CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS TIMÓTEO

Gabriel de Oliveira Santana

USO DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE DE BAIXO CUSTO NA IMPLEMENTAÇÃO DE UMA POLÍTICA DE TRAGA SEU PRÓPRIO DISPOSITIVOS EM REDES ORGANIZACIONAIS DE PEQUENAS E MÉDIAS EMPRESAS

Timóteo

2021

Gabriel de Oliveira Santana

USO DE SOLUÇÃO DE "CONTROLE DE ACESSO À REDE" DE BAIXO CUSTO NA IMPLEMENTAÇÃO DE UMA POLÍTICA DE "TRAGA SEU PRÓPRIO DISPOSITIVO" EM REDES ORGANIZACIONAIS DE PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, campus Timóteo, como requisito parcial para obtenção do título de Engenheiro de Computação.

Trabalho aprovado. Timóteo, 16 de Setembro de 2021:

Prof. Me. Adilson Mendes Ricardo
Orientador

Prof. Dr. Luís Miguel Lopes de Oliveira
Coorientador

Prof. Me. Douglas Nunes de Oliveira
Professor Convidado

Prof. Me. Talles Quintão Pessoa
Professor Convidado

Timóteo
2021

Emitido em 15/09/2021

FOLHA DE ROSTO (PLATAFORMA BRASIL) Nº 1/2021 - DCCTM (11.63.05)
(Nº do Documento: 2)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 26/10/2021 13:38)
ADILSON MENDES RICARDO
PROFESSOR ENS BASICO TECN TECNOLOGICO
CECOMTM (11.51.22)
Matrícula: 2849338

(Assinado digitalmente em 26/10/2021 19:43)
DOUGLAS NUNES DE OLIVEIRA
PROFESSOR ENS BASICO TECN TECNOLOGICO
DCCTM (11.63.05)
Matrícula: 2921288

(Assinado digitalmente em 27/10/2021 09:39)
TALLES QUINTAO PESSOA
TEC EM TELECOMUNICACAO
SEGERTM (11.63.02.01)
Matrícula: 1552920

Para verificar a autenticidade deste documento entre em https://sig.cefetmg.br/documentos/ informando seu número: **2**, ano: **2021**, tipo: **FOLHA DE ROSTO (PLATAFORMA BRASIL)**, data de emissão: **26/10/2021** e o código de verificação: **529fb6f833**

Agradeço a minha família que sacrificou o que pôde para que eu pudesse chegar até aqui.

Agradecimentos

Agradeço pelas amizades que fiz do CEFET-MG, aos professores e funcionários que me ajudaram, ao professor Luís Miguel Oliveira do IPT de Portugal que forneceu os dispositivos necessários para realizar este trabalho, e ao Igor Miranda Oliveira que participou no capítulo de desenvolvimento desta monografia.

Resumo

A política de Traga Seu Próprio Dispositivo se baseia na ideia de que os próprios funcionários de uma empresa usem o dispositivo pessoal, ao em vez de um corporativo, no ambiente de trabalho, o que resulta em efeitos positivos como: redução de custos com *hardware* e *software* por cada funcionário, redução na equipe de suporte técnico e do uso de banda larga, e possivelmente até aumento de desempenho dos funcionários. Entretanto, para reduzir o risco de que esses dispositivos acessem a rede interna infectados por *malware*, o uso de uma solução de Controle de Acesso à Rede, que pode custar milhares ou dezenas de milhares de dólares por ano. Com o intuito de ter uma solução financeiramente mais acessível ás pequenas e médias empresas, foi estudado o uso da solução de código aberto Packetfence, com a integração de ferramentas auxiliares gratuitas (exceto o Active Directory do Windows), que em conjunto identificam e isolam os dispositivos considerados como ameaça à rede, que são os que utilizam aplicações *peer-to-peer*, que realiza *scan* não autorizado na rede, que dissemina *malware* ao estar infectado e especificamente aqueles com sistema operacional Linux e Windows, que não possui antivírus instalado. Para esse último caso foi necessário alterações no código fonte do Packetfence e da ferramenta de *scan* Greenbone Vulnerability Manager e criação de *scripts*. Por fim, foram realizados testes que permitiram fazer acesso à rede como visitante ou membros da rede, detectar e isolar por cada uma das ameaças citadas anteriormente, sendo o usuário apresentado a uma página WEB apresentando qual ameaça e o que fazer para ter acesso à rede (ato de remediação) com a possibilidade de remediação pelo administrador ou pelo próprio usuário, dependendo da ameaça, e durante esses teste, mostrar algumas das funções de visibilidade de rede que o próprio Packetfence oferece.

Palavras-chave: Controle de Acesso à Rede, Traga seu próprio dispositivo, Packetfence, Greenbone Vulnerability Manager, solução de baixo custo.

Abstract

The Bring Your Own Device policy is based on the idea that a company's own employees use the personal device, rather than a corporate one, in the workplace, which results in positive effects such as: reduced hardware and costs. software for every employee, reduced tech support staff and bandwidth usage, and possibly even increased employee performance. However, to reduce the risk of these malware-infected devices accessing the internal network, the use of a Network Access Control solution, which can cost thousands or tens of thousands of dollars per year. In order to have a more affordable solution for small and medium companies, the use of the open source solution Packetfence was studied, with the integration of free auxiliary tools (except Windows Active Directory), which together identify and isolate the devices considered as a threat to the network, which are those that use peer-to-peer applications, which perform unauthorized scans on the network, which spreads malware when infected, and specifically those with Linux and Windows operating systems, which do not have antivirus installed. For the latter case, changes were needed to the Packetfence source code and the Greenbone Vulnerability Manager scanning tool and scripting. Finally, tests were performed that allowed access to the network as a visitor or members of the network, detecting and isolating for each of the aforementioned threats, with the user being presented with a WEB page showing which threat and what to do to access the network (act of remediation) with the possibility of remediation by the administrator or by the user, depending on the threat, and during these tests, show some of the network visibility functions that Packetfence itself offers.

Keywords: Network Access Control, Bring Your Own Device, Packetfence, Greenbone Vulnerability Manager, low cost solution.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

AAA	Authentication, Authorization and Accounting
AD	Active Directory
AP	Access Point
BYOD	Bring Your Own Device
CoA	Change of Authorization
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GSA	Greenbone Security Assistant
GVM	Greenbone Vulnerability Management
HIDS	Host Intrusion Detection Systems
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
LAN	Local area network
MIB	Management Information Base
NAC	Network Access Control
NAS	Network Access Server
NIDS	Network Intrusion Detection Systems
NVT	Network Vulnerability Test
OMP	OpenVAS Management Protocol
P2P	Peer-to-Peer
PoE	Power over Ethernet
PME	Pequena e Média Empresa
PSI	Política de Segurança da Informação

RADIUS	Remote Authentication Dial In User Service
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SO	Sistema Operacional
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol Protocol
VLAN	Virtual local area network
WLAN	Wireless local area network

Sumário

1 Introdução

Para uma empresa que necessita de uma rede corporativa para seu funcionamento, a velocidade e segurança dos dados são cruciais para prover um serviço de qualidade aos seus usuários. Para isso é necessário se preocupar com acesso de pessoas não autorizadas, disseminação de *malwares* e ataques à rede interna, tanto de funcionários de dentro da corporação, seja ou não intencionalmente, quanto de ameaças externas (INFOWATCH, 2018).

Uma solução para mitigar os problemas citados anteriormente é fornecer dispositivos da empresa para os funcionários, sendo aqueles pré configurados com certificado digital, programas necessários para utilização do aparelho para trabalho e ferramentas de segurança, como agentes e anti *malware*. Isso exige que a empresa disponha de tempo e dinheiro para distribuir, configurar e atualizar os aparelhos (o que também exige mais pessoas na equipe tecnologia da informação (TI) para executar tais tarefas), além de ter de treinar os funcionários que utilizarão os aparelhos (FARIA et al., 2013).

Diante disso, políticas de "Traga seu Próprio Dispositivo", conhecida como *Bring Your Own Device* (BYOD), tem sido implementadas em empresas de diversos tamanhos, uma vez que seus funcionários usam seus próprios aparelhos, com os quais já estão familiarizados. Porém existe o risco de os dispositivos estarem infectados com a algum *malware* ou utilizando aplicativos não permitidos dentro da empresa (CHANG J. MORRIS, 2014), além disso, como diferenciar um dispositivo autorizado de um não autorizado? Para resolver isso é necessário um Controle de Acesso à Rede, conhecida como *Network Access Control* (NAC).

Uma solução NAC autentica os dispositivos que se conectam à rede e avaliam se eles estão de acordo com as políticas de segurança da empresa como: antivírus instalado, aplicação de *torrent* desativada, sistema operacional atualizado. Caso esteja, poderá entrar na rede, caso contrário, ficará numa zona de quarentena com o mínimo de acesso possível que será usado apenas para que o usuário possa fazer alterações para poder entrar em conformidade com os parâmetros de segurança da rede interna.

Entre as soluções NAC disponíveis há o Packetfence, uma opção Open Source e gratuita que oferece acesso tanto para funcionários quanto para visitantes de uma rede, além de oferece suporte a *switchs* e *access points* (APs), integração com softwares de segurança e autenticação de diversas empresas além de uma robusta documentação e uma comunidade ativa para discutir soluções de problemas na configuração da ferramenta (PACKETFENCE. . . , 2021).

1.1 Problema

Para consolidar uma política de BYOD, existem soluções de NAC no mercado como o da InfoExpress ou ForeScout para auxiliar nesse processo, entretanto cada uma delas tenta se diferenciar das outras, com focos diferentes, o que pode criar confusão sobre o que é um NAC (GEER, 2010). Outra questão é que a maioria dessas ferramentas são pagas, de alto custo, com compatibilidade restrita a dispositivos de redes do mesmo fabricante, como o da Cisco, ou com ferramentas de seguranças também pagas, como o da Extreme Networks (ROBB, 2021). Sendo assim, cabe a iniciativa de definir sucintamente o conceito de *Network Access Control* e investigar meios financeiramente acessíveis de implementa-lo para que possa ser utilizado o BYOD nas pequenas e médias empresas (PME), definidas pelo Instituto Brasileiro de Geografia e Estatística (IBGE) aquelas que, respectivamente, possuem até 49 funcionários e as que possuem entre 50 a 99 funcionários no setor comercial (fora do setor industrial) (AGUIAR, 2021).

1.2 Objetivo

O objetivo desse trabalho é avaliar uma solução NAC gratuita para implementar uma política de Traga seu Próprio Dispositivo (BYOD) em PMEs com pouco recurso financeiro e técnico para o uso dessa solução, levando em conta os seguintes fatores: facilidade de configuração, compatibilidade com dispositivos de rede de fabricantes diferentes, integração de softwares com o menor custo financeiro possível, preferencialmente todos sendo gratuitos.

Segue abaixo a lista de objetivos específicos deste trabalho:

- Esclarecer o conceito de NAC;
- Projetar, montar e configurar um ambiente para simulação com o uso de uma soluçao NAC gratuita;
- Responder se a documentação possui detalhes suficientes para implementação da solução por técnicos com pouco ou nenhuma experiência em NACs;
- Responder se o fórum de perguntas é ativo e se é possível encontrar respostas a problemas que podem ser encontrados durante a implementação NAC;

1.3 Justificativa

Somente entre 2012 e 2014 no Brasil a política de Traga seu Próprio Dispositivo (BYOD) cresceu 84% e se mostra como uma tendência nas empresas, o que indica que tal atitude trouxe

alguns benefícios (BRADLEY et al., 2012).

Os motivos para esse crescimento são o aumento da produtividade dos funcionários e corte com gastos em suporte e compra de equipamentos. Um estudo da Cisco mostra que, no Brasil por exemplo, 41% dos funcionário afirmam terem economizado no mínimo 2 horas ou mais de tempo de trabalho por usar seus próprios dispositivos com os quais já estão familiarizados (FARIA et al., 2013). O mesmo estudo também mostra que no Brasil as empresas que adotaram o BYOD economizam cerca de $110,00 por funcionário a cada ano.

Se mesmo assim ainda houver desconfiança de se realmente a sua organização se beneficiará com essa política e não quiser arriscar algum dinheiro para obter uma solução NAC do mercado, ainda seria viável testar uma gratuita, preferencialmente em um ambiente simulado, já que se houver algum prejuízo financeiro na implementação, ele seria ainda menor. Caso tudo isso funcione e a rede cresça em larga escala, essas ferramentas geralmente oferecem suporte técnico especializado, mas pago para suprir essa necessidade (INVERSE, 2021a).

2 Revisão da literatura

Este capítulo contém uma revisão dos conceitos de arquitetura de rede de computadores (seção 2.1), rede local (seção 2.2 e seção 2.3), dispositivos de rede (seção 2.4), padrões de tecnologia (seção 2.5) e protocolos (seção 2.6) e políticas de segurança da informação (seção 2.7), que são parte da base de rede de computadores e segurança de dados e esses conceitos serão usados com recorrência neste trabalho.

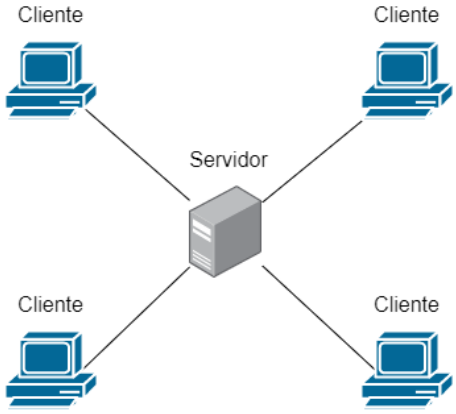
2.1 Arquitetura de rede de computadores

Existem dois tipos de arquitetura de rede de computadores, cada uma com suas características e estrutura diferentes: Cliente e servidor (Figura 1); e ponto a ponto (Figura 2), ou conhecido por *peer-to-peer* (p2p), onde as linhas representam a conexão entre os dispositivos numa rede (ELIAS; LOBATO, 2013).

Cliente e Servidor

Essa arquitetura se baseia em pelo menos um *host* que oferece um ou mais serviços, o servidor, e os *hosts* que requisitam tais serviços , os clientes. Todo dado pacote para chegar de um cliente ao outro, obrigatoriamente passa pelo servidor, ou seja, é uma arquitetura centralizada e fácil de ser gerenciada.

Figura 1 – Arquitetura Cliente/Servidor

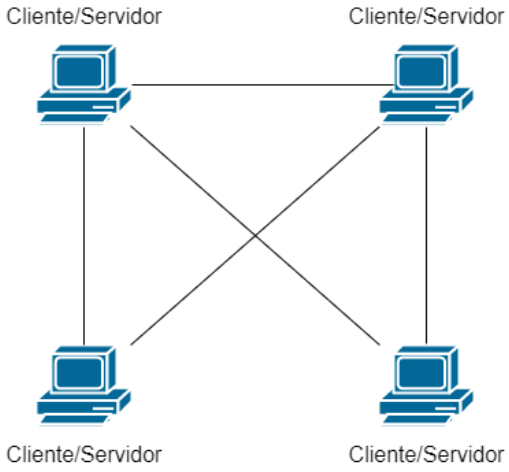


Fonte: Autoria própria

Ponto a Ponto

Na arquitetura Ponto a Ponto, ou *peer-to-peer* (p2p), todo *host* na rede desempenha o papel de cliente e de servidor sem necessariamente ter um intermediador, como no cliente-servidor, isso significa uma descentralidade da rede, o que dificulta seu gerenciamento.

Figura 2 – Arquitetura ponto-a-ponto



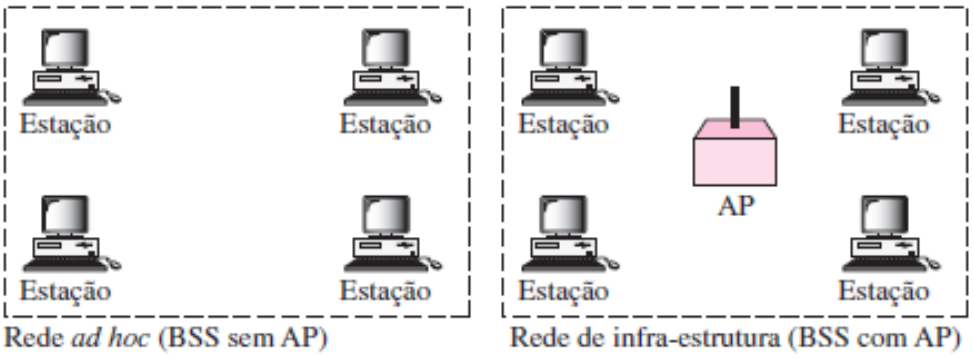
Fonte: Autoria própria

2.2 Rede Local

Uma rede local (LAN) é o conjuntos de *nodes* (ou nós) interligados através de cabos de rede dentro de uma corporação. Uma LAN pode ser tanto uma estrutura simples de um computador e uma impressora, quanto uma estrutra complexa de uma organização com multiplos computadores, dispositivos de rede, servidores e telefones, ou seja, qualquer dispositivo capaz de se conectar à rede, conjunto de aparelhos esses chamados de *host* (TANENBAUM, 2003).

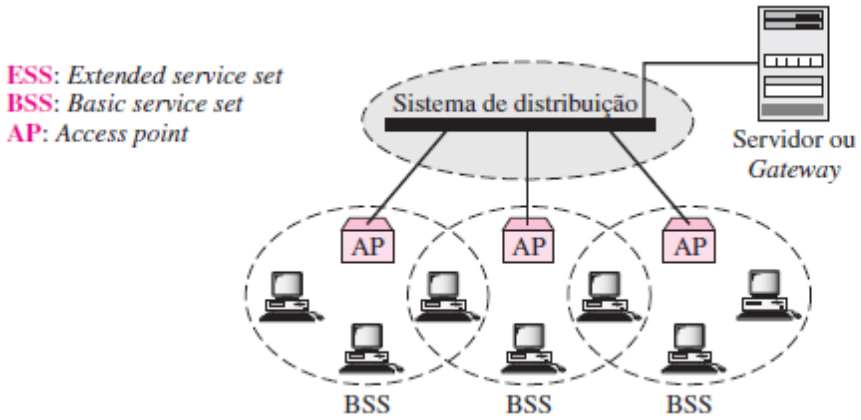
Redes LAN sem fio são denominadas de WLAN e seguem os padrões IEEE 802.11, que define os termos *Basic Service Set* (BSS) na Figura 3 e o *Extended Service Set* (ESS) na Figura 4. A base de uma WLAN é a BSS, um conjunto de *hosts wireless* que se comunicam ou entre si ou através de um ponto de acesso, chamado também de *access point* (AP), essas duas arquiteturas são chamadas respectivamente de ad hoc e infra-estrutura. Uma Extended Service Set (ESS) é a interligação entre multiplas BSS com APs e a LAN (FOROUZAN; A., 2008a).

Figura 3 – Exemplo de BSS



Fonte: (FOROUZAN; A., 2008a)

Figura 4 – Exemplo de ESS



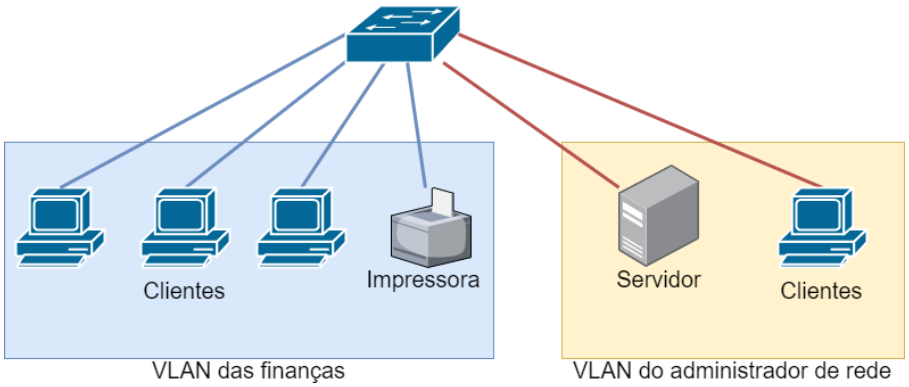
Fonte: (FOROUZAN; A., 2008a)

2.3 LAN virtual

A LAN virtual, ou *virtual LAN* (VLAN), é um artifício para dividir uma LAN física em grupos denominados de LANs lógicas, tudo a partir de *software*. Essa segmentação é comum quando uma rede local possui serviços que não devem ser acessados por todos os usuários conectados a LAN (ROTONDARO; GUEDES, 2016), como mostra o exemplo da Figura 5, um funcionário do departamento das finanças não deve ter acesso para configurar servidores, uma atribuição dos administradores da rede.

O uso de VLANs oferece flexibilidade à rede uma vez que se for necessário mover um computador de um grupo para o outro, basta configurar a rede para que aquele *host* pertença a nova

Figura 5 – Divisão de uma rede local em VLANs



Fonte: Autoria própria

VLAN, sem alterar a sua localidade física.

2.4 Dispositivos de rede

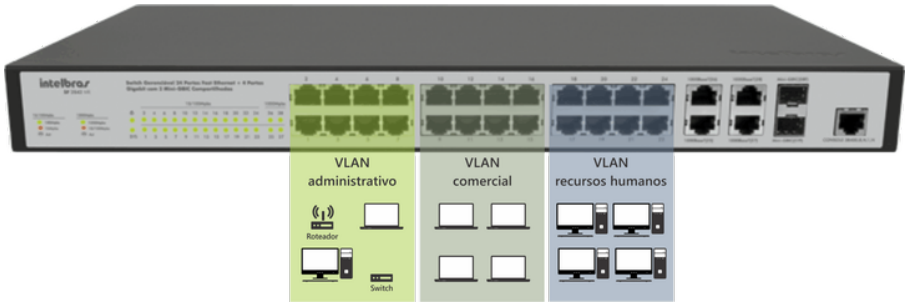
Dispositivos de redes são *hardware* usados para construir a estrutura das redes de computadores. Nesta secção será abordado sobre o que é e como funciona um: *switch*, *access point* e um roteador.

Switch

O *switch* é um dispositivo de rede que permite encaminhar pacotes de dados entre *hosts* que estão na mesma LAN através de uma tabela de comutação e, quando é gerenciável, é possível criar VLANs para segmentar logicamente uma rede local. Para isso é definido quais portas estão associadas a quais VLANs, como pode ser visualizado na Figura 6. Quando um *switch* possui multiplas VLANs passando por uma mesma porta, essa recebe a denominação de *trunk* (DIAS, 2012).

Os *switchs* tradicionais funcionam até a camada 2 do modelo OSI, uma estrutura dividida em 7 camadas (*layers*) que padroniza e possibilita a comunicação nas redes de computadores, sendo a 2º camada chamada de enlace (FOROUZAN; A., 2008b). Os dispositivos dessa camada utilizam uma tabela de comutação que associa a porta do *switch* ao endereço físico da placa de rede do *host* ali conectado, para o envio de pacotes. Vale destacar que não é possível pacotes de uma LAN para outra sem o auxílio de um roteador, mas existem aqueles que conseguem, os *layer 3*.

Figura 6 – Visão lógicas das portas do *switch*

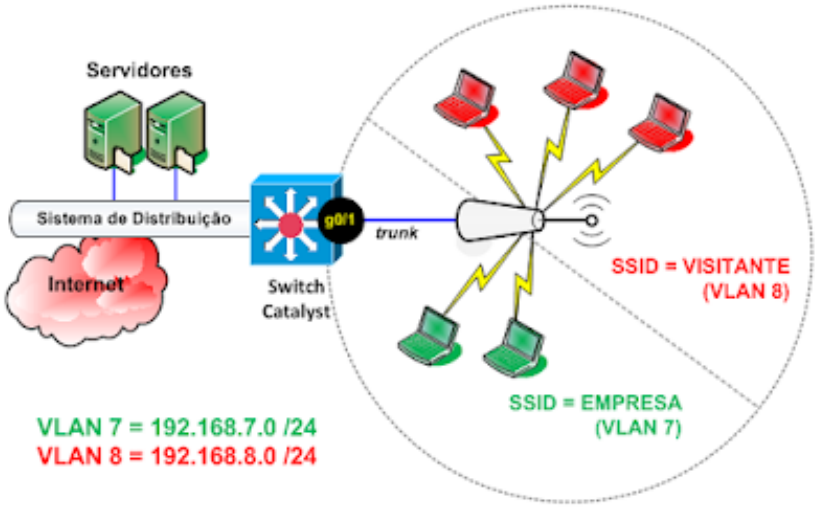


Fonte: (MICHAEL, 2017)

Access Point

Um Access Point é um hardware que intermedia a comunicação entre *hosts* de uma WLAN ou com os da LAN. Assim como o *switch*, é possível segmentar uma WLAN, mas a partir de um *service set identifier* (SSID) que é o nome que identifica cada BSS, sendo essa associada a uma VLAN (FOROUZAN; A., 2008a). Essa associação de VLAN com SSID pode ser entendida pela Figura 7.

Figura 7 – Exemplo de APs com multiplas SSID em VLANs diferentes



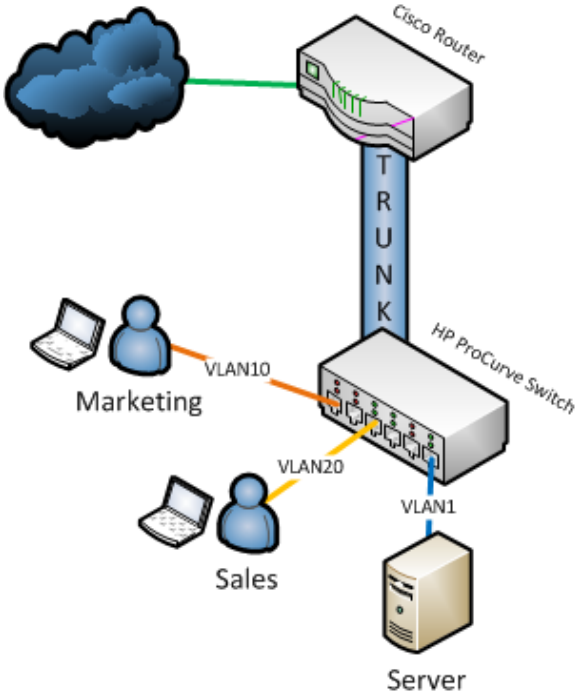
Fonte: (HENRIQUE; BRITO, 2016)

Roteador

O roteador é o que faz a comunicação entre LANs e com a *internet* ou um link dedicado (MICHEL, 2013), usando rotas e lista de controle de acesso, que define um conjunto de regras as

quais decidem onde pacotes podem ou não serem enviados, essa lista é comumente chamada de Access Control List (ACL) e assim como nos *switchs*, é possível a mesma porta transportar múltiplas VLANs, como mostra a Figura 8. Em geral, o roteador também consegue desenvolver outras funções como servidor DHCP.

