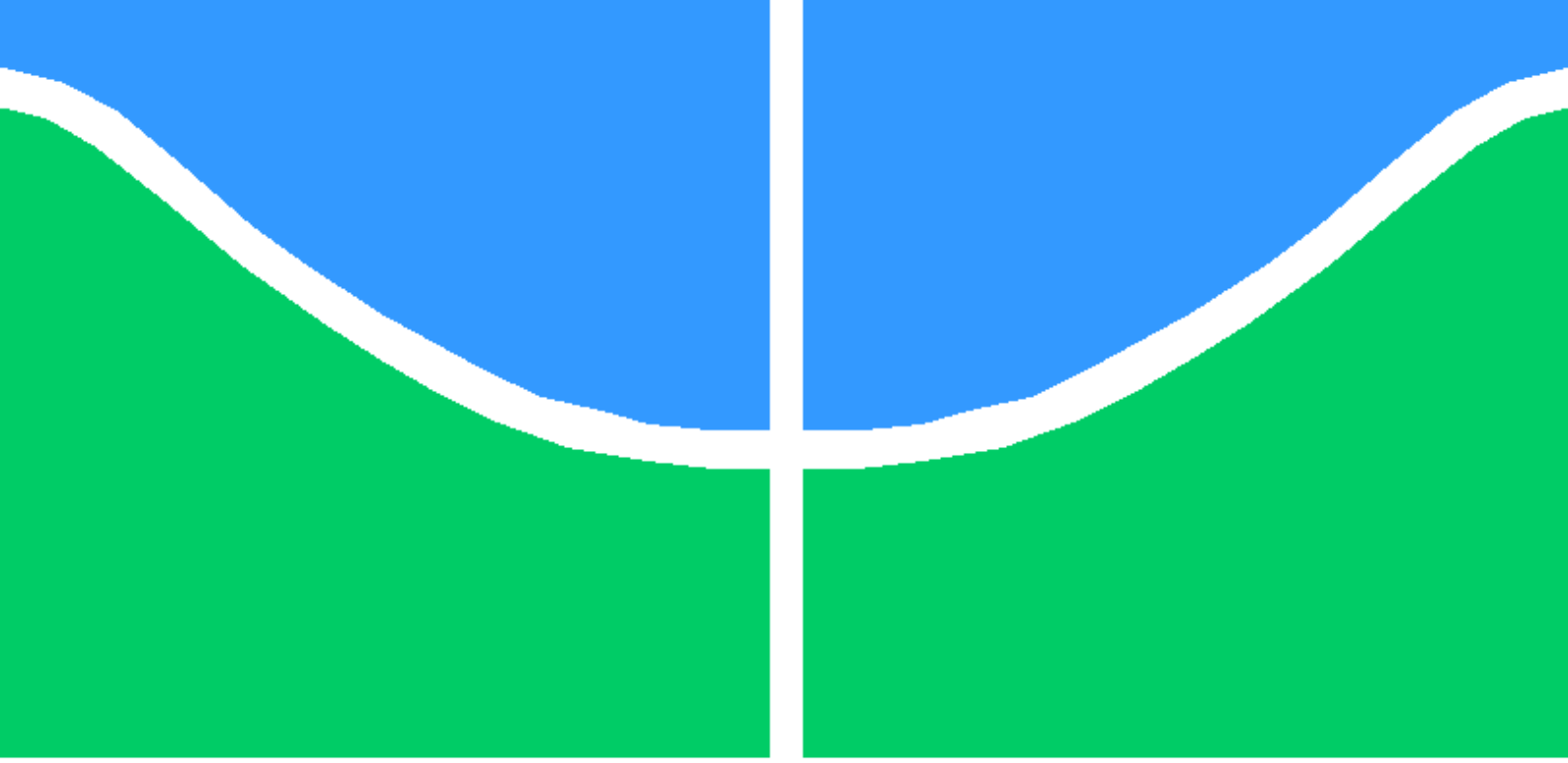

TRABALHO DE GRADUAÇÃO

PROCESSO DE AVALIAÇÃO DE RISCOS DE ATIVOS DE REDE APOIADO PELO MOODLE

Aline dos Santos Pereira

Yuri Freitas Gomes Santos

Brasília, Junho de 2017

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

PROCESSO DE AVALIAÇÃO DE RISCOS DE ATIVOS DE REDE APOIADO PELO MOODLE

Aline dos Santos Pereira

Yuri Freitas Gomes Santos

Relatório submetido ao Departamento de Engenharia Elétrica, como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Edgard Costa Oliveira, CIC/UnB _____
Orientador

Prof. Georges Daniel Amvame Nze, ENE/UnB _____
Examinador Interno

Prof. Edna Dias Canedo, FGA/UnB _____
Examinador Externo

Agradecimentos

Agradeço a todos aqueles que sempre me apoiaram, acreditaram no meu potencial, e desejaram o meu sucesso. Especialmente o meu orientador Edgard Costa Oliveira, que soube transmitir seus conhecimentos com muita dedicação e entusiasmo.

Aline dos Santos Pereira

A graduação não representa um fim, e sim novos começos e responsabilidades. Agradeço a minha família, amigos e profissionais envolvidos nessa conquista. Espero representar bem a UnB e a Engenharia de Redes de Comunicação daqui pra frente.

Yuri Freitas Gomes Santos

RESUMO

Apesar dos inúmeros benefícios que o desenvolvimento da computação e, consequentemente, das redes computacionais trazem aos ambientes organizacionais, o número de riscos em ambientes de redes aumenta a cada dia. Embora a área de Gestão de Riscos esteja cada vez mais presente em empresas, as soluções em *software open source* disponíveis no mercado como apoios às atividade de Gestão são escassas. Este projeto busca aliar o Processo de Avaliação de Riscos (parte da Gestão de Riscos) focada em ativos de redes computacionais com o *Moodle*, plataforma originalmente usada para ensino a distância, mas que pode ser customizada para diversas finalidades.

Os resultados se mostraram satisfatórios, pois conseguimos aplicar as atividades do Processo em uma empresa fictícia, usando o Moodle e um de seus *plugins* (H5P) como apoio, mostrando que podem ser de grande utilidade também em ambientes organizacionais reais.

Palavras-chave: Gestão de Riscos, Processo de Avaliação de Riscos, ativos de rede, Moodle

ABSTRACT

Despite the benefits that networks and computing brings to the organizational environments, the number of risks that arise in network environments grows everyday. Although Risk Management is currently more present in companies, there are few open source software solutions available to support management activities. This project aims to ally the Risk Assessment Process, (part of Risk Management) focused on network assets, with the plataform Moodle a distance learning tool that can be customized to serve various purposes.

The results were good, because we could do the Process' activities in a fictional company, using Moodle and one of its plugins (H5P) as support, showing that they can be very useful in real organizational environments as well.

Keywords: Risk Management, Risk Assessment Process, network assets, Moodle

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

Acrônimos

ARP	*Address Resolution Protocol*
BGP	*Border Gateway Protocol*
CARF	Conselho Administrativo de Recursos Fiscais
CIA	*Confidentiality, Integrity and Availability*
CIC	Departamento de Ciências da Computação
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Denial-of-service*
DDoS	*Distributed Denial-of-service*
DTP	*Dynamic Trunking Protocol*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
ICI	Infraestrutura Crítica da Informação
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LAMP	Linux, Apache, MySQL e PHP
LAN	*Local Area Network*
MAC	*Media Access Control*
MITM	*Man-in-the-middle*
MOODLE	*Modular Object Dynamic Learning Environment*
PIBIC	Projeto de Iniciação Científica
RIP	*Routing Information Protocol*
SGSI	Sistema de Gestão de Segurança da Informação
SMTP	*Simple Mail Transfer Protocol*
SQL	*Structured Query Language*
SSL	*Secure Socket Layer*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
VLAN	*Virtual LAN*

Capítulo 1

Introdução

A Gestão de Riscos é um campo que está ganhando popularidade nesses últimos anos, sendo cada vez mais utilizada pelas organizações. Pelo fato de possuírem informações valiosas e confidenciais, todas as organizações podem estar sujeitas aos mais variados tipos de riscos, que podem ser, citando apenas alguns, de natureza tecnólogica, financeira, operacional e ética. Os riscos apresentados no escopo deste trabalho são de natureza tecnológica, relacionados mais especificamente aos ativos que fazem parte das redes de comunicação.

As redes computacionais fazem parte da Infraestrutura Crítica da Informação (ICI) essencial para o funcionamento de todos os sistemas informatizados laborais. Nesse aspecto, a identificação dos riscos relacionados aos ativos de rede se torna fundamental para a correção proativa de ameaças e vulnerabilidades que possam comprometer, direta ou indiretamente, o alcance dos objetivos organizacionais. Riscos materializados em ativos de rede podem comprometer toda a cadeia de infraestruturas críticas existentes devido ao forte acoplamento e interdependência existente entre todos os componentes.

Em uma sociedade cada vez mais informatizada, os ataques às redes são um dos problemas mais sérios dos ambientes organizacionais. De acordo com [1] houve, pelo mundo, um aumento de 38% desses ataques, que podem representar o vazamento de dados pessoais, causando prejuízos reputacionais e financeiros. A frequência de extrações de dados por atacantes está aumentando a cada ano, por isso 91% das empresas em relação ao ano anterior adotaram uma política de Gestão de Riscos para garantir a segurança de suas informações [1].

Historicamente, os ataques mais noticiados, e considerados prejudiciais, são os que partem de agentes externos a organização. Por conta disso, as empresas investem em segurança com o intuito de prever ataques externos, mas esquecem que os ataques mais comuns e possivelmente mais danosos são os que partem de agentes internos [2]. Devido ao fato de possuirem acesso privilegiado à rede e aos sistemas da empresa, estes tipos de ataque são mais difíceis de prevenir e detectar, sendo, por isso, necessário as organizações disporem de atenção especial a essa questão.

Dentre as diversas soluções propostas por gestores de risco, a maioria delas envolve o uso de *softwares* que realizam a automatização ou apoio às atividades que compõem a Gestão de Risco. Apesar de necessárias, são alternativas de custo elevado, influenciando a escolha de adotar ou não

um sistema que auxilie na proteção dos ativos da corporação. Sistemas gratuitos e *open source* são praticamente inexistentes.

Sendo assim, neste projeto propomos o uso do *Moodle*, ferramenta já consolidada na área de educação à distância, como suporte as atividades que formam o processo de Avaliação de Riscos. A união do *Moodle* com a Avaliação de Riscos dá a base necessária à Gestão de Riscos que, aplicada aos ativos de rede, se pretende materializar neste Trabalho de Conclusão de Curso.

1.1 Definição do Problema

Ataques às redes, sejam originários de agentes internos ou externos, são cada vez mais comuns no ambiente organizacional, ocorrendo nas mais diversas áreas incluindo tanto pequenas quanto grandes empresas.[1] Tais problemas poderiam ser evitados, ou mais facilmente detectados, com uma rotina de prevenção de riscos.

É importante reconhecer que as informações manipuladas em ambientes organizacionais são, na maioria das vezes, confidenciais e sensíveis, sendo, por essa razão, os ativos mais importantes a serem protegidos. As redes e os equipamentos que as compõem têm o papel fundamental de transportar e armazenar essas informações de forma segura, portanto devem ser protegidos da mesma forma. Assim, propomos realizar o Processo de Avaliação de Riscos focado nos ativos de rede de um ambiente organizacional fictício.

1.2 Motivação

A ideia do tema deste projeto se deu a partir de um convite feito pelo professor Edgard Costa Oliveira para participação em Projeto de Pesquisa científica (PIBIC), juntamente com o mestrando em Computação Aplicada João Batista Ribas de Moura, também orientado pelo professor Edgard. A dissertação do mestrando João Batista Ribas de Moura diz respeito a Gestão de Riscos, apoiada pelo *Moodle*, no Conselho Administrativo de Recursos Fiscais (CARF) do Ministério da Fazenda [3], local de trabalho do mesmo. Então, surgiu a ideia de utilizar o tema aplicado à área de ativos de redes e ampliar o trabalho a nível de Projeto Final de Graduação.

Nessa ampliação e pesquisa, foi reconhecido que ataques às redes computacionais estão cada vez mais frequentes e contra organizações das mais diferentes naturezas. Além disso, soluções em *software* gratuitas no mercado são escassas, e poucas empresas estão dispostas a realizar uma Gestão de Riscos personalizada, focando nos ativos de rede.

Portanto, um processo de Gestão de Riscos feito em típico cenário alvo juntamente com o desenho de uma solução para o Processo de Avaliação de Riscos de ativos de redes por meio da customização de um ambiente computacional, inspirado em normas internacionais (ISO), são as bases deste trabalho. Esta análise é viável para todos os tipos de corporações que reconheçam a necessidade de proteção dos seus ativos de rede.

1.3 Objetivo Geral

O objetivo deste trabalho é propor uma sistemática que permita organizar as informações necessárias para identificar, analisar e avaliar os riscos de um contexto de gerência e segurança em redes. Em outras palavras, propor o *Moodle* como uma ferramenta que auxilie no processo de Avaliação de Riscos em um ambiente de redes computacionais.

1.3.1 Objetivos Específicos

Para melhor entendimento, detalhamos o objetivo geral dividindo-o em objetivos específicos.

Objetivo Específico 1: estabelecer o contexto da Gestão de Riscos, considerando um ambiente de redes e ativos de conectividade.

Objetivo Específico 2: realizar o Processo de Avaliação de Riscos do contexto estabelecido, realizando as atividades de Identificação, Análise e Avaliação de Riscos.

Objetivo Específico 3: utilizar o *Moodle* como ferramenta de apoio ao Processo de Avaliação dos Riscos.

Objetivo Específico 4: gerar uma lista com sugestões de tratamento para os riscos identificados, analisados e avaliados.

