráfego de rede no Debian 11 Bullseye**. 2022. Disponível em: ⟨https://www.networkmanagementsoftware.com/snmp-tutorial/⟩. Acesso em: 21 nov. 2022.

MAIA, I. da S. N.; REHEM, S. H. P. **Sistemas de prevenção de intrusão baseado em software livre: debian e snort**. 2005. Disponível em: ⟨https://pt.scribd.com/document/13224983/Sistema-de-Prevencao-de-Intrusao-com-Snort-Igor-Neiva-e-Sandro-Herman-UCB⟩. Acesso em: 06 nov. 2022.

MENEZES, E. da S.; SILVA, P. L. L. **Gerenciamento de Redes: Estudos de Protocolos**. 1998. Disponível em: ⟨https://www.cin.ufpe.br/~flash/ais98/gerrede/gerrede.html⟩. Acesso em: 04 fev. 2022.

MICROSOFT. **O que é um ataque cibernético?** 2022. Disponível em: ⟨https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-cyberattack⟩. Acesso em: 02 fev. 2022.

NAISBITT, J. **A nova fonte de poder não é o dinheiro... John Naisbitt**. 2020. Disponível em: ⟨https://www.pensador.com/frase/MTUy/⟩. Acesso em: 20 jan. 2022.

NETO, J. E. dos S.; ALMEIDA, A. M. G. de; LUCAS, T. J. **IMPLANTAÇÃO DA FERRAMENTA IDS/IPS FAIL2BAN COMBINADA COM FIREWALL NETFILTER/IPTABLES NA MITIGAÇÃO DE ATAQUES COMBINADOS**. 2014. Disponível em: ⟨https://www.fatecourinhos.edu.br/retec/index.php/retec/article/view/206⟩. Acesso em: 21 nov. 2022.

OLIVEIRA, I. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. 2022. Disponível em: ⟨https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/⟩. Acesso em: 02 jan. 2022.

OLIVEIRA, J. G. S.; GARCIA, R. **Comunicação de Computadores e a Evolução do Protocolo IP**. 2014. Disponível em: ⟨http://intertemas.unitoledo.br/revista/index.php/ETIC/article/view/4378/4137⟩. Acesso em: 14 dez. 2020.

PERES, N. **IPFW e SNORT: Experimento aplicado a ataques de força bruta em servidores SSH.** 2017. Disponível em: ⟨http://ric.cps.sp.gov.br/bitstream/123456789/765/1/20171S_VIRENathaliaPeres_OD0199.pdf⟩. Acesso em: 21 nov. 2022.

PINHEIRO, J. M. dos S. **Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar**. 2007. Disponível em: ⟨https://revistas.unifoa.edu.br/cadernos/article/download/885/790⟩. Acesso em: 07 nov. 2022.

RAULINO, F. **Gerência de Redes**. 2002. Disponível em: ⟨https://docente.ifrn.edu.br/filiperaulino/disciplinas/gerencia-e-seguranca-de-redes/aulas/Aula%2002_Arquitetura%20de%20gerenciamento.pdf⟩. Acesso em: 02 fev. 2022.

REHMAN, J. **Advantages and disadvantages of wide area network (WAN)**. 2023. Disponível em: ⟨https://www.itrelease.com/2018/07/advantages-and-disadvantages-of-wide-area-network-wan/⟩. Acesso em: 20 jan. 2023.

REMONTTI, R. **SNMP Basics: What is SNMP How Do I Use It?** 2017. Disponível em: ⟨https://blog.remontti.com.br/6255⟩. Acesso em: 21 nov. 2022.

RIOS, R. O. **Protocolos e Serviços de Redes**. 2012. Disponível em: ⟨http://proedu.rnp.br/bitstream/handle/123456789/709/Protocolos_e_Servi\%C3\%A7os_de_Redes_marcadecorte.pdf?sequence=3&isAllowed=y⟩. Acesso em: 02 fev. 2022.

RODRIGUES, G. A. P. **ANÁLISE DE TRÁFEGO MALICIOSO DIRECIONADO A UMA HONEYNET COM INSPEÇÃO PROFUNDA DE PACOTES**. 2017. Disponível em: ⟨https://bdm.unb.br/handle/10483/27805⟩. Acesso em: 21 nov. 2022.