Figura 8 – Exemplo de roteador usando trunk



Fonte: (MICHAEL, 2012)

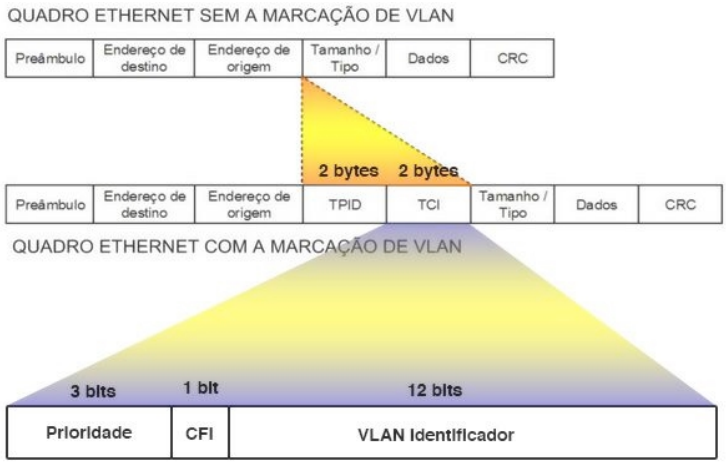
2.5 Padrões IEEE 802

IEEE 802 é um conjunto de padrões de rede para tecnologias como LAN e WLAN. Esses padrões incluem práticas recomendadas a serem utilizadas em tais tecnologias e uma vez seguidas, possibilita que diferentes dispositivos de rede funcionem corretamente (GILLIS, 2020).

2.5.1 802.1Q - Etiquetas

O padrão IEEE 802.1q permite a inserção de um identificador dos quadros Ethernet de uma etiqueta, ou *tag*, que indica a qual VLAN ela pertence (ROTONDARO; GUEDES, 2016). Esse procedimento de inserir dados auxiliares a um quadro se denomina encapsulamento e pode ser observado na Figura 9 (FOROUZAN; A., 2008c).

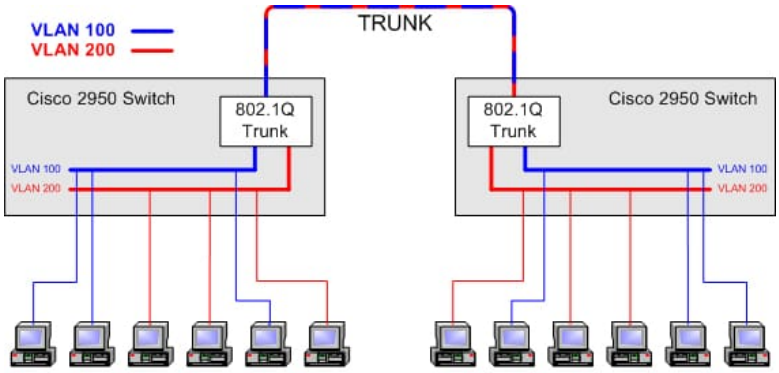
Figura 9 – Encapsulamento da *tag* VLAN



Fonte: (ROTONDARO; GUEDES, 2016)

Essa etiqueta é importante para que todos os dispositivos de rede que suportam esse padrão possam saber para qual VLAN deve-se encaminhar um determinado quadro, independente do fabricante do *switch* ou do roteador. No Exemplo da Figura 10, é possível visualizar essa comunicação entre dois *switch*.

Figura 10 – Comunicação entre dois *switchs*



Fonte: (VIDENCENTER'S, 20–)

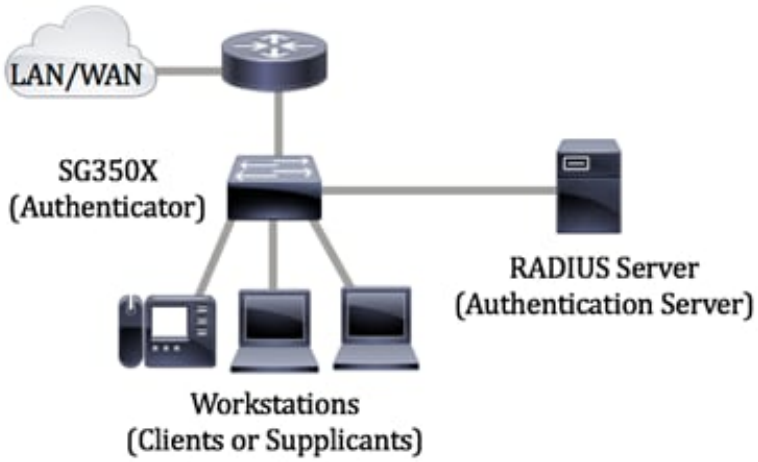
Uma VLAN não está necessariamente associada a uma etiqueta, isso deve ser configurado explicitamente quando necessário. Ao configurar quais VLANs pertencem a uma porta do *switch*, deve-se indicar se usa etiqueta (modo *tagged*) ou não (modo *untagged*), sendo possível apenas uma VLAN como *untagged* na mesma porta. Em geral, os dispositivos terminais não utilizam 802.1Q, portanto esses só identificam pacotes vinda da VLAN *untagged*.

2.5.2 802.1X

Esse padrão permite o fazer um controle de acesso á rede na porta do *switch*, esse tipo de controle é chamado de *port-based network access control* (PNAC). Uma vez conectado a uma porta configurada com 802.1X, o *host* está impossibilitado de iniciar uma comunicação até que esteja autenticado, enquanto isso não ocorre, a porta bloqueará qualquer pacote que não seja para a autenticação, sendo assim o inicio da autenticação parte do um dispositivo autenticador, como um *switch* ou AP, que procura novos *hosts* conectados à rede (PIEROBON, 2020).

Uma vez identificado um *host* não autenticado, ou seja, desconhecido, o dispositivo autenticador intermedia a comunicação com o servidor autenticador, sendo esse o que autentica, ou seja, verifica se quem solicita o acesso está realmente habilitado a isso. Resumindo, existem 3 *hosts* numa rede que utiliza o IEEE 802.1X e que estão ilustrado na Figura 11, o Cliente ou *suplicant*, que deseja acessar a rede, o servidor de autenticação, que autentica o usuário e o autenticador ou ou *Network Access Server* (NAS), que intermedia a comunicação entre os dois anteriores (CISCO, 2019a).

Figura 11 – Estrutura de uma rede com 802.1X



Fonte: (CISCO, 2019b)

É importante destacar que esse padrão não é responsável pela autenticação, ele apenas impede o acesso daqueles ainda não autenticados. Para isso é necessário de outras tecnologias como *Extensible Autentication Protocol* (EAP) e *Remote Authentication Dial-In User Service* (RADIUS) que foi detalhado respectivamente nas seções 2.6.1 e 2.6.2.

2.6 Protocolos

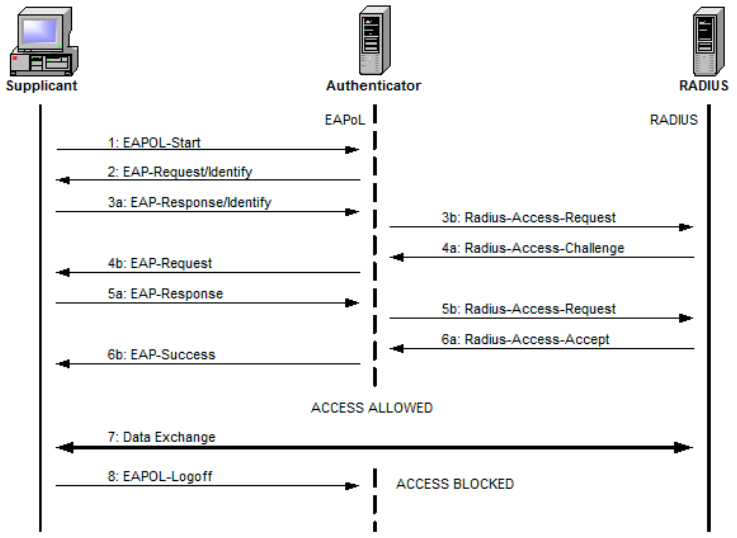
Forouzan sintetiza a definição de protocolo como "[...] um conjunto de regras que controlam as comunicações de dados"(FOROUZAN; A., 2008d). Uma vez que os *hosts* sigam tais regras, eles serão capazes de entender a informação que um transmite ao outro, como um idioma. Como este trabalho necessita fazer essa comunicação para ser finalizado, é de nosso interesse explicar os protocolos que foram utilizados.

2.6.1 *Extensible Autentication Protocol*

Extensible Autentication Protocol (EAP) é uma estrutura (em inglês *framework*) utilizado para implementar diferentes métodos de autenticação entre o cliente e o servidor de autenticação sem que o NAS precise suportar tal método e apenas repasse as mensagens entre os dois *hosts* (ABOBA et al., 2003).

O EAP utiliza basicamente 4 tipos de mensagens para se comunicar: EAP-Request para requisitar dados do cliente para o autenticador; EAP-Response para responder à requisição do NAS; EAP-Success e EAP-Failure para indicar que a autenticação foi, respectivamente, bem ou mal sucedida. Além disso, dentro de uma rede com 802.1X, se utiliza *Extensible Autentication Protocol over LAN* para iniciar a autenticação (EAPoL start) ou desautenticação (EAPoL logoff) em uma porta. Na Figura 12 podemos observar um exemplo das mensagens utilizadas pelo EAP

Figura 12 – Comunicação EAP



Fonte: (TECHNOLOGIES, 2021)

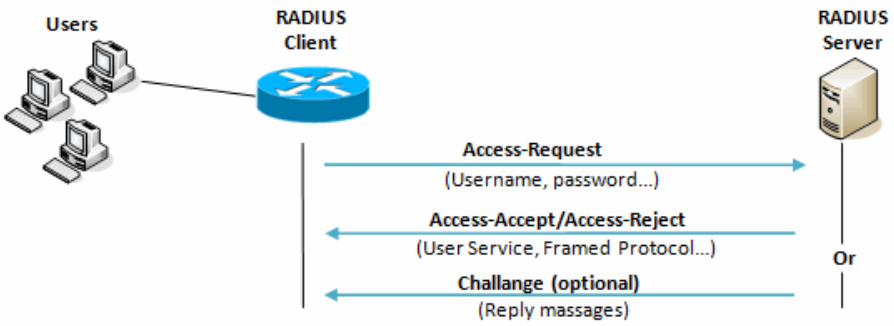
2.6.2 *Remote Authentication Dial In User Service*

O *Remote Authentication Dial In User Service* (RADIUS) faz parte do grupo de protocolos AAA, os quais oferecem 3 serviços que dá origem à sigla: autenticação, que verifica a identidade de quem deseja acessar a rede, autorização, que permite quais serviços pode acessar, e *accounting*, que contabiliza o tempo de acesso dos usuários autenticados, sendo esse ultimo opcional e não será abordado nesta monografia (SECURITY, 2019).

A autenticação e autorização do protocolo RADIUS funciona através de troca de mensagens, como pode ser visto na Figura 13, e funciona da seguinte maneira:

1. O NAS envia uma mensagem EAP com o pedido de acesso, ou *Access-Request*, com as credenciais do usuário caso, como email e senha, ou outra informação importante solicitada;
2. Se for necessário mais alguma informação para permitir a autenticação, como uma chave secreta, ela será pedida pelo servidor ao NAS com uma mensagem EAP de *Access-Challenge* e volta ao item 1;
3. Se todos os dados enviados foram suficientes e as credenciais pertencem a alguém com permissão para acessar a rede, será enviado uma mensagem de acesso aceito juntamente com o nível de autorização, ou *Access-Accept*. Caso contrário será enviado uma mensagem EAP de acesso rejeitado, ou *Access-Reject*, e a comunicação se encerra.

Figura 13 – Troca de mensagens no RADIUS



Fonte: (SECURITY, 2019)

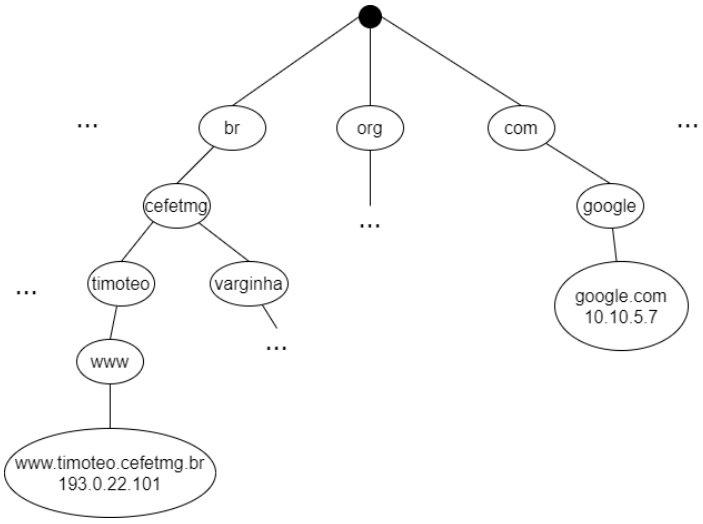
2.6.3 *Domain Name System*

A comunicação entre *hosts* se dá pelo conhecimento do seu endereço IP (*Internet Protocol*), entretanto é difícil para o ser humano lembrar de uma sequência de números para identificar algo,

pois estamos acostumados a fazer isso através de nomes. Sendo assim, *Domain Name System* (DNS) é um serviço que armazena IPs e os associa a um nome através de um estrutra de dados hierárquica chamada árvore, o que facilita no momento de gravar na mente a identificação de um *host* para uma pessoa. Resumidamente, ele traduz um nome para um endereço IP ou vise-versa (REMOALDO, 1998).

Quando um usuário da *internet*, por exemplo, acessa um site, ele está fazendo uma comunicação entre seu aparelho com o servidor que disponibiliza o site para ser visualizado. Pensando nesse caso, fica mais fácil saber acessar o site da Google através do nome google.com, ao em vez de um IP como 10.10.5.7. Esse exemplo pode ser visualizado na Figura 14

Figura 14 – Exemplo fictício de uma árvore DNS



Fonte: Autoria própria

2.6.4 *Dynamic Host Configuration Protocol*

O *Dynamic Host Configuration Protocol* (DHCP) é um protocolo que oferece, principalmente, um endereço de IP a um *host* quando solicitado e atribuído automaticamente, sendo tal endereço necessário para que seja possível a comunicação dentro da rede. Além disso é possível oferecer o servidor DNS e o *default gateway*, o endereço ao qual deve ser encaminhado um pacote, quando o *host* que o detém não sabe onde se encontra o destinatário (PINTO, 2014).

A configuração desse servidor consiste em definir um conjunto de IPs a serem distribuídos aos *hosts*, podendo ser um endereço determinado pelo próprio DHCP ou um endereço fixo para um *host* específico determinado pelo administrador. Em servidores DHCP como os da Microsoft, por exemplo, é possível criar um conjunto de IPs que nunca devem ser oferecidos automáticos ou endereço fixo (o *host* pode ter ip).

No exemplo da Figura 15 podemos observar a criação de uma *pool* que oferece IPs para a LAN 192.168.10.0/24. O intervalo de endereços está entre 192.168.10.50 e 192.168.10.150, o IP do servidor DNS 192.168.10.25 é o *default gateway* que é 192.168.10.1. Além disso existe um IP estático 192.168.10.20 a ser definido para o *host* que possui uma interface de rede com o MAC 08:00:27:58:c7:3d, neste caso, um servidor WEB.

Figura 15 – Exemplo de configuração DHCP em CentOS 6

```
subnet 192.168.10.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.10.255;
    option routers 192.168.10.1;
    option domain-name-servers 192.168.10.25;
    range 192.168.10.50 192.168.10.150;
}

host WEBserver {
    hardware ethernet 08:00:27:58:c7:3d;
    fixed-address 192.168.10.20;
}
```

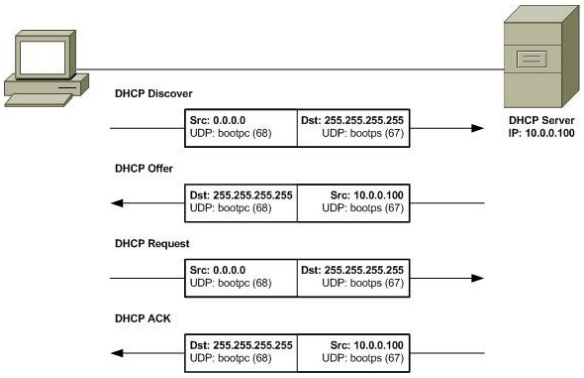
Fonte: Autoria própria

A troca de mensagens nesse protocolo ocorre na seguinte sequência: uma vez que o *host* define que deseja utilizar tal protocolo, ele envia uma mensagem de *DHCP Discovery* para procurar e solicitar um IP a um servidor DHCP através de um *broadcast*; ao chegar a um servidor DHCP, ele responde uma mensagem de *DHCP Offer* com a sugestão de um endereço; o cliente responde com um *DHCP Request* para avisar que irá usar aquele IP e pede reserva-lo, novamente por *broadcast*, para que assim nenhum outro *host* na rede tenha o mesmo endereço; por fim o servidor responde com *DHCP Acknowledgement*, avisando ao cliente que o pedido foi cumprido. Toda a sequência pode ser vista na Figura 16.

2.6.5 Syslog

Sendo que um pacote Ethernet possui tamanho máximo de 1.518 bytes, ou 12.144 bits, e a velocidade mínima dos dispositivos que usam o padrão Ethernet é 10 Mbps (megabits por segundo), ou seja 10.485.760 bits por segundo, podemos calcular que nesse caso a rede pode transmitir numa velocidade mínima de 863 pacotes por segundo, aproximadamente. Esse é o cenário de uma rede com pouco fluxo, visto que pacotes Ethernet podem ter tamanho mínimo de 56 bytes e existem padrões 10 Gbits (gigabits por segundo) por segundo (KROHN; CUNHA.,). Sendo assim é impossível gerenciar uma rede olhando seu fluxo manualmente, portanto isso pode ser somente feito automaticamente.

Figura 16 – Troca de mensagens DHCP



Fonte: (PINTO, 2014)

O Syslog é um protocolo que permite a analisar pacotes e gerar relatórios, ou *log*, que indica a categoria e o nível de severidade, para que seja possível a administração de uma LAN. Esse protocolo é importante meio de comunicação entre servidores e o gerenciador da rede, pois ele avisa quando um acontecido, ou comumente chamado de evento, relevante surge.

Para isso, é estabelecido uma série de regras que definem quais tipos de eventos deseja ser avisado, chamado de *facility*, a partir de qual nível de severidade, chamado de *Severity level*, e para onde deve ser enviado o *log* (LONVICK, 2001).

2.6.6 *Simple Network Management Protocol*

Para possibilitar o gerenciamento de uma rede, é necessário que o servidor responsável por tal tarefa, denominado de gerente, consiga se comunicar com os *hosts*, denominado de agente, obtendo informações necessárias que forneça uma visibilidade do estado em que LAN se encontra para que então, com base nisso, o administrador da rede tomar providências quando necessário. Essa comunicação é possível através do *Simple Network Management Protocol* (SNMP) (MANAGEENGINE, 2021).

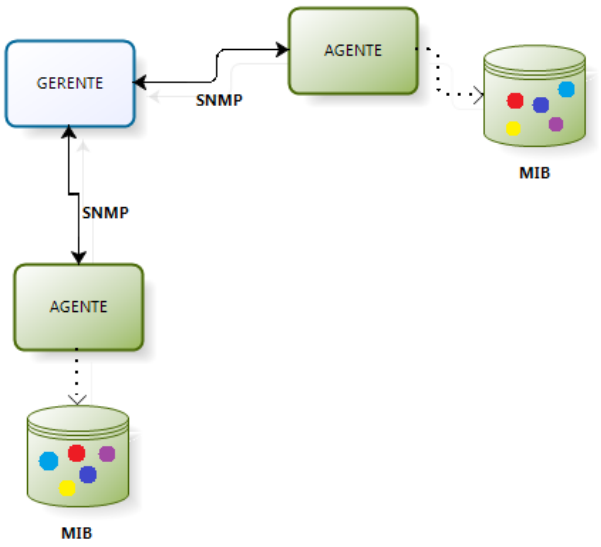
O protocolo com mensagens padronizadas de três tipos resumidamente:

- Get: O gerente requisita um dado ao agente;
- Set: O gerente fornece um dado ao agente para que seja armazenado;
- Trap: O agente avisa ao gerente a ocorrência um evento.

Porém o SNMP necessita de outros dois protocolos auxiliares, o *management information base* (MIB), uma base de dados estruturada hierarquicamente por uma árvore de dados responsável por armazenar as informações, nomeado de objetos, do agente que o implementa, e o *Structure*

of Management Information (SMI), que "[...] define as regras de atribuição de nomes a objetos, estabelece tipos de objeto (inclusive sua abrangência e comprimento) e mostra como codificar objetos e valores"(FOROUZAN; A., 2008e). A relação entre gerente, agente, SNMP e MIB está ilustrada na Figura 17.

Figura 17 – Estrutura de gerenciamento de rede



Fonte: (MANAGER, 2021)

2.7 Políticas de segurança da informação

Uma política de segurança da informação (PSI) é a documentação regras necessárias para cumprir os requisitos da empresa, os princípios da segurança da informação e a lei e que deve ser seguida pelos usuários e administradores da rede, portanto ela deve ser de conhecimento de todos na organização. O não cumprimento dessas regras pode aumentar os risco a segurança da informação, reduzir a qualidade do serviço prestado e até a multas por violação da legislação local, por isso a PSI deve estabelecer punições para qualquer comportamento que vá contra essas regras. Vale destacar que uma PSI não é o sistema de segurança propriamente dito, mas sim uma diretriz de como configurar e auditar sistemas computacionais e redes (COMPUGRAF, 2013).

Existem normas internacionais voltadas para a segurança da informação, como a ISO 27001, que explicita as 11 seções (sendo as quatro primeiras opcionais) e os Controles do anexo A (quando aplicável na Declaração de Aplicabilidade) necessárias para cumprir os requisitos desse padrão e receber um certificado que atesta que essa empresa segue os princípios dessa ISO (LEAL, 2021). Sendo assim, seria interessante ao menos lê-la para usa-la como base na elaboração de uma PSI

dentro da empresa, uma vez que ela é faz parte da referência em segurança da informação no mundo.

2.7.1 Políticas de segurança comuns

Cada organização define sua própria política, pois cada uma delas têm seus próprios requisitos e estão sob leis de diferentes regiões do mundo (COMPUGRAF, 2013). Entretanto existem algumas políticas convergem em alguns pontos mesmo em diferentes empresas e que devem ser levados em contas por todos que desejam implementar sua própria PSI. A seguir temos alguns exemplos de políticas comuns aplicadas em LANs empresariais.

Exigência de antivírus atualizado

O antivírus é um *software* que detecta e previne a infecção de dispositivos por *malwares*, que são programas maliciosos instalados para trazer algum prejuízo ao usuário (KASPERSKY, 2021). Por isso é importante que os usuários da rede tenham essa ferramenta instalada e também atualizada pois os antivírus descobrem novas atividades maliciosas e como se previnir delas. O relátorio da Kaspersky (KASPERSKY, 2018) detectou que em 2018, 30% dos seus usuários no Brasil enfrentaram algum grande risco de serem infectados por programas maliciosos online, o que indica um alto número de ataques no país e consequentemente, uma necessidade de se investir na segurança dos computadores.

Detecção e prevenção de escaneamento de rede

Existem ferramentas de fácil instalação capazes de descobrir e auditar a segurança dos *hosts* na rede para identificar vulnerabilidades e então tomar medidas preventivas, como o Nmap (NMAP, 2020?). O conhecimento dessas falhas deve ser evitado ao máximo por pessoas não envolvidas com gerenciamento da rede diretamente, a equipe técnica, ou indiretamente, os seus superiores, caso contrário a rede empresarial estará mais suscetível a ataques bem sucedidos. Portanto é importante identificar escaneamento da rede por usuários não autorizados a fazer a auditoria na rede corporativa, prevenir ou remediar a tentativa e em seguida, punir legalmente o responsável.

Proibição de *torrent*

Em geral, os arquivos de *torrent* estão associados a disponibilização de conteúdo audiovisual pirateado para *download* na *internet*, ou seja, é ilegal. Em alguns países, como na Alemanha, essa atividade costuma ser rastreada e a empresa pode ser multada em 800 euros por arquivo baixado

(GOMES, 2017). Além disso, o download consome largura de banda e prejudica a disponibilidade da rede, portanto bloquear essas atividades é algo importante a ser feito.

3 Ferramentas, soluções e trabalhos correlatos

Neste capítulo está explicitado o que são as ferramentas de *Captive Portal* (seção 3.1), *Serviço de Diretório* (seção 3.2), *Scanner* de Vulnerabilidades (seção 3.3), Sistema de Detecção de Intrusão (seção 3.4) e as soluções de *Bring Your Own Device* (seção 3.5) e *Network Access Control* (seção 3.6) que são necessárias para cumprir o objetivo deste trabalho, quais produtos foram utilizados dessas ferramentas e soluções e o motivo(seção 3.7), e por último facilitar o entendimento dos trabalhos correlatos (seção 3.8).

3.1 *Captive Portal*

Quando se necessita previamente de que um *host* concorde com termos de uso de uma empresa, e/ou forneça credenciais, e/ou permita acesso a informações de alguma rede social, como mostra a Figura 18, para que então seja permitido acesso a *Internet*, o *Captive Portal*, ou também chamado de *WEB Authentication*, é uma opção que facilita esse processo.

Figura 18 – Exemplo de *Captive Portal* com credenciais

Fonte: Autoria própria

Uma vez que um aparelho tente se conectar a LAN empresarial e não esteja autenticado, aparecerá uma página WEB automaticamente, no caso da maioria dos *smartphones* e tablets, ou após abrir o navegador, nos demais casos. Essa página pode apresentar, por exemplo, um texto com os termos de uso daquela rede junto a uma semelhante a "concordo com os termos uso"e/ou

campos de login e senha e/ou permissão para postar em sua rede social que está acessando a Internet na empresa Xpto Ltda e em ambos os casos, juntamente com um botão escrito "conectar".

Em termos técnicos, o que acontece é que quando um *host* não está autenticado, ele é direcionado para uma VLAN de registro, onde apenas o tráfego de pacotes de HTTP, HTTPS, DNS e NETBIOS é permitido, e o servidor DNS sempre o redicionará o *host* para o *captive portal* até que a autenticação seja feita. Vale destacar que o controle de tráfego não é feito pelo *Captive Portal*, mas por servidor SNMP ou dispositivo de redes (NETGEAR, 2016).

