Ontologia de Vulnerabilidades e Ataques a VLAN

Marcio Silva Cruz

Julho / 2023

Dissertação de Mestrado em Ciência da Computação

Ontologia de Vulnerabilidades e Ataques a VLAN

Esse documento corresponde a Dissertação apresentada à Banca Examinadora para a defesa de Mestrado em Ciência da Computação da UNIFACCAMP – Centro Universitário Campo Limpo Paulista.

Campo Limpo Paulista, 06 de julho de 2023.

Marcio Silva Cruz

Prof. Dr. Ferrucio de Franco Rosa (Orientador)

Ficha catalográfica elaborada pela

Biblioteca Central da Unifaccamp

C963o

Cruz, Marcio Silva

Ontologia de vulnerabilidades e ataques a VLAN / Marcio Silva Cruz. Campo Limpo Paulista, SP: Unifaccamp, 2023.

Orientador: Prof. Dr. Ferrucio de Franco Rosa

Dissertação (Programa de Mestrado Profissional em Ciência da Computação) – Centro Universitário Campo Limpo Paulista – Unifaccamp.

1. Ataques a VLAN. 2. Ontologia. 3. Prevenção em VLAN. 4. Segurança em redes. 5. Segmentação de redes. 6. Web semântica. 7. Taxonomia. 8. VLAN. 9. Vulnerabilidades em *switches*. 10. Protocolos de camada de rede. I. Rosa, Ferrucio de Franco. II. Centro Universitário Campo Limpo Paulista. III. Título.

CDD – 005.8

DEDICATÓRIA

Dedico este trabalho a meu inesquecível pai Genilson da Silva Cruz (in memorian), o qual eternizou em minha mente a afirmação que, "se estudo não é tudo, é quase tudo"

AGRADECIMENTOS

Primeiramente, agradeço a Deus que nos orienta e mostra os caminhos que devemos seguir.

Agradeço ao meu orientador, professor Dr. Ferrucio de Franco Rosa, pela oportunidade, pelos ensinamentos e pela confiança atribuída a mim no desenvolvimento deste trabalho de pesquisa. Suas orientações foram cruciais para a elaboração deste trabalho, sendo grande parte do crédito atribuído a ele.

Aos membros da banca examinadora, professores Dr. Rodrigo Bonacin, Dr. Wellington Roque e Dr. Luiz Mariano del Val Cura, pelas importantes sugestões de melhorias.

Agradeço a todos os professores do programa de Mestrado em Ciência da Computação e funcionários da UNIFACCAMP, que sempre me atenderam prontamente, com cortesia e muita competência.

Ao Centro de Tecnologia da Informação Renato Archer (CTI) pela oportunidade e pelo apoio que me foram dados para que eu pudesse desenvolver este trabalho concomitantemente com minhas atividades de pesquisador.

Agradeço a minha mãe Ozelina da Silva Cruz e aos meus irmãos, que contribuíram direta ou indiretamente para que eu pudesse progredir.

Finalmente, um especial agradecimento a minha sobrinha Cibelly Nicolly Rodrigues Silva Cruz, com cinco anos, que mesmo sem entender o grau de dificuldade deste trabalho, me incentivava com suas brincadeiras.

Resumo

Defender as redes de computadores de ataques cibernéticos é uma atividade crucial e recorrente, e ao se trabalhar com a probabilidade destes eventos ocorrerem, faz-se necessário calcular cuidadosamente os riscos. Virtual Local Area Network (VLAN) é uma tecnologia capaz de separar redes em domínios específicos proporcionando um certo nível de segurança, e por ser amplamente usada nos ambientes de redes, torna-se necessário um melhor entendimento das suas vulnerabilidades e ataques. Ferramentas automatizadas para detectar vulnerabilidades e ataques a sistemas computacionais estão disponíveis em aplicativos da Web, porém não fornecem reutilização e compartilhamento de conhecimento. Ontologias podem contribuir neste contexto, pois são ferramentas de modelagem que possibilitam a formalização dos conceitos principais e de seus relacionamentos, e essas informações se transformam em conhecimento de forma organizada, representando tal conhecimento de maneira formal e estruturada, além de possibilitar a criação de regras semânticas que podem ser usadas por sistemas inteligentes. Com o objetivo de desenvolver uma modelagem conceitual visando a proteção de redes segmentadas, propõem-se OVAV (Ontologia de Vulnerabilidades e Ataques a VLAN), que é uma ontologia de domínio voltada a identificar e modelar as vulnerabilidades e ataques a VLANs. A partir do mapeamento do domínio, por meio de OVAV, são propostas estratégias de proteção ou de mitigação de ataques a VLANs, permitindo a construção de métodos e técnicas sistemáticas para proteção de infraestruturas críticas.

Palavras-chave: Ataques a VLAN, Ontologia, Prevenção em VLAN, Segurança em Redes, Segmentação de Redes, Web Semântica, Taxonomia, VLAN, Vulnerabilidades em Switches, Protocolos de Camada de Rede.

Abstract

Defending computer networks from cyber-attacks is a crucial and recurrent activity, and when working with the probability of these events occurring, it is necessary to carefully calculate risks. Virtual Local Area Network (VLAN) is a technology capable of separating networks into specific domains providing a certain level of security. Automated tools for detecting vulnerabilities and attacks on computer systems are available in web applications, but they do not provide for knowledge sharing and reuse. Ontologies can contribute to this context, as they are modeling tools that enable the formalization of the main concepts and their associations, and this information becomes knowledge in an organized way, representing such knowledge in a formal and structured way, in addition to enabling the creation of semantic rules that can be used by intelligent systems. With the aim of developing a conceptual model aimed at protecting segmented networks, we propose OVAV (VLAN Attacks and Vulnerabilities Ontology), which is a domain ontology aimed at identifying and modeling vulnerabilities and attacks on VLANs. From domain mapping, through OVAV, strategies are proposed for the protection or mitigation of attacks on VLANs, allowing the construction of systematic methods and techniques for the protection of critical infrastructures.

Keywords: VLAN Attacks, Ontology, VLAN Prevention, Network Security, Network Segmentation, Semantic Web, Taxonomy, VLAN, Vulnerabilities in Switches, Network Layer Protocols.

SUMÁRIO

GLOSSÁRIO

Abreviatura/Sigla	Significado
ALC	*Attributive Language with Complements*
ANSI	*American National Standards Institute*
APT	*Advanced Persistent Threats*
ARP	*Address Resolution Protocol*
CAM	*Content Addressable Memory*
CDP	*Cisco Discovery Protocol*
CSV	*Comma-separated values*
CTI	*Cyber Threat Intelligence*
CVE	*Common Vulnerabilities and Exposures*
DAI	*Dynamic ARP Inspection*
Dos	*Denial of Service*
DDos	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DL	*Description Logic*
DNS	*Domain Name System*
DoS	*Denial of Service*
DTP	*Dynamic Trunking Protocol*
FCoE	*Fibre Channel over Ethernet*
G ARP	*Gratuitous Address Resolution Protocol*
HTTP	*Hypertext Transfer Protocol*
IBM	*International Business Machines*
ID	*Identification*
IDS	*Intrusion Detection Systems*

IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Enginnering Task Force*
IoT	*Internet of Things*
IP	*Internet Protocol*
IPV4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
ISL	*Inter Switch Link*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
LAN	*Local Area Network*
LD	*Linked Data*
MAC	*Media Access Control*
MASs	*Multi-agent Systems*
MITM	*Man In The Middle*
MPLS	*Multiprotocol Label Switching*
OF	*Open Format*
OL	*Open License*
OSI	*Open Systems Interconnection*
OVAV	Ontologia de Vulnerabilidades e Ataques a VLAN
OWL	*Ontology Web Language*
PDF	*Portable Document Format*
RDF	*Resourse Description Framework*
RDF-S	*Resourse Description Framework Schema*
RE	*Readable Machine*
RFCs	*Request for Comments*
SCADA	*Supervisory Controland Data Acquisition*

SNMP	*Simple Network Management Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URI	*Unified Resource Identifier*
VLANs	*Virtual Local Area Networks*
VoIP	*Voice Over Internet Protocol*
VPN	*Virtual Private Network*
VTP	*VLAN Trunking Protocol*
W3C	*World Wide Web Consortium*
WAN	*Wide Area Network*
XLS	*Microsoft Excel Spreadsheet*
XML	*Extensible Markup Language*

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO

As organizações têm cada vez mais agregado tecnologias a seus processos a fim de diminuir custos e aumentar os lucros; este aumento de soluções e consequentemente de informações trafegando pela rede aumentam as preocupações relacionadas ao congestionamento dos links e segurança. Quando se trabalha com a probabilidade de um evento catastrófico ocorrer (e.g., vazamento de dados, negação de serviços etc.), faz-se necessário calcular cuidadosamente os riscos. Neste contexto, merece atenção especial a camada 2 (*data link*) do modelo OSI (*Open Systems Interconnection*) (Tanenbaum & Wetherall, 2011), que é um modelo de referência para projetos de protocolos de rede. Nessa camada se encontram as VLANs (*Virtual Local Area Networks*), que são alvos atraentes para atacantes (Convery, 2004).

VLAN é uma tecnologia capaz de separar redes em domínios específicos, o que permite aplicar controles mais adequados à necessidade de cada grupo dentro do conjunto. Um exemplo é a criação de grupos de usuários com necessidades distintas de acesso às informações armazenadas, o que possibilita implementar o princípio do privilégio mínimo, evitando que usuários tenham mais acesso do que possam necessitar, aumentando os riscos de vulnerabilidades. Ao segmentar a rede, criam-se grupos de trabalho evitando o fluxo de quadros de broadcast a terminais fora da VLAN, onde somente os dispositivos daquele grupo, com permissão, acessam os recursos; isso proporciona bom desempenho das atividades, com um nível definido de segurança (Soares Barros, 2006).

Ataques às VLANs podem afetar as camadas superiores, causando interrupções nos serviços e outros problemas de segurança. Usualmente, estes ataques exploram características operacionais das VLANs para ter acesso às informações. Como as VLANs são amplamente usadas nos ambientes de redes, é requerido um melhor entendimento das suas vulnerabilidades e de todos os possíveis ataques. VLANs devem ser configuradas para não estarem expostas a vulnerabilidades conhecidas (e.g., VLAN *hopping*). Por exemplo, em um serviço de VoIP (*Voice over Internet Protocol*) que usa uma VLAN, os tráfegos de voz e de dados são divididos pela segmentação lógica da rede, minimizando os efeitos de um possível ataque DoS (*Denial of Service*) (Thermos & Takanen, 2007). Contudo, o uso de *softphones* no computador, os quais usam a mesma interface de rede para dados e voz, anulam a aplicação da VLAN. Desta forma, seria necessária uma

segunda interface de rede configurada para o uso do *softphone*, levando-se em consideração as recomendações de segurança (Porter & Gough, 2007).

Identificar e tratar vulnerabilidades e seus respectivos ataques a VLANs de maneira sistemática e formal é essencial para manter seguros os ambientes computacionais. No entanto, existe sobreposição de domínios, conceitos são ambíguos, a terminologia é confusa, e importantes conceitos não estão definidos; contudo, as ontologias podem contribuir neste contexto (de Franco Rosa et al., 2018).

Ferramentas automatizadas são usadas para detectar vulnerabilidades e ataques (e.g., em aplicativos da *Web*), porém estas não possibilitam reutilização e compartilhamento de conhecimento. Uma ontologia contém objetos, conceitos e relações, e essas informações se transformam em conhecimento de forma organizada, representando tal conhecimento de maneira formal e estruturada, o que possibilita gerar regras semânticas que podem ser usadas por sistemas inteligentes (Shenbagam & Salini, 2014). Embora metodologias destaquem o desenvolvimento de ontologias em várias disciplinas e domínios, identificou-se a falta de ontologias que tratem de VLANs.

1.1 Questão de Pesquisa, Contribuição Principal e Objetivos

A partir da problemática exposta, aborda-se a seguinte **questão de pesquisa**: "*Como representar de maneira sistemática a reutilização e compartilhamento de conhecimento visando a proteção de VLANs ?*"

Como **contribuição principal** propõe-se: i) uma ontologia de domínio que modela vulnerabilidades e ataques a VLANs, e ii) conjunto de estratégias de prevenção de ataques para robustecimento de VLANs. O modelo conceitual proposto visa a identificar, formalizar e relacionar conceitos importantes, mapear vulnerabilidades e ataques, além de fornecer parâmetros e termos formalizados para definir estratégias para proteção de VLANs. Apresenta-se o desenvolvimento dos conceitos principais e uma aplicação de mundo real. Termos importantes, como VLAN, vulnerabilidade, ataque, impacto, contramedida, propriedade de segurança e seus relacionamentos, são

formalizados por meio de uma ontologia de domínio em formato OWL, disponível para os pesquisadores usarem, editarem ou mesclarem.

Como **Objetivos** da pesquisa, destacam-se: i) Conceber e desenvolver a modelagem conceitual visando a proteção das redes VLAN; ii) Especificar o domínio; iii) Formalizar e relacionar conceitos importantes; iv) Mapear vulnerabilidades e ataques conhecidos; v) Propor estratégias de proteção ou mitigação de ataques a VLAN; e v) Criar uma ontologia de domínio em OWL.

1.2 Estrutura da Dissertação

Os capítulos subsequentes estão organizados da seguinte forma: O Capítulo 2 apresenta um referencial teórico voltado a introduzir conceitos importantes que serviram de base para o desenvolvimento de OVAV, tais como Web Semântica, Ontologia e Redes de Computadores; O Capítulo 3 apresenta uma síntese de uma revisão sistemática da literatura sobre ontologias de vulnerabilidades e ataques a VLAN, além de métodos com objetivos similares ao proposto neste projeto; No Capítulo 4, apresenta-se OVAV.owl e os conceitos principais da conceptualização; O Capítulo 5 apresenta a aplicação de OVAV, por meio da proposição de estratégias de proteção para VLAN; O Capítulo 6 apresenta as considerações finais, os resultados da pesquisa e os desafios para pesquisas futuras.

2 REFERENCIAL TEÓRICO

Este capítulo tem por finalidade descrever as abordagens teóricas e tecnológicas que norteiam esta proposta. A Subseção 2.1 discorre sobre *Web* Semântica, RDF, RDF-S Ontologias e OWL; a Subseção 2.2 discorre sobre redes de computadores, VLANs e protocolos da camada de atuação.

2.1 *Web* Semântica

A *Web* revolucionou o consumo de documentos, no entanto, saber trabalhar com grandes quantidades de dados procedentes de diversas localidades e com diferentes formatos torna-se um grande desafio (Davenport & Patil, 2012). O conteúdo produzido para a Internet, em sua maioria, tem por objetivo o consumo apenas por seres humanos, onde os dados são lidos por mecanismos automatizados, porém, não são passiveis de interpretação (Lassila & Swick, 1999). A automatização da descrição ou interpretação de dados na Internet demanda alta complexidade e em função de seu volume de dados, qualquer operação manual é inviável, sendo que a solução comumente proposta para essa tarefa é a adoção de metadados, os quais permitem a descrição de recursos na Internet, atribuindo a capacidade de compreensão a mecanismos automatizados (Lassila & Swick, 1999).

A recuperação de informação na *Web*, de forma eficiente, requer que esta tarefa seja feita de maneira automática, ou seja, contando com o auxílio de computadores. Assim, é necessário que aparatos computacionais sejam capazes de tratar as ambiguidades inerentes às palavras que são utilizadas em consultas e buscas de informação na *Web.*

A *Web* Semântica, uma extensão da *Web* atual, é uma representação capaz de associar significados explícitos aos conteúdos dos documentos disponíveis na Internet, sendo que sua principal meta é possibilitar que programas processem e interpretem automaticamente esses documentos, além de possibilitar que computadores sejam capazes de acessar dados estruturados e de definir regras de inferências, transformando grandes volumes de dados em informação (Berners-lee et al., 2001). Se uma máquina possuir a capacidade de analisar a estrutura semântica de um documento, não interpretará apenas os

caracteres que compõem esse documento, mas compreenderá o sentido deste documento, o que proporcionará a realização de sofisticadas tarefas para os usuários.

Como parte do desenvolvimento da *Web* Semântica, surgiu o conceito de *Linked Open Data*. O termo se refere a um conjunto de boas práticas para publicação e conexão de dados estruturados na *Web*, usando padrões internacionais recomendados pelo W3C (*World Wide Web Consortium*), com o objetivo de levar a *Web* ao seu potencial máximo. A fim de incentivar a publicação de dados em conformidade com a *Web* Semântica, Barners-Lee desenvolveu um sistema de classificação através de cinco estrelas, onde a classificação subsequente depende do acúmulo dos requisitos anteriores (Berners-Lee, 2009). O sistema de classificação para publicação de dados na Internet é representado por níveis que apresentam características distintas, conforme apresentada na Figura 2.1.

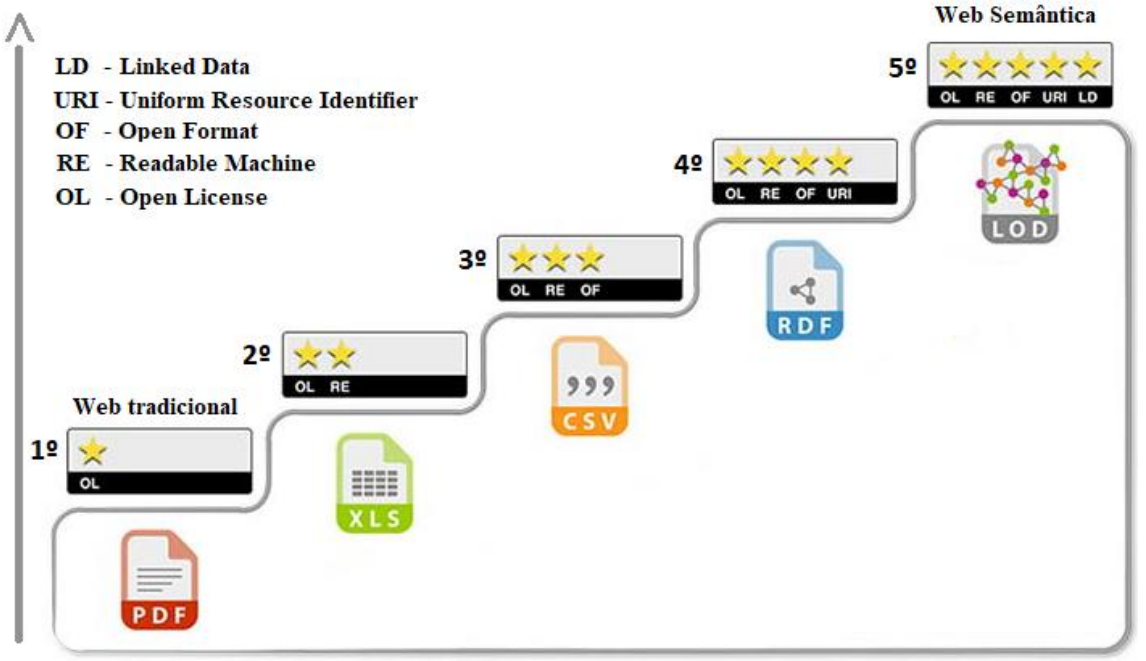

Figura 2.1 – Linked Open Data. Adaptado de (Berners-Lee,2009)

O primeiro nível da classificação, com uma estrela, indica que os dados estão disponíveis na *Web* em qualquer formato, por exemplo, PDF, mas com licença aberta. Duas estrelas indicam que os dados estão disponíveis na *Web* como dados estruturados, por exemplo, um arquivo *Excel* com extensão XLS. Três estrelas indicam que os dados estão disponíveis na *Web* de maneira estruturada e em formato não proprietário, por exemplo, CSV em vez de *Excel*. Quatro estrelas indicam a satisfação de todas as

características anteriores, mas dentro dos padrões estabelecidos pelo W3C, por exemplo, RDF e SPARQL. Por fim, cinco estrelas indicam a satisfação de todas as características anteriores, além de vincular seus dados a outros dados para fornecer contexto, alcançando assim o grau máximo no conceito *Linked Open Data*.