1.4 Metodologia

Para alcançar os objetivos citados anteriormente, realizamos os seguintes procedimentos:

Estudo de normas internacionais e livros. Primeiramente, foi feita a identificação e o estudo de normas internacionais (ISO) e de livros relacionados ao tema. Foram analisadas as normas da família 31000 [4], que tratam de Gestão de Riscos, e as da família 27000 [5], que abordam a Segurança da Informação.

Em relação aos livros, foram utilizados, dentre outros a serem citados posteriormente, dois como base para este trabalho: *Simple Tools and Techniques for Enterprise Risk Management* [6] e *Cyber-Risk Management* [7]. O primeiro, se mostrou interessante no que diz respeito à exposição de técnicas no processo de Gestão de Riscos em ambientes organizacionais e na abordagem processual das atividades. O segundo realiza uma abordagem mais específica da Gestão de Riscos no contexto cibernético e segurança cibernética.

Alguns outros livros que abordam conceitos de Segurança de Redes e redes computacionais também foram utilizados no decurso deste trabalho, e serão citados ao longo do texto.

Estabelecimento do Contexto. Houve a necessidade de adquirir experiência na área de Gestão de Riscos e ativos de rede para o projeto. Então, o aluno Yuri Freitas foi convidado por João Batista para realizar estágio superior no CARF, na área de Gestão de Riscos, onde foi possível observar o processo em um ambiente organizacional, bem como realizar a instalação e customização

do *Moodle* em ambiente virtualizado. A aluna Aline dos Santos, por sua vez, realizou um estágio no Departamento de Ciências da Computação (CIC) da UnB, que permitiu expandir os conhecimentos em equipamentos e em estrutura de redes de computadores para familiarização da manipulação dos mesmos e suas possíveis vulnerabilidades.

A necessidade de elaboração de um contexto organizacional genérico foi facilitado com os conhecimentos adquiridos nesses ambientes de trabalho, onde foi possível estabelecer um contexto inspirado em empresas reais. Entretanto, não foi possível realizar o Processo de Avaliação de Riscos em uma empresa real, por questões de segurança e sigilo.

O contexto simulado foi elaborado para servir como um ambiente genérico que necessite da Avaliação de Riscos. Sendo assim, o processo de Avaliação de Riscos deste contexto fictício servirá para muitos ambientes que utilizam redes computacionais.

Implementação do ambiente computacional. Nesta etapa, realizamos a instalação do *Moodle* (em plataforma *Linux*), bem como seus *plugins* (H5P) e customização dos mesmos. O *Moodle* será utilizado principalmente na atividade de Identificação de Riscos, onde serão elaborados questionários e fóruns para auxiliar no processo como um todo.

Foi feita também a instalação do simulador GNS3 juntamente com os ativos de rede do fabricante Cisco virtualizados, que juntos formaram o ambiente de simulação. Com o ambiente definido, ferramentas de testes de penetração puderam ser instaladas e testadas. Tais ferramentas seriam, posteriormente, utilizadas na atividade de Análise de Riscos como mecanismo de verificação de vulnerabilidades. Maiores detalhamentos sobre as ferramentas computacionais utilizadas serão mostrados no terceiro capítulo.

Estudo técnico. Com a escolha dos ativos a serem simulados, foi necessário realizar um estudo mais detalhado das possíveis vulnerabilidades e ataques realizáveis no ambiente de simulação, além de todas as configurações técnicas necessárias. Para isso, utilizamos *Cisco LAN Security* [9] que apresenta diversos ataques a *switches* e um livro de treinamento para a certificação CCNA, da Cisco [10].

Processo de Avaliação de Riscos. A união do conhecimento e práticas obtidas permitiu a realização do processo de Avaliação de Riscos aplicados aos ativos de rede no contexto de uma organização fictícia. O processo realizado utiliza abordagens de [6] e [7], detalhando todas as etapas e atividades pertinentes. O método utilizado para tratar cada informação necessária do processo foi baseado no modelo de Gestão de Riscos abordado em [6] e descrito na seção 2.1.2, modelo este que trata as atividades como processos, possuindo entradas, delimitações, mecanismos e saídas. De uma forma geral, as entradas são transformadas em saídas por meio dos mecanismos, seguindo as restrições impostas pelas delimitações.

Feita a definição dos objetivos e métodos, podemos, neste momento, explorar os conceitos teóricos que farão parte do Processo de Avaliação de Riscos de ativos de rede.

Capítulo 2

Fundamentação Teórica

Este capítulo traz a base teórica dos conteúdos utilizados no Processo de Avaliação de Riscos. Além do detalhamento das etapas que compõem o processo de Gestão de Riscos, também são abordadas a Segurança da Informação e suas variantes, bem como uma breve descrição técnica de alguns conceitos de redes de computadores.

2.1 Gestão de Riscos

Uma das definições mais simples do conceito de risco o define como a probabilidade de um incidente e sua consequência para um ativo [7]. Em relação ao conceito de ativos, estes são definidos como qualquer coisa de valor para a organização, empresa, pessoa ou grupo onde a avaliação dos riscos está sendo conduzida [7]. Neste trabalho o foco será no ambiente organizacional.

Gestão de Riscos são atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos [4]. A Gestão de Riscos será tratada com uma abordagem de processo, que se define como uma atividade ou conjunto de atividades que utiliza recursos e é gerenciada de forma a possibilitar a transformação de entradas em saídas [8].

A figura 2.1 mostra as atividades e como se relacionam, definidas pela norma [4]. Apesar de alguns autores usarem implementações levemente diferentes da aqui mostrada, a representação é suficiente para uma visão geral.

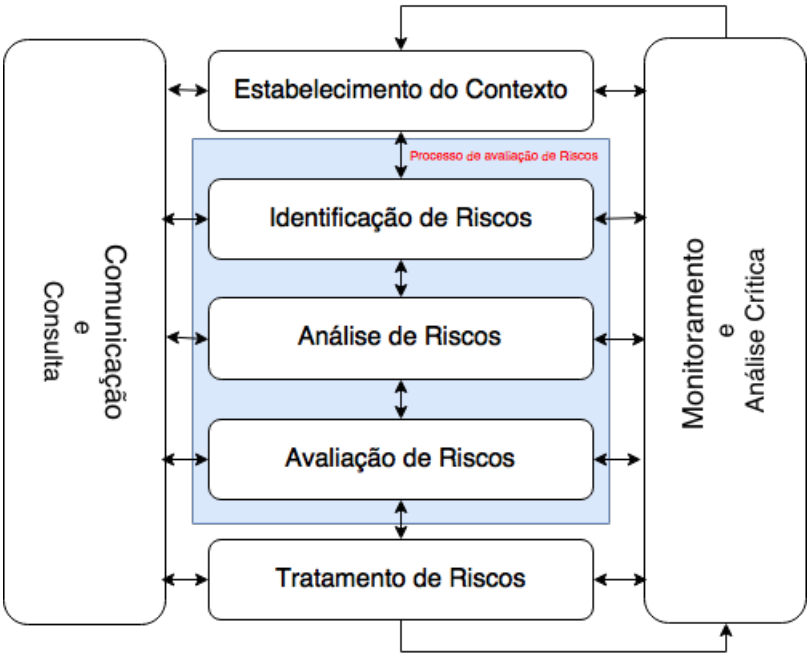

Figura 2.1: Processo da Gestão de Riscos. Fonte: [4] - adaptado

2.1.1 Atividades da Gestão de Riscos

As atividades que compõem o Processo de Gestão de Riscos são:

2.1.1.1 Estabelecimento do Contexto

Estabelecimento do Contexto é a primeira atividade do processo de gestão de riscos. A primeira parte é definir contexto externo, interno, metas, e alvos da avaliação. Depois disso, delimitações internas, que incluem escopo, foco e premissas.

O contexto externo é composto pelo ambiente (cultural, social, político, legal) do qual a organização faz parte. Por sua vez, contexto interno abrange, dentre outros aspectos, as políticas internas da empresa. As metas são o que se deseja alcançar por meio da a Gestão de Riscos. Os alvos da avaliação incluem os processos, ativos, pessoas e todas as outras entidades relevantes durante o processo [7].

As delimitações são formadas por subaspectos nomeados escopo, foco e premissas. O escopo é o "tamanho"da avaliação, ou seja, o que é importante e será considerado nela. O foco é o principal problema que a Avaliação de Riscos aborda. Premissas são o que previamente se considera como verdadeiro a respeito do contexto. [7]

Todas as informações do contexto externo e interno, metas, alvos da avaliação e delimitações internas devem ser documentadas.

Através dos documentos, é possível definir as escalas e critérios de avaliação dos riscos. As escalas

são compostas por probabilidade e consequência, podendo estes serem quantitativos ou qualitativos. Critérios de avaliação, por sua vez, são termos de referência pelos quais a significância do risco é avaliada, variando de um ativo para outro [7], A fórmula mais empregada para definir o risco se dá em termos do produto das probablidades e da consequência, ou seja:

$$\text{Riscos} = \text{Probabilidades x Consequência}$$

Após todas as tarefas desta atividade estarem concluídas e documentadas, inicia-se o chamado Processo de Avaliação de Riscos (região azul da figura 2.1), que é formado pelas etapas de identificação, análise e avaliação dos riscos.

2.1.1.2 Identificação de Riscos

A atividade de identificação de riscos é composta de tarefas que possibilitam identificar e descrevê-los, apontando a fonte da ameaça, a ameaça, e a vulnerabilidade. O resultado desses eventos levam à um risco, mostrado na figura 2.2.

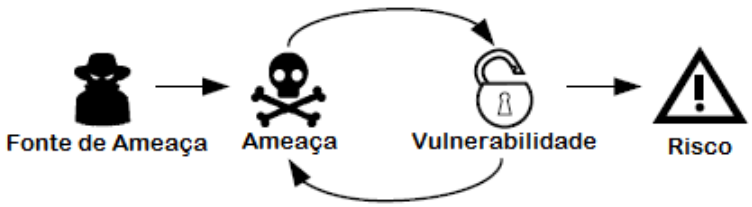

Figura 2.2: Ciclo de formação de um risco. Fonte: [7] - adaptado

Fontes de Ameaças: de acordo com [7], fontes de ameaças são os responsáveis pelos incidentes, podendo ser humanas ou não-humanas, interna ou externas à empresa.

Ameaças: após a identificação das ameaças, é necessário identificar quais ameaças podem surgir daquelas fontes, (figura 2.2). Segundo [7], ameaça é tudo aquilo que é executado pela sua fonte e que de alguma maneira causa um incidente no ambiente afetado.

Vulnerabilidades: fragilidade no ambiente que pode ser explorada por uma ameaça, ou seja, uma fraqueza, falha ou deficiência [7].

Há diversas técnicas e métodos que são realizados com o objetivo de identificar os riscos. Alguns destes métodos incluem: análise de dados históricos (com a possível presença de diagramas e estatísticas), entrevistas com funcionários (utilizando perguntas específicas), *workshops*, *brainstorming* e reuniões. Os mecanismos escolhidos podem variar, por exemplo, de acordo com o número de funcionários, a cultura da organização com relação a Gestão de Riscos e também com o contexto, já documentado na atividade anterior.

2.1.1.3 Análise de Riscos

O objetivo da atividade Análise de Riscos é estimar e determinar o nível de probabilidade e consequência dos riscos identificados, ou seja, o que configura o nível do risco. Na atividade de Estabelecimento do Contexto, foram definidas as escalas (probabilidade e consequência) que fariam parte do Processo de Avaliação de Riscos, portanto, agora deve-se quantificá-las.

Além dos métodos citados na atividade de Identificação dos Riscos (questionários, reuniões, etc.), a estimação das probabilidades dos riscos pode precisar de ferramentas mais técnicas, como *softwares* de simulação. Quando tratamos da consequência, pelo fato da análise ser mais subjetiva, são preferidas as técnicas que envolvam conferências e debates entre os funcionários.

2.1.1.4 Avaliação de Riscos

É a última atividade do Processo de Avaliação de Riscos, consolidando-o. Enquanto na atividade anterior determinou-se o nível de probabilidade e consequência dos riscos, nesta atividade deve-se usar os critérios de avaliação definidos no etapa de Estabelecimento do Contexto para precisar o nível dos riscos e decidir quais deles seguirão para a etapa de tratamento.

Além disso, outra tarefa da Avaliação de Riscos é a agregação de riscos considerados semelhantes. Isto é, riscos que apresentam características semelhantes consequentemente serão agregados. Desta forma, somente o valor do impacto aumenta, o que torna o risco mais perigoso. Esta é uma etapa crucial que exige discussão e reflexão por parte dos tomadores de decisão.

2.1.1.5 Tratamento de Riscos

De um modo geral, Tratamento de Riscos tem como objetivo reduzir o nível dos riscos, diminuindo aspectos como a probabilidade de incidência e consequência. Porém, às vezes o risco pode ser tão diminuto, improvável, ou exigir um tratamento dispendioso fazendo com que decisão pode seja de apenas retê-lo, isto é, aceitá-lo. Outras decisões possíveis são as de evitar o risco e a de compartilhá-lo.

Antes de efetivamente tratar o risco, deve ser realizada uma tarefa de identificação dos tratamentos adequados, usando técnicas semelhantes as já citadas na atividade de Identificação de Riscos.

2.1.1.6 Comunicação e Consulta

É fundamental que todos os documentos, de entrada e saída, das atividades sejam devidamente comunicados aos responsáveis e consultadas quando necessário. As tarefas programadas (por exemplo, uma sessão de *brainstorming* na etapa de Identificação de Riscos), devem ser planejadas e previamente comunicadas aos participantes, de forma que todos colaborem ou justifiquem sua ausência a tempo.

2.1.1.7 Monitoramento e Análise Crítica

Todas atividades devem ser monitoradas a fim de se checar sua validade e efetividade. Eventos inesperados podem levar a alterações na probabilidade de ocorrência de determinado risco, por exemplo, o que obriga a revisão das atividades de análise de risco. O monitoramento também aborda o uso de indicadores de desempenho, como por exemplo, tempo gasto na atividade e satisfação dos participantes que, dependendo dos resultados, podem promover mudanças significativas no processo.