Comparado ao 802.1X que impede comunicação entre *host* não autenticado e os outros (exceto o servidor de autenticação), o *Captive Portal* é menos seguro por dar ao *host* um acesso à rede (ainda que limitado) mesmo se não estiver autenticado, já que ainda permite a transmissão de pacotes que não são exclusivos para autenticação (como o DNS, explicado na subseção 2.6.3), ou seja, a chance de ser bem sucedido em um ataque é maior. Portanto é importante que o gerente da rede faça configurações extras para limitar ainda mais o acesso à rede na VLAN de registro.

3.2 Serviço de Diretório

De acordo com (HOFFMANN; WONZOSKI; RIVEROS, 2017) "O Serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, como por exemplo, usuários, computadores, impressoras, servidores entre outros recursos de rede.", ele armazena de forma organizada e hierárquica, como um banco de dados, essas informações da empresa em formato de objeto e as mantém disponível para acesso pela rede apenas por *hosts* autorizados.

A estrutura de dados utilizada para guardar essas informações é a de árvore, como pode ser observada na Figura 19, onde existem um nó raiz, por onde começa uma busca, e passa pelos nós filhos até chegar ao dado que se deseja encontrar (JUNIOR, 2008).

Um exemplo da utilização de serviço de diretório é o de verificar a autenticidade de um funcionário que deseja acessar a rede corporativa a partir do acesso aos atributos a ele relacionados, como email e senha, para então conceder ou não a permissão de entrada.

3.3 *Scanner* de Vulnerabilidades

De acordo com Eugene Howard Spafford, especialista em segurança da computação, "O único sistema verdadeiramente seguro é aquele que está desligado, preso a um bloco de concreto e trancado em uma sala revestida de chumbo e com guardas armados"(REBELLO et al., 2016). Como essa solução não é viável, podemos admitir que todo *host* está sujeito a vulnerabilidades e uma vez descobertas por um atacante, passa a se tornar efetivamente uma ameaça para a segurança do dispositivo ou até da rede em que se encontra.

Figura 19 – Estrutura de dados em formato de árvore

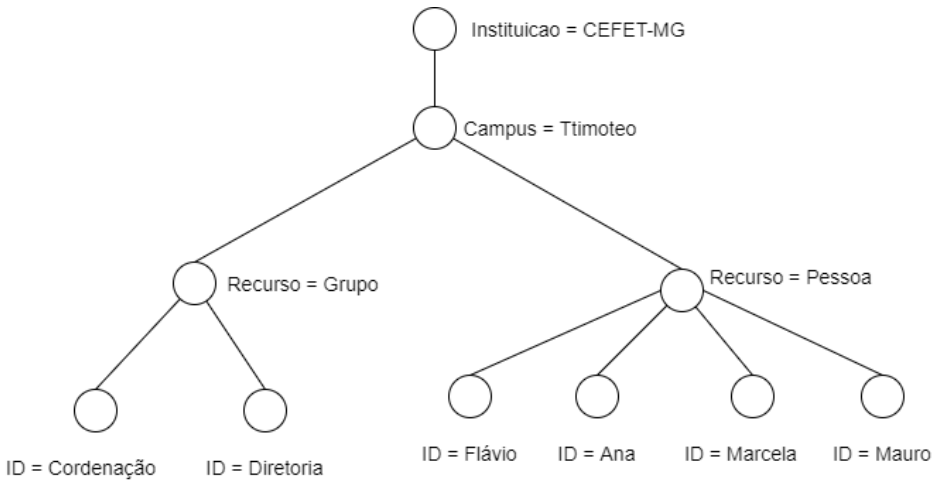


Figura adaptada da fonte (FOUNDATION, 2021)

Portanto é interessante que o responsável pela segurança da LAN corporativa identifique essas vulnerabilidades antes de um futuro atacante e a partir disso, oferecer orientações de como resolver essas vulnerabilidades. Tal identificação pode ser feita por automaticamente por um *scanner* de vulnerabilidades.

Esses *softwares* possuem uma lista de vulnerabilidades comuns e amplamente conhecidas pela *Internet*, sendo tal lista atualizada a medida de se descobre novas vulnerabilidades. A partir dessa lista ele executa testes, também chamados de Network Vulnerability Tests (NVT), em um *scan* de um ou mais *hosts*, com possibilidade de ser feito periodicamente e gerando alertas ao gerenciador da rede quando detecta vulnerabilidades críticas (INFOSEC, 2021).

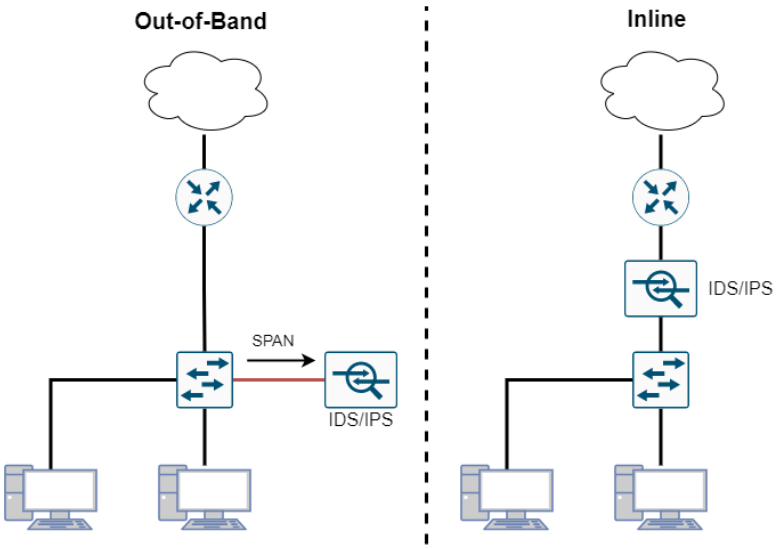
3.4 Sistema de Detecção de Intrusão

Uma síntese da definição de Sistema de Detecção de Intrusão, ou *Intrusion Detection System* (IDS) é "[...] um sistema que monitora uma rede em busca de eventos que possam violar as regras de segurança dessa rede."(REBELLO et al., 2016). Um Sistema de Detecção de Intrusão tem dois tipos de localização, detecção de eventos e comportamento.

Localização

O IDS pode estar localizado em cada *host*, o *Host Intrusion Detection System* (HIDS), que permite um monitoramento mais efetivo entretanto difícil de gerenciar, ou pode estar localizado em um ponto estratégico da rede, o *Network Intrusion Detection System* (NIDS), que oferecem um mo-

Figura 20 – *out-of-band* e *inline*



Fonte: Autoria própria

nitoramento mais genérico, mas centralizado, o que facilita o administração. Esse ponto estratégico depende de qual modo irá funcionar o NIDS, se é *inline* ou *out-of-band* como mostra a Figura 20.

No modo *inline*, todos os pacotes vindos de fora da rede interna passam obrigatoriamente pelo NIDS antes de ir para a LAN, funcionando como um *firewall* (dispositivo de rede que filtra pacotes vindos da rede externa para a rede interna), o que torna mais seguro contra ataques externos, porém pode reduzir a velocidade da rede uma vez que cada pacote deve ser analisado antes de entrar na LAN.

No modo *out-of-band*, a ferramenta permite o pacote passar livremente, mas recebe uma cópia dos pacotes através de uma técnica chamada de *Port Mirror* ou *Switched Port Analyzer* (SPAN) e quando detectado algum pacote suspeito, ele manda o pacote a origem e o destinatário para reiniciar a conexão entre eles até que se inicie uma nova conexão que esteja de acordo com as regras do IDS (DILLARD, 2020).

A desvantagem desse método é que a resposta do IDS pode não ser rápida o suficente para impedir uma atividade identificada como maliciosa, pois ele pode receber o pacote segundos depois dele ter sido recebido pelo destinatário. Outro problema é essa conexão só existe por protocolos que utilizam o *Transmission Control Protocol* (TCP) da quarta camada do modelo OSI, a de transporte, sendo que os pacotes que utilizam *User Datagram Protocol* (UDP) não há como forçar um reinicio da conexão, o que torna mais dificil interromper ataques vindos dessa última *videoIDS*.

Detecção de eventos

O modo de detecção de eventos pode ser feito por assinatura, ou seja, um conjunto de regras pré configuradas que identificam um tipo de evento dito como indesejado, ou pode ser feito através de uma análise do comportamento da rede.

Uma avenida por exemplo possui um fluxo de carros que segue, em partes, um padrão dependendo do horário. Se durante as 15h00 se observa um congestionamento, um horário não muito comum de movimentação de carros, significa que algo está errado, assim funciona o IDS por análise do comportamento da rede, ele detecta um fluxo anômalo de dados e assim gera alertas. Entretanto cada rede possui seu fluxo próprio padrão de comportamento, portanto o IDS precisa de um tempo monitorando a rede para "aprender"o que é um fluxo normal ou anormal, usando para isso uma inteligência artificial.

Comportamento

O comportamento dessa ferramenta pode ser apenas de detecção, o *Intrusion Detection System* (IDS), identifica um evento e avisa ao administrador da rede para que então seja tomado alguma providência manualmente, ou pode tomar alguma atitude automaticamente, o *Intrusion Prevention System* (IPS).

3.5 *Bring Your Own Device*

O *Bring Your Own Device* (BYOD) é uma política que permite os funcinários de uma empresa a trazerem seus próprios dispositivos, como celular e notebook, para serem usados no trabalho e com acesso a rede corporativa.

3.5.1 Motivações para ser implantado

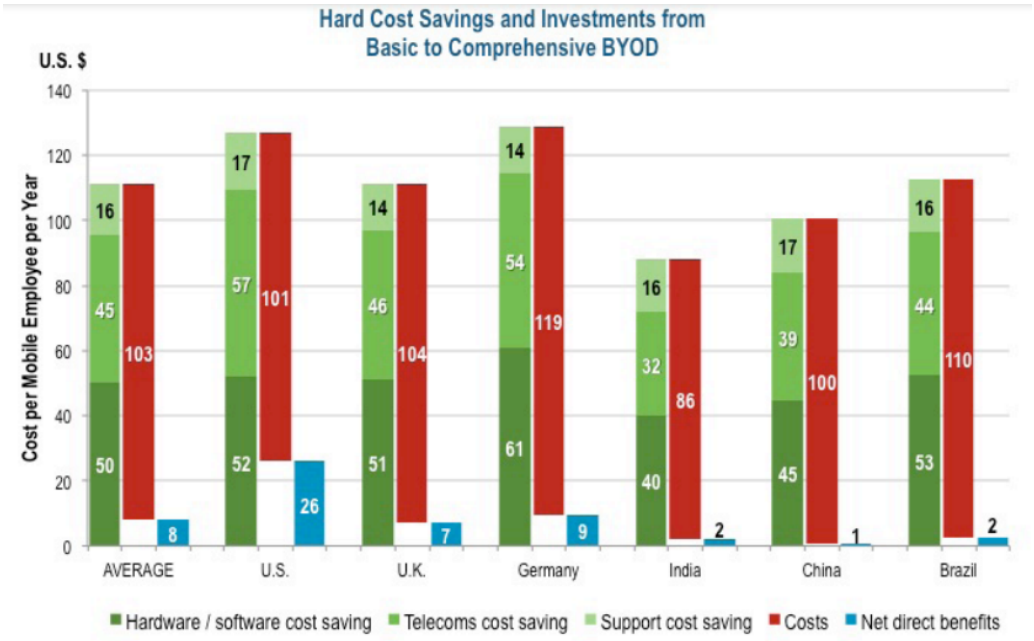
Permitir acesso à LAN apenas aos dispositivos da empresa, que necessitam de configurações prévias e manutenções para obter um alto nível de segurança na rede, é uma tarefa exaustiva que demanda mais tempo e pessoas para cumpri-la a medida que aumenta a estrutura da rede. Sendo assim, o uso de dispositivos dos próprios funcionários para trabalho tem sido analisado como alternativa para aumentar flexibilidade e escalabilidade da empresa, uma vez que a manutenção dos aparelhos fica a cargo de cada empregado.

Relatórios, como o da (FARIA et al., 2013), têm identificado efeitos positivos na adoção de BYOD nas empresas, entre elas redução de custos financeiros, na equipe de suporte técnico, no uso de banda larga e até mesmo ganho de desempenho entre funcionários.

Redução de custos

Estudando a implantação do BYOD, foram identificados vantagens relevantes no que diz respeito a redução de custos financeiros, recursos humanos e largura de banda. Esses três quesitos juntos ofereceram uma economia aproximada de $110,00 por funcionário a cada ano no Brasil, como pode ser observado na Figura 21 (FARIA et al., 2013).

Figura 21 – Economia por funcionário



Fonte: (FARIA et al., 2013)

Uma vez que os funcionários irão usar seus próprios aparelhos para trabalhar, logo é possível uma redução drástica nos custos financeiros da empresa, pois não há necessidade de comprar um computador e/ou celular para cada empregado ou substituir peças defeituosas ou até mesmo furtadas ou roubadas. O estudo aponta uma economia $53,00 por funcionário a cada ano no Brasil (FARIA et al., 2013).

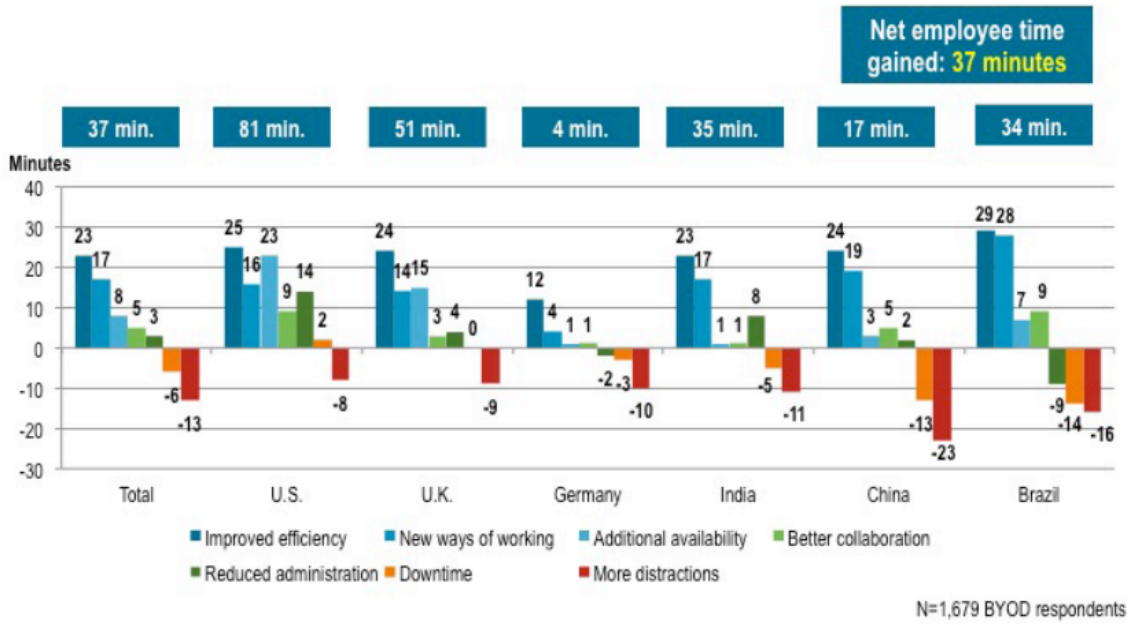
Existe também uma redução no esforço de se encontrar, contratar e manter uma equipe técnica de redes, pois como os dispositivos já estão parcialmente ou totalmente configurados, logo é possível diminui-la. O estudo aponta uma economia $44,00 por funcionário a cada ano no Brasil (FARIA et al., 2013).

Também é possível reduzir o uso de largura de banda, uma vez que os funcionários, quando considerarem oportuno utilizar o próprio plano de dados móveis em vez de usar a rede local. O estudo aponta uma economia $16,00 por funcionário a cada ano no Brasil (FARIA et al., 2013).

Ganho de desempenho dos funcionários

Foi observado que quando os funcionário estão utilizando seu próprios dispositivos e softwares, eles economizam tempo ao aumentar a eficiência, colaboração, novas formas de trabalhar e disponibilidade adicional e que compensa alguns minutos perdidos a mais de distrações, tempo de inatividade e administração. O estudo aponta um ganho de 34 minutos diários por funcionário no Brasil, como podemos ver na Figura 22 (FARIA et al., 2013).

Figura 22 – Tempo aproveitado por dia



Fonte: (FARIA et al., 2013)

3.5.2 Desafios de implantar

A política de BYOD abre brechas de segurança uma vez que está sendo permitido o acesso a rede corporativa por dispositivos que pela maior parte de tempo estão em posse do empregado, sendo assim, sob menos controle da empresa e que por isso está mais suscetível a não estar em conformidade com as políticas de segurança.

Dentre os desafios de segurança que são enfrentados ao implementar uma solução de BYOD, identificamos que a prevenção de vazamento de dados, prevenção de *Malware* e *Compliance Enforcement* são os tópicos mais recorrentes citados entre cinco fontes diferentes as quais dividem cada desafio em tópicos. Na Quadro 1 é possível observar relacionamento de cada uma dessas três categorias com o conteúdo de cada tópico com a respectiva fonte.

Quadro 1 – Categorias de desafios em BYOD

Categoria de desafios mais recorrentemente citados	**Tópico e fonte**
Vazamento de dados	*Physical Theft* (GUPTA, 2011)
	Lost or stolen devices (BONUCCELLI, 2016)
	Data compliance issues (BONUCCELLI, 2016)
	Fired employees (BONUCCELLI, 2016)
	Hacking issues (BONUCCELLI, 2016)
	a wide variety of security risks(MSP, 2020)
	issues with data removal and retrieval(MSP, 2020)
	Difficulty Retrieving Data After an Employee Quits Or Is Fired(MDM, 2020)
	Device Security(CHANG J. MORRIS, 2014)
Malware	*Malware Prevention* (GUPTA, 2011)
	Malicious apps (BONUCCELLI, 2016)
	Vulnerability to malware (MSP, 2020)
	Malware (CHANG J. MORRIS, 2014)
Compliance Enforcement	*Policy Enforcement* (GUPTA, 2011)
	BYOD compliance issues (MSP, 2020)
	inefficient password management (MSP, 2020)
	Enforcing Compliance Becomes More Difficult (MDM, 2020)
	Enforcement (CHANG J. MORRIS, 2014)

Tabela construida pelo próprio autor usando como base as fontes: (GUPTA, 2011; BONUCCELLI, 2016; MSP, 2020; MDM, 2020; CHANG J. MORRIS, 2014)

Vazamento de Dados

A informação obtida dentro da organização é um ativo de valor para agregar o negócio e que por isso o funcionário que a obtém deve se responsabilizar pela segurança desses dados. Apesar disso, o relatório de (INFOWATCH, 2018) mostra que em 2018, 53,5% dos casos de vazamento de dados detectados por eles ocorreram por funcionários internos da empresa, independente se foi intencional ou por erro humano.

Sendo assim, o uso de dispositivos gerenciados pelos próprios funcionários e que podem eventualmente manter informações empresariais armazenadas nos aparelhos pessoais abre mais possibilidades de vazamento de dados, portanto é importante que a empresa estabeleça PSI e utilize ferramentas para mitigar ao máximo esse cenário.

Prevenção de *Malwares*

Dispositivos pessoais são mais suscetíveis à infecção por malwares, uma vez que eles estão geralmente exposto diariamente a *Internet* e acessando aplicações e sites que não oferecem muita

segurança, diferente de computadores da empresa que estarão ativos apenas durante a jornada de trabalho e na maior parte do tempo acessando serviços *business-to-business* (de empresas para empresas) que em suma são mais seguros.

Uma vez que existe um *host* infectado por um *malware* dentro da LAN empresarial, ele pode se tornar a fonte de uma ataque à rede e resultar desde serviços temporariamente indisponíveis, denominados de *Deny of Service* (DoS), a até encriptação dos dados da empresa para serem vazados ou serem objeto de estorção como foi o caso do *ransonware* WannaCry que arrecadou entre o dia 12 e 17 de Maio de 2017 112 mil dólares (PROOF, 2017).

Para evitar esses riscos, é de suma importância a utilização de ferramentas de checagem de *host* para identificar se estão infectados por *malware* ou pelo menos se estão a utilizar um antivírus, por exemplo, que mitigaria esse problema e só então permitir o acesso à rede interna.

Compliance Enforcement

Compliance Enforcement é o método para fazer com que os usuários da LAN corporativa estejam de acordo com as políticas de segurança da informação na organização antes de conseguir acesso aos serviços da rede empresarial. Por exemplo, se for exigido a um antivírus dentro da LAN, o dispositivo que não cumpre essa exigência não conseguirá acessar a rede. Dessa forma, o *Compliance Enforcement* é um instrumento para a implementação de uma PSI e assim, mitigar riscos à segurança.

Vale relembrar que na seção 2.7 já foi explicado que a PSI são os pré requisitos necessários para cumprir os anseios por segurança de uma organização e podem resultar em prejuízos caso não sejam acatadas.

3.6 *Network Access Control*

Network Access Control é uma solução que oferece visibilidade e controla o acesso à rede ao permitir apenas que dispositivos autenticados, seguros e que estejam de acordo com a PSI possam se conectar, além de definir quais serviços um usuário poderá ter acesso, por exemplo, a partir de segmentação por VLAN (ILLUMIO, 2021).

Essa solução pode ser um *software* instalado em algum servidor ou em uma máquina virtual ou pode ser um dispositivo de *hardware*, como é o caso da solução da Extreme (EXTREME, 2021).

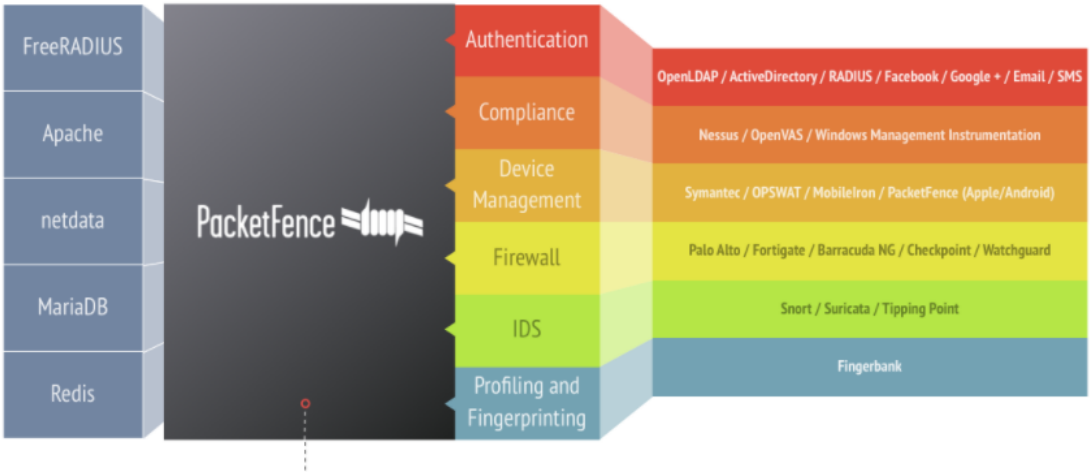
O NAC utiliza ferramentas de segurança de *Compliance Enforcement* e monitoramento de rede para verificar se os *hosts* da rede estão seguindo as regras de segurança da rede. Uma vez identificado o descumprimento de alguma dessas regras, o aparelho é movido para uma rede de quarentena, onde ele tem acesso limitado a rede interna e recebe instruções sobre quais configu-

rações devem ser alteradas e como faze-las, geralmente por uma interface *WEB*, para que ele ser reavaliado pelo sistema e possa ser movido para devida LAN (ENTERASYS, 2009).

O que se observa nessas soluções de mercado é que elas não necessariamente incluem todas as ferramentas de segurança, autenticação, autorização e visibilidade e sim integram a si mesmas outros produtos do mesmo fabricante ou de terceiros, funcionando assim como um servidor que centraliza o controle e as mensagens geradas por cada ferramenta de segurança e disponibilizando uma interface WEB para facilitar o gerenciamento de boa parte do aparato necessário na segurança da rede (ROBB, 2021).

Essa relação entre NAC e outras ferramentas pode ser vista no Packetfence, *Network Access Control* desenvolvido pela Inverse, onde a Figura 23 ilustra o produto no meio, em sua esquerda os serviços inclusos nele e em sua direita os produtos que podem ser integrados a ele.

Figura 23 – Relação do Packetfence com outras ferramentas



Fonte: (PACKETFENCE. . . , 2021)

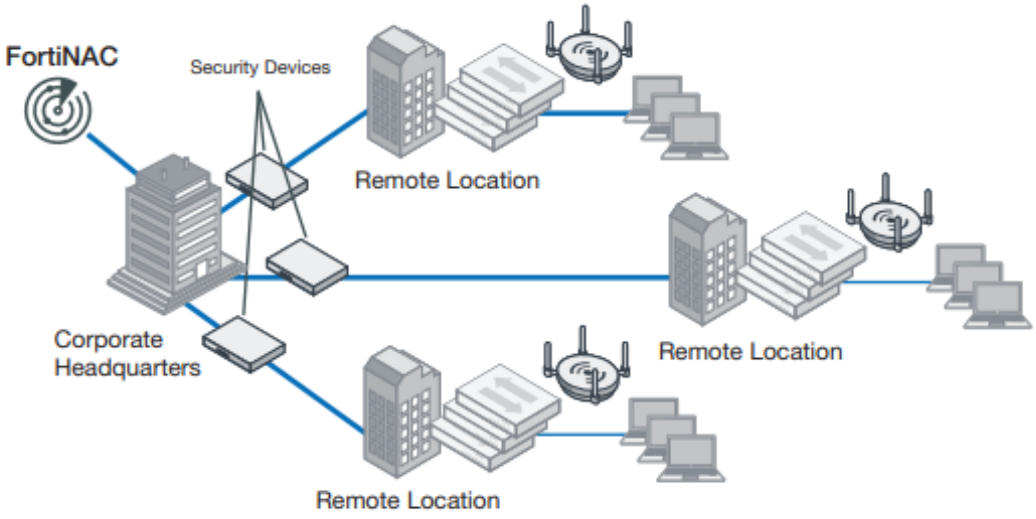
O NAC tem dois modos de operações diferentes (dependendo do fabricante, os dois modos podem funcionar paralelamente, como o Packetfence) (PACKETFENCE. . . , 2021), os dois são o *inline* e o *out-of-band*, parecido com a do IDS em relação apenas ao posicionamento do *host* dentro da rede visto na seção 3.4.