Os sistemas de representação e organização do conhecimento são considerados processos fundamentais, em meio a uma crescente produção de informações. Estes sistemas visam a proporcionar a representação, recuperação e o intercâmbio de informações, de acordo com necessidades e ambientes específicos.

2.1.1 *Resource Description Framework* (RDF)

O modelo de dados em RDF (*Resource Description Framework*) é uma forma de representar expressões utilizadas para atribuir significado aos dados, permitindo que recursos possam ser descritos formalmente e sejam processados por máquinas. Com o objetivo de descrever a relação entre recursos, o RDF oferece uma estrutura de triplas do tipo <*sujeito*> <*predicado*> <*objeto*> (Berners-lee et al., 2001). Proposto pelo W3C (*World Wide Web Consortium*), o RDF organiza o conhecimento por meio da ideia de redes semânticas, e permite a representação de conceitos, taxonomia de conceitos e relações binárias (Almeida & Bax, 2003).

Segundo Lassila & Swick (1999), RDF é a tecnologia base para o processamento de metadados, provendo interoperabilidade entre aplicações que trocam e processam informações na *Web*. Para os autores, um dos objetivos do RDF é possibilitar a criação de semântica para dados baseados em XML.

O RDF provê uma representação minimalista do conhecimento na *Web* (Shadbolt et al., 2006). Para referenciar e descrever um recurso descrito pelo RDF, de forma única e não ambígua, faz-se necessário um identificador único e global, o URI (*Unified Resource Identifier*). Segundo Isotani & Bittencourt (2015), o URI encontra-se inserido na arquitetura da *Web*, a qual é composta de três bases fundamentais, a saber: (i) Recurso único – URI, que provê uma maneira simples e única de identificar recursos na *Web*; (ii) Interação, permitindo a comunicação cliente-servidor através do protocolo HTTP

(*Hypertext Transfer Protocol*) e; (iii) Formatos, que são representações de arquivos em um determinado formato, contendo informação de metadados e dados (Isotani & Bittencourt, 2015).

Para expressar a semântica por meio de triplas, identificadas também como vocabulário RDF, é necessária a definição de *tags*. RDF-Schema (RDF-S) é uma extensão do RDF utilizada para este propósito, sendo a especificação que define classes, propriedades e seus relacionamentos, descrevendo triplas. Isso inclui a definição de *tags* e sua estrutura hierárquica. Assim, RDF-S fornece os elementos mínimos para a descrição de ontologias (Isotani & Bittencourt, 2015). Embora RDF-S possa ser usado para descrever ontologias, este possui algumas limitações, especialmente para apoiar o raciocínio computacional dos dados disponíveis na *Web* (Patel-Schneider, 2005). Segundo Staab et al. (2001), os dados em RDF são fracamente interligados, de modo que a *Web* Semântica necessita de técnicas mais sofisticadas.

2.1.2 Ontologia

Segundo Almeida & Bax (2003), técnicas de tratamento e organização da informação podem ser classificadas de diversas formas, por exemplo: i) a partir de seus termos, em glossários ou dicionários; ii) por meio de classificação e criação de categorias, através de taxonomias; e iii) por meio de conceitos e seus relacionamentos, usando ontologias, tesauros ou redes semânticas.

As ontologias são vistas como a tecnologia de consolidação para a construção da Web Semântica, a qual necessita de representação com um grau significativo de estruturação. As ontologias são geralmente expressas em uma linguagem baseada em lógica, de modo que distinções detalhadas, precisas, consistentes, sólidas e significativas possam ser feitas (Heflin, 2004). No que se refere à sua estrutura, ontologias são compostas essencialmente por um conjunto de conceitos estruturados hierarquicamente, propriedades e relacionamentos que descrevem o domínio modelado.

A definição mais conhecida para ontologia é apresentada por Gruber (1995), “uma ontologia é uma especificação explícita de uma conceitualização”. O autor também

esclarece a necessidade de algum formalismo comum para o compartilhamento por aplicativos baseados em conhecimento. Borst (1997) apresenta a seguinte definição: “uma ontologia é uma especificação formal e explícita de uma conceituação compartilhada”. Esta definição é classificada por Almeida & Bax (2003) como simples e completa. Os autores afirmam que, nessa definição, “formal” significa legível por computadores; “especificação explícita” diz respeito a conceitos, propriedades, relações, funções, restrições, axiomas, explicitamente definidos; “compartilhado” quer dizer conhecimento consensual; e “conceituação” diz respeito a um modelo abstrato de algum fenômeno do mundo real.

Embora apresentem definições relativamente diferentes, tanto Gruber quanto Borst destacam que o principal propósito na construção de ontologias é permitir o compartilhamento e a possibilidade de reuso do conhecimento por diversas aplicações.

As ontologias possuem elementos básicos que fazem parte de sua estrutura, a saber: (1) Classes – representam os conceitos de um domínio específico; (2) Relações – representam os tipos de interação ou conexão entre as classes; (3) Axiomas – representam a modelagem de sentenças sempre verdadeiras, definindo restrições e regras; e (4) Instâncias – representam determinados objetos de um conceito, com base nas classes propostas (Gruber, 1995)(Noy & McGuinness, 2001) e (Isotani & Bittencourt, 2015).

A partir da observação de grupos de ontologias, pode-se verificar a existência de tipos bem definidos. Guarino (1998) propôs uma classificação baseada na generalidade da ontologia, sendo identificados e descritos pelo autor os seguintes tipos: ontologias de alto nível, ontologias de domínio, ontologias de tarefa e ontologias de aplicação. A Figura 2.2 representa os tipos de ontologias.

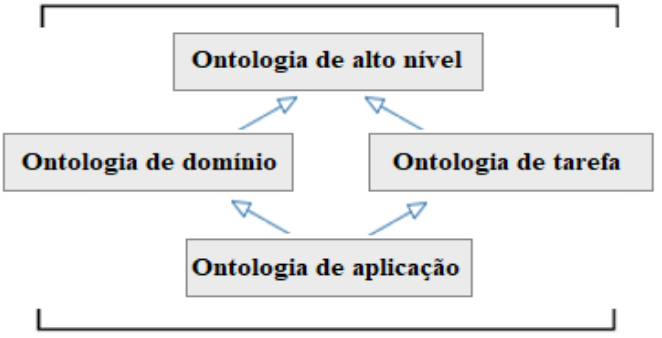

Figura 2.2 – Tipos de Ontologias. Adaptado de (Guarino,1998)

Ontologias de alto nível ou nível superior independem de um problema ou domínio particular, elas descrevem conceitos genéricos, o que possibilita sua reutilização na confecção de novas ontologias. Ontologias de domínio descrevem o vocabulário relacionado a um domínio específico através de especialização dos conceitos. Ontologias de tarefa descrevem o vocabulário relacionado a uma atividade ou tarefa genérica, através de especialização dos conceitos presentes na ontologia de alto nível. Ontologias de aplicação descrevem conceitos que dependem tanto de um domínio particular quanto de uma tarefa especifica, sendo especializações de ambas as ontologias relacionadas. Estes conceitos normalmente correspondem a regras aplicadas a entidades de domínio na execução de determinada tarefa.

A representação das ontologias pode ser realizada de duas maneiras: (i) Gráfica: usada para a compreensão humana; e (ii) Formal: usada para que as ontologias possam ser consumidas por mecanismos automatizados, sendo que nesta representação as linguagens mais populares para descrever ontologias são RDF/RDF-S e OWL (Isotani & Bittencourt, 2015).

2.1.3 *Ontology Web Language* (OWL)

OWL (*Ontology Web Language*) é uma linguagem para definição e instanciação de ontologias *Web*. Uma ontologia OWL pode formalizar um domínio, definindo classes e propriedades destas classes, definir indivíduos e afirmações sobre eles e, usando-se a semântica formal OWL, especificar como derivar consequências lógicas, isto é, fatos que não estão presentes na ontologia, mas são vinculados pela semântica (Smith et al., 2004). Ontologias baseadas em OWL possuem recursos ricos para definir inequivocamente relações e hierarquias complexas e verificar suas consistências por meio de inferência, além de representar informações que não são apenas legíveis por humanos, mas também legíveis e compreensíveis por máquinas (Syed et al., 2016).

Em 2004, a W3C publicou a linguagem de marcação semântica OWL como recomendação para representar e compartilhar ontologias na *Web* (Smith et al., 2004). OWL é uma linguagem baseada nas especificações de RDF e RDF-S; isso significa que

ela herda as características do RDF, como a estrutura baseada em triplas, a descrição de recursos com URI, além da semântica descrita no RDF-S.

Segundo Horridge et al. (2004), OWL trabalha com suposições de mundo aberto, isso implica na impossibilidade de assumir que algo não existe até que isso seja explicitamente definido, ou ainda, algo não pode ser definido como verdadeiro pelo fato de não poder ser assumido como falso, pois o conhecimento pode existir sem ter sido adicionado à base de conhecimento. Esse entendimento é apresentado por Isotani & Bittencourt (2015) ao demonstrarem que apesar dos arquivos OWL armazenarem informações (instâncias) e consequentemente o armazenamento de dados, a principal diferença entre bancos de dados e OWL é a semântica utilizada em cada um deles. Os autores descrevem os bancos de dados como mundos fechados (do inglês, *Closed-World Assumptions*), e as ontologias como mundos abertos (do inglês, *Open-World Assumptions*), e concluem que se determinado fato não está presente em um banco de dados, ele é considerado falso, enquanto em OWL (mundos abertos) se determinado fato não está presente, ele é considerado desconhecido, pois é possível que seja verdadeiro.

OWL provê três sub-linguagens com expressividade crescente: OWL Lite, OWL DL (*Description Logic*) e OWL Full, onde a distinção se observa pelas características relacionadas ao vocabulário, recursos e capacidades de expressividade. OWL Lite suporta necessidades primárias, como classificação de hierarquia e construções simples, entretanto, possui restrições de cardinalidade e tem um número menor de propriedades. O uso desta sub-linguagem é recomendado para migração de tesauros e outras taxonomias. OWL DL e OWL Full compartilham a máxima expressividade, incluindo todas as construções da linguagem OWL, mas em OWL DL com certas restrições. Por exemplo, uma classe pode ser uma subclasse de muitas classes, mas não pode ser uma instância de outra classe (Harmelen & McGuinness, 2004).

Assim como a Web Semântica é uma extensão da *Web* Tradicional, a revisão e extensão da OWL resultou na OWL 2, com o objetivo de tornar o conteúdo da *Web* mais acessível às máquinas, sendo a sua expressividade relacionada às especificações semânticas (W3C OWL Working Group, 2012).

Segundo Isotani & Bittencourt (2015) podemos dividir a OWL em dois níveis, sendo um para descrever a sintaxe e outro para a semântica. Na prática, uma sintaxe é

necessária para armazenar ontologias OWL 2 e trocá-las entre ferramentas e aplicativos. A sintaxe de troca primária para OWL 2 é RDF/XML; embora o RDF/XML forneça interoperabilidade entre as ferramentas OWL 2, outras sintaxes também podem ser usadas, conforme Tabela 2.1 (W3C OWL Working Group, 2012).

Tabela 2.1 – Formato de Serialização OWL

Sintaxes	Propósito
RDF/XML	Intercâmbio, lido e escrito por *software* compatível com OWL2.
OWL/XML	Processamento simples com ferramentas XML.
Sintaxe Funcional	Visualização simples da estrutura formal das ontologias.
Sintaxe *Manchester*	Leitura e escrita simples de Ontologias DL.
Turtle	Leitura e escrita simples de triplas RDF.

O propósito da OWL é representar conhecimento e, sendo assim, na modelagem do conhecimento em OWL são considerados aspectos básicos tais como: Entidades – elementos usados para referenciar um objeto do mundo real; Expressões – combinação de entidades para formar descrições mais complexas e; Axiomas – declarações básicas que permitem realizar inferências sobre as entidades (Isotani & Bittencourt, 2015).

No nível semântico, as duas formas alternativas de atribuir significado às ontologias OWL 2 são a Semântica Direta, que atribui significado para as ontologias em OWL através da Lógica de Descrição e a Semântica baseada em RDF, que é utilizada para a visualização de grafos RDF (W3C OWL *Working Group*, 2012); (Isotani & Bittencourt, 2015).

2.2 Redes de Computadores e Segmentação

Uma rede de computadores é um conjunto de dispositivos conectados por links de comunicação denominados nós (e.g., um computador, uma impressora, um switch ou qualquer outro dispositivo), capaz de enviar ou receber dados gerados por outros nós da rede (Forouzan, 2010). Sua classificação pode ser feita de acordo com sua área geográfica ou organizacional. Por exemplo, uma rede local (*Local Area Network – LAN*) é definida como uma área de comunicação de dados interligada de abrangência restrita e altas taxas de transmissão, onde um pacote de difusão dissemina-se para todos os pontos de acesso ativos (Tanenbaum & Wetherall, 2011).

A comunicação em uma rede local pode ser *unicast*, *multicast* ou *broadcast*. Dizemos que uma comunicação é *unicast* quando os dados são enviados de um dispositivo e endereçado a um destino específico. Na comunicação *multicast* a transmissão é feita para um grupo específico de dispositivos. Quando os dados são enviados para todos os outros dispositivos conectados, a comunicação é classificada como *broadcast* (Tanenbaum & Wetherall, 2011).

A Segmentação de Redes limita a disseminação de broadcast em uma rede local, onde dispositivos de redes (*switches* e roteadores) são usados para bloquear a passagem de pacotes de *broadcast* quando atravessam suas interfaces. Segundo Forouzan (2010), a principal característica atribuída ao uso de VLANs (*Virtual Local Area Networks*) é a possibilidade de se agrupar estações, ou nós, pertencentes a uma ou mais LANs físicas para formar um único domínio de *broadcast*, garantindo a comunicação entre elas, mesmo que façam parte de segmentos físicos diferentes, pois a ideia central da tecnologia VLAN é dividir uma LAN em segmentos lógicos em vez de físicos. O autor afirma ainda que VLANs fornecem uma medida extra de segurança, sendo que usuários pertencentes ao mesmo grupo podem enviar mensagens em *broadcast* com garantia de que usuários de outros grupos não as receberão.

VLANs se baseiam em *switches* especialmente projetados para oferecer este recurso. Na configuração de uma rede com VLANs, o administrador de rede decide a quantidade de VLANs, seus respectivos nomes e quais serão os computadores ligados a cada uma delas (Tanenbaum & Wetherall, 2011). A Figura 2.3 apresenta uma rede LAN com três grupos de computadores compartilhando o mesmo *switch* e a Figura 2.4 mostra a segmentação de uma LAN em três redes locais virtuais.

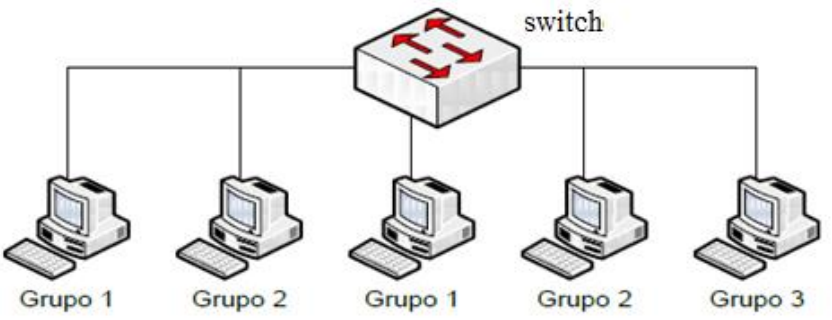

Figura 2.3 – Grupos de Computadores em uma Única Rede Local

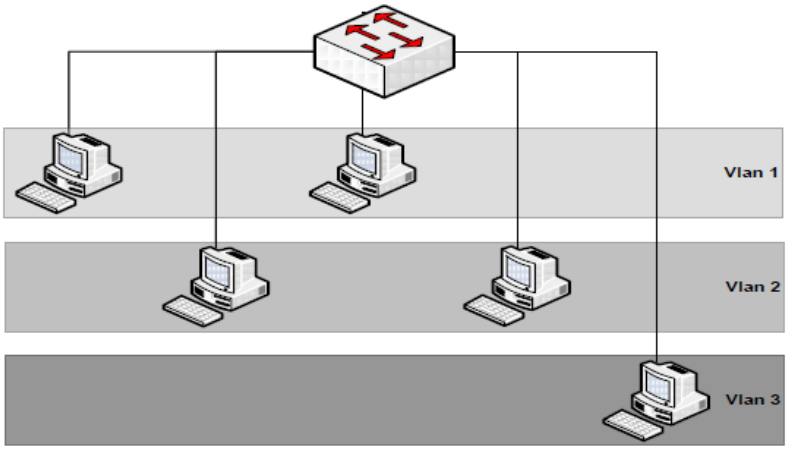

Figura 2.4 – Computadores Isolados Logicamente Através de Redes Virtuais

Para que os pacotes de dados trafeguem de uma origem até um destino, através de uma rede, é importante que todos os dispositivos da rede usem a mesma linguagem, ou protocolo. Com a necessidade de padronizar a comunicação sobre a arquitetura de redes surgiram o modelo de referência OSI (*Open System Interconnection*) e o protocolo TCP/IP. O modelo OSI, desenvolvido pela ISO (*International Standards Organization*), é uma proposta constituída por sete camadas hierárquicas (1 – Física, 2 – Enlace, 3 – Rede, 4 – Transporte, 5 – Sessão, 6 – Apresentação e 7 – Aplicação), que executam funções bem definidas, as quais foram escolhidas com base nas definições de protocolos padronizados internacionalmente. Segundo Tanenbaum & Wetherall (2011), cada camada é uma espécie de máquina virtual, oferecendo determinados serviços à camada situada imediatamente acima dela.