RöHRS, R. **Elasticsearch (ELK)**. 2021. Disponível em: ⟨https://www.ufsm.br/pet/sistemas-de-informacao/2021/06/08/elasticsearch-elk/⟩. Acesso em: 21 nov. 2022.

SANTOS, V. **Sistemas de Detecção de Intrusões (IDS – Intrusion Detection Systems) usando unicamente softwares Open Source**. 2010. Disponível em: ⟨https://seginfo.com.br/2010/06/21/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-\softwares-open-source/⟩. Acesso em: 05 nov. 2022.

SCOTA, D. **O que é um TCP/IP e como ele funciona?** 2019. Disponível em: ⟨https://www.avast.com/pt-br/c-what-is-tcp-ip⟩. Acesso em: 20 dez. 2022.

SILVA, M. A.; RODRIGUES, F. B. **MONITORAMENTO DE REDES UTILIZANDO O FRAMEWORK OPENSOURCE OSSIM**. 2019. Disponível em: ⟨https://www.faculdadedelta.edu.br/revistas3/index.php/gt/article/view/28⟩. Acesso em: 20 jan. 2023.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de Computadores: Das LANs, MANs e WANs às Redes ATM**. [S.l.]: Campus, 1995.

SOBRINHO, A. B. **MODELO DE CYBER SITUATIONAL AWARENESS PARA SISTEMAS AUTÔNOMOS UTILIZANDO NETFLOW**. 2021. Disponível em: ⟨https://repositorio.unesp.br/bitstream/handle/11449/214674/sobrinho_ab_me_sjrp.pdf?sequence=5&isAllowed=y⟩. Acesso em: 21 nov. 2022.

SOUSA, L. S. de. **Gerenciamento de rede**. 2019. Disponível em: ⟨http://www.ic.uff.br/~lsousa/redes_ii/cap-9.pdf⟩. Acesso em: 20 dez. 2022.

SOUZA, A. C. **Redes de Computadores**. 2009. Disponível em: ⟨http://www.ifba.edu.br/professores/antoniocarlos/index_arquivos/redesdecomputadores.pdf⟩. Acesso em: 02 fev. 2022.

SURFSHARK. **Data breach statistics by country in 2021**. 2022. Disponível em: ⟨https://surfshark.com/blog/data-breach-statistics-by-country-in-2021⟩. Acesso em: 07 nov. 2022.

SêMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva**. [S.l.]: Campus, 2003.

TANENBAUM, A. S. **Redes de Computadores**. [S.l.]: Elsevier, 2003.

TELECOM, C. **O que é Internet**. 2022. Disponível em: ⟨https://www.copeltelecom.com/site/blog/o-que-e-internet/⟩. Acesso em: 03 fev. 2022.

TERENSE, A. C.; FREITAS, R. N. de. **Estudo sobre a Viabilidade de uso de Nat no IPV6**. Revista. Tec. Fatec AM, 2016. Disponível em: ⟨https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/63/73⟩. Acesso em: 23/12/2020.

UEYAMA, J. **Redes de Computadores**. 2012. Disponível em: ⟨http://wiki.icmc.usp.br/images/f/ff/Rc02-intro-info.pdf⟩. Acesso em: 21 nov. 2022.

APÊNDICE A – DADOS COLETADOS E *SCRIPT* DESENVOLVIDO

Segue abaixo o *link* do repositório do *Github* onde se encontram os arquivos *CSV* coletados pelo *ELK*, o código desenvolvido em *Python* e algumas análises realizadas no *jupyter notebook*:

- ⟨https://github.com/camila-alvesapa/TrabalhoConclusaoCurso⟩

ANEXO A – TUTORIAL DE INSTALAÇÃO DO ELK + PLUGIN ELASTIFLOW

Segue o link que disponibiliza o tutorial de instalação e configuração:

- ⟨https://github.com/robcowart/elastiflow/blob/master/INSTALL.md#requirements⟩

ANEXO B – INSTALAÇÃO DO PYTHON NO WINDOWS

Segue abaixo o link para *download* do *Python*:

- ⟨https://www.python.org/⟩

UFVJM