O modo *inline* é utilizado principalmente para gerir equipamentos não gerenciaveis. A principal desvantagem desse modo é na escalabilidade, pois funcionará como *firewall* (que também funciona como roteador) todo pacote que trafega entre um *host* gerenciado por esse modo e qualquer outro *host* de outra rede deve passar obrigatoriamente pelo NAC, o que torna a estrutura da rede mais complexa a medida que ela cresce e também ficará mais lenta. Essa complexidade pode ser evitada utilizando múltiplas soluções NAC em cada espaço físico (prédio, campus, condomínio).

Em contrapartida o modo *out-of-band* é utilizado quando os equipamentos são gerencia-

veis e apenas uma solução NAC é suficiente para fazer o controle de acesso de diferentes locais no mundo sem prejudicar na escalabilidade, como pode ser visualizado na Figura 24 (PACKETFENCE. . . , 2021).

Figura 24 – Exemplo de escalabilidade com FortiNAC em *out-of-band*



Fonte: (FORTINET, 2021)

O NAC costuma ter a opção de trabalhar em conjunto ou não com um agente, software instalado no dispositivo do usuário usado para fazer *Compliance Enforcement* automaticamente, como acontece na solução InfoExpress (INFOEXPRESS, 2018?).

O agente pode ser do tipo persistente, o qual fica instalado e monitorando o computador durante todo o período em que o aparelho está ligado ou conectado a LAN da empresa (esse caso é mais comum entre aparelhos da própria empresa), ou pode ser um agente dissolvível, o qual é baixado e instalado temporariamente no dispositivo ao tentar acessar a rede e quando finaliza o *Compliance Enforcement* ele é removido do dispositivo (geralmente são contratados serviços de nuvem que fornecem o download desse agente).

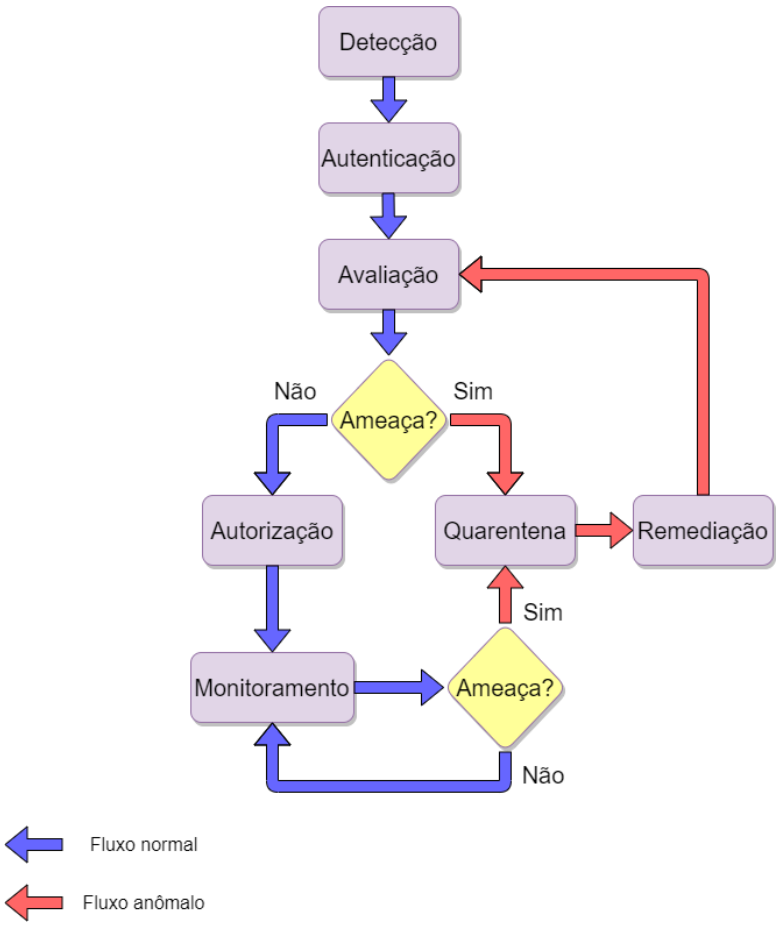
Também é possível identificar vulnerabilidades com solução sem agente, ou *agentless*, como é o caso da solução da ForeScout que permite avaliar se um *host* é ou não seguro antes de permitir o acesso à rede (FORESCOUT, 2019).

3.6.1 Fluxo de uma solução NAC

Para facilitar o entendimento das funcionalidades de uma solução NAC, foi explicitado um fluxo do acesso a rede por um cliente e que pode ser visualizado na Figura 25 elaborado pelo autor

baseado nas informações obtidas durante o desenvolvimento deste trabalho. Primeiramente detecta-se a presença de um *host* que se conecta à rede, caso seja a primeira vez na rede, o seu endereço MAC será gravado em sua lista de computadores identificados, caso não seja, apenas atualiza para indicar que esse computador está online na rede.

Figura 25 – Fluxo do NAC



Fonte: Autoria própria

A seguir é feito a autenticação, para verificar se aquele usuário pode ter acesso à LAN; uma vez autenticado, o aparelho é avaliado a partir de um *scan* para definir se está vulnerável a ataques ou se está de acordo com a PSI e assim decidir se é uma ameaça à rede. Se for avaliado como seguro a acessar a rede, inicia o processo de autorização e finalmente o cliente já pode usufruir dos serviços na rede local.

Entretanto, um *host* ser avaliado como seguro ao entrar na rede corporativa, não significa que ele estará assim continuamente, por exemplo, o cliente pode ativar uma aplicação *torrent* futuramente, portanto é necessário o constante monitoramento da rede para identificar se a PSI continua sendo cumprida pelos funcionários.

Caso durante o monitoramento ou a avaliação for identificado alguma atividade indesejada, o *host* será redirecionado a uma VLAN de quarentena, onde há acesso restrito aos serviços da empresa e com apenas o necessário que possibilite fazer as "remediações"necessárias para se enquadrar novamente às políticas de rede da empresa. Uma vez feito as alterações, ele solicita uma reavaliação para verificar e se tudo estiver de acordo com os conformes poderá acessar a rede normalmente.

3.7 Escolha das Ferramentas e soluções

Esta seção é dedicada a esclarecer a razão da escolha de cada ferramenta e solução para desenvolvimento do trabalho.

NAC *open source*

Dentre os NACs *open source* que poderiam ser utilizados, encontramos estes três: OpenNAC, FreeNAC e Packetfence (NUNOO-MENSAH; AKOWUAH; BOATENG, 2014). Entretanto o FreeNAC teve sua ultima atualização em 2013, bem antigo comparado as outras duas soluções, o que nos indicaria que foi descontinuado (FREENAC, 2013). Quanto ao OpenNAC sua ultima atualização foi em 2019 e para acessar a sua documentação é necessário fazer um cadastro e esperar a aprovação do administrador, mas desde o dia 08 de Setembro de 2021, fizemos o cadastro e ainda não foi aprovado (OPENNAC, 2019).

Portanto decidiu-se usar o Packetfence, que já possui uma atualização de 2021, com guias como a de instalação, atualização e configuração de dispositivos de rede, todas dividas em tópicos, o que facilita o seu entendimento, todos disponíveis sem necessitar de um cadastro, suporta dispositivos de redes de aproximadamente 37 fabricantes e que permite a integração de múltiplas ferramentas como as de autenticação, IDS e scan de vulnerabilidades além de alguns serviços inclusos como o captive portal e o RADIUS (PACKETFENCE. . . , 2021).

IDS

Dentre os IDS compatíveis com o Packetfence temos: Security Onion, Snort, Suricata e StreamScan Comprimise Detection System esse último foi descartado da nossa solução por não ser gratuito (STREAMSCAN, 2021). O Security Onion é uma ferramenta mais complexa com múltiplos serviços, alguns deles que o Packetfence já oferece como informações do estado do sistema (Grafana no Onion Security), e que necessita de mais recursos de hardware (recomendado 200GB de disco, 4 cores e 16GB de RAM no modo Standalone) em um ambiente de produção (SOLUTIONS,

2021). Devido a redundância de serviços, limitações de recursos de hardware e complexidade de configuração, descartamos essa ferramenta.

Sendo assim, o Snort ou Suricata seriam os mais indicados entre as opções de IDS nesse projeto. Como necessitamos de apenas um deles, o Suricata é o mais indicado pois é de fácil instalação, pois tem menos passos a serem seguidos comparado com o Snort (SURICATA, 2019).

Esse projeto inicialmente utilizou esse IDS e um dos passos foi seguido incorretamente e foi percebido apenas ao final, quando ao testar a ferramenta ela não funcionou, e por isso foi necessário reinstalar uma nova máquina e configura-la desde o início. Portanto, caso se opte por usar o Snort, sugere-se que faça *snapshots* da máquina virtual antes de seguir cada capítulo do manual de instalação, assim se algo der errado na instalação, apenas volte ao último *snapshot*, sem perder toda a configuração (SNORT, 2021).

O motivo da troca foi porque, apesar de o Snort estar especificado como suportado pelo Packetfence em sua página inicial e aparece como opção de Sysparser (analisador de syslog do Packetfence) em suas configurações, ele não é citado no manual de instalação e nem há alerta de eventos feitos especificamente para regras do Snort no Packetfence.

Scan de Vulnerabilidade

Entre as ferramentas de scan temos: InsightVM, Nessus, Windows Management Instrumentation (WMI) e Greenbone Vulnerability Manager (GVM), esse último sendo o antigo OpenVas. O Nessus e o InsightVM apenas tem versão de teste como gratuitas e as versões para produção os valores anuais mais baratos são respectivamente de $2,990 e $6,250. Por conta do preço, descartamos essas ferramentas (RAPID7, 2020?; TENABLE, 2021). O WMI também foi descartado, isso porque em uma solução BYOD espera-se suportar aparelhos de diversos sistemas operacionais e como esse serviço é específico para ambientes Windows, não é o mais adequado para a nossa solução (SATRAN et al., 2018a).

O GVM é um solução *open source* capaz de fazer *scans* em *hosts* macOS, Windows e Linux, e possui uma versão gratuita chamada de Greenbone Security Manager Trial (GSM Trial) que apesar de ter a palavra *trial* em seu nome, que indicaria que ele expiraria depois de um tempo, ele funciona plenamente, mas sem atualizações diárias de vulnerabilidades e algumas ferramentas não são inclusas (RESILIENCE, 2020b).

Apesar deles disponibilizarem uma VM já configurada, funcionalidades como alertas não estão disponíveis, apesar de supostamente estarem disponíveis na versão gratuita, portanto fizemos a instalação em um Kali Linux. Também é possível usar uma máquina com Debian (vale ressaltar que o Kali é baseado no Debian), entretanto são necessários muitos mais passos, sendo esses não explicados pelo próprio fabricante, o que torna mais complexa a sua instalação, diferente do Kali que necessita de apenas um *apt install* para fazê-lo (SPLENDORBITS, 2021).

Autenticação e autorização

As ferramentas de autenticação e autorização suportados pelo Packetfence são gratuitos, dentre elas escolhemos o Active Directory por ser o mais popular e que necessita de uma licença vitalícia do Windows Server (atualmente à venda está a versão 2019 pelo preço mínimo $501), apesar de que poderia ser escolhido qualquer outro serviço diretório (SATRAN et al., 2018b). Quanto à autorização, foi utilizado o FreeRADIUS do próprio Packetfence, onde será feito as regras de autorização.

Fingerprint

Fingerprint é uma técnica utilizada para identificar o sistema operacional (SO) a partir de peculiaridades que cada um têm ao transmitir dados na rede (CID, 2003). Ele pode ser usado para visibilidade (saber quais SOs mais utilizadas), usar métodos de diferentes de controle de acesso baseado no sistema operacional do usuário e identificar anomalias na transmissão de dados (Se o sistema é Windows, ele não deve se comunicar como um Linux, caso contrário o dispositivo é suspeito). O FingerBank é uma solução simples que oferece *fingerprint* de 300 request por hora gratuita e foi desenvolvido junto com o Packetfence (INVERSE, 2021b).

Visão geral das ferramentas e soluções escolhidas

Dessa forma ficou decidido:

- PacketFence como solução NAC (que possui RADIUS e captive portal incluso);
- Active Directory como Serviço de Diretório para autenticação;
- Suricata como NIDS;
- GVM como ferramenta de scan de vulnerabilidade;

Relembrando o fluxo de um NAC na subseção 3.6.1, temos as seguintes ferramentas e soluções responsáveis por cada parte do fluxo:

- Detecção: Fingerbank;
- Autenticação: AD e Packetfence;
- Avaliação: GVM;
- Autorização: FreeRADIUS (incluso no Packetfence);

- Monitoramento: Suricata;
- Quarentena: Packetfence;
- Remediação: Packetfence;

3.8 Trabalhos Correlatos

O trabalho da (GONçALVES, 2017) indica que apesar dos benefícios que a política de *Bring Your Own Device* pode trazer, ela aumenta complexidade da segurança da informação devido a quantidade de dispositivos e dados espalhados a serem gerenciados, portanto a autora aponta a necessidade de fazer usar metodologias de gestão de risco e análise financeira devido a esse impacto que uma solução como o BYOD gera à segurança da informação e propõe um modelo de suporte para auxiliar as empresas nas decisões para implantar essa política utilizando como referência outros modelos já existentes como o Modelo de ações relacionadas com custo-benefício ou o Modelo para o estabelecimento de uma Política de Segurança BYOD.

Um dos pré requisitos para a adesão de aparelhos pessoais dentro da LAN corporativa é o uso de múltiplas ferramentas de segurança de rede e dispositivos. Devido a essa gama o autor (PERINI, 2017) se sentiu motivado a elaborar um protótipo nomeado de BYOD Manager Kit, que foi desenvolvido em Java, que integra ferramentas *open-source* (ferramentas de código aberto, disponível na *Internet* para ser utilizado e alterado sem restrições) de segurança e gerenciamento de rede e de *hosts* BYOD, facilitando o controle junto a uma interface gráfica.

O autor (SANTOS, 2017) também analisa soluções de controle e segurança mitigar os possíveis riscos que uma rede com dispositivos móveis pessoais podem ocasionar, mas voltado a soluções mais complexas e já existentes como *Mobile Device Management* e *Network Access Control* e também voltado à criptografia para proteção de dados.

Quanto às soluções NAC, (CUSTOIAS; MENDONçA; CUNHA, 2020?) realiza uma análise comparativa entre as soluções essas no mercado e aprofunda especificamente nas diferenças entre os produtos ISE - Identity Service Engine, Forescout CounterACT® e Aruba ClearPass. Lendo o trabalho, o que pode ser indicado é que o objetivo principal do autor era de orientar na escolha do melhor produto *Network Access Control* para redução de riscos de ataques cibernéticos. Apesar de realizar seu trabalho direcionado a *Internet* das Coisas, conhecido como *Internet of Things* (IoT), ele admite a possibilidade do uso de NAC na segurança para dispositivos BYOD.

4 Desenvolvimento

Neste capítulo foi configurado um ambiente para dar acesso para visitantes, autenticação para alunos e professores com *captive portal* e autenticação para administrador com 802.1X, além de integração com AD para regras de autorização, Suricata para monitorar pacotes na rede, e o GVM para identificar presença de antivírus (e ao final todos os serviços do NAC foram reiniciados).

Neste projeto de pesquisa, como a rede de visitantes funcionou apenas para para fornecer *internet*, ela não tem conectividade com a rede interna (termo que aqui se refere às VLANs de aluno, professor e administrador), diminuindo assim impacto na segurança dos dados da universidade, foi decidido não escanear esse *host* antecipadamente, o que aumenta a velocidade acesso à rede (devido à espera pelo fim do *scan*) e reduz o uso da rede pelo GVM. Já os administradores, como são responsáveis da redes, foi assumido que eles seguiram todas as medidas de segurança por conta própria, portanto foram excluídos do *scan* prévio e a detecção de eventos de segurança.

Para verificar a viabilidade da solução proposta neste trabalho, simulou-se uma LAN (com fio e sem fio), os seus usuários e suas políticas de segurança a partir de um ambiente de virtualização, dispositivos e serviços de gerenciamento de rede. Para facilitar o gerenciamento remoto das máquinas, e sendo os computadores listado na sessão anterior utilizados apenas para virtualização, foi escolhido o *hypervisor* VMware ESXi, que é do tipo 1 e permite criar VMs com uma licença gratuita de 60 dias, porém existem outras opções gratuitas, como o KVM ou instalar os servidores diretamente e separadamente em cada *hardware*.

Devido da pandemia de covid 19, foi necessário utilizar um clientes remotos para ter acesso a rede interna e configurar o servidores durante o fechamento das universidades em Portugal, onde foi desenvolvido todo o projeto. Nas Figura 26 e Figura 27 estão as fotos dos dispositivos de rede e servidores usados, respectivamente.

Foi simulado uma rede de uma universidade e onde existe as VLANs: alunos, professores, gerenciamento, visitante, registro e quarentena. A estrutura da rede está ilustrada na Figura 28, as portas classificadas como *trunk* contém todas as VLANs citadas anteriormente como *tagged*, exceto a VLAN de gerenciamento que foi marcado como *untagged* nos servidores e o AP.

Os dispositivos utilizados na rede são:

- Roteador Cisco 1900 Series;
- Switch Cisco Catalyst 2960 Series 24TT-L (com IOS 15.0(2)SE11);
- Aerohive AP305C (alimentado por *Power over Ethernet*, o qual usa o cabo Ethernet tanto para dados quanto para fornecimento de energia);

Figura 26 – Dispositivos de rede

Fonte: Autoria própria

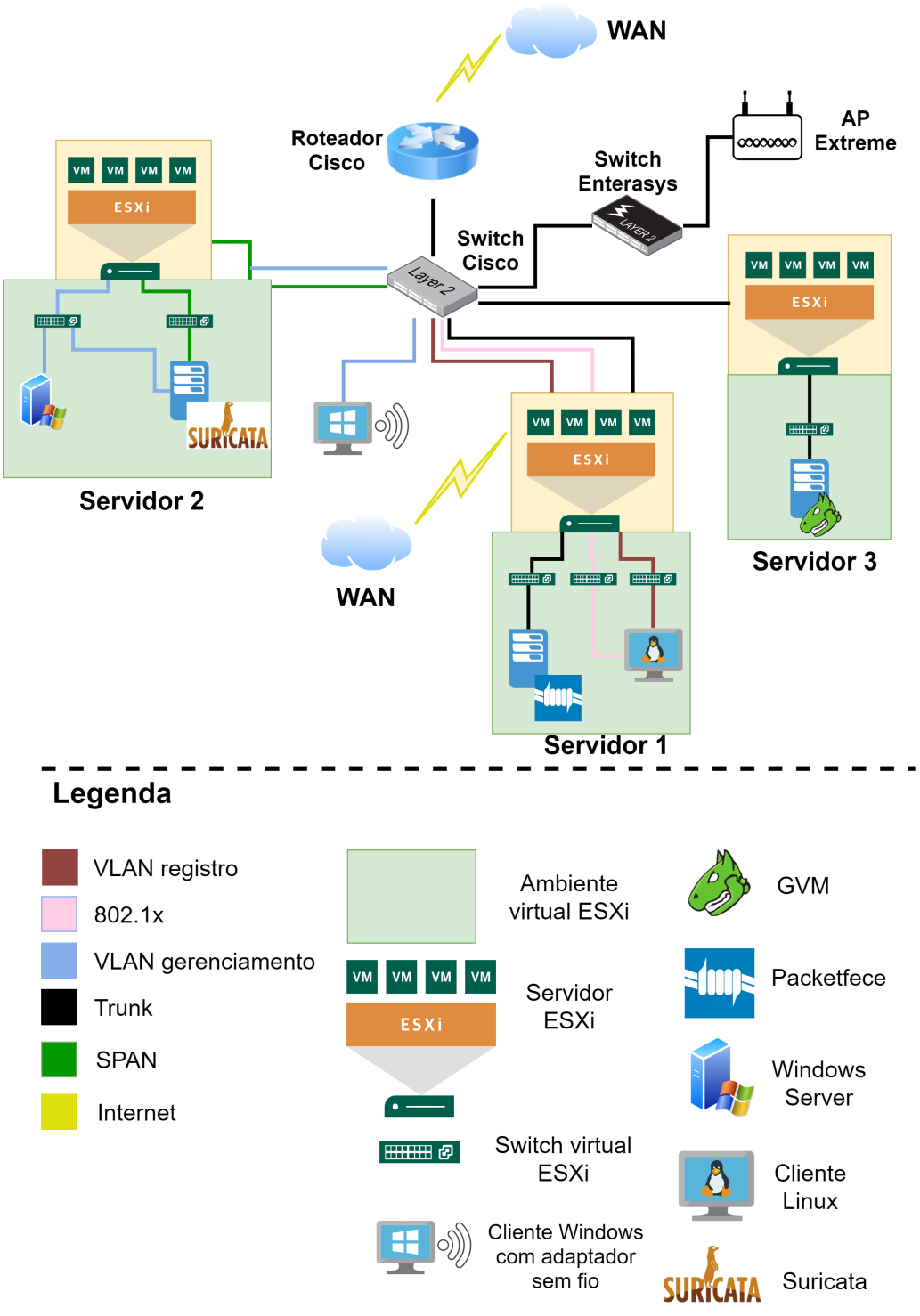
Figura 27 – Servidores

Fonte: Autoria própria

- Switch EnteraSys SecureStack B2 (que suporta *Power over Ethernet* para alimentar o AP);
- Um Servidor octacore, 16GB de RAM e 4 interfaces de rede (Servidor 1);
- Um Servidor quadcore, 8GB de RAM e 2 interfaces de rede (Servidor 2);

- Um Servidor quadcore, 8GB de RAM e 1 interfaces de rede (Servidor 3);

Figura 28 – Diagrama de Rede



Fonte: Autoria própria

A Quadro 2 indica as configurações de hardware dos servidores, as configurações utilizadas nas máquinas virtuais e os SOs utilizados em cada um dos serviços da solução proposta.

Quadro 2 – Lista de Máquins virtuais

Servidor	**Hardware**	**Máquinas virtuais**	**Sistema Operacional**	**Serviços**
Servidor 1	CPU 8 *cores* (20GHz) 16 GB de RAM 4 interfaces de rede 250 GB de HD	8 *cores* (10GHz) 10 GB de RAM 2 interfaces de rede 80 GB de HD	CentOS 7.10	Packetfence
		CPU 8 *cores* (4GHz) 4 GB de RAM 2 interfaces de rede 50 GB de HD	Ubuntu Cliente 20.04	Cliente remoto
Servidor 2	CPU 4 *cores* (6.4GHz) 8 GB de RAM 1 interface de rede 500 GB de HD	CPU 4 *cores* (2GHz) 3 GB de RAM 2 interfaces de rede 20 GB de HD	Ubuntu Server 20.04 LTS	Suricata
		CPU 4 *cores* (3.4GHz) 6 GB de RAM 1 interfaces de rede 50 GB de HD	Windows Server 2016	Active Directory
Servidor 3	CPU 4 *cores* (6.4GHz) 8 GB de RAM 1 interfaces de rede 250 GB de HD	CPU 4 *cores* (5.4GHz) 6 GB de RAM 1 interfaces de rede 30 GB de HD	Kali 2021.02	GVM

Fonte: Autoria própria

Os grupos do Active Directory foram usados como critério de qual VLAN e a rede que o usuário deve ser redirecionado, a Quadro 3 mostra a relação entre as VLANs, a rede e a *role*, que é o papel que aquele usuário desempenha na rede (exemplos: administrador da rede ou aluno).

Quadro 3 – Relação entre as VLANs, *roles* e as redes

Role	**VLAN ID**	**Rede**	**Descrição**
Administrador	2	192.168.2.0/24	Administrador da rede
alunos	15	192.168.15.0/24	Alunos da universidade
professores	20	192.168.20.0/24	Professores da universidade
guest	30	192.168.30.0/24	Visitantes registrado na rede
registration	100	192.168.100.0/24	Visitante ainda no processo de autenticação
isolation	200	192.168.200.0/24	Usuário avaliado como ameaça

Fonte: Autoria própria

Quanto à PSI, foi definido que não será permitido o uso de torrent, fazer *scan* da rede (exceto pelo GVM), a partir do Suricata, e o exigir o uso de antivírus, a partir do GVM.

4.1 Instalação e configuração inicial do Packetfence

Neste projeto, utilizou-se a ZEN (*Zero Effort NAC*), uma VM criada pelo próprio Packetfence com o NAC já instalado e pronto para iniciar a configuração (o usuário e senha padrão é root e p@ck3tf3nc3, respectivamente). Ao iniciar, foi acessado a página de configuração do Packetfence no navegador a partir do link indicado pela própria VM e iniciou-se a configuração inicial em 4 etapas.

Na primeira etapa, definiu-se uma interface de rede para cada VLAN para que ele possa fazer o processo de *change of authorization* (CoA), o qual troca a *role* que foi atribuída ao usuário. Isso será usado para alterar um usuário de visitante para aluno ou para mover um usuário para a quarenta, por exemplo.

O Packetfence estabelece tipos de interfaces. O *management* (deve haver apenas um desse tipo) é o que será utilizado acessar a página configuração do NAC e por isso ficará na VLAN de gerenciamento. As interfaces para as VLANs de registro e isolamento devem ser do tipo *register* e *isolation*, respectivamente, e marcar a opção *enable DHCP Server*, que fará com que o NAC funcione como servidor DHCP para essas duas VLANs. Já as VLANs administrador, alunos e professores serão do tipo *others* e em *Additional listening daemon(s)* deve ser adicionado *dhcp-listener* que recebe os pacotes de outro servidor DHCP (no caso, o roteador) dessas VLANs e assim manter sua lista de *nodes* atualizado. É importante avisar que ao alterar o IP da interface de gerenciamento, o endereço da página *web* também mudará (o acesso é feito pelo *link* https:\\IP_INTERFACE_MANAGEMENT:1443).

Na segunda etapa, na área de *administrator*, indicou-se o usuário e senha a ser utilizado na página *web* de configuração do Packetfence; na terceira etapa indicou-se o API key da conta criada no FingerBank; na quarta etapa foi feito um *print screen* das credenciais e foi finalizada a instalação.

Ao logar na página que aparece do servidor recém instalado do Packetfence, clicou-se em *Policies and Access Control*; *Roles*; e em *New Role* foram criadas as *roles* do Quadro 5 (*guest*, *registration* e *isolation* já estão criadas por padrão).

4.2 Integração de ferramentas

Esta seção trata da integração das ferramentas utilizadas em conjunto com o Packetfence: o *Active Directory* (serviço de directório); Suricata (IDS) e o GVM (ferramenta de *scan* de vulnerabilidades).