Switches de rede podem operar tanto na camada de enlace de dados (Camada 2) quanto na camada de rede (Camada 3) do modelo OSI, de acordo com suas especificações. A camada de enlace é responsável por controlar o fluxo de dados (recepção, delimitação e transmissão de quadros ou pacotes) e estabelece um protocolo de comunicação entre sistemas diretamente conectados; a camada de rede é responsável por enviar os dados entre múltiplas redes ou de uma rede local para outra.

Neste contexto, um switch L2 (camada 2) atua na camada de enlace do modelo OSI utilizando as identificações (MAC *address*) dos dispositivos para identificar os pacotes de dados recebidos e tomar a decisão de melhor encaminhamento para o endereço

de destino. Esse *switch* executa essencialmente a função de ponte entre os segmentos da LAN, uma vez que encaminha os quadros de dados com base em seu endereço de destino, ignorando qualquer preocupação com o protocolo de rede que está sendo usado. As funções básicas de um *switch* L2 são: Aprender os MAC *address* de origem dos dispositivos conectados às suas portas; encaminhar ou filtrar quadros conforme o endereço de destino dos quadros e evitar os *loops* de camada de enlace possibilitando caminhos redundantes.

Um *switch* L3 (camada 3) atua na camada de enlace e rede do modelo OSI, ou seja, possui as funcionalidades de switch e roteador, suportando o uso dos endereços lógicos do protocolo TCP/IP. Isso permite que dispositivos conectados na mesma sub-rede ou VLAN troquem informações com maior velocidade. Os *switches* L3 não se limitam apenas ao uso do MAC *address* para endereçar os pacotes, eles também incorporam tabelas IP que permitem gerenciar o tráfego dentro de uma LAN com várias localidades.

Apesar de *switches* L3 e roteadores possuírem funções de roteamento, eles não podem ser classificados como concorrentes, pois um roteador tem como principal função o roteamento de pacotes entre várias redes, e um *switch* L3 tem como função interconectar dispositivos dentro da mesma rede. Além disso, um roteador suporta serviços como MPLS (*Multiprotocol Label Switching)*, VPN (*Virtual Private Network*) e possui tecnologias de segurança como o *firewall*, sendo que um *switch* de rede não suporta esses serviços e não possui portas WAN (*Wide Area Network*); no entanto, é equipado com *hardware* otimizado para o encaminhamento interno de dados na rede lhe proporcionando maior velocidade.

2.2.1 Protocolos da camada de enlace

A topologia de rede de computadores pode ser dividida em física e lógica. A topologia física é a combinação dos nós e as conexões físicas entre eles. A topologia lógica é o modo como uma rede transfere dados ou quadros de um nó para outro. Regras estabelecidas tem a propriedade de propor harmonia em um determinado meio, onde bits que trafegam pela rede podem ser controlados entre dispositivos, assim como o fluxo das taxas de transmissão e a determinação de caminhos, origem e destino (Forouzan, 2010).

Segundo Kurose & Ross (2013), um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão ou no recebimento de uma mensagem. Protocolo e padrões podem ser vistos como sinônimos de regra e regras pré-acordadas respectivamente. Os padrões são desenvolvidos por meio da cooperação de comitês de criação de padrões, fóruns e órgãos governamentais reguladores (Forouzan, 2010).

Os protocolos e padrões de tecnologia de telecomunicações são definidos geralmente por empresas de comunicações ou organizações de engenharia como IEEE (*Institute of Electrical and Electronics Engineers*), ITU (*International Telecommunication Union*), ISO (*International Organization for Standardization*), e ANSI (*American National Standards Institute*) (Tanenbaum & Wetherall, 2011). Os serviços e especificações da camada de enlace são geridos por vários padrões de acordo com a tecnologia e o meio físico integrado por tais protocolos. A Tabela 2.2 destaca as organizações e alguns dos mais importantes protocolos da camada de enlace de dados.

Tabela 2.2 – Protocolos Padrões da Camada de Enlace de Dados

Organização	**Protocolos: Camada de Enlace**

IEEE	• 802.1: Lans *architecture*
	  • 802.1AB: LLDP (*Link Layer Discovery Protocol*)
	  • 802.1Q: *Frames to* VLANs
	  • 802.1D: STP (*Spanning Tree Protocol*)
	  • 802.1W: RSTP (*Rapid* STP)
	  • 802.1S : MSTP (*Multiple* STP)
	• 802.2: LLC (*Logical Link Control*)
	• 802.3: *Ethernet* (*wired networks*)
	• 802.4: *Token Bus*
	• 802.5: *Token Ring*
	• 802.11: *Wireless LAN*

ITU	• Q.921: *User-network interface - Data link layer specification* • Q.922: *Frame Relay*
ISO	• HDLC (*High Level Data Link Control*)
ANSI	• 3T9.5: FDDI (*Fiber Distributed Data Interface*) / MAC • ADCCP (*Advanced Data Communications Control Protocol*)

Existem protocolos alternativos que não são adequados para redes com equipamentos de múltiplas marcas, pois pertencem a uma organização particular que os utilizam em seus equipamentos. Por exemplo, protocolos de propriedade Cisco (Empson & Schmidt, 2014), a saber:

DTP (*Dynamic Trunking Protocol*), direcionado a negociar o entroncamento entre dois *switches* com reconhecimento de VLAN e negociar o tipo de encapsulamento a ser usado;

ISL (*Inter-Switch Link*), voltado à interconexão de vários switches e manutenção de informações de VLAN. Quando dois *switches* Cisco conectados negociam automaticamente um tronco com DTP, eles escolherão ISL em vez de 802.1Q. Cabe observar que a Cisco descontinuou o ISL e alguns dos *switches* mais recentes não os suportam.;

CDP (*Cisco Discovery Protocol*), voltado à descoberta de equipamentos na rede, facilitando a compreensão da topologia da rede e de sua arquitetura (semelhante ao LLDP);

VTP (VLAN *Trunking Protocol*), direcionado a manter a consistência da configuração de VLAN, gerenciando a adição, exclusão e renomeação de VLANs em toda a rede.

A instituição IETF (*Internet Enginnering Task Force*) especifica os padrões que serão implementados e utilizados em toda a Internet. Ela mantém as RFCs[1] (*Request for Comments*), documentos técnicos que detalham o funcionamento de todos os aspectos do protocolo proposto (Forouzan, 2010). O número de um RFC é único, porém se o padrão (protocolo) necessitar de atualizações a IETF gera um novo RFC com as devidas melhorias, mantendo as características do modelo original. Caso seja aprovado pelo Comitê, esse documento se torna uma nova RFC com uma numeração diferente da original, que não é excluída (Forouzan, 2010). A Tabela 2.3 apresenta alguns exemplos de RFCs referenciados neste trabalho.

[1] https://www.rfc-editor.org/

Tabela 2.3 – Protocolos e RFCs

Protocolo	RFC
ARP	826
DHCP	2131, 2132
DNS	1034, 1035,
HTTP	1945, 2068, 2109
IPV4	791
IPv6	1550, 2460
SNMP	1157
TCP	793
UDP	768

3 REVISÃO BIBLIOGRÁFICA

Este capítulo apresenta uma síntese da revisão sistemática de literatura (Cruz et al., 2021) que foi conduzida para identificar trabalhos que apresentam ontologias de vulnerabilidades e ataques a VLAN. Na Seção 3.1, é descrito o protocolo de revisão; na Seção 3.2, é apresentado o resultado da revisão; e, na Seção 3.3, os trabalhos relacionados são apresentados.

3.1 Protocolo de Revisão

O mapeamento sistemático da literatura foi baseado, com adaptações, nos métodos de (Mendonça et al., 2019) e (Kitchenham, 2004). O estudo teve como principal objetivo responder a seguinte questão de pesquisa: "*Quais trabalhos apresentam ou fazem uso de abordagens ontológicas para lidar com vulnerabilidades e ataques a VLANs?*". Com base na questão de pesquisa, uma busca exploratória foi realizada com o objetivo de levantar os parâmetros da revisão literária, e.g., período de busca, bases científicas, palavras-chaves, e área de conteúdo (e.g., título, resumo).

O processo proposto consiste em 3 fases: planejamento, condução e síntese. O planejamento foi realizado com base em um protocolo de revisão, contendo o tema e os objetivos da revisão. Foram selecionadas as seguintes bases de dados científicas, uma vez que abrangem pesquisas relevantes sobre o tema: IEEE *Xplore*, Google *Scholar* e *Springer Link*.

Os seguintes critérios de inclusão foram definidos: (1) Artigos oriundos de periódicos ou anais de eventos científicos, cujo texto completo esteja disponível nas bases de dados científicas; (2) Trabalhos publicados após 2010; (3) Trabalhos que apresentam ontologias de vulnerabilidades e ataques a VLANs; (4) Trabalhos publicados na língua inglesa. Os seguintes critérios de exclusão foram definidos: (1) Área de pesquisa diferente de Ciência da Computação; (2) Trabalhos que não enfocam tópicos relacionados a esta revisão; (3) Artigos curtos e resumos. Foram definidas as palavras-chave e uma string de busca: "(*ontology* AND *vulnerability* AND *attack* AND *VLAN* AND *network*)".

Durante a fase de condução, a string de busca foi adaptada à sintaxe e particularidades de cada base de busca (Tabela 3.1); especificamente, foram consideradas a forma de inserção de palavras-chave, campos selecionados e refinamento nas buscas. No caso de retorno nulo de artigos, as palavras-chave foram ajustadas para uma restrição menor.

Tabela 3.1 – Strings de Busca e Quantidade de Artigos Coletados

Bases de dados científicas e *string* de busca específica	**Coletados**
IEEE Xplore (2010-2020): ("Document Title": ontology AND vulnerability AND attack AND VLAN AND network).	15
Springer Link (2010-2020): field “where the title contains”: “ ontology AND vulnerability AND attack AND VLAN AND network”.	12
Google Scholar (2010-2020): allintitle: "Ontologies of Vulnerability and Attacks on VLAN Networks".	242

A Restrição do período de busca dos artigos publicados se deu entre 2010 e 2020. Foram considerados 30 primeiros artigos por ordem de relevância. Os critérios de inclusão e exclusão forma definidos por um processo iterativo de leitura dos trabalhos (na busca exploratória) com relevância ao tema proposto. Os artigos remanescentes foram submetidos aos critérios de inclusão e exclusão, considerando-se na primeira avaliação o título, resumo e palavras-chave.

Na fase de síntese, 11 artigos foram excluídos referentes ao resumo. Os 19 artigos categorizados como trabalhos com possibilidade de aderência ao tema da pesquisa foram avaliados em sua totalidade perante os critérios, e 2 artigos foram citados pelos estudos analisados, sendo um de 2004 incluso na revisão; 2 estudos foram identificados como não aderentes e 4 trabalhos são revisões de literatura relacionadas ao tema.

3.2 Resultados da Revisão

Nesta seção, uma análise sintética dos trabalhos selecionados é apresentada. Os estudos apresentam soluções baseadas em ontologias para análise de vulnerabilidades, detecção e ataques a sistemas computacionais. A Subseção 3.2.1 apresenta trabalhos que fazem uso de ontologias; e a Subseção 3.2.2 apresenta trabalhos que propõem ontologias.

3.2.1 Trabalhos que fazem uso de ontologias

Bhandari & Gujral (2014) propuseram um framework, que usa uma ontologia desenvolvida como base de conhecimento, para percepção do estado de segurança da rede. A ontologia é usada para inferir o impacto de vários eventos que acontecem no status de segurança da rede, sendo vulnerabilidade, rede e ataque as principais classes da ontologia. Segundo os autores, rede de computadores é uma entidade dinâmica cujo estado muda com a introdução de novos serviços, instalação de novo sistema operacional de rede e adição de novos componentes de *hardware* e criação de novas funções de usuário, propiciando constantes ataques. Vários mecanismos de segurança empregados na rede não fornecem a imagem completa da segurança de toda a rede.

Shenbagam & Salini (2014) apresentam uma abordagem baseada em ontologia para defender de ataques no nível do aplicativo. Um sistema de previsão de ataques baseado em ontologia é proposto para classificar os ataques de aplicativos da *Web*.

Si et al. (2014) apresentam um método de fusão de elementos de situação de segurança de rede baseado em ontologia; é construído um modelo de fusão que contém o ambiente de rede, a vulnerabilidade da rede, o ataque à rede, o incidente de segurança da rede e o sensor como classe principal. O foco dos autores está na técnica para mostrar que o método pode tornar os elementos da situação uniformemente descritos.

Choi et al. (2015) analisam o código de uma APT (*Advanced Persistent Threat*) para propor um método para detecção desse tipo de ataque, com base em uma ontologia de comportamento do ataque. Um ataque inteligente de APT é usado para definir regras de inferência sobre o comportamento do ataque.

Krauß & Thomalla (2016) apresentam uma abordagem baseada em ontologia para detecção de ataques cibernéticos a sistemas SCADA (*Supervisory Controland Data Acquisition*). Os logs do sistema fornecem os eventos que os sistemas de detecção de intrusões (IDS) podem reconhecer como suspeitos e podem fazer parte de um ataque. O modelo proposto usa bases de dados de vulnerabilidades conhecidas para identificar ataques contínuos.

Xu et al. (2017) apresentam um modelo de reconhecimento de situação de segurança de rede para dispositivos IoT (*Internet of Things*). A proposta usa um método

de raciocínio de situação baseado em ontologia e regras semânticas definidas pelo usuário. Segundos os autores, ontologias podem fornecer uma descrição unificada e formalizada para resolver o problema de heterogeneidade semântica no domínio de segurança de IoT.

3.2.2 Trabalhos que propõem ontologias

Gao et al. (2013) classificam os ataques em uma taxonomia adequada para avaliação de segurança e apresentam uma estrutura baseada em ontologia para avaliação de segurança de sistemas. Os autores descrevem a utilização da ontologia na avaliação de segurança e um método para avaliar o efeito de ataques ao sistema quando este está sob ataque. A taxonomia proposta consiste em cinco dimensões, que incluem impacto de ataque, vetor de ataque, alvo de ataque, vulnerabilidade e defesa. Os conceitos relacionados ao ataque incluídos nas cinco dimensões e os relacionamentos entre eles são formalizados e analisados em detalhes, construindo uma ontologia de acordo com a taxonomia.

Karande & Gupta (2015) propõem um IDS (*Intrusion Detection Systems*) baseado em uma ontologia de segurança de aplicativos *Web*. A captura de informações por contexto de *links* e *scripts* é a premissa do sistema proposto; o modelo de ontologia estabelece um relacionamento semântico entre ataques e redes; O modelo ontológico do IDS proposto detecta ataques de protocolos específicos e identifica *scripts* maliciosos, além de identificar os tipos de ataques e vulnerabilidades. Os autores enfatizam que a ontologia proposta é recomendada para descrever conceitos de segurança de serviços da *Web* e que os modelos de segurança mapeados para a ontologia parecem ser eficazes.

Kshirsagar et al. (2015) propõem uma ontologia para detecção de ataques que exploram a vulnerabilidade que permite o ataque de divisão de resposta HTTP (*HTTP response splitting*). A ontologia proposta possibilita a geração de regras semânticas.

Chavan & Tamane (2016) apresentam uma ontologia para construção de regras de política de segurança. Com base nas arquiteturas de nuvem, regras de segurança para proteção de ataques a aplicativos da *Web* podem ser especificadas. Os autores analisam o estudo, o *design* e o objetivo da ontologia, que contém algoritmos de criptografia. A ontologia descreve a especificação de regras de segurança e o algoritmo de criptografia

descreve a comparação de desempenho entre diferentes algoritmos. No trabalho são discutidas outras abordagens, tais como ataques de serviços da *Web* baseados em nuvem e detecção de tráfego malicioso pela Internet.

Mohsin & Anwar (2016) propõem uma estrutura ontológica para IoT (*Internet of Things*) com o objetivo de proteger contra APTs. A estrutura compreende o entendimento dos padrões de ataque e as vulnerabilidades, e os alinha à semântica da rede para avaliar sua aplicabilidade nos sistemas de IoT. Em seguida, deduz automaticamente soluções eficientes para alterar as táticas de ataque, realizando análises de custo-benefício de contramedidas viáveis por meio de raciocínio ontológico baseado em regras. Ontologias de padrões de CTI (*Cyber Threat Intelligence*) são estendidas com novos conceitos e alinhadas com uma nova ontologia de IoT.

Falodiya & Das (2017) apresentaram uma ontologia para gráficos de ataque com o objetivo de analisar vulnerabilidades de segurança em redes corporativas. Segundo os autores, o gráfico de ataque ajuda na modelagem de vulnerabilidades de segurança, bem como na identificação de possíveis caminhos em uma rede corporativa que podem ser usados por um invasor na exploração das vulnerabilidades de rede.

Choi & Choi (2019) propõem uma ontologia de contexto de segurança partindo da análise de vulnerabilidades de segurança de um sistema de energia em um ambiente IoT-*Cloud* de energia. A ontologia possibilita a definição de regras para inferência do contexto de segurança de infraestruturas críticas.

Zhu et al. (2019) propõem uma ontologia de vulnerabilidade, com base nos bancos de dados públicos de segurança da informação. O objetivo principal é padronizar e descrever as informações sobre vulnerabilidades conhecidas.

Heerden et al. (2012) apresentam um método usando ontologia para classificar ataques a redes de computadores. Segundo os autores, devido os ataques serem diversos, não há uma classificação padrão. Afirmam que se um ataque pudesse ser classificado, ele poderia ser mitigado de acordo. Uma taxonomia de ataques à rede de computadores forma a base da ontologia. A ontologia desenvolvida usa a classe "Attack Scenario", que se baseia em outras classes para caracterizar e classificar ataques a redes de computadores. Um cenário de ataque é composto por fases, tem um escopo e é atribuído a um ator e

agressor que possuem um objetivo. Concluem que ataques de rede de computadores de alto perfil, como Stuxnet e ataques da Estônia, agora podem ser classificados por meio da classe "Attack Scenario".

3.2.3 Análise sintética dos artigos selecionados

Manter a segurança e a privacidade das informações na nuvem se torna um problema crítico (Chavan & Tamane 2016). O uso cada vez maior de aplicativos da *Web* leva a uma grande quantidade de ameaças e vulnerabilidades; 81% dos ataques de *hackers* são direcionados a aplicativos da *Web*, que impõem uma grande ameaça à segurança de bancos *on-line*, comércio eletrônico e outras organizações (Kshirsagar et al. 2015). A principal preocupação de segurança para comunidades de *e-business* e compartilhamento de informações é a segurança de aplicativos da *Web;* 75% dos ataques são executados na camada de aplicação e praticamente 90% dos aplicativos possuem alguma vulnerabilidade (Shenbagam & Salini 2014).