2.1.2 Modelo do Processo de Avaliação de Riscos

Como citado anteriormente cada atividade do Processo de Avaliação de Riscos seguirá o esquemático apresentado na figura 2.3, baseado em [6].

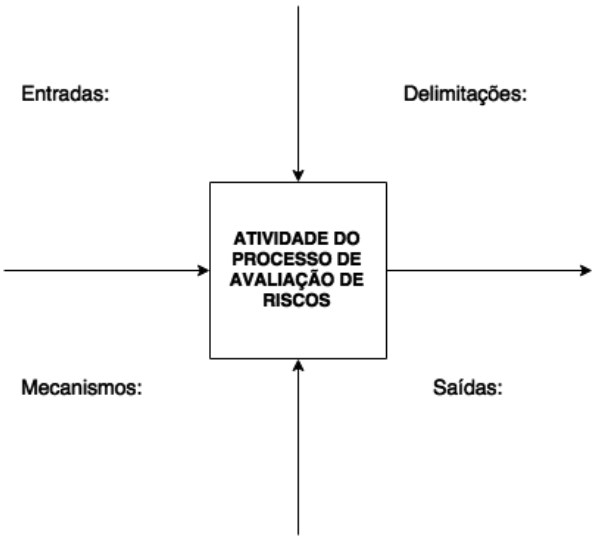

Figura 2.3: Modelo utilizado no Processo de Avaliação de Riscos. Fonte: [6] - modificado

Entradas: as entradas são classificadas de duas formas: a primeira forma trata as entradas como informações que já estão em mãos, obtidas por meio de observação ou por meio da saída de atividades anteriores; a segunda forma trata as entradas como informações que se deseja obter nessa mesma atividade com auxílio dos mecanismos.

Delimitações: são os fatores que impedem, de alguma forma, a realização plena da atividade. Não é necessariamente igual e nem diferente em cada atividade.

Mecanismos: são os artifícios utilizados para transformar as entradas da atividade. Assim como nas delimitações, os mecanismos podem ou não ser iguais em cada atividade. Para o nosso Processo de Avaliação de Riscos, a maioria dos mecanismos utilizados são diferentes entre si.

Saídas: neste trabalho, a saída será necessariamente um documento que mostra as entradas e as descobertas através dos mecanismos. O objetivo desse documento é auxiliar como entrada já

obtida das próximas atividades.

2.2 Segurança da Informação

Informação é um ativo essencial para a organização e deve ser protegido e conservado [5]. Existem três importantes princípios a serem adotados quando se fala em Segurança da Informação. Tais princípios compõem a chamada tríade CIA, composta por Confidencialidade, Integridade e Disponibilidade.

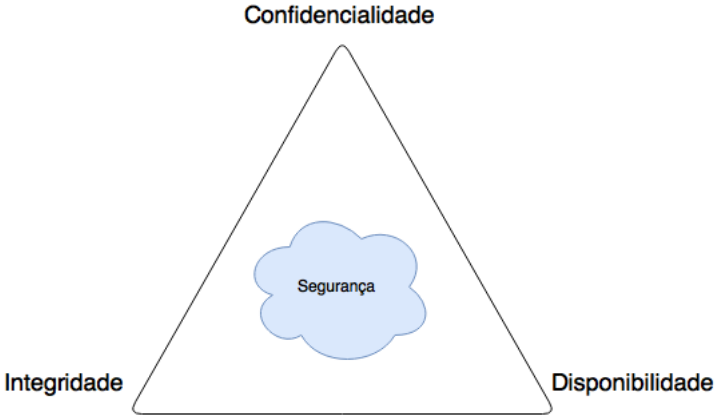

Figura 2.4: Tríade CIA, os três pilares da Segurança da Informação. Fonte: [9] - adaptado

Confidencialidade assegura que a informação não seja acessível, nem divulgada, a qualquer entidade não autorizada. Integridade é a alteração ou destruição da informação somente por pessoas autorizadas. Por fim, Disponibilidade é o acesso a informação sob demanda por entidades autorizadas. [9, 11]. Sendo assim, Segurança da Informação envolve a proteção dessas três propriedades da informação em dispositivos que armazenam, manipulam e transmitem informação através de produtos, pessoas e procedimentos [12]. Nenhum sistema ou protocolo é considerado seguro se não cumprir as regras da tríade CIA.

Com o intuito de assegurar as propriedades da tríade de segurança, as normas da família 27000 abordam requerimentos, guias e boas práticas com o objetivo de auxiliar a implementação de um sistema de gestão da segurança da informação (SGSI) num ambiente organizacional.

De maneira mais específica, um SGSI é uma abordagem sistemática para estabelecer, implementar, operar, monitorar, rever, manter e melhorar a Segurança da Informação numa organização com o intuito de se alcançar seus objetivos, de acordo com a norma 27000 [5]. Para isto, todos os passos explicitados anteriormente na seção 2.1 (identificar, análisar, avaliar e tratar riscos) são abordados pelas normas, porém no contexto da Segurança da Informação.

Além das normas, [10] e [12], apesar de serem mais técnicos e voltados a certificação, citam a Gestão de Riscos como componente importante da Segurança da Informação, exemplificando a importância e ligação intrínseca entre estes dois conceitos.

2.3 Segurança Cibernética

Importantes definições, vistas em [7] são necessárias para tratar deste assunto.

Espaço cibernético. Coleção de ambientes computacionais interconectados, incluindo serviços, computadores e controladores, bem como informação armazenada ou em trânsito.

Sistema cibernético. Sistema que usa um espaço cibernético.

Segurança cibernética. Proteção de sistemas cibernéticos contra ameaças cibernéticas (ameaça que explora um espaço cibernético).

A Segurança da Informação tem como foco preservação da Confidencialidade, Integridade e Disponibilidade da informação. Porém essa definição não se aplica exclusivamente a sistemas cibernéticos,como também abrange fontes de ameaças físicas e humanas, por exemplo. A Segurança Cibernética trata apenas de ameaças originárias de espaços cibernéticos, o que pode incluir ativos de informação que façam uso de um espaço cibernético.

2.4 Segurança de Redes

A Segurança de Redes diz respeito a proteção dos três pilares da Segurança da Informação no âmbito de dispositivos interconectados num espaço cibernético (ativos de redes) bem como das informações repassadas por eles. Vê-se na figura 2.5 um diagrama de Venn que relaciona os conceitos de Segurança de Redes, Segurança da Informação e Segurança Cibernética.

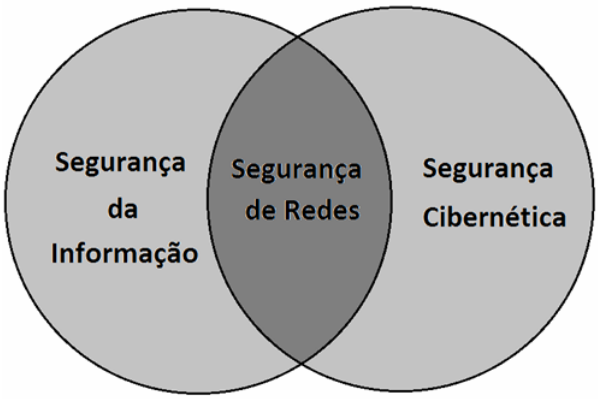

Figura 2.5: Diagrama de Venn relacionando conceitos de Segurança. Fonte: autores

Em Segurança de Redes, as ameaças podem advir tanto das possíveis vulnerabilidades vindas da Segurança da Informação, como um acesso não autorizado a um servidor, (comprometendo a Confidencialidade), como da Segurança Cibernética, tal qual um vírus vindo da Internet que inutiliza um roteador, (comprometendo a Disponiblidade dos dados). Estas semelhanças ilustram os motivos para a Segurança de Redes estar na interseção entre a Segurança da Informação e a Segurança Cibernética.

2.5 Arquitetura em camadas

Antes de adentrarmos maiores detalhes sobre as vulnerabilidades e ataques às redes computacionais, é importante introduzir conceitos básicos sobre as mesmas. Há diversas formas de abordagem de redes computacionais, sendo a mais utilizada o modelo de referência em camadas. Decidimos utilizar o modelo TCP/IP, de cinco camadas, assim como em [13].

2.5.1 Protocolos pertencentes às camadas do TCP/IP

A seguir, uma breve descrição dos protocolos presentes nas cinco camadas do modelo de referência TCP/IP [13].

Aplicação: provavelmente o protocolo mais conhecido de redes está presente nesta camada: o HTTP, que realiza a transferência de dados na *web*. Além dele, destaca-se o SMTP (utilizado nos emails), o DNS (procotolo de tradução de endereços) e o DHCP (configuração dinâmica de endereços). A camada de aplicação é implementada nos sistemas finais, como computadores pessoais, servidores e *laptops*. A nomenclatura dos pacotes nesta camada é mensagem. Os protocolos da camada de aplicação e de transporte (detalhada adiante) são separadas pelas chamadas portas (*sockets*), interfaces virtuais. Cada aplicação utilza uma ou mais portas numa conexão.

Transporte. Os dois principais protocolos da camada de transporte são o TCP e o UDP. O primeiro é orientado a conexão e provê transferência confiável de dados, alcançando confiabilidade utilizando mecanismos como retransmissão seletiva e janelas deslizantes. O TCP é utilizado em aplicaçãoes como email e HTTP. O UDP, por sua vez, não fornece transferência confiável dos dados, sendo, por isso, mais utilizado em aplicações onde não haja tanto prejuízo com eventuais perdas, como o protocolo DNS e *streaming*. Assim como na camada de aplicação, a camada de transporte é implementada nos sistemas finais. A nomenclatura dos pacotes nessa camada é segmento.

Rede. O protocolo mais utiilzado na Internet, IP, está presente nesta camada. A função do IP é transportar os dados entre os sistemas finais, utilizando endereços IP para isso. Além do IP, protocolos de roteamento, que têm a missão de calcular melhores rotas (como o RIP e o BGP) e protocolos de gerência, como o ICMP, também fazem parte desta camada. A camada de rede é implmentada em roteadores. A nomenclatura dos pacotes nesta camada é datagrama.

Enlace. Enquanto a camada de rede tem a missão de transportar dados entre os sistemas finais, a camada de enlace faz o transporte de dados entre nós, que incluem além dos sistemas finais, roteadores e *switches*. Para que o transporte seja realizado, são utilizados endereços MAC, protocolos como o ARP (que traduz endereços IPs para endereços MAC) e a Ethernet protocolo mais utilizado em redes locais (LANs). A nomenclatura dos pacotes nessa camada é *frame*.

Física. Nível mais baixo e menos complexo do modelo de referência TCP/IP. Na camada física, os *bits* são movidos de um nó a outro. Os protocolos dependem do tipo de cabeamento utilizado, como fios de cobre ou fibra ótica, e também do protocolo da camada superior (enlace) implementado.

2.6 Ativos de Rede

As redes de comunicação expandiram-se muito rapidamente durante os últimos anos, principalmente as redes computacionais devido ao grande desenvolvimento da computação. Dentre os diversos ativos de redes, nosso foco está nos roteadores, *switches*, *firewalls* e servidores.

2.6.1 Switches

Switches são dispositivos que operam na segunda camada, enlace. Eles têm a capacidade de dividir domínios de colisão, isto é, cada porta do *switch* possui o segmento livre, não existindo colisões entre *frames* que competem para usá-lo. Domínios de *broadcast*, cujo dispositivo de roteamento não é necessário para conectar seus componentes, são separados apenas nos roteadores. É importante fazer essa distinção pois, se os domínios de *broadcast* forem muito grandes, o desempenho da rede como um todo fica prejudicado.

A utilização dos *switches* se dá em ambientes de redes locais (LANs). O principal motivo para usá-los é otimizar a performance dos usuários, promovendo maior largura de banda para cada hospedeiro da LAN [10].

Uma das alternativas mais utilizadas para separar domínios de *broadcast* de forma lógica, isto é, virtual, é através de VLANs, LANs virtuais. Dessa maneira é possível, na mesma rede local, isolar segmentos. Uma ação útil para, por exemplo, isolar seções com funções administrativas diferentes em uma organização. No entanto, para haver comunicação entre as VLANs é necessário o uso de um roteador.

Existem dois tipos de portas em *switches* da empresa Cisco: acesso e *trunk*. Portas de acesso pertencem a apenas uma VLAN e não identificam os *frames* que passam entre os *switches*. No que lhe diz respeito, portas do tipo *trunk* são, por padrão, membros de todas as VLANs que existam no *switch* e transportem dados para todas as VLANs entre eles. Para realizar esse transporte, são utilizados protocolos especiais de identificação (ISL ou 802.1q) que ficam inseridos no *frame Ethernet*. [14]. O protocolo propietário da Cisco, DTP, realiza a configuração de conexões *trunk* de forma automática, porém apresenta vulnerabilidades de segurança, como veremos posteriormente.

2.6.2 Roteadores

Roteadores são dispositivos que atuam na terceira camada, camada de rede, implementando interconexões entre redes. Neles são implementados os protocolos de roteamento, que calculam rotas e melhores caminhos em redes internas, como por exemplo, o protocolo RIP e para redes externas, protocolo BGP. É também comum que roteadores sejam configurados como servidores DHCP. Ao contrário dos *switches*, os roteadores separam domínios de *broadcast*, otimizando a largura de banda.

Os roteadores são pontos de acesso entre uma rede interna e a Internet, ou seja, muitas vezes a porta de entrada para invasores. Por isso, são ativos muito importantes e devem ser protegidos e

configurados da maneira correta.

2.6.3 Servidores

Apesar de não conseguirem fazer nenhum tipo de comutação, os servidores podem ser considerados um dos principais ativos de rede, pois fornecem serviços aos clientes quando solicitado. Estes serviços podem variar entre *e-mails*, arquivos, páginas *Web* ou endreços DNS, citando apenas alguns. Um servidor *Web*, por exemplo, muitas vezes vem acompanhado de um servidor de banco de dados, que carrega informações pessoais dos usuários cadastrados naquele site. Por isso, os servidores devem ser muito bem protegidos e monitorados.