4.2.1 *Active Directory*

Para integrar o AD, clicou-se em *Policies and Access Control*; *Active Directory Domains*; *New Domain* e informou-se o IP do Active Directory, o *Workgroup*. Depois de salvar, clicou-se em *Join* (ação de integrar o AD); ao aparecer uma caixa de mensagens e informou-se o usuário e senha com privilégios de administrador do Windows; depois de alguns minutos ele informou que a integração foi bem sucedida. Logo ao lado existe *realms*, onde deve ser adicionado tanto no *realms null* quanto no *default* o AD recém criado na opção *domain*.

Em um primeiro momento, o AD estava conectado diretamente a uma interface de rede do Packetfence (tipo *others*), como pode ser visto no capítulo 5 *Getting started* do *Installation Guide*, apesar de haver conectividade com ambos (testado a partir de um comando de ping) a integração com os dois falhava. Ao procurar no fórum do Packetfence, o problema era pela interface de rede que comunica com o AD não ser do tipo *management* (COMES, 2018; INVERSE, 2021a). Como só uma interface *management* pode existir e ela deve estar acessível a todos os administradores da rede, o AD foi conectado no *switch* com acesso à VLAN de gerenciamento.

4.2.2 Suricata

Para que o Packetfence possa identificar uma irregularidade na rede a partir de eventos detectados pelo Suricata, esse último deve enviar os *logs*, a partir de uma regra que deve ser criada no RSyslog (uma das ferramentas de Syslog usadas no Linux), e o NAC deve permitir que esses relatórios sejam recebidos, feita pelo SysParser que os guarda em uma estrutura de dados chamado fila, para que o Packetfence identifique um evento que transgrida alguma regra de segurança e envie o responsável para a quarentena.

No IDS, foi definido que todos os *logs* vindo do Suricata serão do *facility* local5 (escolhido arbitrariamente) e que eles seriam enviados via UDP. O protocolo UDP não garante que o pacote enviado foi recebido corretamente pelo destinatário, diferente do TCP, e por isso ele é mais rápido e consome menos rede. No nosso caso, quando ocorre uma infração no uso da rede (como o uso de *torrent*), múltiplos pacotes serão identificados, portanto se um deles for perdido durante o transporte entre o NAC e o IDS, haverá outros que podem chegar e basta identificar apenas um deles para o Packetfence enviar o usuário que transmite esses pacotes para a quarentena, logo não é necessário garantir que todos os relatórios sejam devidamente enviados, por isso ele foi escolhido.

No suricata foi criada a seguinte regra "if ($programname contains "suricata"and (($msg contains "ET SCAN"and not ($msg contains "} 192.168.100.110"or $msg contains "} 192.168.200.110")) or ($msg contains "ET P2P") or ($msg contains "ET MALWARE"))) then @192.168.2.100:514 & stop"o qual envia apenas os logs referentes a *scan* (exceto as do GVM), P2P e *malware* para não inundar a rede com *logs* que não serão utilizados pelo Packetfence.

No Packetfence, criamos a fila de análise pelo comando mkfifo /usr/local/pf/var/suricata. No arquivo /etc/rsysconfig.conf foi habilitado receber pacotes UDP na porta 514 ao descomentar as linhas $ModLoad imudp e $UDPServerRun 514 e as enviamos à fila se ele vier do programa Suricata com a linha if $programname == 'Suricata' then /usr/local/pf/var/suricata . Ao colocar logo abaixo a linha indicamos que se essa regra for cumprida, ela não seguirá para as próximas regras.

Na página de configuração do Packetfence *Integration*; *Syslog parser*; *New syslog parser*; Suricata. No formulário informou-se *Alert pipe*, que é o caminho onde o arquivo de fila deve ser criado, nesse caso ela fica em "/usr/local/pf/var/suricata". Após isso, foi criado o arquivo no caminho citado com o comando "mkfifo suricata".

4.2.3 *Greenbone Vulnerability Management* (antigo OpenVAS)

De acordo com o manual de instalação do Packetfence (INVERSE, 2021a), a comunicação entre o OpenVAS e o NAC é feita usando um alerta de HTTP e linhas de comando OMP (OpenVAS Management Protocol), entretanto a ferramenta foi integrada em um novo produto chamado *Greenbone Vulnerability Management* (GVM), o omp já está depreciado e o Packetfence não reage aos alertas enviados da ferramenta de *scan*. Por isso, foi adotado outras medidas.

Primeiramente é necessário instalar o "gvm-tools"no Packetfence para executar comandos do GVM (RESILIENCE, 2020a). Entretanto alguns dos scripts em Python que são obtidos na instalação ou são antigos e/ou incompletos, portanto foi necessário copiar os arquivos do diretório da biblioteca do GVM (no nosso caso se encontra em "/usr/lib/python3/dist-packages/gvm") instalados no Kali para o Packetfence.

Há uma versão gratuita do *Greenbone Vulnerability Management* que permite apenas executar comandos do "gvm-tools"via socket (que funciona localmente), portanto para fazer o *scan* remotamente será necessário fazer um tunel SSH e para garantir que ele esteja sempre funcionando, foi criado um *script* chamado "gvm_socket.sh"no Apêndice D, que faz a verificação e se não tiver ativo, ele remove o tunel anterior e cria outro e usando o crontab, um comando do linux que permite agendar execução de scripts, para executar "gvm_socket.sh"constantemente (nesse trabalho foi definido uma vez por minuto), além de programar atualizações semanais dos dados do GVM, entre eles os NVTs.

Alterações em módulos e criação de *script* em Perl para *scan*

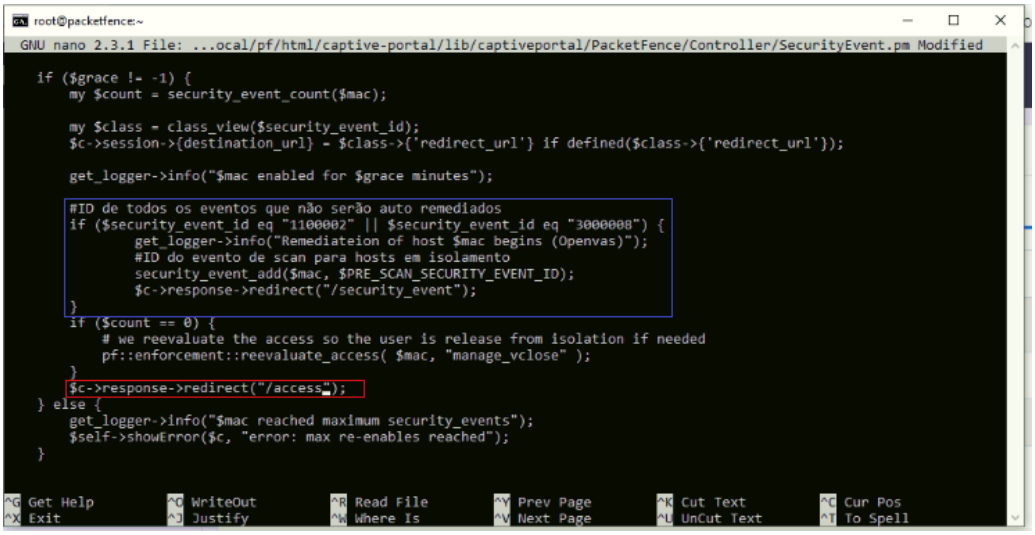
Um dos novos comandos do GVM é o "gvm-*script*"que utiliza scripts em Python. Primeiramente foi utilizado como base os scripts criados pelo Greenbone (RESILIENCE, 2020a) e criar o nosso próprio para fazer o *scan* remotamente e avaliar o relatório, disponível no Apêndice A. Também foi alterado o conteúdo do modulo Perl do Packetfence chamado "openvas.pm", respon-

sável por solicitar o *scan* e acionar um evento de segurança dependendo da avaliação do relatório. Agora o modulo apenas recebe os paramêtros e os envia para um *script* Perl chamado "request_and_trigger.pl"que solicita os *scans* e após acionar eventos de segurança em segundo plano se for necessário.

O motivo da separação é que o usuário será redirecionado para a tela de espera do *scan* após o modulo ser finalizado. Portanto se o módulo ficar a espera do *scan* terminar para depois verificar se aciona eventos de segurança, travaria a página do *captive portal* e além disso, o Packetfence tem um tempo padrão de espera da finalização de um módulo de 15 segundos (que pode ser alterado) e caso seja ultrapassado ocorrerá um erro. O módulo e o *script* estão disponíveis no Apêndice B e Apêndice C.

Outro modulo alterado foi o SecurityEvent.pm que em seu código original, ao permitir a reavalição, sempre permitia o *host* ser reenviado à sua VLAN de origem, um comportamento não desejado quando é necessário fazer uma nova avaliação através de *scan* antes de permitir ter acesso à rede interna. Por isso, foi comentado o código dentro do retângulo vermelho, o qual direciona o *host* diretamente para a página de acesso, e foi adicionado o código dentro do retângulo azul na Figura 29 o qual verifica se o evento de isolamento é o de falha de *scan* ou falta de antivírus (no caso desse trabalho, ID 1100002 e 3000008, respectivamente) e em seguida aciona o evento "*pre_scan*"e redireciona o *host* ao *link security_event* (conceito apresentado na seção 4.6) que apresenta a página do último evento ativo, nesse caso, o tela de *scan*.

Figura 29 – Alterações no módulo SecurityEvent.pm



Fonte: Autoria própria

Acesso local para *scan* profundo

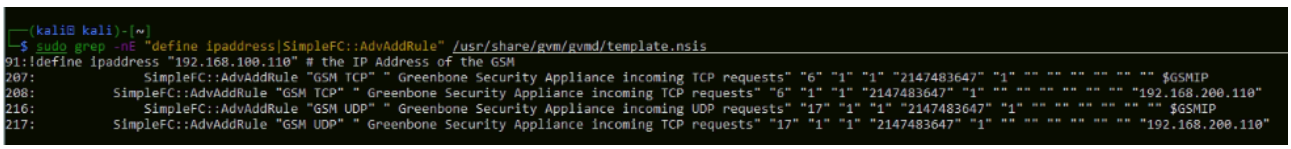
Para fazer um *scan* mais profundo, como identificar programas instalados no *host*, seria necessário acesso local a ele. Para isso, a ferramenta permite usar uma credencial a partir de um executável (no windows) ou uma chave SSH (no Linux ou macOS) para criar um usuário local e ter acessa-lo remotamente a partir dos protocolos Server Message Block (SMB) e o Secure Shell (SSH) respectivamente. O *scan* local foi configurado apenas em *hosts* Windows e Linux para verificação se nele existe um antivírus instalado e em *hosts* macOS para verificação se ele está livre de vulnerabilidades, caso contrário o *host* é enviado para a quarentena (inclusive se o *scan* falhar).

Para o *scan* em Linux, foi criado uma chave SSH para fazer a autenticação, sem precisar de uma senha, e um *script* que o usuário deve executar toda vez antes de entrar na rede. Esse *script* cria um usuário linux com uma senha aleatória, cria regras no *firewall*, insere a chave SSH nele e inicia o serviço de SSH. Por motivos de segurança, o *script* depois de alguns minutos (foi definido 10 minutos) desliga o serviço para evitar que a porta fica exposta. Esse *script* se encontra no Apêndice C.

Para o *scan* em Windows, foi necessário resolver problemas relacionados ao nsis, ferramenta *open source* para criação de instaladores no Windows. Além da instalação do GVM usando um repositório do Kali (mas não oficial da Greenbone), foi necessário instalar o nsis e baixar alguns dos seus plugins que estavam faltando (COMES, 2019). Para resolver esse problema, foi copiado do *Greenbone Security Management* (GSM), VM com o GVM configurado gratuitamente da Greenbone, para o servidor Kali o arquivo que cria o executável "template.nsis"e os plugins do nsis (no nosso caso, o diretório no Kali se encontra em "/usr/share/nsis/Plugins/x86-ansi"). Ainda assim, foi preciso alterar o arquivo, como mostra a Figura 30 onde se encontra a definição do IP de registro (no lugar do de gerenciamento), junto com as regras de *firewall* do Windows para TCP e depois UDP, respectivamente.

Já para *scan* em macOS, por ser legalmente permitido utilizar esse SO apenas em um *hardware* da Apple e não o ter a disposição para fazer o projecto, não foi desenvolvido nenhum *script* para esse SO (BLUEFIRESTORM, 2019).

Figura 30 – Alterações e adições no template.nsis



Fonte: Autoria própria

Configuração do GVM para realizar o *scan*

Sobre as NVTs, elas são dividas em famílias pelo GVM (NVT family). Aquelas que possuem *Local Security* no nome significa que elas só terão efeito se forem executadas localmente, ou seja, necessita de uma credencial. Existem outros testes que necessitam de acesso local, como a detecção de produtos instalados.

Na interface do GVM, o Greenbone Security Assistant (GSA), em *scan config*, foi um *scan* para detectar antivírus em *hosts* Linux e Windows, que estão listados na *NVT family product detection*.

Nesse trabalho foi configurado apenas para se detectar os antivírus AVG e Avast do Windows e o ClamAV no Linux, apesar de existirem outros que podem ser detectados pelo GVM. O motivo é que são muitos esses produtos e demandaria muito tempo a ser testado cada um, além de que teria que fazer uma excessão no DNS do Packetfence para o domínio de cada fabricante.

Ambos também possuem do *NVT family port scanners* o NVT *Nmap (NASL wrapper)* e em *NVT preferences* foi desabilitado *Nmap OS Identification* (já que a identificação do sistema operacional já é feito pelo fingerbank) e em *TCP scanning technique* foi selecionado o *SYN scan* (uma opção menos intrusiva de *scan* que descobre se uma porta está aberta, mas sem estabelecer a conecção). Essas modificações irão reduzir o tempo do *scan*.

Em *credential* foi criado as duas credenciais (uma para Linux e outra para o Windows) e obter acesso local ao *host* para fazer o *scan* mais profundo. Para reduzir ainda mais o tempo de *scan*, em *port list* foi criado uma lista com apenas as portas usadas pelo SSH e o SMB (portas TCP 22, 139 e 445) para os clientes Windows e Linux, já que *scan* de portas não é necessário para identificar a presença de antivírus.

Configuração no Packetefence

O tipo de arquivo do nosso relatório será sempre o txt e como não usou-se também o *alert*, foi alterado o formulário do NAC para adicionar a ferramenta de *scan* e foi modificado *alert* e *report format*, para *credential* para *port list*, já que *alert* e *report format* agora são valores constantes e o *port list* e *credential* serão variáveis (é necessário um conhecimento mais profundo no Packetfence para saber todos os arquivos a serem alterados para mudar o nome dos inputs). Para fazer a alteração, foi localizado a linha que contém o texto que deseja substituir nos dois arquivos en.po e na linha seguinte, onde há "msgstr"foi inserido o novo texto.

Também será necessário criar excessões no DNS do Packetfence e dar acesso aos sites de antivírus anteriormente citados ou *mirrors* que serão usados para baixar o *openssh-server* e o ClamAV (em SO Linux) se o *host* ainda não o tem. Para isso, em *Networking Configuration*; *Fencing*; foi

ativado o *Passthrough* e *Passthrough Isolation* além de ter sido adicionado em *Passthrough Domains* e *Passthrough Domains Isolation* "*.avast.com, *.avg.com, *.clamav.net, mirrors.up.pt, http.kali.org"

Enfim, nas configurações do Packetfence em *Compliance*; *Scan Engine*; *New Scan Engine*; OpenVAS. Assim, foi criado 2 *scans*, apenas para Windows, outro apenas para Linux. O tempo de *scan* também será utilizado como input nos scripts Python e Perl e ele indicará o tempo máximo a ser esperado até o *scan* finalizar (conhecido também como *timeout*) e deve ser sempre em segundos. Nesse projeto foi definido 120 segundos, mas se esse projeto for replicado utilizando um hardware com uma CPU com mais potência, esse tempo pode até ser reduzido. Também foi habilitado o *Scan on registration*, que define que todo *host* seja avaliado depois de ser autenticado. Vale ressaltar que se o SO do *host* não for identificado, nenhum *scan* será feito, por isso é importante o uso do Fingerbank nesse processo.

4.3 *NAS*

O Packetfence só permite que um NAS se comunique com o FreeRADIUS quando ele está registrado nele, caso contrário a requisição é rejeitada (tão pouco aparece nos logs do Packetfence), tal registro foi feito na seção *Policies and Access Control*; *Switches* (Apesar do nome, ele inclui também *access point*). Todo *switch* deve pertencer a um *Switch Groups* (grupo de *switch*), e uma vez que isso acontece, ele utiliza todas as configurações feitas nesse grupo. Como usou-se poucos dispositivos de rede, todos foram inserido em apenas um grupo.

Foi removido o *switch* e o *switch group* padrão e criou-se um novo *switch group*; External Portal Enforcement foi habilitado; na aba *role* selecionou-se a opção *role by VLAN ID* (essa opção indica que seja associada uma *role* a uma VLAN) e indicou-se o ID da VLAN referente a cada role, baseado no Quadro 3; na aba RADIUS foi indicada a *Secret passphrase*. Após a criação do grupo, foi criado os dois NAS com as configurações listadas no Quadro 4.

Quadro 4 – Lista de NAS no Packetfence

Modelo	**Template**	**IP**	**Deauthentication Method**
AP305C	AeroHive - Extreme Access Point	192.168.2.28	RADIUS
Cisco Catalyst 2960 Series	CiscoCatalyst::2960	192.168.2.50	SNMP

Fonte: Autoria própria

4.4 *Authentication Sources* e regras de autorização

As fontes de autenticação (*Authentication Sources*) definem que serviços são utilizado na autenticação e em cada uma delas é possível criar as regras de autorização (as internas e as externas). No caso deste trabalho foram criados dois deles: Active Directory e o *Null* (não usa nenhum serviço).

Para criar a fonte de autenticação com Active Directory *new internal source* com nome "AD"; foi informado o endereço IP; Base DN; Bind DN, que é o usuário com privilégio de administrador do Windows usado para fazer as requisições ao diretório junto de sua senha (No botão *test* é possível verificar se as credenciais estão corretas); em *Realms* foi adicionado o *default* e *local*, de acordo com a documentação do Packetfence; e ao final foi adicionado quatro *Authentication Rules*, que apesar do nome, define as regras de autorização que pode ser vista no Quadro 5.

O Packetfence testa cada regra na ordem em que eles aparecem (de cima para baixo) e finaliza quando uma delas se encaixa nas condições dessa regra. Sendo assim, a ordem das regras deve ser da mais restritiva até a menos restriva. No nosso exemplo se a regra para a role *guest* for a primeira (que não há nenhuma condição, portanto a menos restritiva), todo *host* será direcionado a role *guest*, independente se ele pertece a qualquer um dos grupos do Active Directory, gerando assim um comportamento indesejado. Sendo assim, no nosso caso, a regra para a role *guest* foi colocada por último, assim como no Quadro 5.

Quadro 5 – Regras de Autorização

Role	**Regras**	**Descrição**
Administrador (Ethernet)	UID is member of DC=projetoFinal,CN=Builders,CN=Administrators *Connection Type is Ethernet-EAP*	usuário é membro do grupo administratores
Administrador (Wireless)	UID is member of DC=projetoFinal,CN=Builders,CN=Administrators *Connection Type is Wireless-802.11-EAP*	usuário é membro do grupo administratores
alunos	UID is member of DC=projetoFinal,CN=Users,CN=alunos	usuário é membro do grupo alunos
professores	UID is member of DC=projetoFinal,CN=Users,CN=professores	usuário é membro do grupo professores
guest (visitante)	nenhuma regra	demais usuários

Fonte: Autoria própria

4.5 *Connection Profile*

Foi criado dois perfis de conexão (*connection profile*;) à rede foi configurada: *captive portal* e 802.1X. Na aba *Policies and Access Control*; *Connection Profile*; e foi criado os ambos no botão *New Connection Profile*, uma para conexão com IEEE 802.1X e outra com *captive portal*.

IEEE 802.1X

O *connection profile* de 802.1X; habilitar as opções *Automatically register computer*, que registra automáticamente o usuário sem ser apresentado a um *captive portal*, e *Dot1x recompute role from portal*, que usa a *role* definida a partir da credencial do 802.1X ao em vez da *role* de registro inicialmente que é definido aos *hosts* para acessar o *captive portal*; em *Settings* foi criado dois *filters* (filtros), do tipo *Connection Type*, com as opções *Wireless-802.11-EAP* e *Ethernet-EAP*, isso significa que só conexões com EAP (que utilizado ao usar RADIUS), seja com fio ou sem fio utilizou esse perfil de conexão; em *Sources*, foi utilizado o *Authentication Source* "AD"(criado na seção 4.4); em *Scanner* GVM (criado na subseção 4.2.3); ao fim foi salvo o perfil.

Captive Portal

O *connection profile* para visiantes; em *Settings* foi criado dois *filters* (filtros), do tipo *Connection Type*, com as opções *Wireless-802.11-NoEAP Ethernet-NoEAP*, isso significa que as conexões sem EAP (seja com fio ou sem fio) utilizou esse perfil de conexão; em *Sources*, foi adicionado os *Authentication Sources* "Visitante"e "Google"(criado na seção 4.4); em *Scanner* GVM (criado na subseção 4.2.3).

Em *Captive Portal* foi inserido o caminho de outro logo (logo.png); em *Redirection URL* foi inserido "www.google.com"como endereço que o *host* deve ser redirecionado após a autenticação; em *Language* foi selecionado a opção pt_BR para que o *template* HTML seja o português brasileiro. Em *Files*, foi alterado o arquivo aup_text.html e o texto foi substituido por uma mensagem sobre os termos de uso da rede. Ao fim foi salvo o perfil.

A página de HTML aup_text.html, arquivo modelo do termos de uso, foi inserido todas as instruções para o acesso de alunos e professores, incluido os *links* dos sites da AVG, Avast (precisa ser o instalador offline, pois o *host* tem acesso limitado a *internet*) e ClamAV para download dos antivírus e *link* para download do executável e o *script* de SSH citados na subseção 4.2.3, conforme consta no apêndice Apêndice F. Apesar do *script* em Javascript e o *style* do CSS constarem junto ao texto no apêndice, foi necessário separa-los em arquivos diferentes e incluir o *link* CSS no *head* e o *include* do Javascript ao final do *body* do arquivo layout.html, onde está a base de todas as

páginas HTML do *captive portal* do Packetfence. Ao final, temos uma página como a apresentada na Figura 31.

Figura 31 – Página WEB do *captive portal* com as orientações e termos de uso para o acesso à rede interna

Fonte: Autoria própria

Também dentro do *script* existe um código que permite identificar se o acesso é de visitante e caso positivo, não é exibido o conteúdo de isntruções de acesso, mas apenas os termos de uso. Mas para isso será necessário inserir a id "title"na *tag* HTML onde se encontra "[% i18n(title) %]"dentro do arquivo layout.html e o acesso de visitante deve ter a sua descrição como "Visintate"assim como foi definido na seção 4.4.

4.6 *Security Events*

As *Security Events* definem ações a serem feitas quando elas são acionadas, seja diretamente no código fonte ou através de gatilhos, chamados de *trigger*. Aqui foi definidos todos os eventos relacionados à falta de antivírus, falha no *scan* (já existente chamada "*OpenVAS scan*"), detecção de *Malware* (já existente chamada "*Malware*"), aplicações P2P (já existente chamada "*P2P Isolation (snort example)*") e *scans* indevidos.

Como a detecção de aplicações P2P e *scans* indevidos são feitos pelo IDS, os *triggers* deles devem ser do tipo Suricata e a opção de auto remediação foi desativada pelos motivos citados no inicio desta seção. Já que o evento de P2P já existe previamente, foi criado apenas o evento "*Nmap*"com os *triggers* todos aqueles com o texto *NMAP SCAN* e *GPL SCAN*. Além disso, foi ativado os eventos de *Malware* e *Trojan* (também chamado de cavalo de Tróia, um tipo de *malware*

que se disfarça como um *software* seguro) já pré existentes e sem direito a auto remediação (essa atividade é detectada pelo Suricata quando o *malware* tenta se espalhar pela rede).

Já os eventos do GVM, o *OpenVAS scan* (usado para quando o *scan* falha por algum motivo) foi ativado a auto remediação e foi criado o evento de falta de antivírus chamado de "No antivirus detected", todos com um novo *triggers* do tipo Custom e com o valor, respectivamente, "openvas_scan_failed"e 'openvas_antivirus'.

Todos esses eventos tiveram o texto do botão de auto remediação (quando aplicável), conteúdo do *template* HTML alterados, *role* administrador na lista de *ignored roles* (pelos motivos citados no inicio deste capítulo) e o valor de *grace* de 1 minuto (esse último indica que o evento só pode ser chamado uma vez por minuto, evitando ser chamado múltiplas vezes desnecessariamente)

4.7 Avaliação do fórum e documentação do Packetfence

Agora ao final do desenvolvimento, levantou-se algumas informações sobre problemas que ocorreram durante a implementação do NAC e as informações obtidas para resolve-las. As informações deste capítulo foram importantes para fazer as considerações finais.

Dentre os principais problemas enfrentados durante o desenvolvimento, cita-se: problema em fazer *join* entre AD e o NAC; *VLAN enforcement*; Exceções no DNS; DHCP fingerprint; copia de tráfego DHCP; integração e configuração do GVM; integração do IDS; configuração dos *switchs*; *port mirror* para monitoramento da rede; regras de autorização com AD como fonte.

O problema com o *join*, como citado na subseção 4.2.1, já havia sido levantada por outro usuário no fórum e a resposta foi suficiente para resolver o problema, tanto desse trabalho quanto a do autor dá dúvida.

Ao observar o fórum na data do 17/08/2021, foi constatado que 36 postagens no fórum do Packetfence na ala *packetfence-users* foram feitas. Uma das dúvidas abertas, nomeado de "Aruba IAP"do dia 10/08/2021, teve sua primeira resposta no dia seguinte e a última no dia 16/08/2021. Isso é um indício de que a fórum é ativo e que dúvidas podem ser respondidas rapidamente e talvez chegue a uma conclusão em alguns dias.

Entretanto o problema com a integração com o antigo OpenVAS, versão obsoleta do atual GVM, foi levantada mas sem uma solução, por isso foi necessário um esforço maior comparado às outras ferramentas para descobrir uma forma de fazê-lo a partir da leitura, entendimento do código fonte para a partir disso alterar ou criar novos arquivos de integração.

Foram sanadas pelo manual de instalação do Packetfence as dúvidas sobre como obter cópia do tráfego DHCP e *fingerprint* para saber o IP e o SO de todos os *hosts* na rede (capítulo 27.2.2 e 17), além de como fazer *VLAN enforcement* (capítulo 11) e Exceções no DNS (capítulo 14.5.1).