Estudos sobre os riscos e vulnerabilidade provenientes do uso de VLANs em ambientes computacionais são escassos. Pode-se inferir dos trabalhos a necessidade premente de proteção das redes segmentadas, as quais muitas vezes são negligenciadas pelo desconhecimento de vulnerabilidades e ataques.

Foram identificadas soluções baseadas em ontologias para apoiar métodos, modelos e análises de vulnerabilidades, e detecção de ataques a sistemas computacionais. No contexto da modelagem conceitual visando a proteção das redes VLAN, as ontologias podem ser usadas para formalizar e relacionar conceitos importantes, mapear vulnerabilidades e ataques conhecidos, descrever processos de proteção, gerar regras para inferência, entre outras aplicações.

A abordagem empregada nesta revisão da literatura permitiu a verificação e análise de tendências, bem como abordagens tecnológicas adotadas ao longo dos últimos dez anos. Em um universo de 269 artigos inicialmente recuperados, 19 trabalhos foram criteriosamente selecionados, classificados e sintetizados de modo a representar o estado-da-arte das abordagens. Foram apresentadas as técnicas e teorias utilizadas, os aspectos

positivos e limitações dos estudos, bem como apontadas lacunas na literatura e desafios de pesquisa, atuais e futuros.

A Tabela 3.2 apresenta uma síntese dos trabalhos analisados, categorizados por objetivo e domínio de aplicação, conforme segue: *Objetivo*: (Ou) Ontologia - uso; (Oa) Ontologia - apresentação de proposta ; (Mt) Método; (Md) Modelo (F) Framework; (T) Taxonomia. *Domínio de Aplicação*: (1) Vulnerabilidades; (2) Ataques ou Detecção; (3) Mitigação ou Defesa; (4) Status – Rede ou Segurança.

Tabela 3.2 – Síntese dos Trabalhos Analisados

Autores	Objetivo						Domínio			
	Ou	Oa	Mt	Md	F	T	1	2	3	4
Bhandari & Gujral (2014)	X	X		X		X	X	X	X	X
Shenbagam & Salini(2014)	X		X				X	X		
Si et al. (2014)	X		X							X
Choi et al. (2015)	X		X					X	X	
Krauß & Thomalla (2016)	X		X					X	X	
Xu et al. (2017)	X			X						X
Gao et al. (2013)	X	X		X		X	X	X	X	X
Karande & Gupta (2015)		X		X			X	X	X	
Kshirsagar et al. (2015)		X		X				X		
Chavan & Tamane (2016)		X		X				X		X
Mohsin & Anwar (2016)		X		X			X	X	X	X
Falodiya & Das (2017)		X	X				X	X	X	
Choi & Choi (2019)		X		X			X		X	X
Zhu et al. (2019)		X		X			X			
Heerden et al. (2012)		X	X			X	X	X		X

3.2.4 Análise sintética de revisões de literatura similares

Como trabalhos relacionados, quatros artigos são destacados e detalhados nos parágrafos seguintes. Os trabalhos foram considerados relacionados por abordarem aspectos como vulnerabilidades, ataques e segurança de redes, além de apresentarem objetivo semelhante ao proposto nesta dissertação.

Simmonds et al. (2004) basearam a revisão em textos padrão, usando conceitos, categorizações e métodos bem conhecidos, por exemplo, análise de risco usando perfis de ameaças baseados em ativos e perfis de vulnerabilidade. Foram considerados os serviços de segurança de rede, análise das ameaças, vulnerabilidades e modos de falha. A revisão é usada para construir uma estrutura, a qual é usada para definir uma ontologia extensível para ataques à segurança de rede.

Bijani & Robertson (2014), apresentam e classificam os principais ataques em MASs (*Multi-agent Systems*) abertos. Nesta revisão de literatura, os autores pesquisam e analisam as várias técnicas de segurança e as categorizam como abordagens de prevenção e detecção. Adicionalmente, sugerem qual técnica de segurança é uma contramedida apropriada para quais classes de ataque.

Robert Luh et al. (2017), descrevem que a falta de foco específico em APT (*Advanced Persistent Threats*) ou ataques sofisticados em vários estágios, transformam as metodologias apropriadas de domínio em um desafio de pesquisa. Apresentam, dentro deste contexto, um esquema detalhado de avaliação da literatura, além de um modelo para categorização de artigos. Os artigos selecionados são analisados e avaliados de forma abrangente de acordo com as diretrizes de Kitchenham. Os autores combinam novos insights e o *status quo* da pesquisa atual ao conceito de uma abordagem sistêmica ideal, capaz de processar semanticamente e avaliar informações em diferentes aspectos. Os trabalhos apresentados contribuem para a análise ou detecção de ataques direcionados.

Singh et al. (2019), apresentam um estudo estruturado para encontrar potenciais contribuições que analisam e detectam APTs (*Advanced Persistent Threats*); a pesquisa exploratória abrange diversos aspectos, tais como a exploração da infraestrutura da *Web* e protocolos de comunicação. Para superar esses desafios e ataques, os autores apresentam um esquema de avaliação de literatura que classifica e fornece contramedidas ao ataque de APT.

3.2.5 Análise comparativa das revisões de literatura

Destacam-se os seguintes aspectos que diferenciam a revisão de literatura da dissertação das revisões apresentadas: (1) o foco desta revisão está em um estudo sobre ontologias de vulnerabilidades e ataques a redes VLAN, evidenciando os principais

ataques da camada de enlace do modelo de referência OSI; (2) as revisões existentes focam aspectos como vulnerabilidades ataques e segurança para soluções que visam o status de segurança da rede de forma genérica; estas não abrangem, em uma discussão mais aprofundada, os riscos e problemas provenientes do uso de uma rede segmentada; e, (3) os estudos não abordam análises das vulnerabilidades de protocolos de camadas especificas de atuação.

A Tabela 3.3 apresenta uma análise comparativa dos trabalhos relacionados, categorizados por objetivo e domínio de aplicação, conforme segue: *Objetivo*: (Ou) Ontologia - uso; (Oa) Ontologia - apresentação de proposta; (Mt) Método; (Md) Modelo (F) Framework; (T) Taxonomia. *Domínio de Aplicação*: (1) Vulnerabilidades; (2) Ataques ou Detecção; (3) Mitigação ou Defesa; (4) Status – Rede ou Segurança.

Tabela 3.3 – Análise Comparativa das Revisões de Literatura.

Autores	Objetivo						Domínio			
	Ou	Oa	Mt	Md	F	T	1	2	3	4
Simmonds & Sandilands (2004)		X		X		X	X	X	X	X
Bijani & Robertson (2014)				X		X		X	X	X
Robert Luh et al. (2017)				X		X		X		X
Singh et al. (2019)				X		X		X	X	
Esta Revisão de Literatura	*X*	*X*		*X*		*X*	*X*	*X*	*X*	*X*

3.3 Trabalhos Relacionados

Como trabalhos relacionados, 3 artigos sobre ontologias de vulnerabilidades e ataques a redes de computadores são destacados e detalhados nesta seção. Os trabalhos foram considerados relacionados por abordarem aspectos como vulnerabilidades, ataques e segurança de redes, além de apresentarem objetivos semelhantes ao proposto nesta dissertação.

Heerden et al. (2012) apresentam um método baseado em uma ontologia de cenário de ataque a redes. O método proposto pode ser utilizado para caracterizar e classificar ataques a redes de computadores.

Bhandari & Gujral (2014) propõem uma ontologia para identificar o status (seguro, vulnerável ou sob ataque) da segurança da rede.

Falodiya & Das (2017) apresentam uma ontologia para gerar grafos de ataque para analisar as vulnerabilidades de segurança de redes corporativas.

Este trabalho difere dos listados nos seguintes aspectos:

(i) Esta dissertação destaca os principais ataques da Camada 2 (Enlace de Dados) do modelo OSI (*Open Systems Interconnection*), onde estão localizadas as VLANs;

(ii) Os demais estudos não abordam a análise das vulnerabilidades de protocolos de camadas específicas de atuação;

(iii) Os trabalhos analisados focaram em aspectos como ataques, vulnerabilidades e segurança para soluções de software que visam prover o status de segurança de rede de forma genérica; estes não cobrem os perigos ou problemas decorrentes do uso de uma rede de computadores segmentada; e

(iv) Os demais trabalhos não propõem estratégias de defesa ou mitigação de riscos de ataques a partir da ontologia.

A Tabela 3.4 apresenta uma síntese dos trabalhos relacionados e uma comparação com os resultados desta dissertação. Os trabalhos são classificados de acordo com os domínios de aplicação abordados, análise dos recursos de camada, abordagem de segurança, estratégia de defesa e disponibilidade para reuso. Além dos pontos descritos anteriormente e na tabela, destaca-se que OVAV é uma ontologia de domínio e foi desenvolvida utilizando a Web Ontology Language (OWL).

Tabela 3.4 – Análise Comparativa dos Trabalhos Relacionados.

Artigo / Características	Heerden et al. (2012)	Bhandari & Gujral (2014)	Falodiya & Das (2017)	Cruz et al. (2023) Este trabalho
Contexto da Ontologia	*Classificar ataques a redes de computadores*	*Identificar o status de segurança da rede*	*Analisar vulnerabilidades de segurança de redes corporativas*	*Mapear vulnerabilidades e ataques a VLANs propondo estratégias de defesa*
Domínio de aplicação	*Vulnerabilidade Ataque Impacto*	*Vulnerabilidade Ataque Impacto*	*Vulnerabilidade Ataque Impacto Contramedidas*	*Vulnerabilidade Ataque Impacto Contramedidas*
Recursos de camada abordados	*Computador pessoal e Disp. Infraestrutura de rede*	*Componentes de Hardware e S.O*	*Estações de trabalho e Servidores*	*Protocolos camada 2 / OSI Switches e Roteadores*
Abordagem de segurança	*Genérica*	*Genérica*	*Genérica*	*Específica*
Estratégias de defesa	*Não*	*Não*	*Não*	*Sim*
Disponível para reuso	*Não*	*Não*	*Não*	*Sim*
Observações	*Abordagem genérica sem análise dos riscos e ameaças nos dispositivos*	*Abordagem genérica sem análise dos riscos e ameaças nos dispositivos*	*Abordagem genérica sem análise dos riscos e ameaças nos dispositivos*	*Abordagem específica dos riscos e ameaças nos dispositivos e protocolos de camada*

4 ONTOLOGIA DE VULNERABILIDADES E ATAQUES A VLAN (OVAV)

Neste capítulo, apresenta-se a Ontologia de Vulnerabilidades e Ataques a VLAN (OVAV). O modelo conceitual proposto visa a identificar, formalizar e relacionar conceitos importantes, mapear vulnerabilidades e ataques, além de propor estratégias de proteção (Cruz et al., 2023). Termos importantes como VLAN, vulnerabilidade, ataque, propriedade de segurança, impacto, contramedida e seus relacionamentos, são formalizados por meio de uma ontologia de domínio em formato OWL com o suporte da ferramenta Protégé[2].

O projeto de uma ontologia é um processo iterativo para determinar o escopo e definir os conceitos (classes), instâncias, propriedades, relações, axiomas e restrições. A enumeração de termos preza por fontes confiáveis para aquisição do conhecimento relacionado ao domínio específico. Esta etapa foi integralmente realizada usando como fonte o material apresentado na revisão de literatura, o qual apontou métodos, modelos, ferramentas e áreas de atuação, bem como o referencial teórico e especialistas do domínio.

A ontologia de domínio descreve os conceitos explícitos de um domínio específico do conhecimento e seus relacionamentos, sendo observado em seu uso a padronização de conceitos, termos e definições, bem como a facilidade do compartilhamento de conhecimento e auxílio na análise das informações. Ontologias baseadas em OWL possuem recursos ricos para definir inequivocamente relações e hierarquias complexas e verificar suas consistências por meio de inferência, além de representar informações que não são apenas legíveis por humanos, mas também compreensíveis por máquina.

Uma visão geral da ontologia desenvolvida, contendo as principais classes é apresentada na Figura 4.1, e OVAV.owl (Versão 1.0) está disponível no repositório *Github* (Cruz et al., 2022).

O núcleo da ontologia OVAV contém os principais conceitos do domínio específico, permitindo assim a estruturação e compreensão dos conceitos relacionados. As propriedades das classes permitem a definição da relação entre conceitos. A Tabela 4.1

[2] https://protege.stanford.edu/

apresenta a estratégia de relacionamento, com as propriedades destacadas em vermelho; conceitualmente as classes são descritas nos parágrafos e Sessões seguintes.

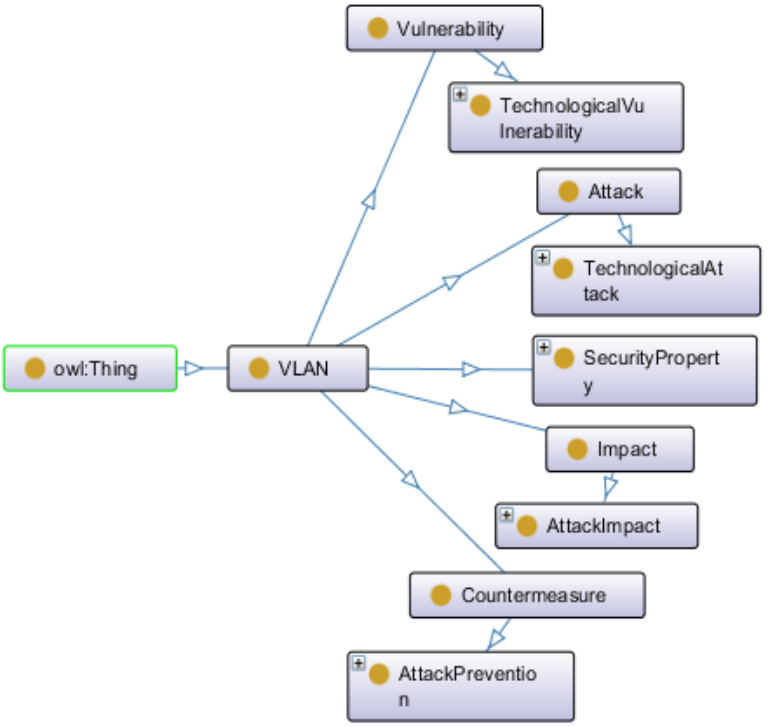

Figura 4.1 – Principais Classes de OVAV.owl

Tabela 4.1 – Representação das Propriedades das Classes

VLAN	Tem	Vulnerabilidade Tecnológica tipo de Vulnerabilidade	é explorada por	Ataque
	Tem	Ataque Tecnológico tipo de Ataque	ameaça	VLAN
			explora	Vulnerabilidade
			causa	Impacto
			viola	Propriedade de Segurança
	Tem	Propriedade de Segurança	é violada por	Ataque
	Tem	Impacto do Ataque tipo de Impacto	é causado por	Ataque
	Tem	Prevenção de Ataque tipo de Contramedida	protege	VLAN
			previne	Ataque

***Vulnerabilidade*:** É a fraqueza de um ativo, a qual pode acontecer durante a sua concepção, implementação, configuração ou operação, podendo ser potencialmente explorada por um ou vários ataques.

***Ataque*:** É a exploração de uma vulnerabilidade por uma ameaça a dispositivos computacionais com propósito malicioso para, por exemplo, destruir, expor, alterar, desativar, roubar ou obter qualquer ganho não autorizado.

***Propriedade de Segurança*:** São atributos ou características de segurança específicas de informações.

***Impacto*:** É um efeito ou consequência de um ataque para uma organização, com relação às propriedades de segurança, sendo medido pelas consequências causadas.

***Contramedida*:** É uma ação de defesa visando as melhores práticas que irão prevenir a exploração de vulnerabilidades por ataques em VLANs.

Na definição das classes utiliza-se uma abordagem *Top-Down*, onde os termos mais gerais são formulados primeiramente, permitindo que termos mais especializados sejam utilizados como subclasses. Para representação na ontologia, cada expressão ou termo possui uma instância. No reuso de outras ontologias, analisou-se uma ontologia de aplicação, proposta por de Franco Rosa *et al*. (2018), e reutilizadas 6 propriedades de segurança. Optou-se por não fazer uso de uma ontologia de nível superior devido às particularidades do domínio de VLAN.

Na Subseção 4.1, descreve-se a Classe *TechnologicalVulnerability* (um tipo de *Vulnerability*), que representa as falhas ou fraquezas nos dispositivos ou protocolos. Na Subseção 4.2, descreve-se a Classe *TechnologicalAttack*, que representa como os ataques atingem os dispositivos. Na Subseção 4.3, exemplos do uso da Classe *SecurityProperty* são apresentados. Considera-se *Impact* a extensão do dano causado por um *Attack*. Na Subseção 4.4, descreve-se a Classe *AttackImpact*, que representa que tipo de *SecurityProperty* um ataque pode impactar.

4.1 Vulnerabilidade Tecnológica

Vulnerabilidades Tecnológicas (Classe *TechnologicalVulnerability*) são tipos de fraquezas provenientes de protocolos ou dispositivos, expondo-os a um possível ataque.

As vulnerabilidades foram mapeadas conceitualmente e classificadas criteriosamente. Listar os tipos genéricos de vulnerabilidades forneceu as informações críticas necessárias para classificá-las.

A seleção das vulnerabilidades foi realizada usando como fonte a base de conhecimento CVE[3] (*Common Vulnerabilities and Exposures*). A Tabela 4.1 apresenta três exemplos de vulnerabilidades críticas de VLAN mapeadas no contexto deste trabalho e a tabela completa (Apêndice I – Tabela A1.1) contém todas as 49 vulnerabilidades mapeadas, e está disponível no repositório *GitHub* (Cruz & de Franco Rosa, 2022).

Tabela 4.2 – Exemplos de Vulnerabilidades Críticas de VLAN Mapeadas

ID	Descrição da Vulnerabilidade	Dispositivos e Recursos Vulneráveis
03	*Protocol* 802.1q	*Protocol* 802.1q / VLAN
21	*Frame flood*	IBM *System Networking* (FCoE), *Switches* (BNT) (NOS)
23	ARP *request*	*kernel in* Juniper Junos 10.4; 11.4; 11.4x27; 12.1; 12.1x44; 12.2; 12.3

Conforme apresentadas na Figura 4.2, as instâncias são identificadas por um losango roxo e as classes são identificadas por meio de um círculo alaranjado.