2.6.4 Firewalls

São ativos que têm como objetivo aumentar a segurança de uma rede. Os *firewalls* podem ser tanto *hardware* como *software*, tendo como objetivo análisar pacotes e aceitá-los ou não, realizando uma filtragem. Esta filtragem pode ser do tipo *stateless*, a qual se baseia nas regras configuradas pelo administrador de rede, ou *statefull*, que mantém o estado da conexão entre um dispositivo interno (rede interna) ou externo (internet) e toma decisões baseadas nesta conexão. Um exemplo para ilustrar a diferença entre filtragens: se um servidor externo iniciar a conexão e tentar enviar um pacote para um dispositivo interno, este pacote pode ser aceito na filtragem *stateless*, enquanto na filtragem *statefull* ele seria rejeitado, pois a conexão não foi iniciada na rede interna. [12]

As ações dos *firewalls* podem ser baseadas em regras, como endereços e portas de fonte e destino, protocolos e direção dos pacotes (para dentro ou fora da rede interna). Muitas vezes são utilizadas listas para explicitar o que for proibido (*blacklists*) ou permitido (*whitelists*) passar pelo *firewall*. Outro tipo de abordagem, mais moderna, está presentes nos chamados firewalls de aplicação, que são mais inteligentes e se embasam na natureza das aplicações, não seguindo necessariamente regras preestabelecidas ou listas.

2.7 Ameaças aos Ambientes de Rede

Há diversas ameaças presentes nos ambientes de redes computacionais. Devido à complexidade do assunto, existindo uma grande quantidade de livros inteiramente dedicados a ele, foi necessário resumir os principais conceitos, no que tange ao escopo deste trabalho.

2.7.1 Fontes de ameaça

Citamos agora algumas fontes de ameaça comuns em um ambiente de rede baseadas em [7].

Script kiddie. Não possui muito conhecimento técnico ou recursos para realização de ataques. Deseja apenas se afirmar e provar sua habilidade em causar dano.

Terrorista cibernético. Tem como objetivo causar sérios danos a sociedade, motivado por razões religiosas, políticas ou ideológicas. Possui muitos recursos e habilidades.

Black hat hacker. Assim como os terroristas cibernéticos, possuem, na maioria das vezes, muitos recursos e conhecimento para realizar os ataques. Porém, são motivados por ganho pessoal e financeiro.

Agente interno. Funcionário desleal motivado por ganhos pessoais ou brigas com seu empregador. Nível técnico varia, porém possui acesso físico ao ambiente da organização, o que já facilita a realização de ataques.

Malwares. *Softwares* maliciosos (*malicious software*) tendo os mais diversos objetivos. De acordo com relatório da empresa de segurança FireEye [15], no ano de 2012, eventos com *malware* ocorriam, em média, uma vez a cada três minutos nas organizações. O nível técnico varia bastante e depende da finalidade e habilidades dos desenvolvedores. Alguns exemplos incluem *trojans*, vírus e *backdoors*.

2.7.2 Técnicas de exploração de um Ambiente de Redes

Segue exemplos de técnicas usadas pelas fontes de ameaça para exploração e análise de um ambiente de redes, tomado como referência o material [11].

Escaneamento. Muitas vezes é a primeira coisa que o atacante faz. O escaneamento tem como objetivo levantar informações relevantes, como endereços IP, MAC e portas abertas na rede que se pretende atacar.

Spoofing. É a falsificação de alguma informação, como endereço MAC ou IP. Com os endereços falsos é possível melhorar a eficiência de alguns ataques.

Sniffing. É a análise dos pacotes por meio de programas conhecidos como *sniffers*, que analisam os protocolos em todas as camadas da comunicação. As informações capturadas pelo atacante devem ser analisadas até que ele encontre o que estava procurando.

2.7.3 Ataques aos Ambientes de Redes

Detalhamos brevemente alguns ataques a ambientes de redes computacionais. Alguns dos ataques mais técnicos serão explicados com conceitos de protocolos posteriormente. Para simplificar, chamaremos as fontes de ameaça apenas de atacantes. Tais conceitos abaixos foram retirados de [11, 12].

Engenharia Social. Ataques que buscam explorar os aspectos sociais, culturais e econômicos de indivíduos com pouca consciência de privacidade e confidencialidade. Têm o objetivo de obter informações confidenciais, muitas vezes nem utilizando a tecnologia para isso. É um dos ataques mais poderosos para obtenção de informações confidenciais.

Exploits. Códigos que exploram falhas de segurança. As falhas muitas vezes são oriundas de erros no próprio desenvolvimento do *software*. Há uma enorme quantidade de pessoas que se dedicam

a encontrar e reportar vulnerabilidades que incluem variados tipos de sistemas, como falhas em aplicações *web* e sistemas operacionais de *switches* e roteadores, por exemplo.

SQL Injection. Tendo como alvo servidores *web* que hospedam banco de dados, o ataque consiste na inserção de comandos SQL em campos de entradas de usuário em páginas *web* para alterar, remover, listar, inserir ou criar dados em bancos de dados. Se uma página *web* for vulnerável a este tipo de ataque, é possível, por exemplo, retornar a lista de todos os usuários e senhas com um único comando SQL. A prevenção consiste em realizar os chamados *encoding* e validação no código do *website*, que filtra os dados que o usuário insere e impossibilita que sejam interpretados como códigos.

Cross-Site Scripting (XSS). Ataques a servidores *web*, consistindo em injeção de *scripts* (sequência de comandos executados pelo computador) maliciosos em campos de entrada de usuários que os redirecionam para sites não confiáveis ou até mesmo roubam dados confidenciais armazenados no navegador Web do usuário. A prevenção é semelhante a do SQL injection (*encoding* e validação).

Negação de serviço (DoS). Consiste no consumo dos recursos de um sistema que leva a indisponibilidade dos dados e até mesmo possível destruição dos mesmos. O tipo mais comum é o distribuido (DDoS), onde o ataque vem de vários fontes ao mesmo tempo.

Man-in-the-middle (MITM). Envolve a usurpação da identidade de dois usuários. O atacante intercepta a totalidade ou parte do tráfego da rede, de forma que possa ficar no meio da comunicação entre as vítimas, se disfarçando e assim obtendo informações das quais não poderia ter acesso. Este tipo de ataque pode ser do tipo passivo, onde o atacante grava as informações capturadas antes de manda-las ao destino original, ou ativo, onde o atacante interpreta e altera as informações antes de enviá-las ao destino. Pode ocorrer em redes locais (mais facilmente) e até mesmo na Internet. Muitas vezes utilizam-se de técnicas de *spoofing*.

MAC flooding. Consiste no inundamento da tabela de endereços MAC em um *switch* sendo considerado, portanto, um ataque DoS. Durante a realização do ataque, a rede interna fica bastante lenta. A indisponibilidade do serviço occorre até mesmo em VLANs diferentes da que o atacante está, prejudicando a comunicação como um todo. A prevenção consiste na limitação de endereços MAC por porta.

VLAN Hopping. Acesso a diferentes VLANs das quais o atacante seria, em primeiro momento, incapaz de acessar. É possível roubar informações confidenciais dos membros da VLAN atacada, bem como injetar códigos maliciosos que podem se alastrar por toda a rede interna. Para que a realização do ataque seja plausível, é necessário que haja um *link* do tipo *trunk* entre dois *switches* e que este *link* esteja na mesma VLAN nativa que as portas do tipo acesso. O ataque é realizado por meio de *double tagging*, ou seja, o *frame* é duplamente enapsulado com o protocolo do *trunk* (802.1q, por exemplo). O uso da VLAN 1 nativa e o protocolo DTP (proprietário da empresa Cisco) não são recomendados nos *switches*, pois facilitam o ataque. [14]

DHCP Scope Exhaustion. Ataque do tipo DoS. O protocolo DHCP não implementa medidas de segurança ao alocar endereços IP, sua principal função. Dessa forma, se um atacante utilizar endereços MAC falsos, por meio de *spoofing*, o servidor DHCP não se importará com a identidade

dos mesmos, alocando endereços IP até eles acabarem. Um usuário legítimo que tentar entrar na rede não terá nenhum endereço IP disponível para tal, impossibilitando, assim, o acesso.

DHCP Rogue Server. Uso de um servidor DHCP malicioso, instalado dentro da rede interna, de forma que ele passa a competir com o servidor DHCP legítimo. O primeiro servidor que receber as solicitações, atribui os endereços ao usuário. Se for o servidor malicioso, ele pode atribuir configurações que direciona a(s) vítima(s) para sites forjados, podendo assim obter informações pessoais. A prevenção tanto deste ataque quanto do *DCHP Scope Exhaustion* inlcui políticas de segurança de portas e o uso de DHCP *snooping*, uma ferramenta de controle que inspeciona a fundo as portas confiáveis em uma VLAN.

ARP Poisoning. Ataque do tipo MITM em que o atacante se aproveita das vulnerabilidades do protocolo ARP (que assim como o DHCP não exige autenticação), para interceptar os pacotes das vítimas na rede local. Para ilustrar, considere uma comunicação entre dois *hosts*, A e B, e um atacante, *host* C, onde os três estão na mesma LAN. O *host* C se posiciona no meio da comunicação entre os hosts A e B, informando o seu endereço MAC como destino ao *switch* da rede local. Se o host A for um PC e o *host* B for um roteador, por exemplo, o atacante pode utilizar um *sniffer* para interceptar até mesmo os pacotes que vão do *host* A (rede local) para a internet. Entretanto, para receber os pacotes vindo da internet, são necesários múltiplos ataques, de forma que a comunicação não seja interrompida. Recomenda-se o uso do protocolo SSL (*secure socket layer*), que criptografa as entradas dos usuários durante a comunicação cliente-servidor.

Em ambientes organizacionais, é comum uma separação de direitos de acesso, ou seja, privilégios diferentes para acessar serviços fornecidos pela rede, *software* ou *hardware*. Um funcionário que trabalha com desenvolvimento terá acesso a mais recursos do servidor do que outro usuário que trabalha com vendas, por exemplo. Ataques desta natureza buscam justamente garantir acesso a usuários não autorizados.

Escalonamento de privilégios. Utilização de *exploits*, ou más configurações no *software* de uma aplicação com o intuito de obter acesso a recursos que eram anteriormente restritos. O ataque pode ser do tipo vertical no horizontal. No vertical, um usuário com poucos privilégios consegue acesso a recursos de usuários com privilégios mais altos. Já no horizontal, um usuário com privilégios restritos consegue acessar diferentes recursos por meio de um usuário que tenha o mesmo nível de privilégio [12].

Após o embasamento teórico dos assuntos que se encaixam no escopo deste projeto, podemos, agora, começar o Processo de Avaliação de Riscos dos ativos de rede de uma organização fictícia.

Capítulo 3

Contexto e Ferramentas Computacionais

Este capítulo é dividido em duas partes: a primeira parte traz a primeira atividade do processo de Gestão de Riscos e o Estabelecimento do Contexto. A segunda parte mostra as ferramentas computacionais utilizadas para execução das atividades do Processo de Avaliação de Riscos, incluindo o Moodle, o software de simulação (GNS3) e as ferramentas de testes de penetração. Também especifica a marca (Cisco) e modelo dos *switches* e roteadores utilizados nas simulações.

3.1 Estabelecimento do contexto

As entradas desta atividade são: contextos (externo e interno), metas, alvos e escalas da avaliação de riscos. As delimitações são dadas pelo escopo, foco e premissas. Os mecanismos são os critérios de avaliação dos riscos e as tabelas para organização. A saída será na forma de um documento detalhando todas as entradas, transformadas pelos mecanismos e respeitando as delimitações. Todos esses itens estão organizados na figura 3.1 no modelo citado na seção 2.1.2.

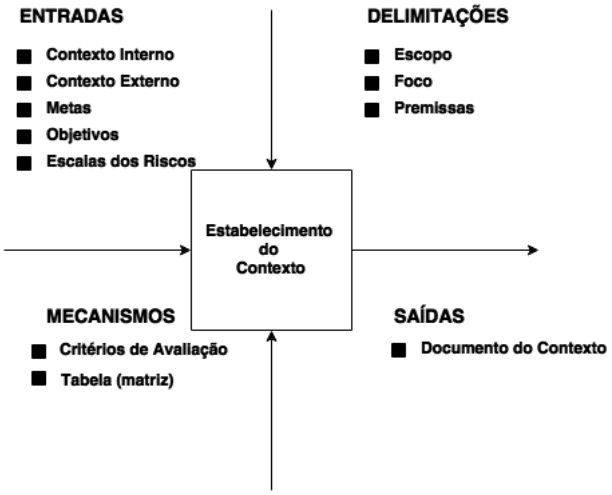

Figura 3.1: Atividade de Estabelecimento do Contexto de A+. Fonte: [6] - modificado

3.1.1 *Entradas*

Detalhamento das entradas da atividade.

Contexto externo. A empresa fictícia, que chamaremos de A+, é uma empresa brasileira inseridad no contexto atual, onde muitas organizações possuem *websites* informativos, além de escritório físico. Recentemente, passou a trabalhar com e-comércio eletrônico (*e-commerce*), incorporando-o ao *website*. É considerada uma empresa de pequeno porte por possuir uma receita bruta que encaixa nos padrões de [16].

A+ vai bem no mercado, pois, atualmente, muitas pessoas preferem comprar produtos *online* por conta dos preços e de uma concorrência mais ampla. Em 2016, a arrecadação do *e-commerce* no Brasil foi de mais de 19 bilhões de reais, representando um crescimento de mais de 5% em relação a 2015. Além disso, foram mais de 20 milhões de clientes online [17]. Apesar de possuir um produto inovador e estar crescendo, A+ possui muitos concorrentes.

Contexto interno. A despeito do crescimento no mercado, A+ não realizou muitos investimentos em Segurança de Redes dentro do escritório físico, onde estão hospedados o *website* (ambiente do *e-commerce*) e o sistema interno. Detalhamos a topologia de rede da empresa para melhor entendimento do cenário.