Instruções mais detalhadas de como receber os relatórios de um servidor syslog, no caso desse trabalho o Suricata, e criar uma fila de eventos que os guarda para serem analisados foram dadas no capítulo 22.3 sobre a ferramenta de *scan* Rapid7 (vale ressaltar que esse conhecimento é sobre Linux e não sobre Packetfence, mas mesmo assim foi documentado) (INVERSE, 2021a).

Instruções de como configurar SNMP, autenticação MAC para *captive portal*, autenticação via RADIUS e 802.1X em dispositivos de redes suportados também está documentado no *Network Devices Configuration Guide* e foi utilizado como base para configurar o *switch* e o AP. Apesar disso, configurações no *switch* e na interface virtual do VMware para fazer *port mirror* não foram explicadas (mas também não envolve conhecimentos sobre o Packetfence, mas sobre dispositivos de rede de cada fabricante e virtualização) (INVERSE, 2021a).

Nenhuma condição para criar regras de autorização com AD como fonte foi exemplificada na documentação e inicialmente não foi consultado o fórum sobre como fazê-lo. Primeiramente foi feito a regra com o atributo *Member Of*, mas o *host* não foi enviado para a VLAN devida. Alterando para o atributo "uid"e usando o operador "*is member of*"o *VLAN enforcement* foi feito corretamente.

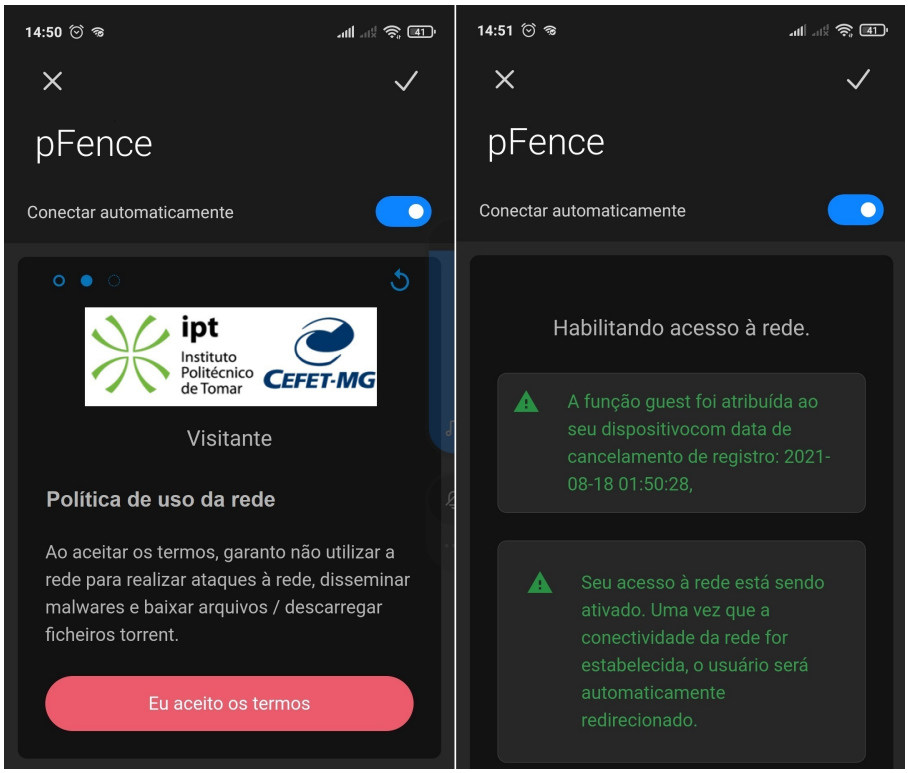
5 Resultados Obtidos

Nesta seção está documentada o resultado de testes feitos de acesso à rede para visitantes, autenticação para alunos e professores com *captive portal* e autenticação para adiministrador com 802.1X. No caso específico de alunos e professores foram testados também o isolamento do usuário por *scan* indevido, uso de aplicações P2P e não detecção de antivírus em SO Linux e Windows.

5.1 Acesso para visitante

Neste teste foi usado um *node* com SO Android e conectou-o no SSID "pFence"do AP para ter acesso à rede de registo. Após receber o endereço IP, o utilizador foi apresentado à página do *captive portal* aceitou-se os termos de uso e a autorização é feita como pode ser observado na Figura 32.

Figura 32 – Acesso de visitante

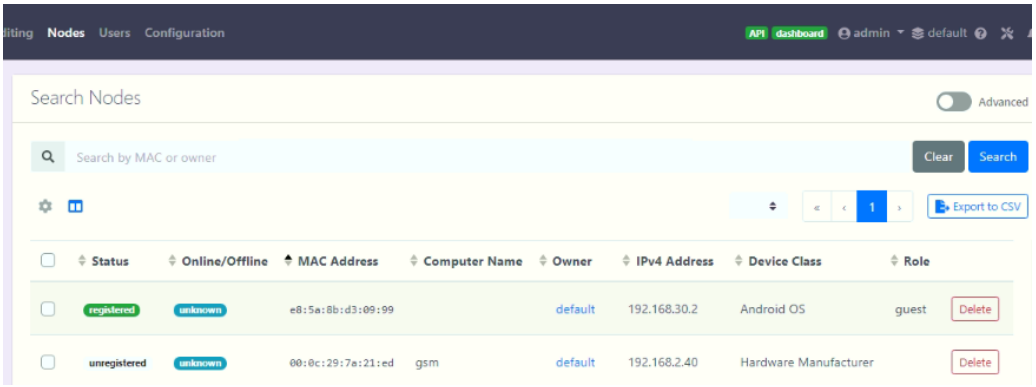


Fonte: Autoria própria

Como resultado, o *host* foi enviado corretamente à VLAN *guest*, além de ter sido identificado

o SO do *node* Android e atualizado o novo IP na lista de *nodes* do Packetfence como pode ser atestado na Figura 33.

Figura 33 – Lista de *nodes*



Fonte: Autoria própria

5.2 Acesso para alunos e professores com avaliação

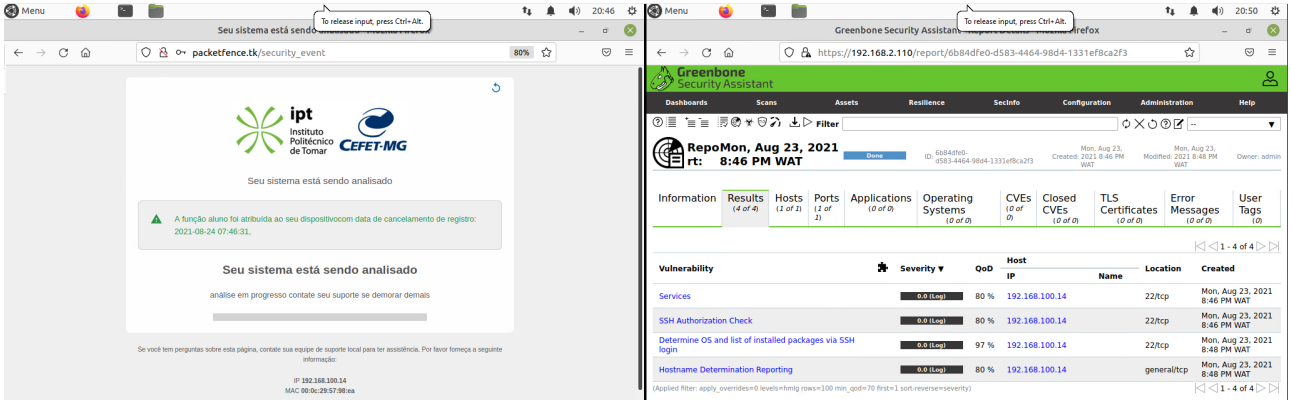
Nesta seção foi feito um teste o qual inicialmente o *host* tenta se autenticar na rede sem possuir antivírus instalado ou tem alguma vulnerabilidade e, ao ser isolado, tenta se remediar, verificando ao final se foi conduzido à VLAN correta. Três testes foram executados referentes ao processo de avaliação do *host* antes de dar acesso à rede: um de *scan* em *host* Linux e outro em *host* Windows, e um teste para identificar quando o *scan* falha.

***Scan* com acesso local à maquina em *host* Linux**

Foi usado um computador com SO Linux para fazer acesso à rede com a credencial do tipo aluno, inicialmente sem antivírus. A Figura 34 mostra a tela que aparece ao usuário quando o *scan* inicia e o resultado do *scan* do GVM, indicando que não foi encontrado nenhuma *Application*, ou aplicação, daquelas definidas no *scan* para antivírus e por conta disso o usuário é redirecionado para a página WEB do *captive portal* de remediação, que está na Figura 35.

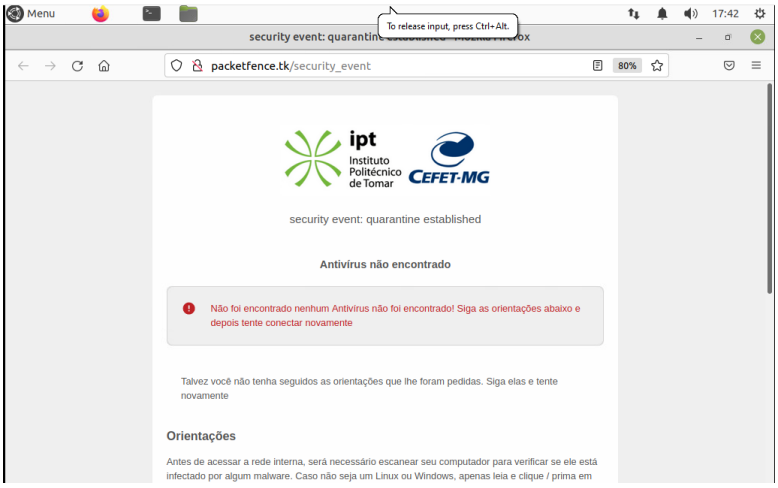
Após instalar o ClamAV, iniciou-se um novo *scan* ao clicar no botão "Conectar novamente"ao final página WEB do *captive portal* anteriormente citada e o resultado do GVM indica que foi identificado a aplicação, como mostra a Figura 36, e por isso o *host* foi redirecionado à VLAN interna.

Figura 34 – Página WEB do *captive portal* de *scan* (à esquerda) e o resultado dele no GVM em um *host* Linux sem antivírus (à direita)



Fonte: Autoria própria

Figura 35 – Página WEB do *captive portal* de isolamento por falta de antivírus em um *host*



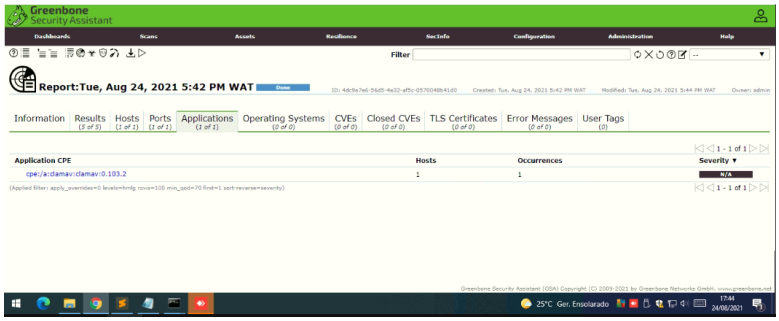
Fonte: Autoria própria

***Scan* com acesso local à maquina em *host* Windows**

Agora com um computador com SO Windows, foi feito o acesso à rede com a credencial do tipo professor, também sem antivírus inicialmente. Ao solicitar o *scan*, o resultado é que nenhum antivírus foi encontrado, como mostra a Figura 37 e por isso foi enviado à quarentena.

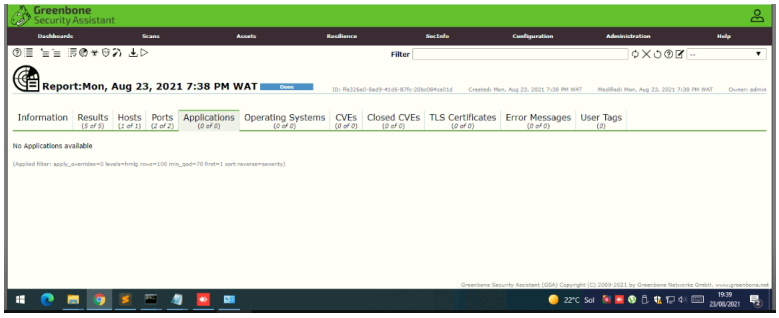
Após instalar o antivírus AVG, seguiu-se o mesmo processo da seção 5.2 e o resultado do GVM indica que foi identificado a aplicação do AVG, como mostra a Figura 38, e por isso o *host* foi redirecionado à VLAN interna.

Figura 36 – Resultado *scan* no GVM para o dispositivo Linux com o antivírus ClamAV instalado



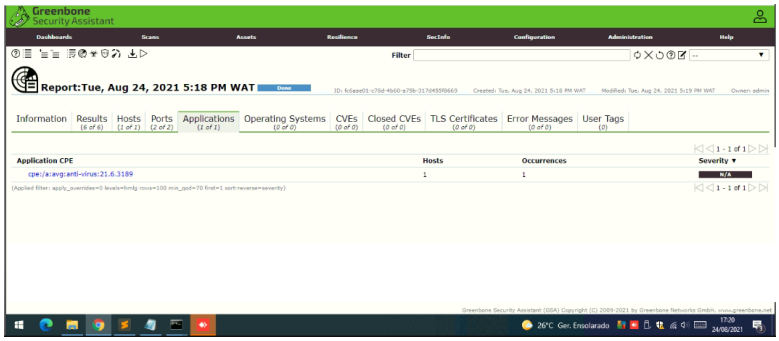
Fonte: Autoria própria

Figura 37 – Resultado *scan* no GVM para em um *host* Windows sem antivírus



Fonte: Autoria própria

Figura 38 – Resultado *scan* no GVM em um *host* Windows com o antivírus AVG instalado



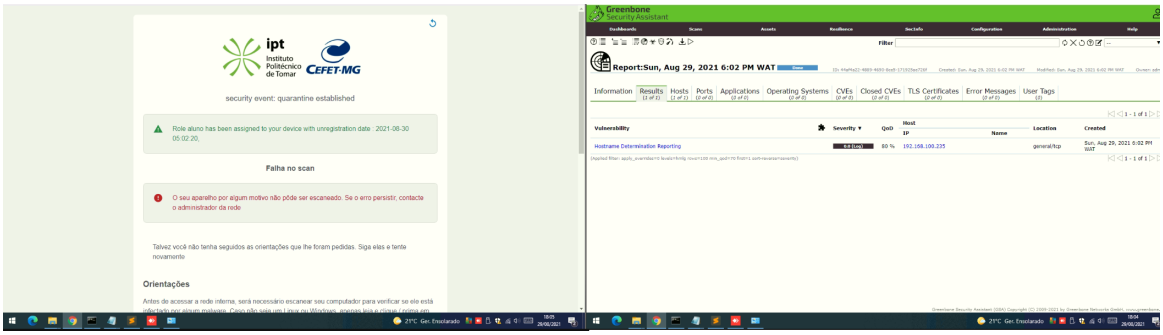
Fonte: Autoria própria

Identificação de falha no *scan*

Para isso, depois solicitar acesso à rede interna quando é feito o *scan*, propositadamente foi desconectado a interface de rede do *host* por 2 minutos e reconectado novamente (simulando uma desconexão acidental com a rede).

Como resultado, o GVM obteve apenas um resultado no seu *scan*, enquanto que aqueles que identificaram antivírus em *hosts* Windows e Linux obtiveram, respectivamente, seis e cinco resultados (como o teste acesso por SSH mostrado no seção 5.2 e por isso foi considerado que o *scan* não foi completo, e por fim o *host* é direcionado à VLAN de isolamento e a ele foi apresentado a página WEB do *captive portal* (mesmo com o antivírus instalado), como mostra a Figura 39.

Figura 39 – Página WEB do *captive portal* de isolamento por falha no *scan* do *host* (à esquerda) e o resultado do *scan* incompleto (à direita)



Fonte: Autoria própria

Após garantir a conectividade do *host* à rede, seguiu-se o mesmo processo da seção 5.2 e ele foi redirecionado à VLAN interna.

5.3 Monitoramento com Suricata

Nesta subseção três testes foram elaborados para detectar eventos dos Suricata que indicam não conformidades com a PSI: detecção *malware*, *scan* não autorizado e uso de aplicação *torrent* como aplicação p2p. Neste trabalho, o relógio do Suricata está uma hora antecipado, por isso nas imagens que estão nesta seção nota-se pelo menos uma hora de diferença em relação ao *host* ou ao Packetfence.

5.3.1 Detecção de aplicação P2P

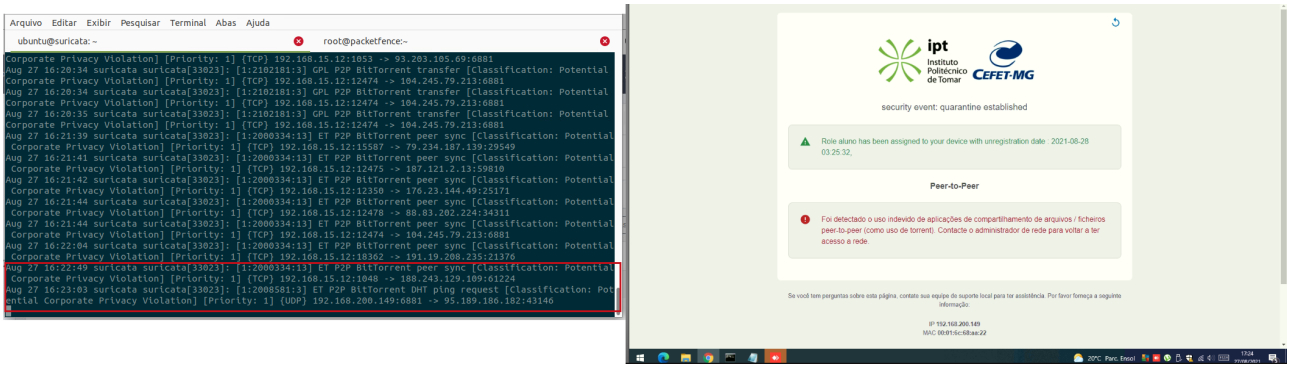
Foi usado o programa µTorrent como a aplicação P2P, que apesar de ser possível usa-lo para baixar conteúdos frutos de pirataria, existem aqueles que podem ser baixados legalmente. Neste trabalho foi baixado um *torrent* do CentOS, uma distribuição Linux que oferece essa opção como *download* sem nenhum problema legal, para ser detectado no Suricata e o Packetfence enviar o *host* para a VLAN de quarentena.

Na Figura 40 temos os *logs* do Suricata identificando pacotes de aplicações P2P sendo baixados do *host* com o endereço IP 192.168.15.14 e especificamente dentro do retângulo vermelho,

observa-se um resultado inesperado, foi detectado ainda um pacote baixado pela aplicação, entretanto com o endereço IP 192.168.200.149 (ou seja, já está na VLAN de isolamento), mas após isso esse tráfego indesejado parou. Além disso há a página WEB do *captive portal* informando que o usuário está na quarentena e que só será redirecionado à VLAN correta após entrar em contato com o administrador da rede.

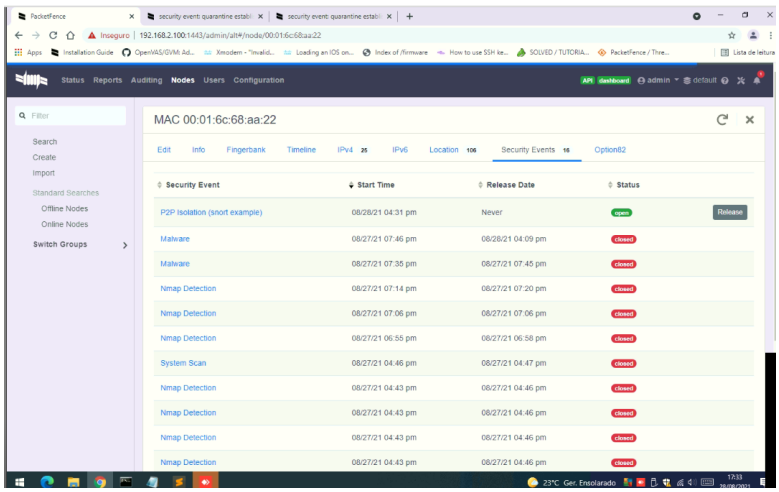
Na Figura 41 mostra a visão do administrador da rede após ser avisado de que um *host* foi detectado usando aplicação P2P. Após clicar no botão *Release*, o *host* foi redirecionado a VLAN correta.

Figura 40 – Suricata identificando tráfego de pacotes de uma aplicação P2P (à direita) e página de isolamento por detecção de aplicação P2P (à esquerda)



Fonte: Autoria própria

Figura 41 – Visão do administrador da rede em relação à lista de *security events* ativados a um *host* específico

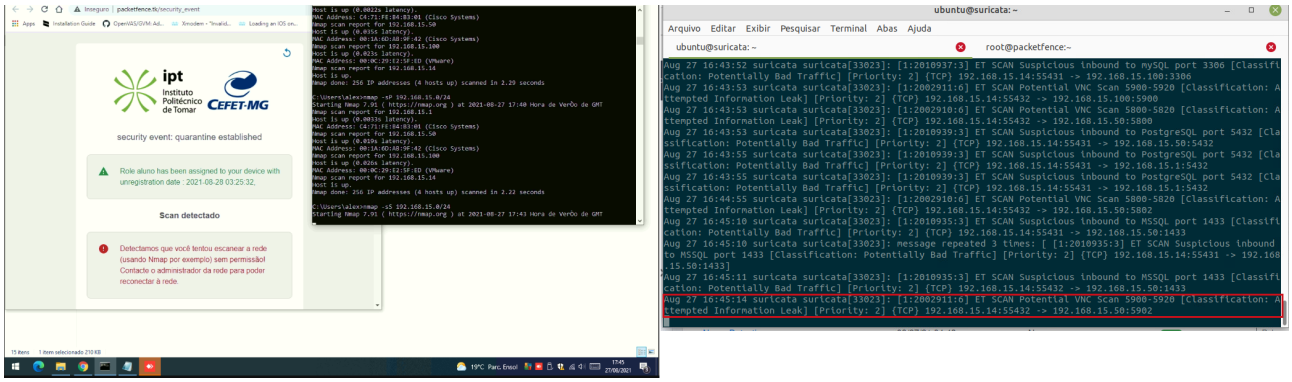


Fonte: Autoria própria

5.3.2 Detecção de *scan* não autorizada

Foi usado o Nmap como programa para fazer *scan* de portas na rede, sem autorização do administrador (de endereço IP 192.168.15.14). Como resultado, o Suricata detectou a atividade na rede, como mostra o texto dentro do retângulo vermelho na Figura 42, além de poder ser visto a página de isolamento do *captive portal* e o comando do Nmap que foi utilizado. Outro resultado interessante é que após o isolamento, o *scan* não foi completado mesmo depois de 30 minutos, sendo que o mesmo comando feito pelo administrador da rede demorava aproximadamente 30 segundos.

Figura 42 – Página WEB do *captive portal* de isolamento por detecção de *scan* não autorizada, com o comando de Nmap (à esquerda) e o Suricata identificando *scan* na rede (à direita)



Fonte: Autoria própria

Ao final, assim como feito no subseção 5.3.1, o *host* foi fechado a evento manualmente pelo administrador da rede e foi reenviado à VLAN correta.

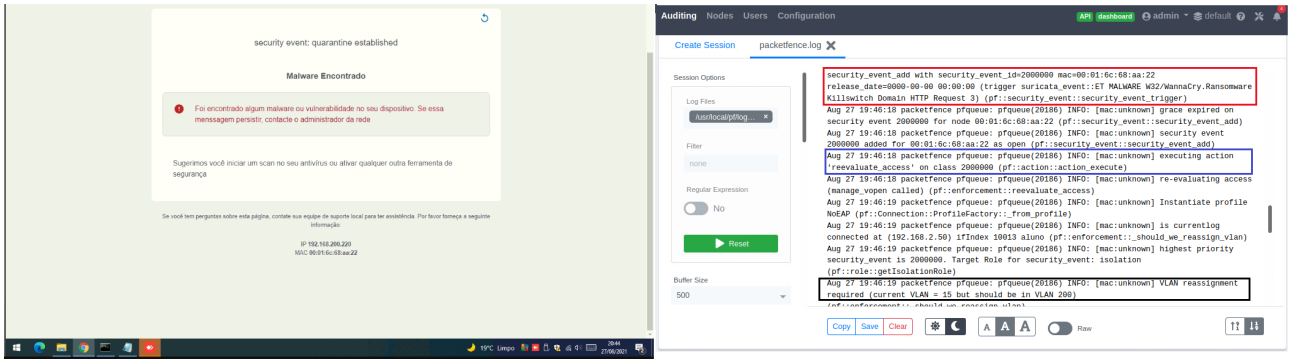
5.3.3 Detecção de *malware*

Para não colocar a rede e os *nodes* usados no trabalho em risco, não foi usado um computador infectado com um *malware* para testar essa detecção, por isso usou-se o comando *logger* do Linux, que cria entradas que passam pelas regras do servidor Syslog, no Suricata e verificar se um *log* foi gerado, enviado ao Packetfence e ativando o evento de segurança criado. Para isso, foi usado o texto de uma das regras referentes ao WannaCry que existe no Suricata junto com o IP do *host* que foi indiciado como aquele que estaria infectado pelo *malware* (no caso, o IP era 192.168.15.15) a partir do comando "*logger -i -t suricata '[1:2024300:6] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3 [Classification: Attempted Information Leak] [Priority: 2] TCP 192.168.15.15:55433 -> 192.168.15.1:5910'*".

O resultado pode ser visto na Figura 43 o qual mostra os *logs* do Packetfence, onde o texto dentro do retângulo vermelho indica que o *malware* WannaCry foi identificado, no retângulo azul uma

ação de reavaliar o *host* após o *security event* do ID 2000000 (referente ao evento de *malware*), e no retângulo preto, indicando que o *host* deve ser enviado à VLAN 200 (isolamento) e por fim, o usuário é apresentado à página WEB do *captive portal* de *scan*, confirmando que ele está em isolamento.