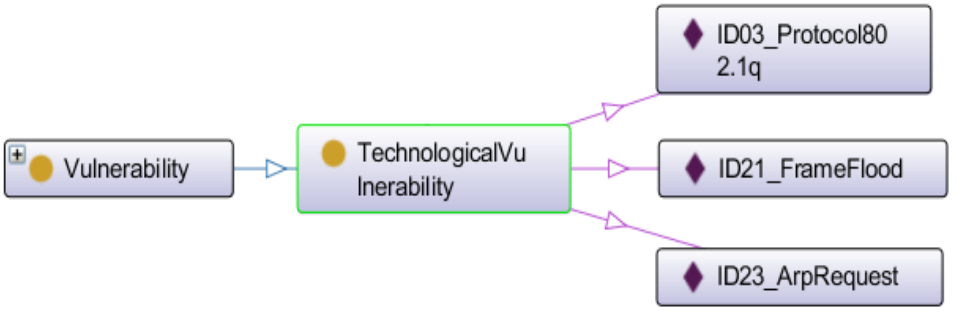

Figura 4.2 – Exemplos de Instâncias Mapeadas da Classe TechnologicalVulnerability

Os exemplos da Tabela 4.2 se referem às instâncias da Classe *TechnologicalVulnerability*, sendo descritas nos parágrafos seguintes.

[3] https://cve.mitre.org/

Protocol 802.1q (ID 03). O protocolo 802.1q permite que intrusos remotos ignorem a segmentação da rede e falsifiquem o tráfego VLAN por meio de uma mensagem com duas *tags* 802.1q, permitindo que a segunda *tag* seja redirecionada de um *switch downstream* após a remoção da primeira *tag*, proporcionando o salto de VLAN *Double Tagging Attack.*

Frame flood (ID 21). O recurso FCoE (*Fibre Channel over Ethernet*), nos *switches* IBM e executando o IBM *Networking Operating System,* permite que intrusos remotos inundem quadros de dados com endereços MAC desconhecidos em todas as interfaces na mesma VLAN. Assim, intrusos podem obter informações confidenciais, espionando o domínio de transmissão. Essa vulnerabilidade pode ser explorada por *CAM Table Overflow Attack.*

ARP request (ID 23). O *Kernel* no Juniper Junos OS, em certas versões ou configurações de VLANs, com configurações irrestritas de arp-resp e proxy-arp, permite que intrusos remotos causem uma negação de serviço (travamento do dispositivo) por meio de uma solicitação ARP criada. Essa vulnerabilidade pode ser explorada por um ataque ARP.

A Figura 4.3 apresenta uma visão geral das 49 instâncias de *TechnologicalVulnerability.*

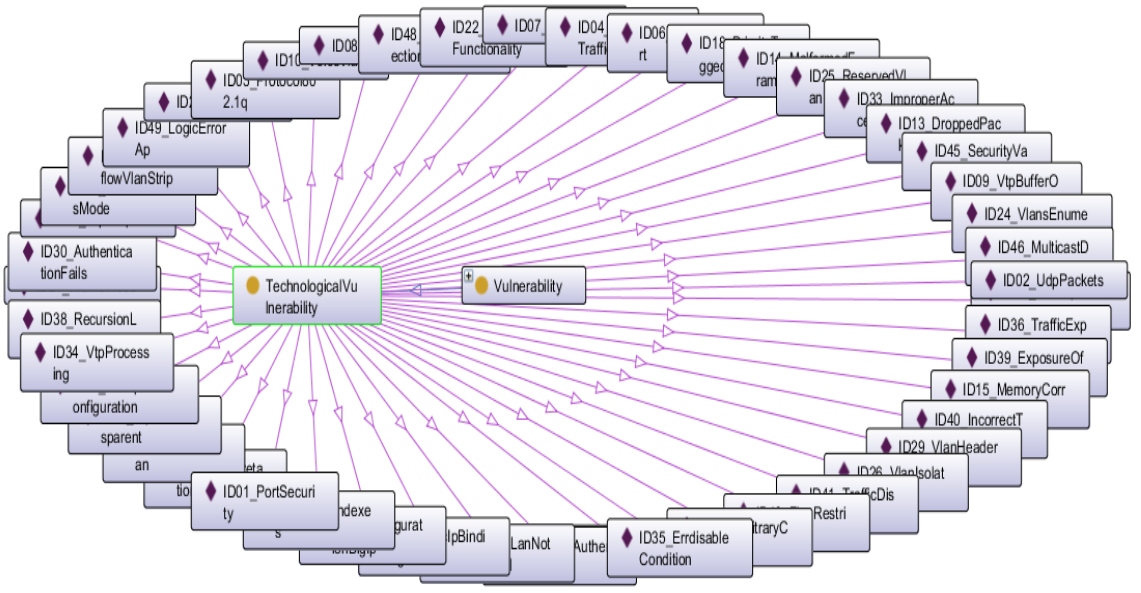

Figura 4.3 – Instâncias da Classe TechnologicalVulnerability

4.2 Ataque Tecnológico

O Ataque Tecnológico (Classe *TechnologicalAttack*) é a exploração de vulnerabilidades, erros ou falhas nos dispositivos computacionais ou manipulação de protocolos, sendo um dos caminhos pelo qual o invasor pode obter acesso a informações ou interrompê-las. Contudo, podem ser requeridas várias vulnerabilidades para se iniciar um ataque bem-sucedido.

Pode ser difícil classificar um ataque tecnológico, pois quando há ataques combinados ou variações de um ataque (e.g., Ataque ARP ou Salto de VLAN), poderão ser usados vários meios para se atingir o alvo (Convery, 2004). No entanto, a identificação e classificação dos ataques pode ser mapeada e expressa em uma ontologia.

Ataques tecnológicos (Apêndice II – Tabela A2.1) foram mapeados e especificados a partir de literatura técnica da área (Vyncke & Paggen, 2008) e (Empson & Schmidt, 2014). A Figura 4.4 apresenta quatro exemplos de instâncias da Classe *TechnologicalAttack*, sendo descritos nos próximos parágrafos. Uma visão geral dos ataques é apresenta na Figura 4.5.

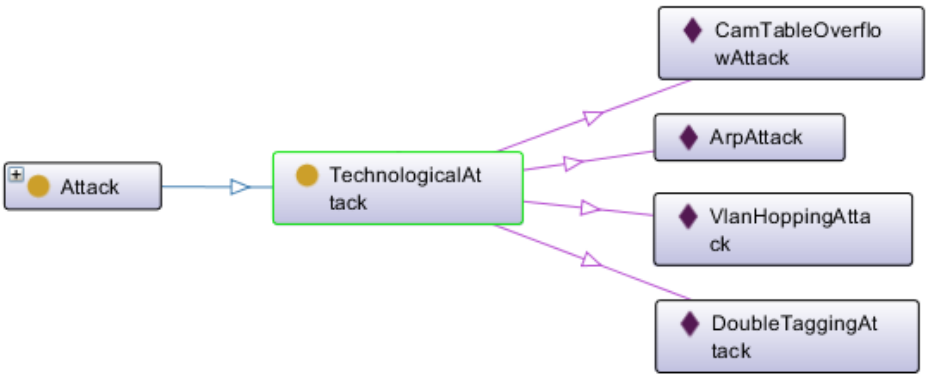

Figura 4.4 – Exemplos de Instâncias da Classe TechnologicalAttack

CAM Table Overflow Attack. Este ataque, também conhecido como *MAC Flooding Attack*, se concentra na Tabela CAM (*Content Addressable Memory*) dos switches, que armazena informações como endereços de MAC (*Media Access Control*) em uma porta física, juntamente com os parâmetros de VLAN associados. Tabelas CAM têm tamanho fixo, o que as torna alvos de ataques. Tal qual um ataque de estouro de *buffer*, o objetivo é preencher a Tabela CAM. O invasor gera um grande número de endereços MAC em uma porta física. Quando a Tabela CAM atinge seu limite, o tráfego sem uma

entrada CAM é enviado em todas as portas da VLAN sob ataque. O tráfego com uma entrada CAM não é afetado, mas os switches adjacentes podem ser (Watkins & Wallace, 2008).

ARP Attack. O Ataque ARP (*Address Resolution Protocol*), conhecido também como ARP *Spoofing Attack* e ARP *Poisoning*, é o uso indevido do protocolo ARP, o qual é utilizado pelos *hosts* para "anunciar" seu endereço à rede local e evitar endereços duplicados. O ARP é responsável por associar endereços IP a um endereço de MAC em uma rede local. Quando um endereço de MAC não é conhecido, um pacote ARP-*REQUEST* é enviado usando uma solicitação de difusão de rede na forma da pergunta "Qual é o endereço MAC de um dispositivo configurado com o endereço IP incluso?". Um dispositivo pode enviar seu endereço MAC a todos, sem que uma solicitação seja feita. Nesse caso, o pacote enviado é um G ARP (*Gratuitous* ARP).

O intruso se aproveita dessas possibilidades e identifica o endereço MAC do dispositivo-alvo, o qual deseja se passar por ele, e envia um G ARP (endereço MAC do dispositivo-alvo). O *switch*, ao recebê-lo, atualizará sua Tabela CAM, e a informação do IP correspondente ao novo endereço MAC recebido será adicionado ao *cache* da Tabela ARP. Assim, todo tráfego que for destinado ao endereço MAC do dispositivo alvo, será encaminhado ao dispositivo do intruso. Através deste ataque, é possível causar DoS (*Denial of Service*), ou ser usado como um ataque MITM (*Man In The Middle*).

VLAN Hopping Attack. VLAN *Hopping* é um ataque à rede segregada em que o intruso envia pacotes destinados a um dispositivo em uma VLAN diferente, normalmente não alcançada por ele. Este tráfego é marcado com um ID de VLAN diferente a que o intruso pertence e, comportando-se como um *switch*, pode negociar entroncamento possibilitando enviar e receber tráfego entre outras VLANs. Como o invasor pode acessar outras VLANs, isso é denominado ataque de salto de VLAN. Na configuração de um sistema, para se passar por um *switch* (*Switch-Spoofing Attack*), exige-se que o intruso tente se conectar usando os protocolos de marcação e entroncamento apropriados, por exemplo, emular o protocolo ISL (*Inter-Switch Link*) ou IEEE 802.1q, protocolo de entroncamento de VLAN, juntamente com o DTP (*Dynamic Trunking Protocol*). Assim, o intruso é capaz de simular uma porta *trunking* e negociar com outro *switch*. Caso obtenha

sucesso, o intruso será membro de todas as outras VLANs. Consequentemente, será possível causar DoS ou MITM.

Double Tagging Attack. O ataque de Marcação Dupla é uma variação do ataque VLAN *Hopping* e envolve a marcação dos quadros transmitidos, com dois cabeçalhos 802.1q, com a intenção de encaminhar os quadros para uma VLAN a qual ele não pertence. Após o encaminhamento do quadro com dois cabeçalhos 802.1q, o primeiro *switch* que receber o quadro retira o primeiro cabeçalho e encaminha o quadro para todas as portas na VLAN correspondente ao primeiro cabeçalho, encaminhando também para as portas *trunk*. Quando esse quadro chegar a uma porta *trunk* e for enviado ao próximo *switch*, o quadro chegará com o segundo cabeçalho e com a VLAN que o intruso pretende alcançar. O *switch*, então, irá verificar o cabeçalho e encaminhará o quadro ao destino ou o inundará, dependendo da existência de entrada na Tabela CAM.

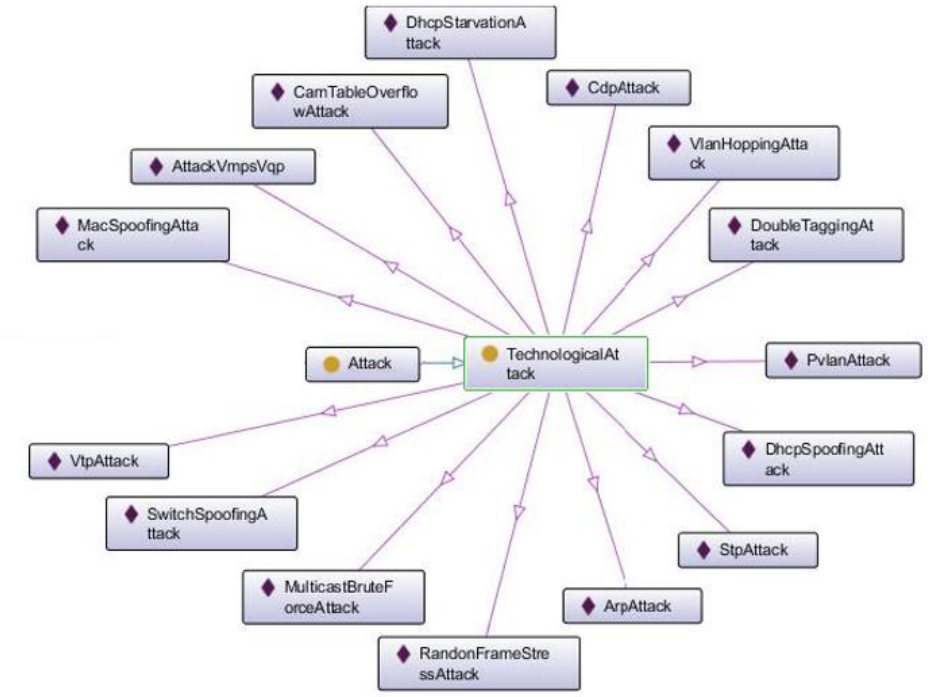

Figura 4.5 – Instâncias da Classe TechnologicalAttack

4.3 Propriedades de Segurança afetadas pelos Ataques

Propriedades de Segurança são atributos ou características da segurança da informação. Embora se tenha utilizado na conceituação 6 propriedades de segurança (*Availability*, *Integrity*, *Confidentiality*, *Authenticity*, *Privacy*, *Resilience*), outras

propriedades podem ser incorporadas, dependendo da abordagem a ser considerada. A Figura 4.6 apresenta as instancias da Classe *SecurityProperty.*

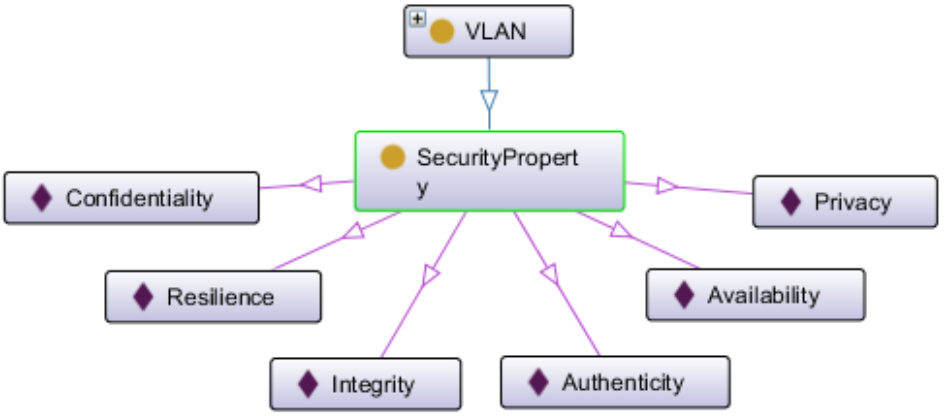

Figura 4.6 – Instâncias da Classe SecurityProperty

As propriedades utilizadas na conceituação são definidas sinteticamente e os principais ataques, no contexto de VLAN, que afetam as propriedades são apresentados nos parágrafos seguintes.

Availability – Esta propriedade refere-se à garantia de que os usuários tenham acesso a informações e recursos. O principal ataque contra a disponibilidade é o DDoS (*Distributed* DoS), onde os recursos de computação e comunicação de um sistema podem ser esgotados rapidamente, impactando a disponibilidade do sistema.

Integrity – Esta propriedade refere-se à capacidade de se proteger contra a modificação indevida das informações, i.e., garantir que as informações dos sistemas não foram interceptadas e modificadas indevidamente. O principal ataque contra a integridade é o *ARP Attack.*

Confidentiality – Esta propriedade é referente à garantia de que as informações dos sistemas não serão divulgadas ou reveladas a entidades não autorizadas. O principal ataque contra a confidencialidade é o *ARP Attack.*

Authenticity – Esta propriedade é referente à confirmação da veracidade de informação, documento ou ato de uma entidade (informação autêntica). Os principais ataques contra a autenticidade são *Phishing* e MITM.

***Privacy* –** Esta propriedade é referente a garantia de que o sistema não divulgará informações pessoais (intimidade pessoal) sem autorização. O principal ataque contra a privacidade é o *ARP Attack.*

***Resilience* –** Esta propriedade é referente à garantia de que o sistema seja capaz de operar sob condições extremas, como ataques cibernéticos. O principal ataque que afeta a resiliência é o DDoS.

4.4 Impacto do Ataque

O Impacto do Ataque (Classe *AttackImpact*) é a violação dos atributos ou propriedades de segurança que consequentemente influenciará o nível de impacto. Métricas de avaliação de impactos de ataques estão relacionadas ao grau de importância e prioridade de cada ativo para uma organização.

Os níveis atribuídos variam conforme critérios estabelecidos. Por exemplo, uma organização pode classificar como baixo, o que outra classificaria como alto, o impacto de um ataque que afete a integridade de um ativo, onde uma modificação de dados é possível, mas o invasor não tem controle sobre a consequência de uma modificação ou a quantidade de modificação é restrita. Dessa forma, a modificação de dados não teria um impacto direto e sério na organização ou ativo afetado.

A Figura 4.7 apresenta as instâncias da Classe *AttackImpact*; O impacto do ataque possui níveis de impacto, de forma qualitativa, sendo descritos nos parágrafos seguintes.

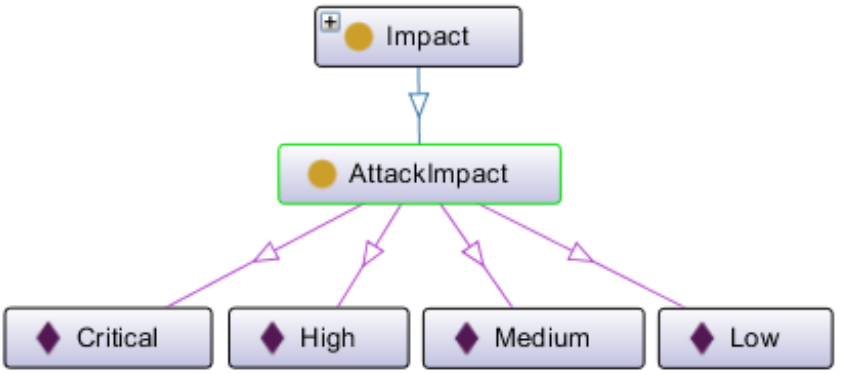

Figura 4.7 – Instâncias da Classe AttackImpact

***Crítico* –** Quando um intruso possui acesso a informações críticas e possui controle total sobre o alvo, o que implica em comprometer os ativos com perdas irreparáveis ou recuperação extremamente difícil.