Topologia. A rede interna da empresa possui quatro diferentes VLANs, que separam as área administrativas: Tecnologia da Informação (TI), Operações I, Operações II e Administrativo (englobando Finanças e Recursos Humanos). Todas as VLANs enlogam os computadores dos funcionários, com o servidor fazendo parte da VLAN da TI. As VLANs estão divididas entre três *switches*, as duas VLANs de Operações estão no mesmo *switch*. Há também um *switch* de distribuição, conectado a todos os outros por meio de links do tipo *trunk* e ao roteador.

No servidor da empresa, estão hospedados o *website* e o sistema interno. O *website*, ambiente do o *e-commerce*, utiliza um banco de dados MySQL. Nesse *website* ocorre a realização dos pedidos pelos clientes e processamento dos pedidos pelos funcionários. O chamado sistema interno é um sistema de controle de vendas acessado por funcionários para registrar cada pedido realizado na loja física detalhadamente.

O roteador, além das funções de roteamento, opera também como um servidor DHCP. Ele está conectado à um *firewall* em *software* antes de se conectar à internet externa. A figura 3.2 ilustra a topologia descrita, com menor número de *hosts* para simplificação.

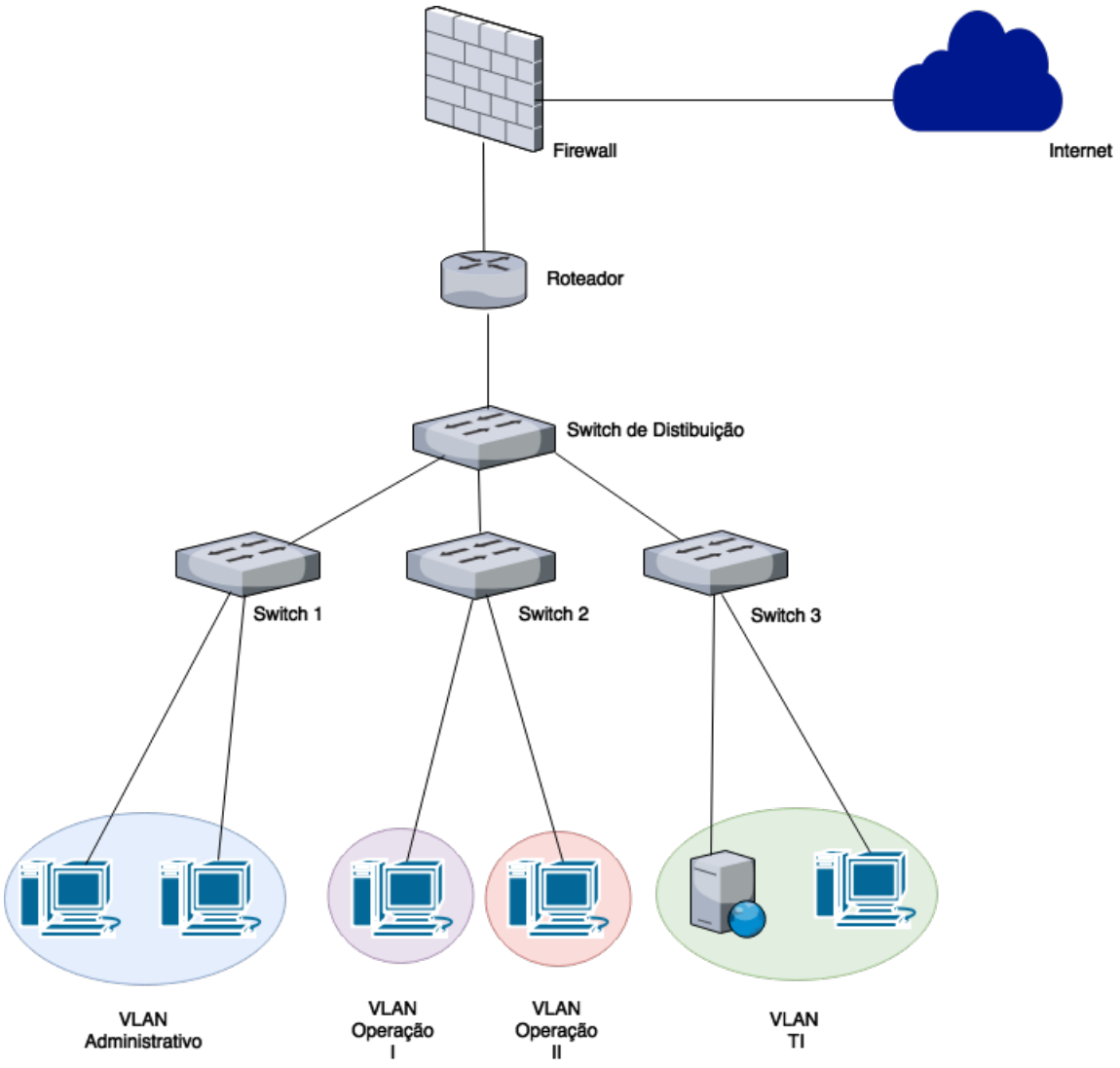

Figura 3.2: Topologia de toda a rede da empresa A+. Fonte: autores

Permissões de Acesso. As quatro VLANs são configuradas de forma que as permissões de acesso estejam de acordo com o setor que a utiliza. Por administrar toda a rede da empresa e desenvolver os sistemas, a VLAN da equipe de Tecnologia da Informação (TI) possui o mais alto nível de privilégios, com acesso a todos os ativos. As VLANs de operação, possuem um acesso igual ao sistema de controle de vendas. Porém, a VLAN de Operação I têm acesso como administrador ao sistema de *e-commerce*, tal qual a VLAN de Operação II não possui. No último nível de privilégios, está a VLAN do Administrativo (Financeiro e Recursos Humanos), nesta rede é possível acessar o sistema interno e o *website* somente para observar os dados.

Juntamente com o controle da equipe de TI, cada funcionário recebe o seu *login* de acesso de acordo com o seu setor de trabalho. Sendo assim, a política de acesso de A+ é controlada por meio de segmentação das VLANs e das permissões dos usuários, utilizando senhas. A figura 3.3 demonstra de uma forma simplificada os diferentes níveis de acesso da empresa.

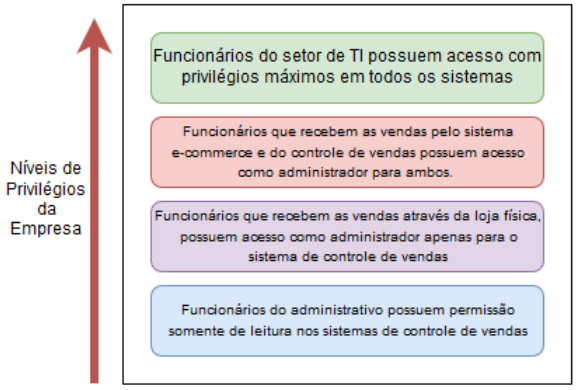

Figura 3.3: Níveis de Privilégios controlados pela equipe de TI da empresa A+. Fonte: autores

Ultimamente os funcionários, principalmente os que administram a parte de rede e de desenvolvimento, notaram que, às vezes, a conexão com a internet cai (ou fica muito lenta) e o *site* e sistema de vendas também ficam fora do ar em certos períodos. Além destes problemas técnicos, funcionários da área de Operação notaram, por meio de clientes e pesquisa, que algumas empresas concorrentes estão desenvolvendo produtos muito parecidos com os seus.

Por conta destas questões, a empresa desconfia que informações a respeito da estrutura interna da empresa, do produto e até mesmo de seus clientes estejam sendo vazadas. Diante dessa situação, foram contratados um Engenheiro de Redes de Comunicação e um Gestor de Riscos. Ambos têm a missão de implementar o Processo de Avaliação de Riscos dos ativos de rede na organização, realizando as atividade de Identificação, Análise e Avalição dos riscos.

A cultura da empresa é de usar *softwares* livres (*open source*). Obedecendo esse requisito, os profissionais contratados para realização do Processo já possuem uma das possíveis soluções *open source* em mente: o *Moodle*.

Metas. A principal meta é identificar, analisar e avaliar os possíveis riscos existentes que podem acarretar em pausa ou até no encerramento da prestação de serviço. A meta secundária é seguir a cultura da empresa, utilizando *softwares* livres.

Alcançada a primeira meta, deve-se ter em mãos documentos obtidos nas saídas de todas as atividades, organizados e de fácil entendimento, de forma que auxilie todas as partes interessadas.

Alvos da avaliação. A Avaliação abordará problemas de segurança oriundos de vulnerabilidades e más práticas que utilizam ou são direcionados aos ativos de rede da organização: *switches*, roteador, servidores e *firewall*.

Escalas dos Riscos. Definidos os alvos da avaliação, começamos agora a definir os níveis dos riscos. Para isso, serão escolhidas as escalas apropriadas para o contexto estabelecido. Diferentemente da fórmula tradicional de classificação de riscos que os definem como o produto da probabilidade e consequência, a consequência neste contexto será substituída por impacto. As abordagens de classificação de probabilidades e impacto foram baseadas em [18].

Escalas de Probabilidade. A probabilidade (P) é definida como a soma das médias dos Fatores

de Ameaça (FA) e dos Fatores de Vulnerabilidade (FV), ou seja:

$$\mathrm{P} = \overline{FA} + \overline{FV}$$

Para cada fator, é atribuído um número inteiro de 0 a 9, onde, quanto mais alto o número, mais prejudicial é o fator.

Fatores de Ameaça. Estimação do nível das ameaças que possam se materializar por meio de suas fontes. Esta é dada por uma média de quatro fatores: nível técnico, motivo, oportunidade e amplitude. A seguir, os números entre parênteses são os possíveis valores para cada caso.

Nível técnico – Nível técnico exigido das fontes de ameaça para realização do ataque. Técnicas de penetração em segurança da informação (9), técnicas de programação e configurações de rede (6), usuário com boa experiência em computação (5), pouco conhecimento técnico (3), nenhum conhecimento técnico (1).

Motivo – Motivação das fontes de ameaça na realização do ataque. Grande recompensa (9), possível recompensa (4), nenhuma ou pouca recompensa (1).

Oportunidade – Recursos ou oportunidades que são requeridos para exploração de vulnerabilidades. Não é necessário recursos ou acesso (9), algum nível de recurso ou acesso (7), acesso ou recursos especiais (4), total acesso ou recursos caros (0).

Amplitude - Quão amplas são as fontes de ameaça. Usuários anônimos da Internet (9), usuários autenticados (6), parceiros (5), usuários da Intranet (4), administradores do sistema (2), desenvolvedores (2).

Fatores de vulnerabilidade . Estimação do nível das vulnerabilidades que possam ser exploradas pelas ameaças. Esta estimação é dada por uma média de quatro fatores: facilidade de descoberta, facilidade de exploração, ciência e detecção de intrusão. A seguir, os números entre parênteses são os possíveis valores para cada caso. Novamente, quanto mais alto o número, mais prejudicial é o fator.

Facilidade de descoberta – Quão fácil é o descobrimento das vulnerabilidades para as fontes de ameaça. Ferramentas automáticas disponíveis (9), fácil (7), difícil (3), praticamente impossível (1).

Facilidade de exploração – Quão fácil é a extorsão das vulnerabilidades pelas fontes de ameaça. Ferramentas automáticas (9), fácil (7), difícil (3), teórico (1).

Ciência – Quão profundo é o conhecimento das vulnerabilidades para as fontes de ameaça. Conhecimento público (9), óbvio (6), escondido (4), desconhecido (1).

Detecção de Intrusão – Quão provável é uma invasão de ser detectada e registrada. Não logado (9), logado sem monitoramento (8), logado e monitorado (3), detecção automática em uma aplicação (1).

Escala de Impacto dos Incidentes. Classificação do impacto que os incidentes causam aos ativos. O critério utilizado foi, simplesmente, para cada dano a um dos três pilares da segurança (integridade, confidencialidade e disponibilidade) é atribuido o valor 3. A escala de impacto será

a soma dos valores.

3.1.2 *Delimitações*

As delimitações do Estabelecimento do Contexto também são válidas para as outras atividades do Processo de Avaliação de Riscos.

Escopo. Serão feitas as atividades do Processo de Avaliação de Riscos no contexto definido. Lembramos que existem vários outros tipos de riscos, porém, o foco está nos relacionados à segurança dos ativos de rede.

Foco. O foco será limitado aos ativos de rede (roteadores , *switches*, servidores e *firewalls*) e também aos pilares da segurança afetados pelos riscos. O contexto e as outras atividades serão concentradas apenas nos riscos relacionados à agentes externos e internos.

Premissas. Assumiremos que a A+ é um potencial alvo de ataques tanto externos quando internos. Tanto por motivações financeiras ou pessoais.

3.1.3 *Mecanismos*

Detalhamento dos mecanismos da atividade.

Critérios de Avaliação de Riscos. A tabela 3.1, onde o x é definido tanto como a probabilidade quanto o impacto, ilustra os critérios de avaliação usados para classificá-los. No caso da probabilidade, o valor é a média da soma dos fatores de agente de ameaça com os de vulnerabilidade. Para o impacto, o valor só pode ser 3, 6 ou 9.

Tabela 3.1: Critérios de avaliação de Riscos. Fonte: [18] - modificado

Critérios de probabilidade e impacto	
$0 < x \leq 3$	BAIXO
$3 < x \leq 6$	MÉDIO
$6 < x \leq 9$	ALTO

Matriz de Riscos. Os riscos são mapeados segundo a tabela 3.2. Basta comparar os critérios de probabilidade e impacto, cruzar os valores e obter o nível do risco correspondente.