Figura 43 – *Logs* do Packetfence ao ser notificado pelo Suricata que existe um *host* infectado por *malware*

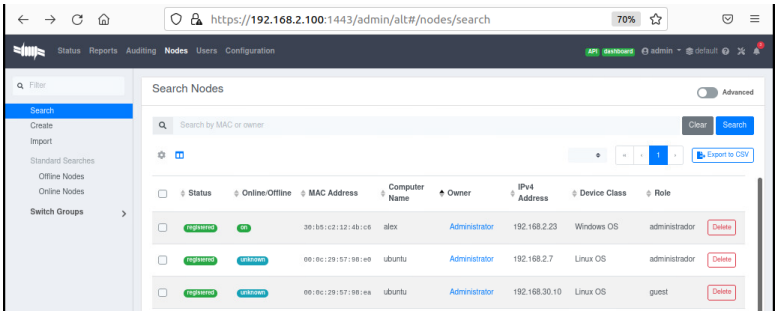


Fonte: Autoria própria

5.4 Acesso para administrador

Foi testados três tentativas de acesso com a mesma credencial do tipo administrador de rede: Um sem EAP, outro como Ethernet-EAP (EAP com fio) e outro com Wireless-EAP (EAP sem fio, pelo SSID "RADIUS-AUTH"). O resultado foi como esperado, a autenticação feita através do *captive portal* (no caso desse trabalho, que não utiliza EAP) envia o *host* para VLAN de visitante, enquanto as outras com 802.1X enviam o para a VLAN de administrador, como mostra a Figura 44.

Figura 44 – Lista de *nodes* do Packetfence com as três tentativas de autenticação com credenciais de administrador



Fonte: Autoria própria

5.4.1 Visão geral do resultado dos testes

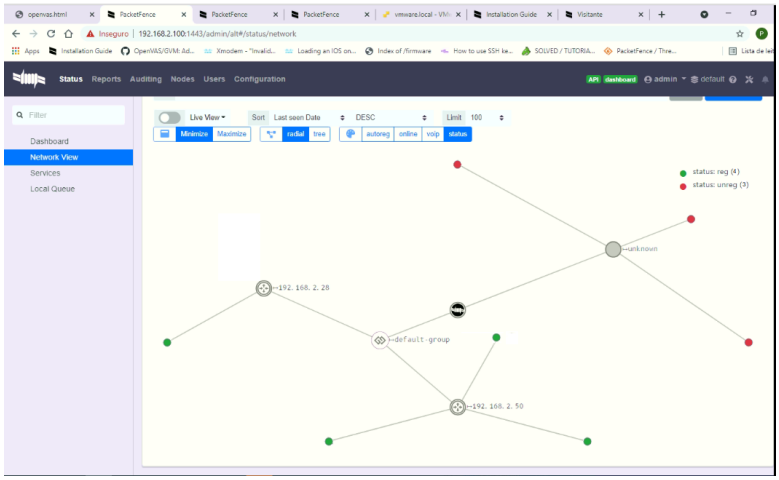
Após todos os testes feitos nesta seção, nota-se que os seguintes resultados:

- Detecção de *nodes*, inclusive do seu SO pelo Fingerbank (necessário para realização de *scan* com acesso local via SSH se for Linux ou SMB se for Windows);
- Autenticação e autorização feitas nos testes de acesso para visitante, aluno, professor e administrador, usando EAP (com 802.1X) e não EAP (com *captive portal*) como mostra a Figura 45, uma das interfaces que fornece visibilidade da rede ao administrador junto com na página WEB do Packetfence da lista *nodes* referênciada nas subseções 5.1 e 5.4 e do diagrama de rede com os dispositivos de redes e *nodes* registrados, como mostra a figura Figura 46;

Figura 45 – Visão geral do resultado dos testes feitos

Fonte: Autoria própria

Figura 46 – Diagrama da rede pelo Packetfence



Fonte: Autoria própria

- Avaliação feita pelo GVM para verificar se o *host* tem um antivírus antes de entrar na rede de alunos e professores;
- Monitoramento da rede feito pelo Suricata para detectar *malware*, uso de aplicação P2P e *scan* não autorizado;
- Registro e isolamento foi realizado pelo Packetfence através dos *security events*;

6 Conclusão

Foi possível neste trabalho reunir informações para detalhar o conceito do que é um NAC, que foram necessárias para chegar ao objetivo de implementar essa solução com o Packetfence, integrando outras ferramentas auxiliares, sendo ela de baixo custo (com o gasto de apenas uma licença vitalícia do Windows Server), que aplique uma PSI a partir da integração com o Suricata, Fingerbank e o GVM, sendo esse último a principal contribuição deste trabalho, que já não funcionava, e assim forneça segurança à rede para mitigar os riscos e implementar a política de BYOD nas PMEs. Além disso, foi identificado o suporte a dispositivos de redes de dezenas fabricantes pelo Packetfence.

A documentação não é detalhista o suficiente para pessoas com pouca ou nenhuma experiência em NACs, mesmo o fórum sendo ativo e ter sido possível encontrar respostas a alguns dos problemas enfrentados, visto as dificuldades que houveram durante o desenvolvimento, o que comprometeria o objetivo de ter uma solução de fácil configuração. Porém, foi possível soluciona-los e fornecer mais detalhes para configurar a solução e por isso, acredita-se que a consulta deste trabalho em conjunto da documentação oficial e o fórum do Packetfence contorna o problema e facilite a configuração por essas pessoas.

Apesar da exigência de antivírus para aceder às VLANs de aluno e professor, não há a garantia que o utilizador mantenha o *software* activo após isso, o que aumenta o risco de infecção por *malware* durante o tempo em que o dispositivo está registado, portanto seria interessante descobrir uma forma de ter um monitoramento constante da presença desse programa nos computadores conectados.

Além disso, ainda há outras que podem ser integradas, como *firewall*, para determinar os pacotes que podem ser transmitidos entre a rede interna e externa por exemplo, ou o uso de Mobile Device Manager, um *software* que é instalado no dispositivo móvel para constantemente monitora-lo, sem a necessidade de estar conectado à rede interna.

Também é possível o uso de provisioner, que configura automaticamente um *host* sem fio para acessar um SSID, mesmo estando escondido, principalmente para facilitar conexões do tipo EAP-TLS, que exige certificado tanto do Packetfence quanto do *host* que tenta acesso à rede, reduzindo as chances de pessoas não autorizadas, mas que obtiveram sem o consentimento da empresa à credenciais de autenticação, a terem acesso à rede interna e, consequentemente, aumentando a segurança.

Em relação ao custo da solução, ela pode ser reduzida ainda mais com a implementação de outros serviços de diretórios, como o Samba 4, que pode substituir o Active Directory e dispensar o gasto com uma licença de Windows Server.

Outra tarefa interessante que poderia ser realizado é incluir nos ficheiros alterados e criados nesse trabalho na integração entre o GVM e o Packetfence, além de criar um *script* para que possa ser feito o *scan* com acesso local às maquinas macOS.

Referências

ABOBA, B. et al. *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*. IETF, 2003. Disponível em: <https://tools.ietf.org/html/rfc3579#section-2>. Citado na página 26.

AGUIAR, E. *PMEs: o que são as pequenas e médias empresas?* 2021. Disponível em: <https://www.cnnbrasil.com.br/business/2021/05/26/saiba-o-que-sao-pmes>. Citado na página 16.

BLUEFIRESTORM. *installing macOS mojave 10.14 from dmg file on vmware*. VMware, 2019. Disponível em: <https://communities.vmware.com/t5/VMware-Workstation-Pro/installing-macOS-mojave-10-14-from-dmg-file-on-vmware/td-p/468492#.YSa75Pxz9o0.link>. Citado na página 58.

BONUCCELLI, G. *Learn what is BYOD (Bring Your Own Device) ?* 2016. Disponível em: <https://www.parallels.com/blogs/ras/what-is-byod/>. Citado na página 41.

BRADLEY, J. et al. *BYOD: A Global Perspective*. [S.l.], 2012. (Survey Report). Disponível em: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf>. Citado na página 17.

CHANG J. MORRIS, H. P.-C. C. T.-C. Securing byod. *IT Professional*, v. 16, n. 5, p. 9 – 11, 2014. ISSN 15209202. Disponível em: <http://search-ebscohost-com.ez107.periodicos.capes.gov.br/login.aspx?direct=true&db=iih&AN=98573165&lang=pt-br&site=ehost-live>. Citado nas páginas 15 e 41.

CID, D. B. *Identificação Passiva de Sistemas Operacionais*. 2003. Disponível em: <http://www.cesarkallas.net/arquivos/apostilas/identificacao_passiva_so.pdf>. Citado na página 48.

CISCO. *Configurar o ajuste da autenticação da porta do 802.1x em um interruptor*. 2019. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/smb/switches/cisco-250-series-smart-switches/smb3202-configure-8021x-port-authentication-setting-on-a-switch.html>. Citado na página 25.

CISCO. *Configurar o ajuste da autenticação da porta do 802.1x em um interruptor*. 2019. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/smb/switches/cisco-250-series-smart-switches/smb3202-configure-8021x-port-authentication-setting-on-a-switch.html>. Citado na página 25.

COMES luca. *Syslog*. SourceForge, 2018. Disponível em: <https://sourceforge.net/p/packetfence/mailman/packetfence-users/thread/VI1PR0701MB23345E3E055163CF7415B1C9DFDC0%40VI1PR0701MB2334.eurprd07.prod.outlook.com/#msg35915066>. Citado na página 55.

COMES luca. *Lsc_user_exe_create: Failed to execute makensis*. Greenbone, 2019. Disponível em: <https://community.greenbone.net/t/lsc-user-exe-create-failed-to-execute-makensis/1413/2?u=gabrielos>. Citado na página 58.

COMPUGRAF. *Segurança da Informação minimiza riscos e preserva dados organizacionais*. 2013. Disponível em: <https://www.compugraf.com.br/seguranca-da-informacao-minimiza-riscos-e-preserva-dados-organizacionais/>. Citado nas páginas 31 e 32.

CUSTOIAS, G. B.; MENDONçA, L. B.; CUNHA, D. V. Estudo sobre solução tecnológica para a mitigação dos riscos cibernéticos no setor financeiro. Universidade Presbiteriana de Mackenzie, 2020? Disponível em: <http://dspace.mackenzie.br/handle/10899/20083>. Citado na página 49.

DIAS, D. *VLAN – Trunk utilizando 802.1q (dot1q)*. 2012. Disponível em: <http://labcisco.blogspot.com/2016/02/configuracao-de-multi-ssid-no-cisco.html>. Citado na página 21.

DILLARD, J. *Sistemas de Detecção de Intrusão*. 2020. Disponível em: <https://www.garlandtechnology.com/blog/the-101-series-out-of-band-vs-inline-network-security>. Citado na página 37.

ELIAS, G.; LOBATO, L. C. Arquitetura e protocolos de rede tcp-ip. In: ____. 2.2.1. ed. [S.l.]: Rede Nacional de Ensino e Pesquisa, 2013. cap. 1, p. 2–6. Citado na página 18.

ENTERASYS. *Understanding Network Access Control*. 2009. Disponível em: <https://www.techdata.ca/techsolutions/networking/files/feb2009/Enterasys%20NAC%20Planning%20Guide.pdf>. Citado na página 43.

EXTREME. *ExtremeControl Technical Specifications*. 2021. Disponível em: <https://cloud.kapostcontent.net/pub/9413dcb9-5cc4-4f56-bbd5-0aa10b28be38/extreme-access-control-ds-1.pdf>. Citado na página 42.

FARIA, F. et al. *The Financial Impact of BYOD*. [S.l.], 2013. (Economic Analysis). Disponível em: <https://www.cisco.com/c/dam/global/ru_ua/assets/pdf/byod-economics_econ_analysis.pdf>. Citado nas páginas 15, 17, 38, 39 e 40.

FORESCOUT. *CounterACT Datasheet*. 2019. Disponível em: <https://www.forescout.com/company/resources/forescout-counteract-datasheet/>. Citado na página 44.

FOROUZAN; A., B. Comunicação de dados e rede de computadores. In: ____. 4. ed. [S.l.]: AMGH Editora Ltda, 2008. cap. 14.1, p. 421–422. Citado nas páginas 19, 20 e 22.

FOROUZAN; A., B. Comunicação de dados e rede de computadores. In: ____. 4. ed. [S.l.]: AMGH Editora Ltda, 2008. cap. 2.2, p. 29–30. Citado na página 21.

FOROUZAN; A., B. Comunicação de dados e rede de computadores. In: ____. 4. ed. [S.l.]: AMGH Editora Ltda, 2008. cap. 2.2, p. 33. Citado na página 23.

FOROUZAN; A., B. Comunicação de dados e rede de computadores. In: ____. 4. ed. [S.l.]: AMGH Editora Ltda, 2008. cap. 1.4, p. 19. Citado na página 26.

FOROUZAN; A., B. Comunicação de dados e rede de computadores. In: ____. 4. ed. [S.l.]: AMGH Editora Ltda, 2008. cap. 28.2, p. 879. Citado na página 31.

FORTINET. *FortiNAC Data Sheet*. 2021. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf>. Citado na página 44.

FOUNDATION, O. S. G. *Authentication with LDAP*. 2021. Disponível em: <https://docs.geoserver.org/stable/en/user/security/tutorials/ldap/index.html>. Citado na página 36.

FREENAC. *FreeNAC*. 2013. Disponível em: <https://github.com/Boran/freenac>. Citado na página 46.

GEER, D. Whatever happened to network-access-control technology? *Computer*, v. 43, n. 9, p. 13–16, 2010. Citado na página 16.

GILLIS, A. S. *IEEE 802 wireless standards*. 2020. Disponível em: <https://searchnetworking.techtarget.com/reference/IEEE-802-Wireless-Standards-Fast-Reference>. Citado na página 23.

GOMES, K. Alemanices: O drama do download proibido. *Deutsche Welle*, 6 2017. Disponível em: <https://www.dw.com/pt-br/alemanices-o-drama-do-download-proibido/a-39181185>. Citado na página 33.

GONçALVES, A. P. J. Suporte à decisão para avaliação de soluções byod. Universidade de Lisboa, 2017. Disponível em: <https://repositorio.ul.pt/bitstream/10451/28247/1/ulfc121989_tm_Ana_Paula_Gonçalves.pdf>. Citado na página 49.

GUPTA, U. *Security Challenges BYOD Presents*. 2011. Disponível em: <https://www.bankinfosecurity.com/security-challenges-byod-presents-a-4258>. Citado na página 41.

HENRIQUE, S.; BRITO, B. *Configuração de Multi-SSID no Cisco Aironet via CLI*. 2016. Disponível em: <http://labcisco.blogspot.com/2016/02/configuracao-de-multi-ssid-no-cisco.html>. Citado na página 22.

HOFFMANN, A.; WONZOSKI, F.; RIVEROS, L. J. M. *SERVIDOR DE DIRETÓRIO COMO AUXILIAR NA GESTÃO DAS INFORMAÇÕES, USUÁRIOS E COMPUTADORES*. 2017. Disponível em: <https://core.ac.uk/download/pdf/235133471.pdf>. Citado na página 35.

ILLUMIO. *What Is Network Access Control (NAC)?* 2021. Disponível em: <https://www.illumio.com/cybersecurity-101/network-access-control-nac>. Citado na página 42.

INFOEXPRESS. *CyberGatekeeper*. 2018? Disponível em: <https://www.infoexpress.com/copy-of-cgx>. Citado na página 44.

INFOSEC, G. *O que é scanner de vulnerabilidade, importância e como integrar*. 2021. Disponível em: <https://www.gat.digital/blog/o-que-e-scanner-de-vulnerabilidade-importancia-e-como-integrar/>. Citado na página 36.

INFOWATCH. *A Study on Global Data Leaks in H1 2018*. [S.l.], 2018. (Data Breach Report). Disponível em: <https://infowatch.com/sites/default/files/report/analytics/Data_Breach_Report_Global_Data_Leaks_H1_2018.pdf>. Citado nas páginas 15 e 41.

INVERSE. *Documentation*. 2021. Disponível em: <https://www.packetfence.org/support.html#/documentation>. Citado nas páginas 17, 55, 56 e 65.

INVERSE. *Fingerbank - Devices index*. 2021. Disponível em: <https://api.fingerbank.org>. Citado na página 48.

JUNIOR, J. R. *OpenLDAP: a chave é a centralização*. Viva o Linux, 2008. Disponível em: <https://www.vivaolinux.com.br/artigo/OpenLDAP-a-chave-e-a-centralizacao?pagina=1>. Citado na página 35.

KASPERSKY. *Incident Response*. [S.l.], 2018. (Statistics). Disponível em: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/08/29102608/Incident-Response-Analytics-Report_EN.pdf>. Citado na página 32.

KASPERSKY. *Aprenda sobre malware e como proteger todos os seus dispositivos contra eles*. 2021. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>. Citado na página 32.

KROHN, K.; CUNHA., N. A. da. *Padrão Ethernet*. Disponível em: <https://wiki.sj.ifsc.edu.br/images/8/88/IER2014-2-PadraoEthernet_Kris_Nivaldo.pdf>. Citado na página 29.

LEAL, R. *O que é a ISO 27001?* Advisera, 2021. Disponível em: <https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/>. Citado na página 31.

LONVICK, C. *The BSD syslog Protocol*. Cisco System, 2001. Disponível em: <https://www.ietf.org/rfc/rfc3164.txt>. Citado na página 30.

MANAGEENGINE. *What is SNMP*. 2021. Disponível em: <https://www.manageengine.com/network-monitoring/what-is-snmp.html>. Citado na página 30.

MANAGER, T. *O que é SNMP?* 2021. Disponível em: <https://www.telcomanager.com/blog/o-que-e-snmp/>. Citado na página 31.

MDM, S. *The Challenges Of A Bring Your Own Device (BYOD) Policy*. 2020. Disponível em: <https://simplemdm.com/challenges-of-bring-your-own-device-byod-policy/>. Citado na página 41.

MICHAEL. *Router on a stick*. 2012. Disponível em: <https://networkguy.de/router-on-a-stick/>. Citado na página 23.

MICHAEL. *Linha de Switches Gerenciáveis Intelbras*. Bradel Distribuição, 2017. Disponível em: <https://blogbradel.wordpress.com/2017/04/26/linha-de-switches-gerenciaveis-intelbras/>. Citado na página 22.

MICHEL, N. Redes de computadores ii. In: ____. Universidade Tecnológica Federal do Paraná, 2013. cap. 1.1, p. 17. Disponível em: <http://proedu.rnp.br/bitstream/handle/123456789/1551/Redes_computadores_II_ISBN.pdf?sequence=1&isAllowed=y>. Citado na página 22.

MSP, S. *Common BYOD Challenges*. 2020. Disponível em: <https://www.solarwindsmsp.com/blog/common-byod-challenges>. Citado na página 41.

NETGEAR. *What is the captive portal and how does it work with my managed switch?* 2016. Disponível em: <https://kb.netgear.com/22006/What-is-the-captive-portal-and-how-does-it-work-with-my-managed-switch>. Citado na página 35.

NMAP. *Nmap: the Network Mapper - Free Security Scanner*. 2020? Disponível em: <https://nmap.org>. Citado na página 32.

NUNOO-MENSAH, H.; AKOWUAH, E.; BOATENG, K. A review of opensource network access control (nac) tools for enterprise educational networks. *International Journal of Computer Applications*, v. 106, p. 975–8887, 12 2014. Citado na página 46.

OPENNAC. *OpenNAC*. 2019. Disponível em: <http://www.opennac.org/opennac/en.html>. Citado na página 46.

PACKETFENCE Overview. 2021. Disponível em: <https://www.packetfence.org/about.html>. Citado nas páginas 15, 43, 44 e 46.

PERINI, V. L. Integração de ferramentas de administração e segurança byod. Universidade de Caxias do Sul, 2017. Disponível em: <https://repositorio.ucs.br/xmlui/handle/11338/3735>. Citado na página 49.

PIEROBON, F. M. *Cisco ISE — Autenticação MAB e 802.1X*. 2020. Disponível em: <https://medium.com/techrebels/cisco-ise-mab-e-802-1x-fba5319759d3>. Citado na página 25.

PINTO, P. *DHCP Poisoning*. Pplware, 2014. Disponível em: <https://pplware.sapo.pt/microsoft/windows/redes-vamos-conhecer-melhor-o-servico-dhcp/>. Citado nas páginas 28 e 30.

PROOF. *WannaCry: o primeiro ransomworm na indústria de cibersegurança*. 2017. Disponível em: <https://www.proof.com.br/2017/05/29/wannacry-ransomworm/>. Citado na página 42.

RAPID7. *InsightVM*. 2020? Disponível em: <https://www.rapid7.com/products/insightvm/>. Citado na página 47.

REBELLO, G. A. F. et al. *Sistemas de Detecção de Intrusão*. Universidade Federal do Rio de Janeiro, 2016. Disponível em: <https://www.gta.ufrj.br/grad/16_2/2016IDS/conceituacao.html>. Citado nas páginas 35 e 36.

REMOALDO, P. *DNS - Domain Name System (ou Service)*. 1998. Disponível em: <https://paginas.fe.up.pt/~mgi97018/dns.html>. Citado na página 28.

RESILIENCE, G. S. *Scripting*. 2020. Disponível em: <https://gvm-tools.readthedocs.io/en/latest/scripting.html>. Citado na página 56.

RESILIENCE, G. S. *Test Now*. 2020. Disponível em: <https://www.greenbone.net/en/testnow/>. Citado na página 47.

ROBB, D. *Top 9 Network Access Control (NAC) Solutions*. 2021. Disponível em: <https://www.esecurityplanet.com/products/network-access-control-solutions/>. Citado nas páginas 16 e 43.

ROTONDARO, R. R. de A.; GUEDES, M. *Redes Locais Virtuais*. FEPESMIG, 2016. Disponível em: <http://repositorio.unis.edu.br/bitstream/prefix/534/1/REDES%20LOCAIS%20VIRTUAIS.pdf>. Citado nas páginas 20, 23 e 24.

SANTOS, W. D. Políticas de uso e segurança da informação: um estudo sobre aplicação byod - bring your own device. Universidade Tecnológica Federal do Paraná, 2017. Disponível em: <http://repositorio.utfpr.edu.br/jspui/bitstream/1/19361/2/CT-TELECOM-III-2018-07.pdf>. Citado na página 49.

SATRAN, M. et al. *Windows Management Instrumentation*. Microsoft, 2018. Disponível em: <https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>. Citado na página 47.

SATRAN, M. et al. *Windows Management Instrumentation*. Microsoft, 2018. Disponível em: <https://jumpcloud.com/blog/whats-better-than-active-directory>. Citado na página 48.

SECURITY, N. *Radius*. 2019. Disponível em: <https://www.networxsecurity.de/glossary-d1/r-d1/radius-d1/>. Citado na página 27.

SNORT. *Snort 3.1.0.0 on Ubuntu 18 & 20*. 2021. Disponível em: <https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/008/108/original/Snort_3_on_Ubuntu_18_and_20.pdf>. Citado na página 47.

SOLUTIONS, S. O. *Security Onion Documentation*. 2021. Disponível em: <https://docs.securityonion.net/en/2.3/index.html>. Citado na página 47.

SPLENDORBITS. *OpenVAS Greenbone Vulnerability Scanner - Setup, Update, Scan on Kali Linux 2021*. 2021. Disponível em: <https://www.youtube.com/watch?v=_eLI8XuXf4I&t=228s>. Citado na página 47.

STREAMSCAN. *Cyberthreat Detection System*. 2021. Disponível em: <https://streamscan.ai/en/solutions/cyberthreat-detection-system>. Citado na página 46.

SURICATA. *Suricata User Guide*. 2019. Disponível em: <https://suricata.readthedocs.io/en/suricata-6.0.0/index.html>. Citado na página 47.

TANENBAUM, A. S. Redes de computadores. In: ____. 4. ed. [S.l.]: Prentice Hall, 2003. cap. 1.2.1, p. 29–30. Citado na página 19.

TECHNOLOGIES, V. *EAPoL – Extensible Authentication Protocol over LAN*. 2021. Disponível em: <https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/>. Citado na página 26.

TENABLE. *A Família Nessus*. 2021. Disponível em: <https://www.tenable.com/products/nessus>. Citado na página 47.

VIDENCENTER'S, T. *IEEE 802.1Q*. 20–. Disponível em: <http://mars.tekkom.dk/w/index.php/IEEE_802.1Q>. Citado na página 24.