***Alto* –** Quando um intruso possui controle significativo sobre o alvo, o que implica em possuir acesso às informações críticas, divulgando, alterando ou as bloqueando, com prejuízo de alto custo e demora na sua recuperação.

***Médio* –** Quando um intruso possui controle moderado sobre o alvo, o que implica em possuir acesso a informações de importância moderada e sua divulgação, alteração ou bloqueio causam consequências suportáveis em custo e recuperação.

***Baixo* –** Quando um intruso possui controle mínimo sobre o alvo, o que implica em possuir acesso às informações relativamente sem importância, não havendo nenhum impacto ou consequência.

Por exemplo, como um Ataque ARP pode afetar tanto a Integridade quanto Confidencialidade e Privacidade; assim, ao se analisar o impacto desse tipo de ataque, o nível pode ser considerado crítico, considerando informações com alto nível de criticidade. A representação do processo na ontologia é apresentada na Figura 4.8.

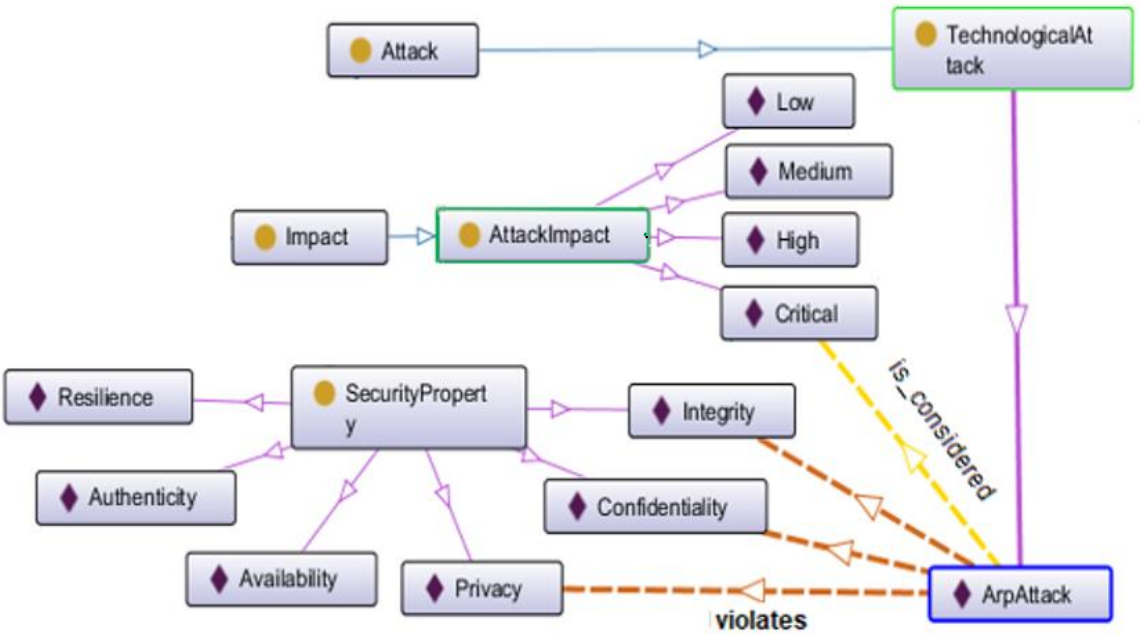

Figura 4.8 – Processo de Modelagem do Nível de AttackImpact em OVAV.owl

Na Figura 4.9, apresentam-se as propriedades presentes em OVAV e os dois exemplos (identificados com seta vermelha) utilizados na representação do processo de modelagem do nível de *AttackImpact*. Como as propriedades permitem a definição da relação entre conceitos, no exemplo, a propriedade *is_considered* propicia a representação do conhecimento relativo a crer-se como crítico, e a propriedade *violates* indica a eliminação de garantia de privacidade.

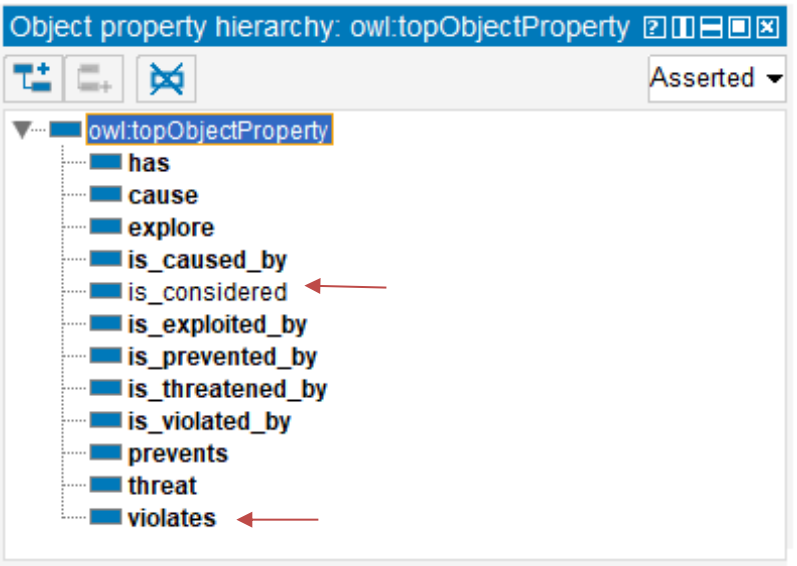

Figura 4.9 – Propriedades definidas em OVAV

5 APLICAÇÃO DE OVAV NA PREVENÇÃO DE ATAQUES A VLAN

OVAV estabelece conceitos e definições com base em melhores práticas de prevenção e bases de conhecimento confiáveis, bem conhecidas e de domínio público, tais como CVE (*Common Vulnerabilities and Exposures*). Contudo, abordar prevenção de vulnerabilidade em dispositivos, requerer, na maioria das vezes, suporte dos fabricantes para a solução de problemas específicos.

Bases de conhecimento de vulnerabilidades muitas vezes não possuem as soluções de fabricantes, as quais são divulgadas a clientes que possuem uma licença válida por questões de segurança. Neste contexto, busca-se propor estratégias de defesa para ataques que possuem soluções irrestritas, i.e., independente de fabricante. Em OVAV.owl, propõe-se um conjunto de estratégias de prevenção de ataques, que é representado pela Classe *AttackPrevention.*

A maioria das vulnerabilidades existentes nos equipamentos, especialmente em redes segmentadas, estão relacionadas ao efeito de negação de serviços. Essas vulnerabilidades podem ser exploradas ou não, pois todo ataque mapeado explora uma vulnerabilidade, mas nem toda vulnerabilidade possui um ataque mapeado.

OVAV é uma ontologia de domínio tendo como um dos objetivos, entre os já descritos, gerar um vocabulário comum de uma área específica do conhecimento. Contudo, poderá derivar uma ontologia de aplicação para algum uso prático, por exemplo, avaliar sua eficiência na proteção de VLANs. Entretanto, OVAV pode ser interpretada por humanos e consequentemente gerar conhecimento de efeito prático.

5.1 Estratégia de Prevenção de Ataques

A partir do mapeamento conceitual, um conjunto de estratégias de prevenção de ataques é proposta, visando a corrigir erros ou falhas nos procedimentos de uso ou configuração dos dispositivos. Diferentes mecanismos de defesa podem ser implementados para melhorar a segurança das VLANs, evitando a exploração de vulnerabilidades.

Exemplos de instâncias da Classe *AttackPrevention* são apresentados na Figura 5.1 e descritos nos parágrafos seguintes. A Tabela 5.1 apresenta um recorte de OVAV.owl, e a estratégia completa de prevenção no formato texto (Apêndice III – Tabela A3.1) está disponível no repositório *GitHub* (Cruz, 2022). A Figura 5.2 apresenta uma visão geral das instâncias da Classe *AttackPrevention*.

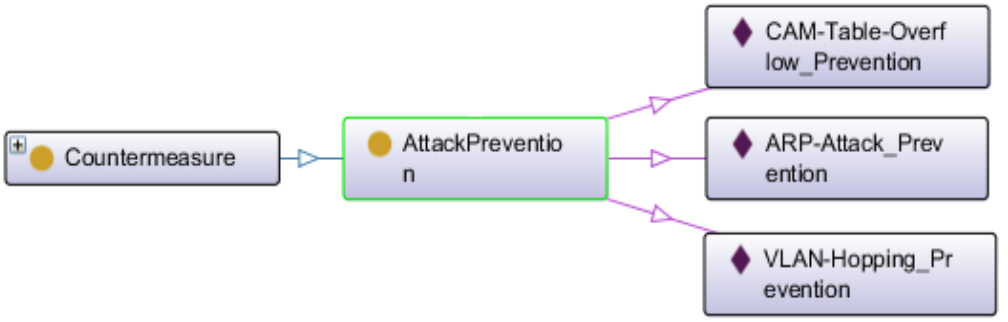

Figura 5.1 – Exemplos de Instâncias da Classe AttackPrevention

CAM-Overflow_Prevention – Prevention of CAM Table Overflow Attack. Para prevenir o *CAM Table Overflow Attack*, recomenda-se: i) Habilitar a configuração de segurança de porta no switch (*port-security*); ii) Restringir o acesso nas portas do *switch*; iii) Limitar o número de endereços MAC que cada porta do *switch* pode aceitar; iv) Ignorar endereços MAC após o limite da porta do *switch* ser atingido.

ARP-Attack_Prevention – Prevention of ARP Attack. Para prevenir um *ARP Attack*, recomenda-se: i) Implementar o DHCP *Snooping*, que deve ser configurado primeiro, pois caso contrário não haverá tabela de vinculação para ser usada na inspeção dinâmica ARP; ii) Implementar o DAI (*Dynamic ARP Inspection*), recurso de segurança que descarta os pacotes ARP com endereço IP e MAC inválidos; iii) Habilitar os recursos de segurança de porta do switch e considerar o ARP estático para roteadores e hosts críticos; iv) Ajustar os sistemas IDS para observar quantidades excepcionalmente altas, de tráfego ARP.

VLAN-Hopping_Prevention – Prevention of VLAN Hopping Attack. Para prevenir um *VLAN Hopping Attack*, recomenda-se: i) Usar ID de VLAN dedicado para todas as portas de tronco; ii) Desabilitar portas não utilizadas e colocá-las em uma VLAN não utilizada; iii) Desabilitar o entroncamento automático nas portas voltadas para o usuário (DTP desativado); iv) Configurar explicitamente o entroncamento em portas de infraestrutura; v) Usar todo o modo etiquetado para a VLAN nativa em troncos; vi) Usar

PC *Voice* VLAN *Access* em telefones que o suportam; vii) Usar *Tag* 802.1q em todas as portas de tronco; viii) Não usar VLAN 1; ix) Evitar configurações padrão.

Tabela 5.1 – Extrato de código OWL com Exemplos de Instâncias da Classe AttackPrevention em OVAV.owl

```
# Individual: :CAM-Table-Overflow_Prevention (:CAM-Table-Overflow_Prevention)
ClassAssertion(<http://www.semanticweb.org/hall/ontologies/2022/10/untitled-
ontology-16#AttackPrevention> :CAM-Table-Overflow_Prevention)
```

```
# Individual: :ARP-Attack_Prevention (:ARP-Attack_Prevention)ClassAssertion
(<http://www.semanticweb.org/hall/ontologies/2022/10/untitled-ontology-16#Attack
Prevention> :ARP-Attack_Prevention)
```

```
# Individual: :VLAN-Hopping_Prevention (:VLAN-Hopping_Prevention)Class
Assertion(<http://www.semanticweb.org/hall/ontologies/2022/10/untitled-ontology-
16#AttackPrevention> :VLAN-Hopping_Prevention)
```

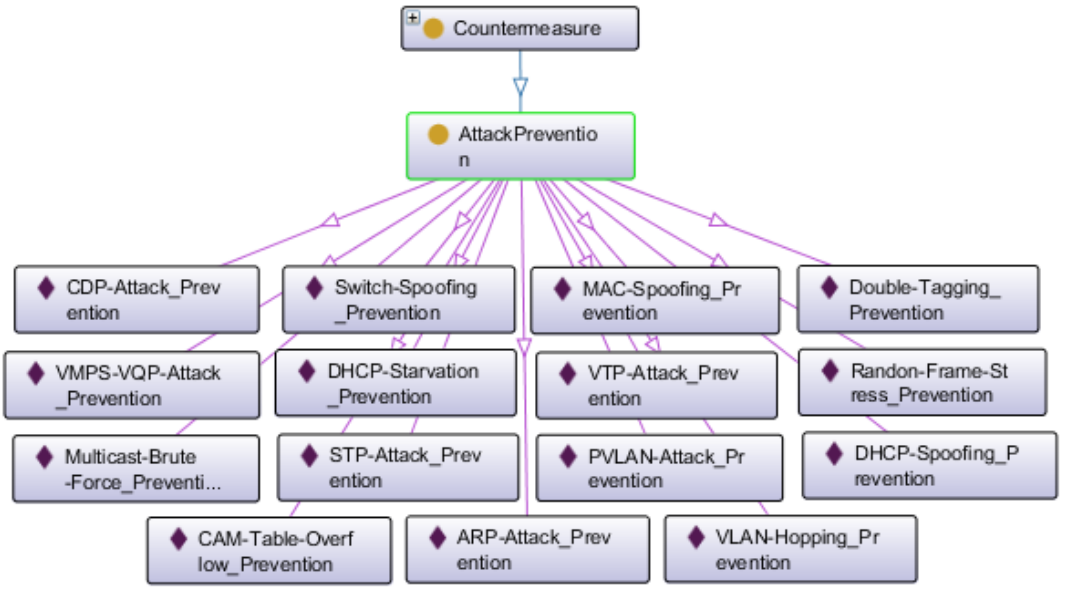

Figura 5.2 – Instâncias da Classe AttackPrevention

A proposta de estratégias, que representam as melhores práticas de prevenção, foi realizada usando como fonte algumas bases de conhecimento técnico, como CISCO, IBM, literatura técnica da área (Vyncke & Paggen, 2008), (Empson & Schmidt, 2014), além de reuniões técnicas com especialista de domínio (doutor em Engenharia de Computação, com experiência em segurança da informação).

Diferentes mecanismos de defesa podem ser implementados para melhorar a segurança das VLANs. A Figura 5.3 apresenta a associação entre as Classes *TechnologicalAttack* e *AttackPrevention*, e seus relacionamentos. A Figura 5.4 apresenta os dois exemplos das propriedades utilizadas, destacando com setas vermelhas a propriedade *prevents*, que representa o conhecimento relativo a evitar/impedir o ataque, e a propriedade *is_prevented_by*, que indica que o ataque é evitado, uma ação inversa.

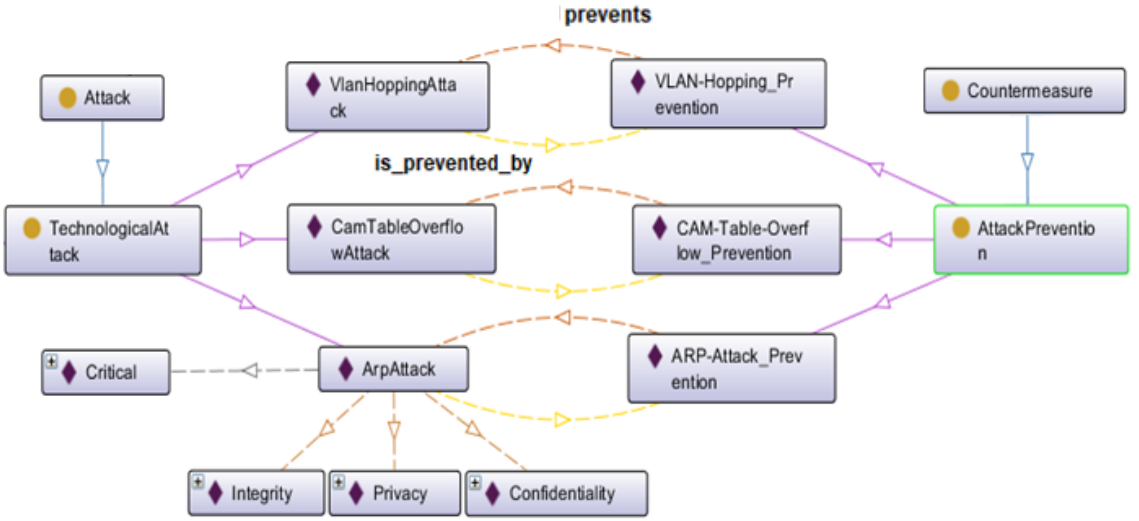

Figura 5.3 – Modelagem das Classes Technological*Attack e AttackPrevention*

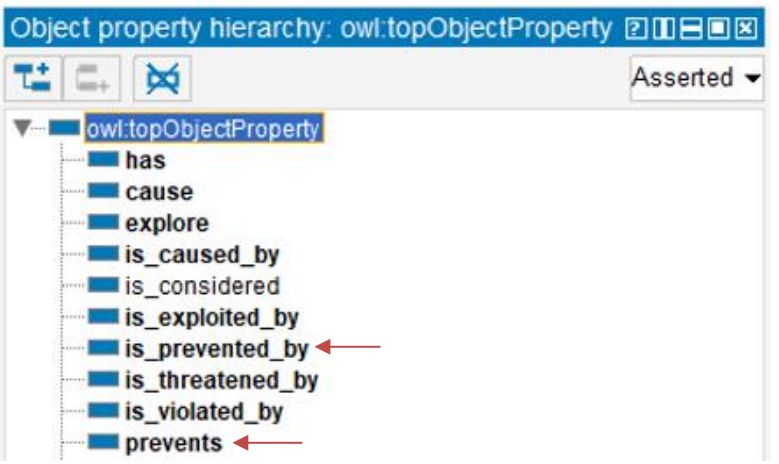

Figura 5.4 – Propriedades das Classes Technological*Attack e AttackPrevention*

6 CONCLUSÕES

Este capítulo apresenta a conclusão desta dissertação. A Seção 6.1 apresenta as contribuições da pesquisa e na Seção 6.2 são apresentados os trabalhos futuros.

Propor estratégias de defesa para infraestruturas computacionais críticas, como as VLANs, é uma tarefa difícil. OVAV é uma proposta de conceituação de um importante campo, cujos conceitos sempre foram considerados separadamente e de forma ambígua. Propõe-se uma ontologia focada em vulnerabilidades e ataques de redes segmentadas, extensível, legível por humanos e por máquinas, e o arquivo em formato OWL está disponível para os pesquisadores usarem, editarem ou mesclarem.