Tabela 3.2: Construção da Matriz de Riscos. Fonte: [18] - adaptado

Matriz de riscos				
IMPACTO	ALTO	MÉDIO	ALTO	CRÍTICO
	MÉDIO	BAIXO	MÉDIO	ALTO
	BAIXO	IRRELEVANTE	BAIXO	MÉDIO
		BAIXO	MÉDIO	ALTO
	PROBABILIDADE			

3.1.4 *Saída*

Será gerado um documento detalhando todos os aspectos citados nesta etapa, devendo ser divulgado a todas as partes interessadas. Este documento será utilizado pelo engenheiro e pelo gestor para auxiliar na próxima etapa, Identificação de Riscos.

3.2 Descrição das Ferramentas Computacionais

Antes de continuarmos descrevendo as atividades do Processo de Avaliação de Riscos, detalhamos as ferramentas computacionais, utilizadas nos próximos capítulos.

Moodle. O *Moodle*, (*Modular Object Dynamic Learning Environment*), é uma plataforma *open source* bastante utilizada para Gestão do Conhecimento, por meio de ambientes de aprendizado personalizados. Além de ser totalmente gratuito, é altamente escalável, customizável e de fácil manuseio. Por esses motivos, é utilizado por mais de 90 milhões de pessoas no mundo inteiro [19]. A própria Universidade de Brasília usa o *Moodle* como apoio às disciplinas, por meio da plataforma Aprender. Seu uso foi iniciado em abril de 2004. No primeiro semestre de 2015, havia cerca de 2 mil cursos/disciplinas registrados e mais de 33 mil contas de usuários cadastradas. [20]

O ambiente mais comum de instalação do *Moodle* é o sistema operacional Linux, contendo um servidor *Web* (Apache, por exemplo), operando por meio da linguagem PHP e em comunicação com um banco de dados (MySQL, por exemplo). A união desses *softwares*, sendo todos eles *open source*, é comumente chamada de LAMP [21] (Linux, Apache, MySQL e PHP). A instalação do ambiente do projeto foi feita utilizando a LAMP.

Com relação a customização, há elementos que podem ser feitos sem a necessidade de programação, como a adição de fóruns de discussão. Outras funcionalidades mais específicas podem ser implementadas por meio do desenvolvimento de novos módulos (*plugins*).

H5P. O H5P é um *plugin* que possui compatibilidade com sistemas como *Wordpress*, *Drupal* e *Moodle*. Desenvolvido pela empresa norueguesa Joubel, é completamente gratuito e *open source*, e possibilita a criação e edição de conteúdos interativos em HTML5, tais como vídeos, apresentações, jogos, *quizzes*, gráficos, dentre outros [22]. Por ser *open source*, é possível criar conteúdos próprios, isto é, desenvolver *plugins* para o *plugin*.

O H5P é de simples manuseio, o escolhemos para customizar recursos do *Moodle* com facilidade. Destacamos que o *software* principal para apoio ao Processo é o *Moodle*, o H5P é apenas para customização e melhora de algumas funcionalidades. Algumas delas serão detalhadas a seguir.

appear.in: ferramenta *online* que possibilita a realização de vídeo conferências, sem registro e de forma bastante simples [23]. O *plugin* faz a integração desta funcionalidade com o H5P, tornando fácil a realização de reuniões a distância, por exemplo.

Questionários: recurso nativo do H5P. Os questionários podem ser do tipo múltipla escolha, verdadeiro ou falso ou de preenchimento de lacunas.

Apresentação de Slides: outro recurso nativo do H5P, que permite a criação e disponiblização de apresentações de *slides*. Pode ser bem útil para apresentações de mudanças na política da empresa, por exemplo.

3.2.1 *GNS3*

O *software* escolhido para simulação dos ambientes foi o GNS3 (*Graphical Network Simulator*). É um dos *softwares* mais utilizado por estudantes de redes de todo o mundo e por empresas famosas, como Intel, IBM e Huawei [24].

A escolha do GNS3 se dá pelo fato de este permitir a instalação de máquinas virtuais nos *hosts* do cenário de simulação, de forma que se tenha um ambiente bem fiel à realidade. Além disso, é possível realizar testes de penetração em ativos de redes virtuais, como forma de simular ataques identificados no Processo de Avaliação de Riscos como possíveis ameaças.

Internet appliance: ferramenta que possibilita conectar os *hosts* virtuais à internet de maneira fácil, via protocolo DHCP.

3.2.2 *Cisco*

Fundada em 1984 pelo casal de cientistas da computação Len Bosack e Sandy Lerner, na Universidade de Stanford, a Cisco Systems hoje é uma das maiores empresas de Tecnologia da Informação do mundo, com um valor de mercado que ultrapassa 100 bilhões de dólares. [25]

A Cisco investe muito em cursos e certificações, muito respeitadas no mercado de trabalho. A *Cisco Networking Academy* é uma plataforma de ensino *online*, que faz parcerias com várias universidades do mundo e tem como objetivo capacitar profissionais da área de TI. [26] Além disso, é uma das marcas mais presentes em ambientes corporativos por isso foram escolhidos equipamentos de redes da Cisco para simulação e análise de vulnerabilidades, a serem realizadas posteriormente neste trabalho.

3.2.3 *Ferramentas de testes de penetração*

As ferramentas utilizadas para os testes de penetração são:

Yersinia. Com o mesmo nome de um gênero de bactérias, o *yersinia* é uma ferramenta bastante utilizada em ataques na camada de enlace, incluindo protocolos propietários Cisco, como o DTP [27].

Ettercap. Ferramenta usada em ataques do tipo MITM, incluindo também opções de escaneamento de redes. Suporta dissecção ativa e passiva de muitos protocolos e inclui muitos recursos para análise de rede e *host* [28].

macof. Ferramenta presente no pacote dsniff, que possui várias outras inclusas e bastante utilizadas em testes de pentração. O objetivo do macof é realizar ataques do tipo MAC *flooding* em

switches, comprometendo o acesso e funcionalidades das redes. Possui dois modos de operação: o simples, que envia pacotes MAC para todas as portas; e o direcionado, que especifica a vítima por meio de seu endereço IP. [30]

Aidcionalmente, também utilizamos o *Wireshark*, que por si só não pode ser considerada uma ferramenta de teste de penetração. É um *software open source* do tipo *sniffer* (analista de pacotes). Nesta categoria, é considerado padrão entre empresas, agências governamentais e instituições educacionais [29]. Foi criado originalmente por Gerald Combs em 1998 e desde então vem sendo melhorado por centenas de colaboradores ao redor mundo.

Agora, daremos continuidade as atividades que compõem o Processo de Avaliação de Riscos.

Capítulo 4

Processo de Avaliação de Riscos

Neste capítulo, abordamos as atividades que compõem o Processo de Avaliação de Riscos para os ativos de rede pertencentes ao contexto estabelecido no capítulo 3. As atividades são Identificação, Análise e Avaliação dos Riscos (figura 4.1), uma fração do processo da Gestão de Riscos. Assim como no estabelecimento do contexto (seção 3.1). Novamente, será utilizado o modelo especificado na seção 2.1.2 para cada atividade do processo.

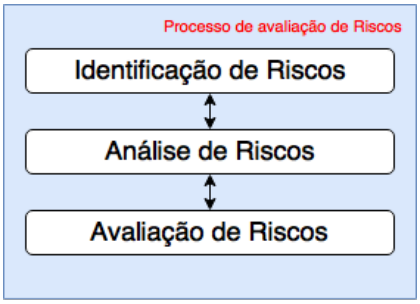

Figura 4.1: Atividades do Processo de Avaliação de Riscos. Fonte: [4] - adaptado

Visão Geral do Processo. Resumidamente, serão considerados vários componentes para que um documento final à respeito da situação da empresa seja gerado. A figura 4.2 demonstra a ligação de cada atividade executada em todo o Processo de Avaliação de Riscos.

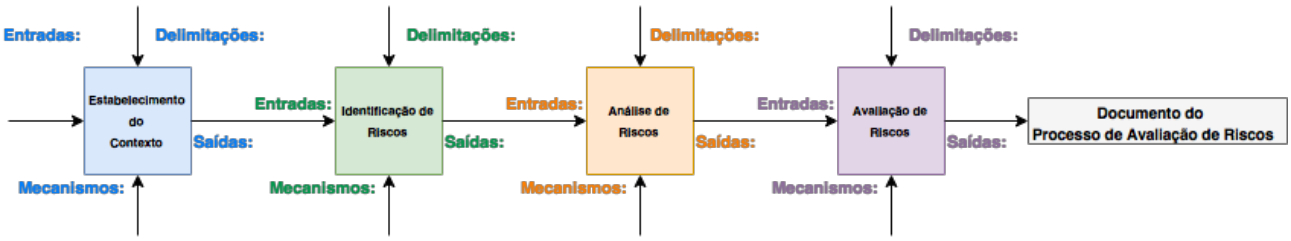

Figura 4.2: Visão geral das atividades. Fonte: autores

4.1 Identificação de Riscos

Com o documento do contexto disponível, iniciamos a atividade de identificação dos riscos da empresa A+. As entradas desta atividade são: as ameaças e suas fontes, vulnerabilidades e incidentes relacionados aos ativos de rede da organização. Os mecanismos incluem ferramentas do *Moodle* e do H5P, além de arquivos de *log* dos ativos e tabelas para sistematização dos dados. O documento de saída deve reunir todas as informações.

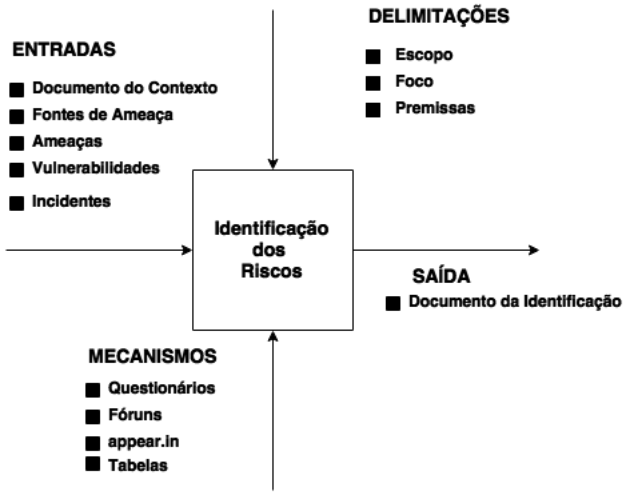

Figura 4.3: Atividade de Identificação de Riscos de A+. Fonte: [6] - modificado

4.1.1 *Entradas*

Detalhamento das entradas da atividade.

Documento do Contexto. Documento do contexto obtido na atividade anterior. Contém informações importantes a respeito do ambiente em que se está executando o Processo.

Fontes de Ameaças. Será feita uma simplificação das fontes de ameaças. Portanto, as fontes de ameaça aqui discutidas serão divididas em internas (como funcionários e parceiros com más intenções) e externas, que não possuem nenhum tipo de acesso físico ao local da empresa. Citamos como premissa que as fontes de ameaça foram pré estabelecidas baseados nos estudos em [7]. **Ameaças**. As ameaças da atividade são as abordadas na seção 2.7.3. Serão maiores detalhadas com uso das tabelas, mecanismos dessa atividade.

Vulnerabilidades. Através das ameaças, é necessário identificar as vulnerabilidades que elas podem explorar para configurar um risco, figura 2.2. Ao contrário das ameaças e suas fontes, as vulnerabilidades serão identificadas por meio do *Moodle* utilizando questionários e fóruns. Para cada vulnerabilidade identificada, foi associada a(s) pergunta(s) do questionário que conduziu a essas identificações. Maiores detalhes na seção 4.1.3.

Incidentes. Listadas as vulnerabilidades, agora será possível identificar quais são os possíveis efeitos que essas ameaças irão causar nos ativos de rede. Esses incidentes podem, de fato, pre-

judicar os equipamentos e os serviços entregues pelos mesmos. É uma entrada dependente das vulnerabilidades.

4.1.2 *Delimitações*

As delimitações da Identificação são as mesmas do Estabelecimento do Contexto, como dito anteriormente. Porém, nessa atividade, o foco também será na identificação de vulnerabilidades e incidentes. Lembrando que, como premissa, além daquela já citada no contexto, tomamos como premissa as entradas fontes de ameaça e ameaças.

4.1.3 *Mecanismos*

Detalhamento dos mecanismos da atividade.

Os mecanismos a seguir foram utilizados por meio da plataforma do Moodle. A figura 4.4 mostra uma *srceenshot* do Moodle, destacando a atividade Identificação de Riscos.

Figura 4.4: *Screenshot* do Moodle. Fonte: autores

Questionários (H5P). Direcionados a funcionários do setor de TI, os questionários apresentam perguntas sucintas e que só assumem duas respostas: sim ou não. As respostas são de grande utilidade, pois podem revelar vulnerabilidades técnicas nos ativos. Por exemplo, descobrir se existem configurações incorretas em um deles pode acarretar na identificação de uma vulnerabilidade antes desconhecida. A figura 4.5 mostra um exemplo de uma pergunta no *Moodle*, feita usando o H5P.

Nesta figura, a resposta selecionada (sim), não identifica uma possível vulnerabilidade, e por isso foi considerada a resposta correta.

Figura 4.5: Pergunta do questionário no Moodle. Fonte: autores

Já a figura 4.6 mostra um exemplo de resposta que identifica uma possível vulnerabilidade, a resposta dada (não) é considerada incorreta.

Figura 4.6: Pergunta do questionário no Moodle. Fonte: autores

O questionário foi elaborado com base em [32] e por meio dos conteúdos de [9, 12]. Foi feito de forma que cada resposta à uma pergunta conduza de forma a identificar as vulnerabilidades associadas. A tabela 4.1 mostra todas as perguntas juntamente com a resposta que pode detectar uma vulnerabilidade.