Apêndices

APÊNDICE A – Script em Python para realizar o scan e avaliar o relatório

```python
# -*- coding: utf-8 -*-
# Copyright (C) 2019-2021 Greenbone Networks GmbH
#
# SPDX-License-Identifier: GPL-3.0-or-later
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.

from base64 import b64decode
import time
import datetime
import sys
import pytz
import subprocess
from argparse import Namespace
from gvm.protocols.gmp import Gmp
from gvm.protocols.gmpv208.entities.targets import get_alive_test_from_string

INTERVAL = 20

#verificar se tem os 7 argumentos
def check_args(args):
    len_args = len(args.script) - 1
    message = """
        This script starts a new scan on the given host.
        It needs one parameters after the script name.

        1. <host_ip>        IP Address of the host system
        2. <scan_config_id> Scan Config UUID for scanning the host system.
        3. <port_list_id>   Port List UUID for scanning the host system.
```

```
41          4. <mac>            Mac address of the host target
42          5. <os>             Operation System of the host target
43          6. <credential_id>  Credential UUID for scanning the host system.
44          7. <max_time>       Timeout of the scan in seconds
45
46                  Example:
47              $ gvm-script --gmp-username name --gmp-password pass \
48  ssh --hostname <gsm> scripts/scan-new-system.gmp.py <host_ip> <scan_config_id> \
49  <port_list_id> <mac> <os> <credential_id> <max_time>
50      """
51      if len_args != 7:
52          print(message)
53          sys.exit()
54
55  #cria o alvo do scan
56  def create_target(gmp, ipaddress, port_list_id, name, credential, os):
57      alive_test = get_alive_test_from_string("Consider Alive")
58      if (os == "linux") :
59          response = gmp.create_target(
60              name=name, hosts=[ipaddress], port_list_id=port_list_id, ssh_credential_id=credential,
                ↪  alive_test=alive_test
61          )
62      elif (os == "windows") :
63          response = gmp.create_target(
64              name=name, hosts=[ipaddress], port_list_id=port_list_id, smb_credential_id=credential,
                ↪  alive_test=alive_test
65          )
66      return response.get('id')
67
68  #cria scan
69  def create_task(gmp, target_id, scan_config_id, scanner_id, name):
70      response = gmp.create_task(
71          name=name,
72          config_id=scan_config_id,
73          target_id=target_id,
74          scanner_id=scanner_id,
75      )
76      return response.get('id')
77
78  #inicia scan
79  def start_task(gmp, task_id):
80      response = gmp.start_task(task_id)
81      return response[0].text
82
83  #recupera o relatório do scan
84  def get_report(gmp, report_id) -> str:
85      response = gmp.get_report(
```

```
86          report_id=report_id, report_format_id="a3810a62-1f62-11e1-9219-406186ea4fc5",
            ↪  filter_string="levels=hmlg"
87      )
88
89      report_element = response.find("report")
90      # get the full content of the report element
91      content = report_element.find("report_format").tail
92
93      #decodifica o relatório
94      report = b64decode(content)
95      return report.decode()
96
97  #verifica se o relatório está pronto a cada minuto e o retorna.
98  #se o tempo máximo de espera for atingido, encerra script com exit(1)
99  def wait_and_get_report(gmp, report_id, max_time, os) -> str:
100     for i in range(0,max_time+1, INTERVAL):
101         report = get_report(gmp, report_id)
102         #subprocess.run(["echo","{} segundos".format(i)])
103         for linha in report.split("\n") :
104             if "Scan ended" in linha:
105                 if "WAT" in linha :
106                     evaluation(gmp, os, report)
107         time.sleep(INTERVAL)
108     #subprocess.run(["echo","Scan não foi finalizado a tempo ou houve algum erro"])
109     sys.exit(1)
110
111 #avalia se o host é suspeito ou não
112 def evaluation(gmp, os, report) -> None:
113     #lista de antivírus suportados
114     antivirus = ["AVG AntiVirus Version Detection (Windows)", "Avast (Free / Business) AntiVirus
        ↪  Version Detection (Windows)"
115     , "ClamAV Version Detection"]
116
117     if "This report contains result 1 of" in report or "This report contains result 2 of" in report :
118         # Host não encontrado
119         sys.exit(1)
120     else :
121         #caso um dos antivírus tenha sido detectado, encerra script com exit(0)
122         #subprocess.run(["echo","Tem antivírus? reposta: {}".format(any(x in report for x in
            ↪  antivirus))])
123         sys.exit(0) if any(x in report for x in antivirus) else sys.exit(2)
124
125
126
127
128 def main(gmp: Gmp, args: Namespace) -> None:
129
130     #checa se todos os 7 argumentos foram enviados
```

```
131     check_args(args)
132
133     # recebe os argumentos
134     ipaddress = args.argv[1]
135     scan_config_id = args.argv[2]
136     port_list_id = args.argv[3]
137     os = args.argv[4]
138     mac = args.argv[5]
139     credential_id = args.argv[6]
140     max_time = int(args.argv[7])
141
142     #verifica se não é Windows ou Linux
143     if os == "other" :
144         # SO não suportado
145         sys.exit(3)
146
147     # cria um nome único para o scan, com data e hora + endereço MAC (Exemplo: 2021-06-01 16:32:18
        ↪  AA:BB:CC:DD:EE:FF)
148     tz = pytz.timezone('Europe/Lisbon')
149     name = "{} {}".format(str(datetime.datetime.now(tz=tz)),mac)
150
151     #criar alvo de scan e receber o seu ID (target_id)
152     target_id = create_target(gmp, ipaddress, port_list_id, name, credential_id, os)
153
154     openvas_scanner_id = '08b69003-5fc2-4037-a479-93b440211c73'
155     #criar scan e receber o seu ID (task_id)
156     task_id = create_task(
157         gmp,
158         target_id,
159         scan_config_id,
160         openvas_scanner_id,
161         name
162     )
163
164     #iniciar scan e receber o seu ID do relatório (report_id)
165     report_id = start_task(gmp, task_id)
166
167     #tenta obter o relatório no tempo máximo (max_time)
168     wait_and_get_report(gmp, report_id, max_time, os)
169     #exit(0) se o host for avaliado como seguro;
170     #exit(1) se não foi possível fazer o scan;
171     #exit(2) se não for seguro
172     #exit(3) se o SO não é suportado
173
174 if __name__ == '__gmp__':
175     # pylint: disable=undefined-variable
176     main(gmp, args)
```

APÊNDICE B – Modulo Perl openvas.pm

```
1  package pf::scan::openvas;
2
3  =head1 NAME
4
5  pf::scan::openvas
6
7  =cut
8
9  =head1 DESCRIPTION
10
11 pf::scan::openvas is a module to add OpenVAS scanning option.
12
13 =cut
14
15 use strict;
16 use warnings;
17
18 use Text::CSV;
19 use pf::log;
20 use MIME::Base64;
21 use Readonly;
22
23 use base ('pf::scan');
24
25 use pf::CHI;
26 use pf::constants;
27 use pf::constants::scan qw($SCAN_SECURITY_EVENT_ID $PRE_SCAN_SECURITY_EVENT_ID
   ↪  $POST_SCAN_SECURITY_EVENT_ID $STATUS_STARTED);
28 use pf::config qw(%Config);
29 use pf::util;
30 use pf::security_event;
31 use Time::HiRes qw(time);
32
33 sub description { 'Openvas Scanner' }
34
35 Readonly our $RESPONSE_OK                   => 200;
36 Readonly our $RESPONSE_RESOURCE_CREATED     => 201;
37 Readonly our $RESPONSE_REQUEST_SUBMITTED    => 202;
38
39 =head1 METHODS
40
41 =over
42
```

```
43  =item new
44
45  Create a new Openvas scanning object with the required attributes
46
47  =cut
48
49  sub new {
50      my ( $class, %data ) = @_;
51      my $logger = get_logger();
52
53      $logger->debug("Instantiating a new pf::scan::openvas scanning object");
54
55      my $self = bless {
56              '_id'               => undef,
57              '_ip'               => undef,
58              '_port'             => undef,
59              '_username'         => undef,
60              '_password'         => undef,
61              '_scanIp'           => undef,
62              '_scanMac'          => undef,
63              '_report'           => undef,
64              '_openvas_alertid'          => undef, #Guarda "Credential ID" ao em vez de "Alert ID"
65              '_openvas_configid'          => undef,
66              '_openvas_reportformatid'    => undef, #Guarda "Port List ID" ao em vez de "Report Format
                ↪  ID"
67              '_targetId'         => undef,
68              '_escalatorId'      => undef,
69              '_taskId'           => undef,
70              '_status'           => undef,
71              '_type'             => undef,
72              '_oses'             => undef,
73              '_duration'           => undef,
74              '_categories'         => undef,
75      }, $class;
76
77      foreach my $value ( keys %data ) {
78          $self->{'_' . $value} = $data{$value};
79      }
80
81      return $self;
82  }
83
84  =item startScan
85
86  That's where we use all of these method to run a scan
87
88  =cut
89
```

```
90  sub returnOS {
91      my ( $self ) = @_;
92      my $logger = get_logger();
93      my @oses = @{$self->{_oses} || [123]};
94      my $os = "other";
95
96      if($oses[0] == 5){
97          $os = "linux";
98      }elsif($oses[0] == 1){
99          $os = "windows";
100     }
101
102     $logger->warn("Os is $os");
103
104     return $os;
105 }
106
107 =item startScan
108
109 That's where we use all of these method to run a scan
110
111 =cut
112
113 #se startScan retornar 0 significa que o scan finalizado com sucesso, caso contrário indica que
    ↪ falhou
114 # e arquivo / ficheiro scan.pm irá acionar um evento de "scan_failed" e o host será isolado
115 sub startScan {
116     my ( $self ) = @_;
117     my $logger = get_logger();
118     my $scan_failed = 1;
119
120     my $user = $self->{_username};
121     my $pass = $self->{_password};
122     my $target_host = $self->{_scanIp};
123     my $scan_config_id = $self->{_openvas_configid};
124     my $port_list_id = $self->{_openvas_reportformatid};
125     my $os = $self->returnOS();
126     my $mac = $self->{_scanMac};
127     my $credential_id = $self->{_openvas_alertid};
128     my $max_time = substr($self->{_duration},0,-1);
129     my $scan_security_event_id = $pf::constants::scan::SCAN_SECURITY_EVENT_ID;
130     $scan_security_event_id = $pf::constants::scan::PRE_SCAN_SECURITY_EVENT_ID if
    ↪ (index($target_host, "192.168.200") != -1);
131
132     # /bin/perl                                          -> localização do comando Perl obtido a
    ↪ partir do comando which
133     # /usr/local/pf/gvm_script/request_and_trigger.pl    -> localização do script Perl que solicita o
    ↪ scan
```

```
134     system("/bin/perl /usr/local/pf/gvm_script/request_and_trigger.pl $user $pass $target_host
        ↪  $scan_config_id $port_list_id $os $mac $credential_id $max_time $scan_security_event_id &");
135
136     return;
137 }
138
139 =back
140
141 =head1 AUTHOR
142
143 Inverse inc. <info@inverse.ca>
144
145 =head1 COPYRIGHT
146
147 Copyright (C) 2005-2021 Inverse inc.
148
149 =head1 LICENSE
150
151 This program is free software; you can redistribute it and/or
152 modify it under the terms of the GNU General Public License
153 as published by the Free Software Foundation; either version 2
154 of the License, or (at your option) any later version.
155
156 This program is distributed in the hope that it will be useful,
157 but WITHOUT ANY WARRANTY; without even the implied warranty of
158 MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
159 GNU General Public License for more details.
160
161 You should have received a copy of the GNU General Public License
162 along with this program; if not, write to the Free Software
163 Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301,
164 USA.
165
166 =cut
167
168 1;
```

APÊNDICE C – Script em Perl para solicitar scan e acionar eventos de segurança

```
use lib qw(/usr/local/pf/lib);
use base ('pf::scan');
use pf::scan::openvas;
use pf::security_event;
use pf::log;

#argumentos
my ($user, $pass, $target_host, $scan_config_id, $port_list_id, $os, $mac, $credential_id, $max_time, $scan_security_event_id) = @ARGV;

my $logger = get_logger();
#  comando do GVM para solicitar o scan
# /usr/local/bin/gvm-script                         -> localização do comando gvm-script obtido a partir do comando which
# /usr/local/pf/gvmd.sock                           -> localização do socket criado pelo tunnel ssh
# /usr/local/pf/gvm_script/scan-new-system.gmp.py   -> localização do script Python (no Packetfence) a ser usado pelo GVM no scan
my $command = "/usr/local/bin/gvm-script --gmp-username $user --gmp-password $pass socket --socketpath /usr/local/pf/gvmd.sock /usr/local/pf/gvm_script/scan-new-system.gmp.py $target_host $scan_config_id $port_list_id $os $mac $credential_id $max_time";

#iniciar scan e esperar resposta
$logger->warn("Scanning ID $scan_security_event_id host $mac. Wait for $max_time seconds (Openvas)");
$logger->warn("command: $command (Openvas)");
my $result = system($command);

if( ($result/256) == 1 ) {
    #Aciona evento de scan que falhou
    print("failed scan \n");
    $logger->warn("Trigger a event to isolate the host $mac (Openvas). The scan failed");
    security_event_trigger( { 'mac' => $mac, 'tid' => 'openvas_scan_failed', 'type' => 'Custom' } );
}elsif( ($result/256) == 2 && ($os eq "windows" || $os eq "linux") ) {
    #Aciona evento de host sem antivírus
    print("no antivirus \n");
    $logger->warn("Trigger a event to isolate the host $mac (Openvas). No antivirus detected");
    security_event_trigger( { 'mac' => $mac, 'tid' => 'openvas_antivirus', 'type' => 'Custom' } );
}elsif( ($result/256) == 3 ) {
```

```
33      #SO não suportado, scan não será feito
34      print("SO não suportado \n");
35      $logger->warn("Os not supported $mac (Openvas). Scan não será feito");
36  }else {
37      #Host seguro à entrar na rede
38      print("hosts ok \n");
39      $logger->warn("Host $mac is secure to enter in the network (Openvas).");
40  }
41
42  #Finaliza evento de scan
43  my $apiclient = pf::api::jsonrpcclient->new;
44  my %data = (
45   'security_event_id' => $scan_security_event_id,
46   'mac' => $mac,
47   );
48  $apiclient->notify('close_security_event', %data );
```

APÊNDICE D – Script Bash para verificar situação do tunel ssh e cria-lo caso não esteja ativo

```
#!/bin/sh

#criar usuário / utilizador
pass="$(date +%s | sha256sum | base64 | head -c 32 ; echo)"
useradd -m -s /bin/bash gvm_host -p "$pass"


# adicionar chave ssh
chave="ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMYpRou+pKTarbh9hKg6Lm5xiI5PcxquphDw0zKOuXaSYATjGCCrHlei
↪ Pj3+PgqH737CewwAxtvF13vLfNAQVu3Jx7TGL/U1RhLDrx2MFCwaaS/itkKT4NpjMy6zkTiL1me8wcEnVypSDxy4ab4TxzszF
↪ unDFoSgwcvwbYht4HgqplrfZGvbCiTNwfVXxC2Ze8kFcgUrx4UqrN3hyS5GkvsNgT9BdSncSe5L6T/U5u7J9qZIMJhAArHP92
↪ 9760VcyG0OU20o6nT1mS2UEzw3oDbEntB/hLWaqdRFPsK0n7/fFFVUYDFIJyufSnyffOzNN22uJvp4me/GQy4+nucJrd6DPAZ
↪ jb3pnbyKA7Or8c1qr+H6JNJgbWmazeo3lwiZx4qn/mhCZs4VUcoYgEmPpCvHNolzmkGuxiKInoDyURhpymDznQErmZ83vmuWv
↪ qfEY22t6VPGSE7zYOejl/Idcx/1S3hHGw4zVvoTASGAIFA6qQ4EsdzgxxAOND2uNV4fsk=
↪ kali@kali"
mkdir /home/gvm_host/.ssh/
touch /home/gvm_host/.ssh/authorized_keys

if ! ( grep -q "$chave" /home/gvm_host/.ssh/authorized_keys ); then
        echo "$chave" >> /home/gvm_host/.ssh/authorized_keys
fi

chown -R gvm_host:gvm_host /home/gvm_host
chmod 700 /home/gvm_host/.ssh
chmod 660 /home/gvm_host/.ssh/authorized_keys

#criar regra de firewall
if (which iptables)
  iptables -I INPUT -s 192.168.100.110 -j ACCEPT
  iptables -I INPUT -s 192.168.200.110 -j ACCEPT
  iptables -I OUTPUT -s 192.168.100.110 -j ACCEPT
  iptables -I OUTPUT -s 192.168.200.110 -j ACCEPT
else if (which firewalld)
  firewall-cmd --add-source=192.168.100.110/24 --permanent
  firewall-cmd --add-source=192.168.200.110/24 --permanent
fi

```

```
32 # iniciar ssh
33 if ( systemctl start sshd ); then
34   echo "Script finalizado com sucesso! "
35   sleep(600)
36   systemctl stop sshd
37 else
38   echo "Houve algum erro no script! "
39 fi
```

APÊNDICE E – Script Bash para inserir chave SSH

```
#!/bin/sh

#criar usuário / utilizador
pass="$(date +%s | sha256sum | base64 | head -c 32 ; echo)"
useradd -m -s /bin/bash gvm_host -p "$pass"


# adicionar chave ssh
chave="ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMYpRou+pKTarbh9hKg6Lm5xiI5PcxquphDw0zKOuXaSYATjGCCrHlei
↪  Pj3+PgqH737CewwAxtvF13vLfNAQVu3Jx7TGL/U1RhLDrx2MFCwaaS/itkKT4NpjMy6zkTiL1me8wcEnVypSDxy4ab4TxzszF
↪  unDFoSgwcvwbYht4HgqplrfZGvbCiTNwfVXxC2Ze8kFcgUrx4UqrN3hyS5GkvsNgT9BdSncSe5L6T/U5u7J9qZIMJhAArHP92
↪  9760VcyG0OU20o6nT1mS2UEzw3oDbEntB/hLWaqdRFPsK0n7/fFFVUYDFIJyufSnyffOzNN22uJvp4me/GQy4+nucJrd6DPAZ
↪  jb3pnbyKA7Or8c1qr+H6JNJgbWmazeo3lwiZx4qn/mhCZs4VUcoYgEmPpCvHNolzmkGuxiKInoDyURhpymDznQErmZ83vmuWv
↪  qfEY22t6VPGSE7zYOejl/Idcx/1S3hHGw4zVvoTASGAIFA6qQ4EsdzgxxAOND2uNV4fsk=
↪  kali@kali"
mkdir /home/gvm_host/.ssh/
touch /home/gvm_host/.ssh/authorized_keys

if ! ( grep -q "$chave" /home/gvm_host/.ssh/authorized_keys ); then
        echo "$chave" >> /home/gvm_host/.ssh/authorized_keys
fi

chown -R gvm_host:gvm_host /home/gvm_host
chmod 700 /home/gvm_host/.ssh
chmod 660 /home/gvm_host/.ssh/authorized_keys

#criar regra de firewall
if (which iptables)
  iptables -I INPUT -s 192.168.100.110 -j ACCEPT
  iptables -I INPUT -s 192.168.200.110 -j ACCEPT
  iptables -I OUTPUT -s 192.168.100.110 -j ACCEPT
  iptables -I OUTPUT -s 192.168.200.110 -j ACCEPT
else if (which firewalld)
  firewall-cmd --add-source=192.168.100.110/24 --permanent
  firewall-cmd --add-source=192.168.200.110/24 --permanent
fi

# iniciar ssh
if ( systemctl start sshd ); then
  echo "Script finalizado com sucesso! "
```

```
35    sleep(600)
36    systemctl stop sshd
37  else
38    echo "Houve algum erro no script! "
39  fi
```

APÊNDICE F – Página HTML inicial para scan

```
<!DOCTYPE html>
<html>
<head>
  <style>
  .collapsible {
    background-color: #777;
    color: white;
    cursor: pointer;
    padding: 18px;
    width: 100%;
    border: none;
    text-align: left;
    outline: none;
    font-size: 15px;
  }

  .active, .collapsible:hover {
    background-color: #555;
  }

  .content {
    padding: 0 18px;
    display: none;
    overflow: hidden;
    background-color: #f1f1f1;
  }

  .border {
    border: 1px solid black;
  }

  .margin-text {
    margin-top: 16px;
    margin-bottom: 16px;
  }
</style>
</head>
<body>
  <div id="msg">
    <h4 class = "margin-text">Orientações</h4>
```

```
41
42      <div id="container">
43
44        <p class = "margin-text">
45          Antes de acessar a rede interna, será necessário escanear seu computador para verificar se
            ↪ ele está infectado por algum malware. Caso não seja um Linux ou Windows, apenas leia e
            ↪ clique / prima em "Aceito os Termos". Caso seja um Linux ou Windows, clique / prima na
            ↪ caixa que corresponde ao seu sistema operacional / operativo e siga as instruções (elas
            ↪ serão necessárias toda vez que acessar a rede). Se as instruções não forem seguidas, não
            ↪ será possível se conectar à rede.
46        </p>
47        <p class = "margin-text">
48          É necessário que você tenha instalado um dos antivírus abaixo para entrar na rede. Caso não
            ↪ tenha ainda, é possível baixar / descarregar e instalar aqui mesmo:
49        </p>
50
51        <button type="button" class="collapsible">Windows</button>
52        <div class="content">
53          <p class = "margin-text">
54            É necessário que você tenha instalado um dos antivírus abaixo para entrar na rede. Caso não
              ↪ tenha ainda, é possível baixar / descarregar (baixe / descarregue o instalador offline,
              ↪ pois seu acesso a internet é limitado) e instalar nos links abaixo:
55          </p>
56
57          <ul>
58            <li><a target="_blank" rel="noopener noreferrer" href="https://www.avg.com/">AVG Antivírus
              ↪ </a></li>
59            <li><a target="_blank" rel="noopener noreferrer" href="https://www.avast.com/">Avast
              ↪ Antivírus</a></li>
60          </ul>
61
62          <h2 class = "margin-text">Instruções (Observação: Você pode pular as instruções abaixo se já
            ↪ o fez anteriormente neste computador e não desinstalou o scan.exe)</h2>
63
64          <p class = "margin-text">
65            <!-- /usr/local/pf/gum_scan/scan.sh => localização do script de scan -->
66            Faça o download / descarregue o executável <span><a href="/common/scan.exe"
              ↪ download>scan.exe</a></span>, depois clique / prima o botão direito do mouse / rato e
              ↪ clique / prima em propriedades. Na janela que se abre, ao final, na área de segurança
              ↪ (se houver) clique / prima na caixa onde diz "desbloquear" e depois em aplicar (caso
              ↪ isso não seja feito o computador poderá bloquear o executável, por ser um programa
              ↪ desconhecido. Não se preocupe, ele apenas criará um usuário / utilizador para escanear
              ↪ o computador e nada mais). Após isso execute o programa e clique / prima "next" e
              ↪ "install".
67          </p>
68          <p class = "margin-text">
```

```
69          Ao fim da instalação, volte a esta página e continue em "Aceito os Termos". Após isso seu
            ↪ computador será escaneado. Quando estiver conectado na rede correta, você pode
            ↪ desisntalar o programa, mas será necessário instala-lo novamente quando for fazer uma
            ↪ nova conexão.
70        </p>
71      </div>
72
73      <button type="button" class="collapsible">Linux</button>
74      <div class="content">
75        <p class = "margin-text">
76          É necessário que você tenha instalado um dos antivírus abaixo para entrar na rede. Caso não
            ↪ tenha ainda, é possível baixar / descarregar e instalar aqui mesmo:
77        </p>
78
79        <ul>
80          <li><a target="_blank" rel="noopener noreferrer"
            ↪ href="https://docs.clamav.net/manual/Installing/Packages.html">ClamAV (Procure no link
            ↪ o comando referente a sua distro de Linux e o execute no terminal)</a></li>
81        </ul>
82
83        <p class = "margin-text">Siga a parte de "Configurações" (se você já o fez anteriormente
          ↪ nesse computador, ignore essa parte) e depois "Abrir para scan" </p>
84
85        <h2 class = "margin-text">Configurações</h2>
86
87        <p class = "margin-text">
88          Será necessário instalar openssh-server e o antivírus para fazer o scan, para isso executa
            ↪ a lista de comandos referente a sua distribuição Linux
89        </p>
90
91        <ul>
92          <li>Ubuntu (com gerenciador de pacotes apt)</li>
93          <p class = "margin-text">
94            <div class="border">
95              sudo mkdir /etc/apt/sources.list.d ;\<br>
96              sudo touch /etc/apt/sources.list.d/porto.list ;\<br>
97              sudo chmod 777 /etc/apt/sources.list.d/porto.list ;\<br>
98              sudo echo "deb https://mirrors.up.pt/ubuntu $(cat /etc/*ease | grep UBUNTU_CODENAME= |
                ↪ cut -c17-100) main restricted universe" > /etc/apt/sources.list.d/porto.list ;\<br>
99              sudo apt-get update -o Dir::Etc::sourcelist="sources.list.d/porto.list" -o
                ↪ Dir::Etc::sourceparts="-" -o APT::Get::List-Cleanup="0" -y ;\<br>
100             sudo apt upgrade -y ;\<br>
101             sudo apt install openssh-server -y
102             sudo apt-get install clamav clamav-daemon clamtk -y
103           </div>
104         </p>
105
106         <li>Debian (com gerenciador de pacotes apt)</li>
```

```
107           <p class = "margin-text">
108             <div class="border">
109               sudo mkdir /etc/apt/sources.list.d ;\<br>
110               sudo touch /etc/apt/sources.list.d/porto.list ;\<br>
111               sudo chmod 777 /etc/apt/sources.list.d/porto.list ;\<br>
112               sudo echo "deb https://mirrors.up.pt/debian stable main" >
                  ↪  /etc/apt/sources.list.d/porto.list ;\<br>
113               sudo apt-get update -o Dir::Etc::sourcelist="sources.list.d/porto.list" -o
                  ↪  Dir::Etc::sourceparts="-" -o APT::Get::List-Cleanup="0" -y ;\<br>
114               sudo apt upgrade -y ;\<br>
115               sudo apt install openssh-server -y
116               sudo apt-get install clamav clamav-daemon clamtk -y
117             </div>
118             Após isso também instale o antivírus
119           </p>
120
121           <li>Kali (com gerenciador de pacotes apt)</li>
122           <p class = "margin-text">
123             <div class="border">
124               sudo apt-get update -y ;\<br>
125               sudo apt upgrade -y ;\<br>
126               sudo apt install openssh-server -y
127               sudo apt-get install clamav clamav-daemon clamtk -y
128             </div>
129             Após isso também instale o antivírus
130           </p>
131
132           <li>CentOS 7 (com gerenciador de pacotes yum)</li>
133           <p class = "margin-text">
134             <div class="border">
135               yum-config-manager --add-repo https://mirrors.up.pt/pub/centos/7/os/x86_64/ ;\<br>
136               yum-config-manager --disablerepo="*"
                  ↪  --enablerepo="mirrors.up.pt_pub_centos_7_os_x86_64_" ;\<br>
137               sudo yum update -y ;\<br>
138               sudo yum upgrade -y ;\<br>
139               sudo yum install openssh-server -y
140               sudo apt-get remove clamav clamav-daemon clamtk -y
141             </div>
142             Após isso também instale o antivírus
143           </p>
144         </ul>
145
146         <p class = "margin-text">
147           Faça o download do arquivo / descarregue o ficheiro <span><a href="/common/scan.sh"
              ↪  download>scan.sh</a></span>.
148         </p>
149
150         <h2 class = "margin-text">Abrir para scan</h2>
```

```
151
152         <p class = "margin-text">
153           clique / prima o botão direito do mouse / rato e clique / prima em propriedades e copie o
              ↪ texto que está escrito a frente de "Localização: ". Após isso abra o terminal e execute
              ↪ os dois comandos abaixo (substitua "localização" pelo caminho onde se encontra o
              ↪ ficheiro. Exemplo: /home/ubuntu/scan.sh):
154         </p>
155
156         <p class = "margin-text">
157           <div class="border">
158             sudo chmod 110 (Localização)/scan.sh<br>
159             sudo (Localização)/scan.sh 2> /dev/null &
160           </div>
161         </p>
162
163
164         <p class = "margin-text">
165           Após isso, clique em continuar "Aceito os Termos" e seu computador será escaneado (você têm
              ↪ 10 minutos para iniciar um scan, caso necessário execute os dois comandos novamente).
166         </p>
167       </div>
168
169
170     </div>
171
172   </div>
173
174   <h2 style="text-align: center;">Termos de Uso</h2>
175   <p class = "margin-text">Ao aceitar os termos, garanto não utilizar a rede para realizar ataques à
      ↪ rede, disseminar malwares e baixar arquivos / descarregar ficheiros torrent.</p>
176
177
178
179   <script>
180     var visitante = document.getElementById("title").innerHTML == "Visitante";
181
182     if(visitante) {
183       document.getElementById("msg").innerHTML = "";
184     }
185
186     var coll = document.getElementsByClassName("collapsible");
187     var i;
188
189     for (i = 0; i < coll.length; i++) {
190       coll[i].addEventListener("click", function() {
191         this.classList.toggle("active");
192         var content = this.nextElementSibling;
193         if (content.style.display === "block") {
```

```
194             content.style.display = "none";
195           } else {
196             content.style.display = "block";
197           }
198         });
199       }
200     </script>
201   </body>
202   </html>
```