A versão 1.0 de OVAV.owl foi submetida a três avaliações, a saber:

1) Expressividade da Ontologia – Atualmente com 284 axiomas e 89 indivíduos, a expressividade DL é ALCHI, conforme avaliação feita com o suporte de *OntoMetrics*[4].

2) Verificação de Inconsistências Conceituais – Com o suporte do *framework* Protégé[5], não foram encontradas inconsistências na modelagem.

3) Análise de Modelagem por Especialistas de Domínio – Três Engenheiros de Software (2 doutores e 1 mestrando) analisaram as definições dos termos e seus relacionamentos. Por exemplo, novas instâncias e classes foram propostas, algumas classes foram convertidas em instâncias, e inconsistências lógicas em hierarquias foram identificadas e corrigidas.

Nesta dissertação, apresenta-se o desenvolvimento dos conceitos principais e uma aplicação de mundo real, onde a ontologia é usada para fornecer parâmetros e termos formalizados para definir estratégias para proteção de VLANs. Este trabalho destina-se a ser útil para pesquisadores que buscam desenvolver métodos e processos sistemáticos baseados em ontologias voltados à proteção de redes segmentadas.

[4] https://ontometrics.informatik.uni-rostock.de/ontologymetrics/
[5] https://protege.stanford.edu/

6.1 Contribuições da Pesquisa

Esta dissertação apresenta contribuição para a área da Ciência da Computação, mais especificamente para o processo de modelagem conceitual por meio de uma ontologia de domínio visando a proteção de VLANs.

Com o objetivo de responder às questões de pesquisas que norteiam este trabalho, foram desenvolvidos estudos e modelos, que constituem as principais contribuições desta pesquisa. Os resultados principais da pesquisa são apresentados na Tabela 6.1, com destaque para dois artigos publicados (Springer - Qualis A4) e a seguir, os abstracts das publicações científicas realizadas ao longo deste estudo.

Tabela 6.1 – Resultados da Pesquisa.

#	Meta	Ações	Status
1	Produzir um artigo de revisão sistemática de literatura sobre abordagens ontológicas que visam vulnerabilidades e ataques a VLAN.	Artigo, apresentado e publicado no *18th International Conference on Information Technology-New Generations* (ITNG 2021) [QUALIS A4] (Cruz et al, 2021)	Publicado
2	Produzir um artigo de proposta de projeto científico da modelagem conceitual.	Artigo, apresentado e publicado no Workshop de Computação da UNIFACCAMP (WCF 2022)	Publicado
3	Desenvolvimento de um conjunto de estratégias de prevenção de ataques a VLANs	Desenvolvido e aprimorado para o artigo principal (#5)	Desenvolvido
4	Desenvolvimento de uma Ontologia de Vulnerabilidade e ataques a VLANs	Desenvolvido para o artigo principal (#5) e aprimorado para esta dissertação.	Desenvolvida
5	Produzir um artigo sobre Ontologia de vulnerabilidades e ataques a VLANs.	Artigo, apresentado e publicado no *20th International Conference on Information Technology-New Generations* (ITNG 2023) [QUALIS A4] (Cruz et al., 2023)	Publicado

Artigos Publicados

Marcio Silva Cruz, Ferrucio de Franco Rosa & Mário Jino, (2023). ***"Ontology of Vulnerabilities and Attacks on VLAN"****, In 20th International Conference on Information Technology-New Generations (ITNG 2023), In S. Latifi (Ed.), Advances in Intelligent Systems and Computing, vol 1445 (First, pp. 89–95). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-031-28332-1_11*

Abstract *— Proposing defense strategies for critical computing infrastructures, such as Virtual Local Area Networks (VLAN), is a hard task. We present a conceptual model aiming at protection of VLANs. We identify, formalize, and relate important concepts, and map vulnerabilities and attacks, in addition to proposing protection strategies. The main contributions of the paper are: i) a domain ontology (OWL format), which models vulnerabilities and attacks on VLANs; ii) a set of attack prevention strategies for protecting VLANs. This work is intended to be used by researchers pursuing to develop systematic methods and techniques aimed at protecting critical infrastructures.*

Marcio Silva Cruz, Ferrucio de Franco Rosa & Mário Jino, (2021*). **"A Study on Ontologies of Vulnerabilities and Attacks on VLAN"**, In 18th International Conference on Information Technology-New Generations (ITNG 2021), In S. Latifi (Ed.), Advances in Intelligent Systems and Computing, vol 1346 (First, pp. 115–119). Springer, Cham. https://doi.org/10.1007/978-3-030-70416-2_14*

Abstract *— Virtual Local Area Network (VLAN) is a technology capable of separating networks into specific domains. Attacks on VLANs could affect computing environments causing service interruptions. These attacks exploit vulnerabilities and operating characteristics of VLANs to gain access to critical information. Conceptual modeling of vulnerabilities and attacks related to VLANs is crucial to enable the construction of systematic methods and techniques for protecting critical infrastructures. Ontologies can contribute in this context, as they are modeling tools that enable the formalization of the main concepts and their relationships, in addition to enabling the creation of semantic rules that can be used by intelligent systems. We present a quase-systematic literature review aiming at describing and classifying studies on ontologies of vulnerabilities and attacks on VLANs. The approach used in this review allowed for the verification and analysis of trends, as well as it uncovers the technological approaches adopted over the past 10 years. The main contributions of this review are: i) a description of the most recent ontologies, taxonomies, techniques and theories, in addition to the contributions and limitations of proposals in the literature; and ii) the identification of gaps in the literature and research challenges. Searches were carried out in the main scientific knowledge bases in the field of computing. Two hundred sixty-nine articles were found; 19 studies were analyzed according to their approaches, themes and related terms,*

pointing out contributions and research issues. This article is intended for researchers looking to conceptually model vulnerabilities and attacks on networks.

6.2 Trabalhos Futuros

Como próximos passos desta pesquisa, espera-se continuar expandindo OVAV e melhorando sua expressividade, incorporando outros conceitos, relações, propriedades e indivíduos. Espera-se também um conjunto mais robusto de axiomas e regras.

Existem metodologias que destacam o desenvolvimento de ontologias em várias disciplinas e domínios; no entanto, até o presente momento, identificamos a falta de Ontologias que abordem questões relacionadas a rede VLAN.

Este estudo restringiu-se às vulnerabilidades e ataques tecnológicos aplicados a VLAN. Incorporar e validar novos conceitos, tais como "*HumanVulnerability*", em um contexto de engenharia social pode ser avaliado como trabalho futuro, com a colaboração de especialistas de domínio.

Por fim, um refinamento e ajustes de parâmetro para a determinação do nível de impacto do ataque poderá permitir uma melhor precisão ao se incorporar novas propriedades de segurança.

BIBLIOGRAFIA

Almeida, M. B., & Bax, M. P. (2003). Uma visão geral sobre ontologias : pesquisa sobre definições , tipos , aplicações , métodos de avaliação e de construção. *Ci. Inf., Brasília*, 7–20. https://doi.org/10.1590/S0100-19652003000300002

Berners-Lee, T. (2009). *Linked Data - Design Issues*. W3.Org. https://www.w3.org/DesignIssues/LinkedData.html

Berners-lee, T. I. M., Hendler, J., & Lassila, O. (2001). The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. *Scientific American*, 12.

Bhandari, P., & Gujral, M. S. (2014). Ontology based approach for perception of network security state. *2014 Recent Advances in Engineering and Computational Sciences, RAECS 2014*, 6–8. https://doi.org/10.1109/RAECS.2014.6799584

Bijani, S., & Robertson, D. (2014). A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review*, *42*(4), 607–636. https://doi.org/10.1007/s10462-012-9343-1

Borst, W. N. (1997). *Construction of engineering ontologies for knowledge sharing and reuse* [PhD Thesis - Research UT, graduation UT, University of Twente]. https://research.utwente.nl/en/publications/construction-of-engineering-ontologies-for-knowledge-sharing-and-

Chavan, S. M., & Tamane, S. C. (2016). Study and design of ontology for cloud based web services attacks: A survey. *Proceedings - International Conference on Global Trends in Signal Processing, Information Computing and Communication, ICGTSPICC 2016*, 24–29. https://doi.org/10.1109/ICGTSPICC.2016.7955263

Choi, C., & Choi, J. (2019). Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service. *IEEE Access*, *7*, 110510–110517. https://doi.org/10.1109/access.2019.2933859

Choi, J., Choi, C., Lynn, H. M., & Kim, P. (2015). Ontology Based APT Attack Behavior Analysis in Cloud Computing. *Proceedings - 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications, BWCCA 2015*, 375–379. https://doi.org/10.1109/BWCCA.2015.69

Convery, S. (2004). *Network Security Architectures – Expert guidance on designing secure* (1ª edição). Cisco Press.

Cruz, M. S. (2022). *Attack Prevention Strategy – VLAN*. Github. https://github.com/Cruzmarcios/Attack-Prevention-Strategy-VLAN.git

Cruz, M. S., & de Franco Rosa, F. (2022). *VLANs Vulnerabilities Table*. Github. https://github.com/Cruzmarcios/VLANs-Vulnerabilities-Table.git

Cruz, M. S., de Franco Rosa, F., & Jino, M. (2021). A Study on Ontologies of Vulnerabilities and Attacks on VLAN. In S. Latifi (Ed.), *Advances in Intelligent Systems and Computing* (1ª, pp. 115–119). Springer, Cham. https://doi.org/10.1007/978-3-030-70416-2_14

Cruz, M. S., de Franco Rosa, F., & Jino, M. (2022). *Ontology of Vulnerabilities and Attacks on VLANs - OVAV*. Github. https://github.com/Cruzmarcios/Ontology-of-Vulnerabilities-and-Attacks-on-VLANs---OVAV.git

Cruz, M. S., de Franco Rosa, F., & Jino, M. (2023). Ontology of Vulnerabilities and Attacks on VLAN. In S. Latifi (Ed.), *Advances in Intelligent Systems and Computing, vol 1445* (First, pp. 89–95). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-031-28332-1_11

Davenport, T. H., & Patil, D. J. (2012). Data Scientist : The Sexiest Job of the 21st Century. *Harvard Business Review, V. 1*, 70–77.

de Franco Rosa, F., Jino, M., & Bonacin, R. (2018). Towards an Ontology of Security Assessment: A Core Model Proposal. *Advances in Intelligent Systems and Computing*, *738*, 75–80. https://doi.org/10.1007/978-3-319-77028-4_12

Empson, S., & Schmidt, C. (2014). *Routing and Switching Essentials Companion Guide* (First prin). Cisco Press, 800 East 96th Street.

Falodiya, K., & Das, M. L. (2018). Security Vulnerability Analysis using Ontology-based Attack Graphs. *2017 14th IEEE India Council International Conference, INDICON 2017*, 1–5. https://doi.org/10.1109/INDICON.2017.8488002

Forouzan, B. A. (2010). *Comunicação de Dados e Redes de Computadores* (4. ed.). AMGH Editora Ltda.

Gao, J. B., Zhang, B. W., Chen, X. H., & Luo, Z. (2013). Ontology-based model of network and computer attacks for security assessment. *Journal of Shanghai Jiaotong University (Science)*, *18*(5), 554–562. https://doi.org/10.1007/s12204-013-1439-5

Gruber, T. R. (1995). Toward Principles for the Design of Ontologies Used for Knowledge Sharing. *International Journal of Human-Computer Studies*, *43*(5–6), 907–928. https://doi.org/10.1006/ijhc.1995.1081

Guarino, N. (1998). Formal Ontology and Information Systems. *Formal Ontology in Information Systems: Proceedings of the 1st International Conference*, *46*(June), 3–15. https://doi.org/10.1.1.29.1776

Harmelen, F. van, & McGuinness, D. L. (2004). *OWL Web Ontology Language Overview*. W3C.Org. https://www.w3.org/TR/2004/REC-owl-features-20040210/

Heerden, R. P. van, Irwin, B., & Burke, I. (2012). Classifying network attack scenarios using an ontology. *7th International Conference on Information Warfare and Security*, *ICIW 2012*, 311–324.

Heflin, J. (2004). *OWL Web Ontology Language - Use Cases and Requirements*. W3C. Org. https://www.w3.org/TR/webont-req/#acknowledgments

Horridge, M., Knublauch, H., Rector, A., Stevens, R., & Wroe, C. (2004). A

Practical Guide To Building OWL Ontologies Using The Protege-OWL Plugin and CO-ODE Tools edition 1.0. *The University of Manchester*, 0–117. https://www.researchgate.net/publication/230585369

Isotani, S., & Bittencourt, I. I. (2015). *Dados Abertos Conectados*. Novatec Editora.

Karande, H. A., & Gupta, S. S. (2015). *Ontology based intrusion detection system for web application security*. 228–232. https://doi.org/10.1109/iccn.2015.44

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(TR/SE-0401), 28. https://doi.org/10.1.1.122.3308

Krauß, D., & Thomalla, C. (2016). Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures. *2016 6th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2016*, 70–73. https://doi.org/10.1109/DICTAP.2016.7544003

Kshirsagar, D., Kumar, S., & Purohit, L. (2015). Exploring usage of ontology for HTTP response splitting attack. *Proceedings on 2015 1st International Conference on Next Generation Computing Technologies, NGCT 2015, September*, 437–440. https://doi.org/10.1109/NGCT.2015.7375156

Kurose, J. F., & Ross, K. W. (2013). *Redes de computadores e a internet - uma abordagem top-down* (6. ed.). Pearson Education do Brasil Ltda.

Lassila, O., & Swick, R. R. (1999). *Resource Description Framework (RDF) Model and Syntax Specification*. W3C. https://www.w3.org/TR/1999/REC-rdf-syntax-19990222/

Mendonça, R. R. De, Rosa, F. D. F., Carlos, A., Costa, T., Bonacin, R., & Jino, M. (2019). *OntoCexp : A Proposal for Conceptual Formalization of Criminal Expressions*. *Itng*, 43–48.

Mohsin, M., & Anwar, Z. (2016). Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics. *Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016*,

23–28. https://doi.org/10.1109/FIT.2016.013

Noy, N. F., & McGuinness, D. L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford Knowledge Systems Laboratory*, 25.

Patel-Schneider, P. F. (2005). Building the Semantic Web Tower from RDF Straw. *Proceedings of the Nineteenth International Joint Conference on Artificial Intelligence (IJCAI)*, 546–551.

Porter, T., & Gough, M. (2007). *How to cheat at Voip security* (C. © 2007 E. I. A. rights Reserved (ed.)). Syngress Media,U.S.; Illustrated Edition. https://doi.org/https://doi.org/10.1016/B978-1-59749-169-3.X5000-2

Shadbolt, N., Hall, W., & Berners-Lee, T. (2006). The Semantic Web Revisited. *IEEE Intelligent Systems*, *21*, 96–101. https://doi.org/10.1109/MIS.2006.62.

Shenbagam, J., & Salini, P. (2014). Vulnerability Ontology for web applications to predict and classify attacks. *2014 International Conference on Electronics, Communication and Computational Engineering, ICECCE 2014*, 268–272. https://doi.org/10.1109/ICECCE.2014.7086625

Si, C., Zhang, H., Wang, Y., & Liu, J. (2015). Network Security Situation Elements Fusion Method Based on Ontology. *Proceedings - 2014 7th International Symposium on Computational Intelligence and Design, ISCID 2014*, *2*, 272–275. https://doi.org/10.1109/ISCID.2014.132

Simmonds, A., Sandilands, P., & Van Ekert, L. (2004). An ontology for network security attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3285*, 317–323. https://doi.org/10.1007/978-3-540-30176-9_41

Smith, M. K., Welty, C., & McGuinness, D. L. (2004). *OWL Web Ontology Language Guide*. W3C. Org. https://www.w3.org/TR/owl-guide/

Soares Barros, O. (2006). *Segurança de redes locais com a implementação de VLANs O caso da Universidade Jean Piaget de Cabo Verde* (p. 67).

http://hdl.handle.net/10961/4220%0A

Staab, S., Maedche, A., & Handschuh, S. (2001). An annotation framework for the semantic web. *Institute AIFB, University of Karlsruhe*, 11. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.33.4680&rep=rep1&type=pdf

Syed, Z., Pädia, A., Finin, T., Mathews, L., & Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology. *AAAI Workshop - Technical Report*, *WS-16-01-*, 195–202.

Tanenbaum, A. S., & Wetherall, D. (2011). *Redes de Computadores* (5ª edição). Pearson Universidades.

Thermos, P., & Takanen, A. (2007). *Securing Voip networks : Threats, vulnerabilities, countermeasures* (1st Editio). Addison-Wesley Professional.

Vyncke, E., & Paggen, C. (2008). *LAN Switch Security - What Hackers Know About Your Switches* (First Prin). Cisco Press, 800 East 96th Street.

W3C OWL Working Group. (2012). *OWL 2 Web Ontology Language: Document Overview (Second Edition)*. W3C.Org. https://www.w3.org/TR/owl2-overview/

Watkins, M., & Wallace, K. (2008). *CCNA Security - Official Exam Certification Guide* (1ª). Cisco Press.