Tabela 4.1: Questionários gerados para obter respostas rápidas dos funcionários de TI

Perguntas - Funcionários Técnicos		Resposta que identifica vulnerabilidade
1	Há um processo em andamento que assegura que os ativos de rede e aplicações estão sempre atualizados?	Não
2	Há um processo de verificação dos *logs* gerados pelos ativos?	Não
3	As senhas que protegem os ativos de rede são criptografadas?	Não
4	As senhas de acesso aos ativos de redes são mudadas periodicamente?	Não
5	Há interrupção do *website* e/ou sistema interno sem motivo aparente?	Sim
6	Há uma política de segurança das portas dos *switches* e roteador?	Não
7	A VLAN 1 (padrão) está sendo utilizada em algum *switch*?	Sim
8	Nos switches, está sendo utilizado o protocolo DTP?	Sim
9	O DHCP *snooping* está implementado no roteador?	Não
10	O protocolo de segurança SSL está instalado no servidor?	Não
11	As entradas de dados pelos usuários no sistema passaram por um processo de validação e/ou *encoding* no código?	Não
12	O firewall é configurado com uma política de *white list*?	Não
13	Apenas usuários autorizados possuem acesso ao mapa da topologia da rede?	Não

Exemplificando: na pergunta 8, se a resposta for positiva, a conclusão imediata é que os *switches* de A+ estão sujeitos a sofrer um ataque do tipo VLAN *Hopping*.

Fóruns. Os fóruns envolvem discussões mais amplas e serão também utilizados para identificar vulnerabilidades, porém de uma forma mais detalhada, direcionados a todos os funcionários da empresa. Este tipo de mecanismo permite que os participantes expliquem quando e como aconteceu situação que eles, por exemplo, consideraram estranha. Além de vulnerabilidades mais técnicas, destacamos a possibilidade de discussões relacionadas a ataques de Engenharia Social (seção 2.7.3).

A figura 4.7 mostra um fórum criado para discussões de possíveis emails suspeitos.

Figura 4.7: Fórum para discussão de e-mails suspeitos. Fonte: autores

A tabela 4.2 mostra todos os fóruns criados para detecção de vulnerabilidades.

Tabela 4.2: Fóruns gerados para discussão dos Funcionários

	Fóruns
1	Houve momentos em que os sistemas cairam sem motivo aparente? Mesmo com o acesso à internet funcionando normalmente? Quando aconteceu?
2	Você recebeu algum e-mail suspeito pedindo para acessar outros sites, instalar alguns programas ou passar informações pessoais? Se sim, como eram esses e-mails?
3	Você já viu pessoas não autorizadas acessando a sala dos equipamentos, ou até mesmo manuseando-os? Se sim, quando aconteceu?
4	Houve reclamações de clientes à respeito de divulgação de dados pessoais? Como foram essas reclamações?

Appear.in (H5P). Utilizado para sessões de *brainstorming* e reuniões à distância. Assim como os fóruns, promove discussões detalhadas entre os funcionários com a vantagem de ser ao vivo e mais pessoal.

Arquivos de log dos equipamentos. Os arquivos de *log* dos ativos atuam como um registro de toda ação que neles ocorre, usado principalmente nos servidores. Uma vez que acontece um incidente, seja um desligamento inesperado, ou alterações em bancos de dados, haverá nesses arquivos informações importantes a respeito desses momentos. Por serem informações à respeito de tudo, como rede, acesso, aplicações e outros, a verificação dos *logs* se torna uma ferramenta poderosa para identificar diretamente do ativo os potenciais riscos ali presentes, determinando uma sequência de eventos em caso de incidentes e se as medidas de segurança tomadas estão surtindo efeito.

Analisando os arquivos de *log*, junto com as informações obtidas pelos fóruns e questionários do *Moodle* através dos funcionários, é possível rastrear o tempo no qual pode ter acontecido um incidente. Sendo assim, com o tempo e características detalhadas pela análise dos arquivos de *log*, é possível compreender o que aconteceu juntamente com o que pode acontecer com os equipamentos.

Tabelas dos elementos de Risco. As tabelas apresentam os conceitos de fontes de ameaça, ameaças, vulnerabilidades e incidentes de forma resumida e sistemática. Além de descrições de cada um, também ilustram outras informações pertinentes obtidas por os outros mecanismos, como perguntas e fóruns relacionados.

Fontes de Ameaças. Tabela 4.3 mostra as fontes de ameaça previamente consideradas, organizada de maneira que facilite a visualização e manipulação das informações. Lembrando que esses dois tipos de ameaça foram definidos na seção 3.1 como premissa para execução do Processo.

Tabela 4.3: Fontes de Ameaça

Fonte de ameaça	Descrição
Interna	Funcionário com más intenções ou agente externo infiltrado, que pode roubar, destruir ou alterar dados confidenciais por meio da rede interna.
Externa	Agentes externos que tentam usar a Internet como porta de entrada para a rede interna da empresa, com o objetivo de roubar dados sigilosos, interromper os serviços ou destruir informações

Ameaças: a tabela 4.4 ilustra a relação entre as ameaças e suas fontes, juntamente com os ativos de rede alvo. Assim como as fontes de ameaça, as ameaças também são uma premissa pré estabelecida em 3.1. Não inserimos a Engenharia Social, pois sua análise é muito subjetiva e não se encaixa nos critérios técnicos a serem realizados na Análise de riscos, próxima atividade.

Tabela 4.4: Ameaças

Fonte(s) de Ameaça	Número da ameaça	Ameaça	Ponto(s) de ataque
Externa	1	DDoS	*Firewall*
Externa, interna	2	XSS no site corporativo	Servidor
Externa, Interna	3	SQL *injection* no banco de dados	Servidor
Interna	4	MAC *flooding*	*Switch*
Interna	5	VLAN *hopping*	*Switch*
Interna	6	DHCP *scope exhaustion*	Roteador
Interna	7	DHCP *rogue server*	Roteador
Interna	8	ARP *poisoning*	*Switch*, servidor
Interna	9	Escalonamento de privilégios	Roteador, *switch*, servidor, *firewall*

Vulnerabilidades. Organizadas em forma de tabela (tabela 4.5), para cada ameaça e vulnerabilidade identificadas, foram associadas perguntas do questionário e fóruns que conduziram às identificações.

Tabela 4.5: Relação entre ameaças e vulnerabilidades identificadas pelo Moodle

Ameaça	Vulnerabilidade(s)	Pergunta(s) relacionada(s)	Fóruns relacionado(s)
DDoS	Configurações técnicas ineficientes no *firewall*; verificação de *logs* ineficiente e/ou inexistente	1, 2, 5 e 12	1, 3
XSS no site corporativo	Falta de *encoding* e/ou validação no código	11	3, 4
SQL *injection* no banco de dados	Falta de *encoding* e/ou validação no código	11	3, 4
MAC *flooding*	Configurações técnicas ineficientes no *switch*; ausência ou ineficiência da política de controle de portas	5 e 6	3
VLAN *hopping*	Uso de DTP no *trunk link*	7 e 8	3, 4
DHCP *scope exhaustion*	Configurações técnicas ineficientes no roteador; ausência ou ineficiência da política de controle de portas; ausência de DHCP *snooping*	6 e 9	3
DHCP *rogue server*	Idem acima	6 e 9	3, 4
ARP *poisoning*	Ausência do protocolo SSL no servidor	10	3
Escalonamento de privilégios	Políticas de acesso ineficientes; senhas de acesso inseguras; disponibilidade de informações da topologia a usuários não autorizados	2, 3, 4 e 13	2 e 3

Incidentes. Relação entre ameaças e possíveis incidentes que podem ser causados pelas mesmas, mostrados na tabela 4.6.

Tabela 4.6: Incidentes

Ameaça	Incidente
DDoS	Indisponibilidade do *website* e/ou sistema interno
XSS no site corporativo	Injeção de *scripts* maliciosos no servidor
SQL *injection* no banco de dados	Injeção de comandos SQL no servidor
MAC *flooding*	*Switch* não funciona, rede interna ou VLAN para
VLAN *hopping*	Invasão de VLANs por usuários não autorizados
DHCP *scope exhaustion*	Esgotamento de endereços IP na rede interna
DHCP *rogue server*	Redirecionamento para sites maliciosos
ARP *poisoning*	Roubo de dados confidenciais da rede interna
Escalonamento de privilégios	Acesso à um ativo ou sistema por usuário não autorizado

4.1.4 *Saída*

A saída desta atividade será um documento onde todas as tabelas feitas e as ocorrências identificadas nos arquivos de *log* são organizados de forma que facilite a próxima atividade, Análise de Riscos).

4.2 Análise de Riscos

Identificados os Riscos aos quais ativos de rede da A+ estão expostos, esta atividade tem como entrada a probabilidade de ocorrência dos riscos e seus impactos, além do documento da atividade anterior. Os mecanismos incluem testes de penetração com o GNS3 e tabelas contendo a estimação dos fatores de ameaças, vulnerabilidade e impacto. Assim como em todas as atividades, a saída traz um documento com todas estas informações.

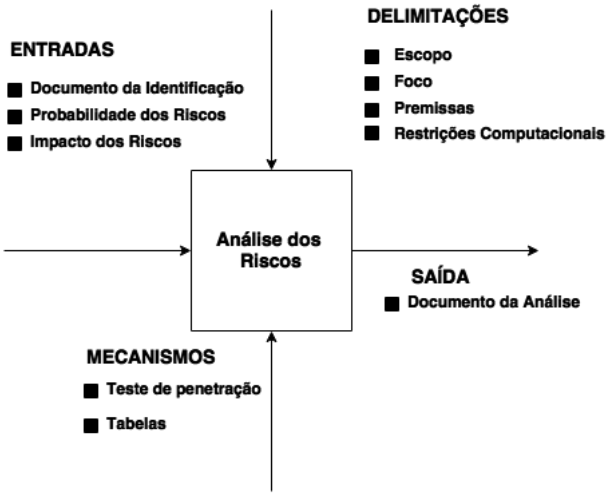

Figura 4.8: Atividade Análise dos Riscos de A+. Fonte: [6] - modificado

4.2.1 *Entradas*

Detalhamento das entradas da atividade.

Documento da Identificação. O documento gerado na saída da Identificação de Riscos contém todas as informações, organizadas em tabelas, documentando as fontes de ameaças, ameaças, vulnerabilidade e incidentes.

Probabilidade dos Riscos. Seguindo as escalas explicitadas na seção 3.1, é necessário encontrar a média dos fatores de ameaça e fatores de vulnerabilidades, obtendo a probabilidade dos riscos.

Impacto Técnico dos Riscos. Assim como a probabilidade, o impacto técnico (seção 3.1) será quantificado utilizando as escalas da seção 3.1.

4.2.2 *Delimitações*

Além daquelas herdadas do Estabelecimento do Contexto, há a delimitação em relação a ferramentas computacionais. Ressaltamos as dificuldades encontradas nesta atividade, principalmente na atribuição de escalas de probabilidade e impacto. Para uma quantificação mais realista, diversos outros aspectos teriam de ser considerados, como linguagens de programação, possbilidade de utilização de ativos de rede reais (e não virtuais) além de uma empresa real.

Restrições computacionais. Devido à limitações computacionais, tornou-se impraticável simular a topologia completa da empresa, figura 3.2. Por esse motivo, simulamos topologias mais simples, porém que também se aplicam ao contexto da A+. Também focamos nas ameaças internas, dado que é impraticável simular ameaças externas.

4.2.3 *Mecanismos*

Detalhamento dos mecanismos da atividade.

Testes de penetração com GNS3. Identificados os riscos, observamos que seria interessante simular alguns ataques para analisar as vulnerabilidades e incidentes que podem ocorrer. Aqui, três ataques detalhados no capítulo 2 e identificados na seção 4.1 serão simulados no GNS3, de forma que seus efeitos possam ser vistos na prática.

MAC flooding

Identificado pelas perguntas 5 e 6, e fórum 3, o principal objetivo do MAC *flooding* é inundar a tabela de endereços MAC de um *switch*.

Topologia de teste: Dois *hosts* conectados a um *switch* e a internet por meio do *internet appliance*.

Contexto organizacional: Se os *switches* não possuirem configurações de segurança ou políticas de controle de portas, qualquer hospedeiro conectado diretamente a um deles pode realizar o ataque. Portanto, os *switches* 1, 2 e 3 da figura 3.2 estariam suscetíveis ao ataque.

Ativo(s) atingido(s): *switch*

Ferramenta utilizada: *Macof*

Procedimento: basta digitar o comando *sudo macof -i enp0s3*, onde enp0s3 é o nome do adaptador de rede, nesse caso da máquina virtual simulada.

Descrição: durante o ataque, a comunicação fica bastante prejudicada, apresentando *pings* com *delay* altíssimo e impossibilidade de acessar algum *site*, pois o *switch* trava totalmente. Quando o ataque para, é possível acessar o *switch* novamente. O comando *show mac address table count*, executado no *switch*, mostra uma grande quantidade de endereços MAC na tabela, evidenciando o inundamento (*flooding*) de endereços.

Análise técnica: ataque bastante simples de ser realizado, não exigindo muito conhecimento técnico. Basta um comando para o *switch* parar. Porém, não traz prejuízos mais sérios como vazamento de dados.

Topologia e efeitos explicitados na figura 4.9.