Xu, G., Cao, Y., Ren, Y., Li, X., & Feng, Z. (2017). Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. *IEEE Access*, *5*, 21046–21056. https://doi.org/10.1109/ACCESS.2017.2734681

Zhu, L., Zhang, Z., Xia, G., & Jiang, C. (2019). Research on vulnerability ontology model. *Proceedings of 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference, ITAIC 2019*, *Itaic*, 657–661. https://doi.org/10.1109/ITAIC.2019.8785783

APÊNDICE I – Vulnerabilidades Tecnológicas de VLAN

Tabela A1.1 – Vulnerabilidades Tecnológicas de VLAN

ID	***Names of Vulnerabilities***	***Vulnerable Assets and Resources***
1	*Port Security*	*Cisco switches that support 802.1x security*
2	*UDP packets*	*kernel Linux 2.6.8*
3	*Protocol 802.1q*	*Protocol 802.1q / VLAN*
4	*Spoof PVLAN traffic*	*Protocol PVLAN*
5	*Arbitrary code*	*Open VMPS (VLAN Management Policy Server) 1.3*
6	*Subset-Advert*	*Cisco IOS 12.1(22)EA3/ switches Catalyst 2950T (VTP Resource)*
7	*Frame VTP*	*Cisco IOS 12.1(19) (VTP)*
8	*VTP update*	*Cisco IOS 12.1(19) and CatOS (VTP)*
9	*VTP buffer overflow*	*Cisco IOS 12.1(19) (VTP)*
10	*Voice VLAN*	*Telephone IP-Touch Alcatel-Lucent - OmniPCX Enterprise 7.0*
11	*VTP not transparent*	*Cisco IOS and CatOS (VTP)*
12	*VLAN not registered*	*kernel Linux before 2.6.34 (function igb)*
13	*Dropped packets*	*Cisco Nexus 1000V(VEM) 4.0(4) SV1(1)*
14	*Malformed frame*	*kernel Linux before 2.6.38*
15	*Memory corruption*	*Linux 2.6.18 Red Hat Enterprise Linux 5 e 2.6.32 (RHEL) 6*
16	*User-space access*	*kernel Linux before 2.6.39.3*
17	*Promiscuous mode*	*Red Hat Enterprise Linux (RHEL) 6 before 2.6.32-218.el6*
18	*Priority-tagged*	*kernel Linux 2.6.32 in Red Hat Enterprise Linux (RHEL) 6*
19	*Flag restriction*	*Net subsystem in the Linux kernel before 3.1*
20	*Spoof user*	*RADIUS extension in PacketFence before 3.3.0*
21	*Frame flood*	*IBM System Networking (FCoE), Switches (BNT) (NOS)*
22	*Encryption functionality*	*Cisco NX-OS on the Nexus 1000V*
23	*ARP request*	*kernel in Juniper Junos 10.4; 11.4/.4x27; 12.1/.1x44; 12.2/.3*
24	*VLANs enumeration*	*SNMP in Cisco NX-OS 7.0(3)N1(1)and Nexus 5000 e 6000*
25	*Reserved VLAN packet*	*Cisco NX-OS 6.1(2)I3(4) and 7.0(3)I1(1) on Nexus 9000 (N9K)*
26	*VLAN isolation*	*Siemens RUGGEDCOM ROS 3.8.0 through 4.1.x*
27	*Sniffing VLAN*	*Siemens RUGGEDCOM ROS before 4.2.1*
28	*VLAN indexes*	*Software SO(VOSS) before 4.2.3.0 e 5.x before 5.0.1.0*
29	*VLAN headers*	*IP stack in the Linux kernel through 4.8.2*
30	*Authentication fails*	*Software Cisco IOS XE-Cisco Catalyst 4000 Series Switches*
31	*Buffer overflow VLAN STRIP*	*VLAN STRIP feature - enabled on the vmx net3 device*
32	*VLAN authentication*	*Juniper Networks Junos OS: 15.1; 16.1 /.2; 17.1 /.2*
33	*Improper access*	*Policy and Charging Rules Function - Cisco Policy Suite (CPS)*
34	*VTP processing*	*Software Cisco IOS and Software Cisco IOS XE*
35	*Errdisable condition*	*Software Cisco IOS XE - errdisable per VLAN feature*
36	*Traffic exposure*	*Openstack-neutron before 13.0.0.b2; 12.0.3; 11.0.5 (vulnerable)*
37	*Configuration BIG-IP*	*On BIG-IP 14.0.0-14.0.0.2 or 13.0.0-13.1.1.1 (Sistem BIG-IP)*
38	*Recursion loop*	*Juniper Networks Junos OS: 16.1 /.2; 17.1 /.2; 17.3 /.4; 18.1 /.2*
39	*Exposure of ports*	*Gateway VLAN feature enabled*

40	*Incorrect traffic*	*Arista EOS : EOS 7170 platforms version 4.21.4.1F*
41	*Traffic discard*	*Junos OS: EX4600, Série QFX5K*
42	*MAC/IP bindings*	*In EVPN VxLAN setups in Arista EOS (some versions)*
43	*Group VLAN configuration*	*BIG-IP Virtual Edition (VE)*
44	*Interpretation conflict*	*Juniper Networks Junos OS - several versions*
45	*Security validation*	*Cisco Nexus 9000 Series Fabric Switches in ACI Mode*
46	*Multicast DNS*	*Cisco Aironet Series AP Software (mDNS) gateway feature*
47	*Layer 2 loop*	*Cisco IOS XE Wireless - Family Cisco Catalyst 9000*
48	*Direct connection*	*FortiAuthenticator HA 6.3.2 e 6.2x; 6.1.x; 6.0.x*
49	*Logic error AP*	*Cisco Access Points (APs) Cisco Aironet Series (some versions)*

APÊNDICE II – Ataques Tecnológicos a VLAN

Tabela A2.1 – Ataques Tecnológicos a VLAN

Technological Attack – VLAN
CAM Table Overflow Attack *– A CAM Table Overflow Attack or Mac Flooding Attack focuses on the CAM (Content Addressable Memory) table which stores information such as MAC (Media Access Control) addresses on a physical port along with the associated VLAN parameters. CAM tables have a fixed size and just like a buffer overflow attack, the goal is to fill that table. The attacker sits on a physical port and generates a large number of MAC entries. When the CAM table is full and there is no space left, the default behavior of a switch is to broadcast messages, usually private, to all ports of the VLAN in question; acting as a hub. This attack could also populate the CAM tables of Adjacent switches.*
Arp Attack *– The Attack ARP(Address Resolution Protocol) is the misuse of the ARP protocol, which is used by hosts to "advertise" their address to the local network and avoid duplicate addresses. ARP is responsible for associating IP addresses with a MAC (Media Access Control) address on a local network. When a MAC address is not known, an ARP-REQUEST packet is sent using a network broadcast request querying the MAC of the device configured with the included IP address. However, any machine can claim that its MAC address is associated with a given IP address using the G ARP (Gratuitous ARP). The intruder takes advantage of these possibilities and identifies the MAC of the target device, which he wants to impersonate, and sends a G ARP (MAC address of the target device). The switch, upon receiving it, will update its CAM table, and the IP information corresponding to the new MAC address received will be added to the ARP table cache. Thus, all traffic destined for the MAC address of the target device will be forwarded to the intruder's device.*
VLAN Hopping Attacks *– The VLAN Hopping Attack consists of the intruder trying to gain access to VLANs that he does not have authorization. The traffic is tagged with a different VLAN ID than the intruder belongs to and negotiate trunking making it possible to send and receive traffic between other VLANs. For example, if a switch port is configured to dynamically establish Trunk-type links with other Switches, and it receives a false command packet through DTP (Dynamic Trunking Protocol), ISL (Inter-Switch Link) or 802.1Q trunking protocols . This port, improperly, may establish a connection to other VLANs.*

Switch Spoofing Attack *- A Switch Spoofing Attack is the act of configuring a system to pretend to be a switch, and emulating the signaling protocols ISL (Inter-Switch Link) or 802.1Q together with DTP (Dynamic Trunking Protocol), trying to establish a trunk connection with the switch . This is only possible when using the default automatic dynamic or desirable dynamic switching modes. For example, any switch port configured for automatic DTP, upon receiving a DTP packet generated by the intruder's device, can become a trunk port and thus accept traffic destined for any VLAN supported on that trunk.*
Double Tagging Attack - *The Double Tag Attack is a variation of the VLAN Hopping attack and involves tagging transmitted frames with two 802.1q headers with the intention of forwarding the frame to a VLAN to which it does not belong. After forwarding the frame with two 802.1q headers, the first switch that receives the frame strips the first header and forwards the frame to all ports in the VLAN corresponding to the first header; also forwarding to the trunk ports. When this frame arrives at a trunk port and is sent to the next switch, the frame will arrive with the second header and with the VLAN that the intruder intends to reach; the switch will then check the header and forward the frame to all ports in the secondary VLAN. (Protocol IEEE 802.*
VMPS / VQP Attack *- It is an attack based on Dynamic VLAN Access Ports. VLAN assignment, based on host MAC addresses, is possible with a VMPS (VLAN Management Policy Server) and the related information stored in a database. Queries are performed using VQP (VLAN Query Protocol), an unauthenticated protocol that uses UDP (User Datagram Protocol). these conditions favor the manipulation by an attacker. As a result, using VQP it is very easy to impersonate hosts, as there is no authentication, which allows the attacker to enter a VLAN that he is not authorized to access.*
Multicast Brute Force Attack - *A Multicast Brute Force Attack looks for flaws in the switch software. The attacker tries to exploit any potential vulnerability in a switch by attacking it with multicast frames. As with the CAM table overflow, the objective is to verify the behavior of the switch that receives a large amount of layer 2 multicast traffic; as frames can leak to other VLANs if routing connects them. While this type of attack is highly speculative, if the switch does not contain all frames within its proper broadcast domain, it becomes an attack vector.*

Random Frame stress Attack - *The Random Frame Stress Attack could be considered "Fuzzying" (art of automatic bug discovery) but in layer 2.In this type of attack. A large number of packets are generated by randomly varying various fields within each packet, keeping the source and destination addresses constants. The goal is to see how the switch software handles meaningless or unexpected values in packets. While this type of attack is highly speculative, bugs can occur that allow unexpected access to other VLANs, which will make it an attack vector.*

PVLAN Attack - *The PVLAN (Private VLAN) attack is sending unauthorized traffic to Layer 2 devices through the router. Private VLAN is a Layer 2 feature that is supposed to restricts direct communications between any two devices connected to the same switch; which makes attacking PVLANs very difficult. However, sand an L3 device (Router) connects to a non-isolated port of a VLAN switch, the L3 traffic can be sent to any VLAN, even if isolated in L2. PVLAN is not designed to protect against a layer 3 attack. So if an attacker creates a frame with the destination MAC address of the router, the source address of the host it is on, and at layer 3 the frame has the IP address of the intended device. The switch will pass this frame to the router that has the destination MAC address, which will in turn forward the frame to the end device.*

STP Attack - *The STP (Spanning Tree Protocol) attack is the attempt to change the topology of a network by an attacker, who through a switch unauthorized, added to the network or spoofing your system, will be the root bridge in the topology. For that the invader sends fake BPDUs (Bridge Protocol Data Units) frames to network switches, forcing them to recalculate the STP. Consequently, the entire layer 2 network topology will be reconfigured, causing the switches to start considering the attacker as the root switch; thus, all network traffic will pass through the attacker who will have access to information or the data.*

Mac Spoofing Attack - *The MAC Spoofing attack consists of generating a malicious frame by spoofing the MAC address of the target device. The intruder generates fake records of the source MAC address and the Sending a single frame with the source address of the other host overwrites the CAM table entry. O switch automatically switches the real host MAC registry entry to the offending port, as the same unicast MAC address cannot reside on multiple ports in a VLAN. This makes it possible for the intruder to receive all the information that was intended for another device.*

DHCP Spoofing Attack *- The DHCP* ***Spoofing*** *Attack or DHCP Rouge, consists of inserting a fake DHCP server into the network to gain access to data. DHCP (Dynamic Host Configuration Protocol) allows a server to automatically assign a host's IP address and information such as subnet mask and default gateway. An attacker acting as a DHCP server can respond to DHCP requests from devices on the network, in competition with the real server. If the device receives an IP from the fake DHCP server, the data sent will first pass through it, which will then send it to the real DHCP server, avoiding its discovery. So the attacker will have access to device information.*
DHCP Starvation Attack *- The DHCP Starvation Attack is carried out through DHCP (Dynamic Host Configuration Protocol) requests with spoofed MAC addresses, sent via broadcast. After exhausting all the IP address space destined for legitimate users (a procedure called "Starvation") the intruder loads his own DHCP server on that VLAN or subnet; since normally DHCP packets include Default Gateway and DNS addresses, the attacker can send his own address as Gateway and DNS. Then, posing as a clandestine DHCP server, it starts responding to DHCP requests on the network. So that the network administrator does not notice, the individual configures the routing on his computer for communication with the other parts of the network and the Internet, making the network users not notice any unavailability.*
VTP Attack *- The VTP attack is the sending of VTP (VLAN Trunking Protocol) messages causing the exclusion of VLANs. VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, or renaming of VLANs throughout the network. When a network administrator makes any changes to the VLAN configuration on a device that functions as a VTP server, that configuration is distributed via the VTP protocol across all switches in the domain. This reduces the need to manually replicate this VLAN configuration across switches. An attacker could impersonate a port trunk and send VTP messages as a server with no VLANs configured, causing all client VTP switches to erase their VLANs once they receive the message, causing a DOS effect.*
CDP Attack *- The CDP (Cisco Discovery Protocol) flood attack consists of sending a large amount of false CDP frames to the switch, with the aim of increasing processor usage, which may cause slowdowns or temporarily paralyze its operation. CDP is a layer 2 protocol and all CDP information is sent over a network in clear text, allowing any attacker to intercept the information through some network analysis software such as Wireshark. May cause DOS/MITM effect.*

APÊNDICE III – Estratégias de Prevenção de Ataques

Tabela A3.1 – Estratégias de Prevenção de Ataques

Attack Prevention Strategy – VLAN
CAM-Overflow_Prevention *– Prevention of CAM Table Overflow Attack. To prevent CAM Table Overflow Attacks, we recommend: i) Enable the port security configuration on devices (port-security); ii) Restrict access to devices ports; iii) Limit the number of MAC addresses that each device port can accept; iv) Ignore MAC addresses after device port limit is reached.*
ARP-Attack_Prevention *– Prevention of ARP Attack. To prevent ARP Attacks, we recommend: i) Implement DHCP Snooping, which must be configured first, otherwise, there will be no binding table to be used in dynamic ARP inspection; ii) Implement DAI (Dynamic ARP Inspection), a security feature that discards ARP packets with invalid IP and MAC addresses; iii) Enable device port security features and consider static ARP for critical routers and hosts; iv) Adjust IDS systems to monitoring exceptionally high amounts of ARP traffic.*
VLAN-Hopping_Prevention *– Prevention of VLAN Hopping Attack. To prevent VLAN Hopping Attacks, we recommend: i) Using dedicated VLAN IDs for all trunk ports; ii) Disable unused ports and place them in an unused VLAN; iii) Disable automatic trunking on user-facing ports (DTP disabled); iv) Explicitly configure trunking on infrastructure ports; v) Use all tagged mode for native VLAN on trunks; vi) Use PC Voice VLAN Access on phones that support it; vii) Use 802.1q tags on VLAN frames on trunk connection; viii) Do not use VLAN 1; ix) Avoid default settings.*
Switch-Spoofing_Prevention *- Prevention of Switch Spoofing Attack. To prevent Switch Spoofing Attack, we recommend: i) Using dedicated VLAN IDs for all trunk ports; ii) Disable unused ports and place them in an unused VLAN; iii) Disable automatic trunking on user-facing ports (DTP disabled); iv) Explicitly configure trunking on infrastructure ports; v) Use all tagged mode for native VLAN on trunks; vi) Use PC Voice VLAN Access on phones that support it; vii) Use 802.1q tags on VLAN frames on trunk connection; viii) Do not use VLAN 1; ix) Avoid default settings.* ***Obs:*** *Some manufacturers have fixed this vulnerability with a new version of their equipment (e.g., IOS and CATOS / Cisco). In reaction to this, the attack was adapted for Double Tagging Attack.*

Double-Tagging_Prevention - *Prevention of Double Tagging Attack. To prevent of Double Tagging Attack we recommend: As it is a variant of VLAN Hopping Attack use the same recommendations.*
VMPS-VQP-Attack_Prevention *- Prevention of VMPS/VQP Attack. To prevent VMPS/VQP Attack, we recommend: i) Consider sending VQP Out-of-Band (OOB) messages; ii) Monitor network traffic; iii) Use ACLs to filter unwanted access.* ***Obs****: VQP and VMPS are rarely used for MAC-based VLAN assignment because of the management burden of maintaining the MAC address to VLAN mapping table. The URT component is also not frequently used, especially since a standards-based method of effectively doing the same thing (802.1x) is now available.*
Multicast-Brute-Force_Prevention *- Prevention of Multicast Brute Force Attack. To prevent Multicast Brute Force Attack, we recommend: i) Storm control limits the amount of broadcast or multicast traffic sent by switches in the network; ii) Port security to limit the number of MAC addresses that can be learned per port on the switch.* ***Obs:*** *This type of attack generally proves ineffective, because the switches must contain all frames within their proper broadcast domain; Layer 2 multicast packets must be restricted within the incoming VLAN. No packets should be 'leaked' to other VLANs.*
Randon-Frame-Stress_Prevention *- Prevention of Randon Frame Stress Attack. To prevent Randon Frame Stress Attack, we recommend: i) Storm control limits the amount of broadcast or multicast traffic sent by switches in the network; ii) Port security to limit the number of MAC addresses that can be learned per port on the switch.* ***Obs:*** *This type of attack generally proves ineffective, because the switches must contain all frames within their proper broadcast domain; Layer 2 multicast packets must be restricted within the incoming VLAN. No packets should be 'leaked' to other VLANs.*
PVLAN-Attack_Prevention *- Prevention of PVLAN Attack. To prevent of PVLAN Attack, we recommend: i) Configure an ACL (Access Control List) on the router interface, preventing IP addresses from talking to each other or; ii) Use VACL (VLAN ACL).*

STP-Attack_Prevention *- Prevention of STP Attack. To prevent STP Attack, we recommend: i) Do not disable STP (network loop would become another attack); ii) Disable spanning tree function for entire user interface; iii) Use BPDU Guard and Root Guard features on switches; iv) The Bridge Protocol Data Units (BPDU) Guard must be run on all user-facing ports and infrastructure-facing ports; v) Root Guard - Configured per port. Disables ports that would become the root bridge due to BPDU advertisement.*
MAC-Spoofing_Prevention *- Prevention of MAC Spoofing Attack. To prevent MAC Spoofing Attack, we recommend: i) IP Source Guard prevents IP/MAC Spoofing.*
DHCP-Spoofing_Prevention *- Prevention of DHCP Spoofing Attack. To prevent DHCP Spoofing Attack, we recommend: i) Multilayer switch that has the ability to drop packets; ii) Use the DHCP Snooping feature, which discards DHCP-OFFER and DHCP-ACK messages on untrusted ports; iii) For switches on the network that do not support DHCP Snooping, configure VLAN ACLs to block UDP port 68.*
DHCP-Starvation_Prevention *- Prevention of DHCP Starvation. To prevent DHCP Starvation, we recommend: i) Enable the port-security feature; ii) Restrict Access on Switch Ports; iii) Limit the number of MAC addresses each switch port can learn; iv) Ignore the number of MAC addresses after the port limit is reached.* ***Obs:*** *(Same recommendations applied in CAM Overflow).*
VTP-Attack_Prevention *- Prevention of VTP Attack. To prevent VTP Attack, we recommend: i) Configuration VTP operating mode to "off" (CatOS only); ii) For devices that don't require the use of VTP, administrators should set the VTP mode to "transparent" ; iii) If VTP is needed, use MD5 authentication.*
CDP-Attack_Prevention *- Prevention of CDP Attack. To prevent CDP Attack, we recommend: i) Limit CDP usage on devices or ports; ii) Disable the CDP protocol on each of the ports on the switch or on the end ports that connect to untrusted devices.* ***Obs:*** *Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. i)To disable LLDP on the interface, configure no lldp transmit and no lldp receive; ii) Update your IOS frequently, current versions of CatOS.*