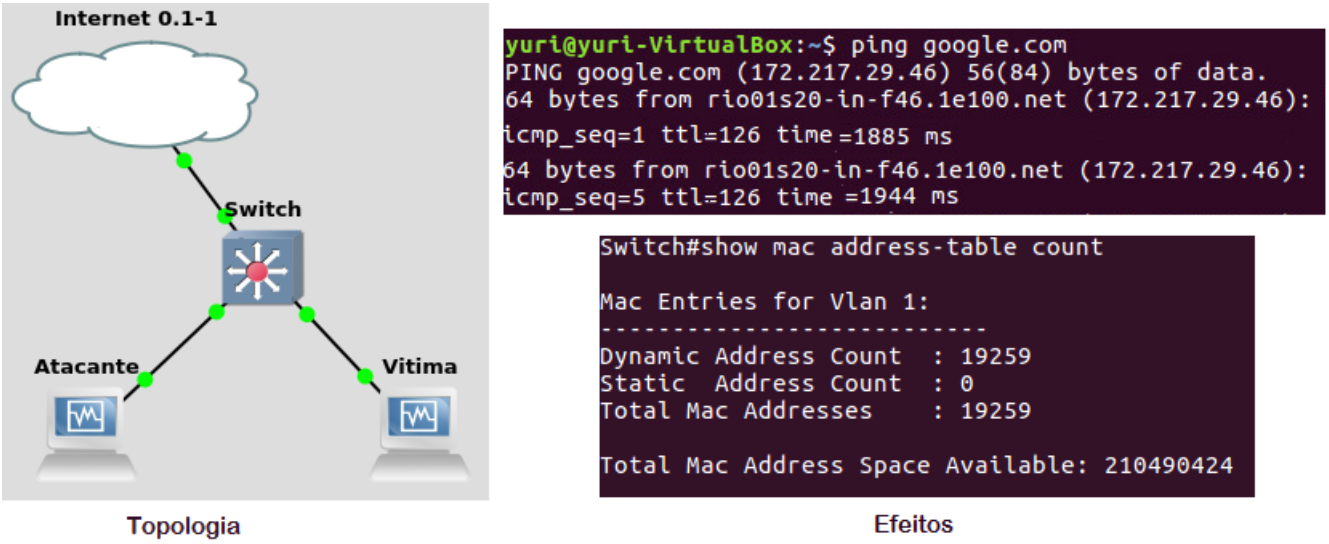

Figura 4.9: Simulação do MAC Flooding. Fonte: autores

DHCP Scope Exhaustion

O ataque DHCP *Scope exhaustion* foi identificado por meio das perguntas 6 e 9 do questionário, e fóruns 3 e 4. Este ataque é usado para esgotar o números de endereços IP do servidor DHCP.

Topologia de teste: hospedeiro atacante conectado ao *switch*, que por sua vez está conectado ao roteador.

Contexto organizacional: o roteador da empresa está configurado como um servidor DHCP, podendo estar vulnerável se não houver uma politica de controle de portas ou uso de DHCP *snooping*.

Ativo(s) atingido(s): roteador

Ferramenta utilizada: *Yersinia*

Procedimento: primeiramente, configurou-se o roteador, com endereço IP 192.168.1.254 como servidor DHCP por meio dos comandos *ip dhcp pool teste*, *default-router 192.168.1.254* e *network 192.168.1.1 255.255.255.0*. Dessa forma o atacante obteve o endereço IP automaticamente. No *yersinia*, foi selecionada a opção de mandar vários pacotes DHCP do tipo *DISCOVER*, um pacote *broadcast* com o objetivo de encontrar o servidor.

Descrição: depois de alguns minutos, todos os endereços IP disponíveis do servidor já tinham sido atribuidos ao atacante. Isso ocorre porque a resposta do servidor ao pacote *DISCOVER* é mandar um do tipo *OFFER*, com os endereços solicitados. O *Yersinia* manda diversos pacotes *DISCOVER* para esgotar a quantidade de endereços disponíveis. Como teste, foi adicionado um *host* do próprio GNS3, que não conseguiu obter um endereço IP, como esperado.

Análise técnica: apesar de ser um pouco mais difícil de realizar do que o MAC *flooding*, exigindo maior conhecimento técnico (uso do yersinia), o DHCP *scope exhaustion* também não traz vazamento de dados.

Topologia, realização e consequência explicitados na figura 4.9.

Figura 4.10: Simulação do DHCP scope exhaustion. Fonte: autores

ARP poisoning

Identificado por meio da pergunta 10 e do fórum 3, o ARP *poisoning* compromete a confidencialidade dos pacotes trocados na rede, sendo capaz de obter credenciais, por exemplo. Utilizaremos o próprio ambiente *web* do *Moodle* como exemplo, que por padrão não possui o protocolo SSL instalado.

Topologia de teste: dois hospedeiros e um servidor com o *Moodle* instalado, conectados no mesmo *switch* e na mesma rede local

Contexto organizacional: passível de ocorrência onde um usuário e atacante estejam na mesma VLAN que o servidor. No caso da A+, usuários da VLAN do setor de TI.

Ativo(s) atingido(s): *switch* e servidor

Ferramentas utilizadas: *ettercap*, *Wireshark*

Procedimento: atacante usa o *ettercap* em modo gráfico (*ettercap* -G) e seleciona *unified sniffing*. Em seguida, realiza um escaneamento, encontrando na rede local os endereços MAC e IP dos dois alvos: servidor e o hospedeiro da vítima. O atacante então seleciona os dois (*target 1 e 2*) e elege a opção *ARP poisoning*, no menu MITM *attack*.

Descrição: depois que o ataque for realizado, é possível obter um detalhamento dos pacotes trocados entre as vítimas por meio do *Wireshark*. De fato, os *frames* do protocolo ARP originarios do servidor e do hospedeiro da vítima são anunciados para o atacante, o qual está no meio da comunicação, confirmando o sucesso do ataque tipo *man-in-the-middle*. Um usuário sem o devido conhecimento técnico dificilmente suspeitará de alguma coisa estranha na comunicação. Se a vítima fizer o *login* no servidor com o *Moodle* e o mesmo não possuir o protocolo de segurança SSL instalado, o atacante poderá ter acesso ao *login* e senha sem nenhum tipo de criptografia. O mesmo poderia ser obtido até mesmo se a vítima tivesse acesso a internet, e realizasse *login* em sites que não implementam o protocolo SSL.

Análise técnica: vimos agora um exemplo de simulação que necessitou de muito mais conhecimento técnico do que os anteriores. O ARP *poisoning* necessita de entendimento dos protocolos de rede

para obtenção de dados pessoais em sistemas vulneráveis, por isso apesar de ser mais difícil de ser realizado, traz maiores recompensas para o atacante.

Topologia e consequência explicitados na figura 4.11.

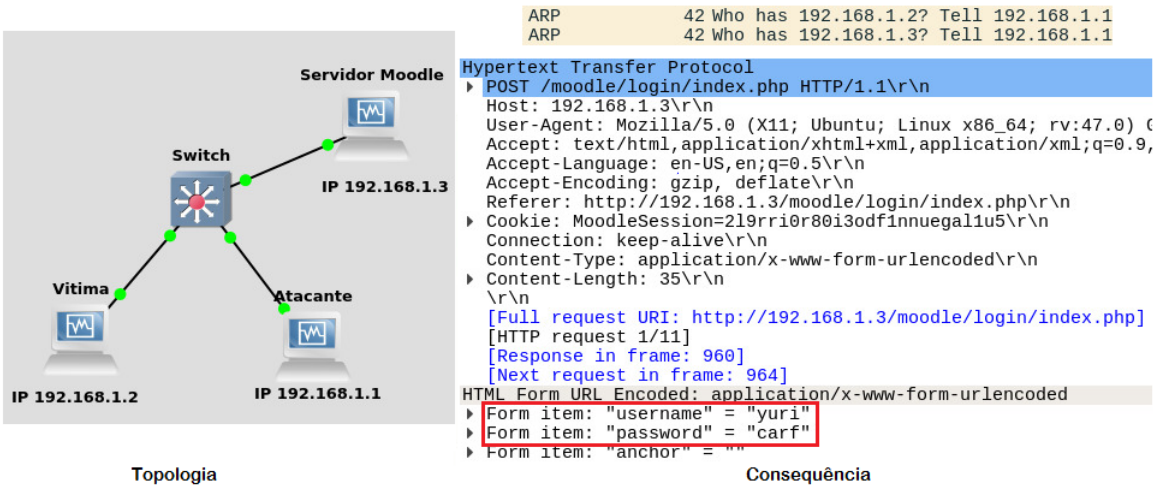

Figura 4.11: Simulação do ARP poisoning. Fonte: autores

Tabelas das Análises de Riscos: elaboração de tabelas explicitando as escalas de probabilidade e impacto dos incidentes avaliados. Para isso, dividimos em fatores de ameaça, vulnerabilidade e impacto dos incidentes.

Fatores de Ameaças. Cada ameaça listada na tabela 4.7 será quantificada com os critérios expostos na seção 3.1. Para cada ameaça foi associado um valor para nível técnico, motivo, oportunidade e amplitude de acordo com as suas próprias características. As ameaças que possuem fontes externas e internas (XSS e SQL *injection*) possuem dois números, um para cada fonte. A média portanto foi calculada com 8 valores e não 4.

Tabela 4.7: Análise e estimação das ameaças

	Fatores de ameaça				Média
Ameaça	Nível Técnico	Motivo	Oportunidade	Amplitude	
DDoS	6	4	7	9	6,5
XSS no site corporativo	6, 6	9, 9	9, 7	9 , 4	7,375
SQL *injection* no site corporativo	6, 6	9, 9	9, 7	9 , 4	7,375
MAC *flooding*	3	1	4	4	3
VLAN *hopping*	6	4	4	2	4
DHCP *scope exhaustion*	3	1	7	4	3,75
DHCP *rogue server*	6	9	4	2	5,25
ARP *poisoning*	5	9	7	4	6,25
Escalonamento de privilégios	não se aplica	9	7	4	6,66

Legenda: números em vermelho - fonte de ameaça interna
números em roxo - fonte de ameaça externa

Fatores de Vulnerabilidades: cada vulnerabilidade também foi quantificada com os critérios da

seção 3.1: facilidade de descoberta, exploração, ciência e detecção de intrusão. As vulnerabilidaes presentes na tabela 4.8 foram simplificadas e associadas aos números de cada ameaça que pode se aproveitar daquela vulnerabilidade. Novamente, as ameaças que têm fontes externas e internas possuem dois números, um para cada fonte. Observação: a vulnerabilidade "configurações ineficientes nos ativos"diz respeito aos outros diversos aspectos técnicos dos ativos não detalhados no segundo capítulo. Tais configurações podem ser relacionadas a protocolos e falta de atualização, por exemplo.

Tabela 4.8: Análise e estimação das vulnerabilidades identificadas

Fatores de vulnerabilidade						Média
Ameaças associadas	**Vulnerabilidade**	**Facilidade de descoberta**	**Facilidade de exploração**	**Ciência**	**Detecção de Intrusão**	
1, 4, 5, 6, 7, 8	Configurações técnicas ineficientes nos ativos	7, 3	7, 7	6, 1	8, 8	**5.875**
Todas	Verificação de logs ineficiente e/ou inexistente	7, 3	7, 7	6, 1	8, 8	**5.875**
2, 3	Falta de *encoding* e/ou validação no código	3, 3	3, 3	4, 4	9, 3	**4**
4, 5, 6, 7	Ausência ou ineficiência da política de controle de portas (switch e roteador)	7	7	6	9	**7.25**
5	Uso de DTP no trunk link	3	3	4	8	**4.5**
6, 7	Ausência de DHCP snooping	7	7	4	8	**6.5**
9	Senhas de acesso sem criptografia	3	7	4	9	**5.75**
5, 9	Disponibilidade de informações da topologia a usuários não autorizados	7	7	6	9	**7.25**
2, 3, 4, 5, 6, 7, 9	Configurações de acesso aos ativos ineficientes	7	7	6	9	**7.25**
8	Ausência do protocolo SSL no servidor	3	3	4	9	**4.75**

Legenda: números em vermelho - fonte de ameaça interna
números em roxo - fonte de ameaça externa

Sendo assim, com o valor da média de cada vulnerabilidade, foi calculada a média para cada ameaça. Por exemplo, para a ameaça 1 (DDoS), ela se aproveita de duas vulnerabilidades com valores 5.875 cada uma. Então, a média dessas duas vulnerabilidades será 5.875.

Impacto dos Incidentes: o impacto dos incidentes foi classificado de acordo com a quantidade de pilares da segurança que ele atinge (seção 2.2). Cada X na tabela equivale ao valor 9, assim, o fator de impacto é média de quantos X possui marcado para os 3 pilares.

Tabela 4.9: Análise e estimação dos Impactos identificados

Fatores de impacto					Fator de Impacto
Ameaça	**Incidente**	**Dano a integridade**	**Dano a confidencialidade**	**Dano a disponibilidade**	
DDoS	Indisponibilidade do *website* e/ou sistema interno	X		X	6
XSS no site corporativo	Injeção de scripts maliciosos no servidor		X	X	6
SQL injection no banco de dados do site corporativo	Injeção de comandos SQL no servidor	X	X	X	9
MAC flooding	Switch não funciona, rede interna ou VLAN para			X	3
VLAN hopping	Invasão de VLANs por usuários não autorizados	X	X		6
DHCP scope exhaustion	Esgotamento de endereços IP na rede interna			X	3
DHCP rogue server	Redirecionamento para sites maliciosos	X	X		6
ARP poisoning	Roubo de dados confidenciais da rede interna		X		3
Escalonamento de privilégios	Acesso à um ativo ou sistema por usuário não autorizado	X	X	X	9

Tabela Geral dos Riscos: com todos os valores obtidos, elaboramos uma tabela (tabela 4.10) com os riscos listados, mostrando a média de probabilidade entre vulnerabilidades e ameaças, e impacto.

Tabela 4.10: Lista de Riscos com suas respectivas probabilidades e impactos

Número do risco	Incidente	Ameaça	Probabilidade de Ameaças	Probabilidade de Vulnerabilidades	Impacto	Probabilidade Final
1	Indisponibilidade do *website* e/ou sistema interno	DDoS	5.875	6,5	6	6.1875
2	Injeção de *scripts* maliciosos no servidor	XSS no site corporativo	5.70	7,375	6	6.5375
3	Injeção de comandos SQL no servidor	SQL Injection no site corporativo	5.70	7,375	9	6.5375
4	*Switch* não funciona, rede interna ou VLAN para	MAC flooding	6.56	3	3	4.78
5	Invasão de VLANs por usuários não autorizados	VLAN hopping	6.33	4	6	5.165
6	Esgotamento de endereços IP na rede interna	DHCP scope exhaustion	6.55	3,75	3	5.15
7	Redirecionamento para sites maliciosos	DHCP Rogue server	6.55	5,25	6	5.9
8	Roubo de dados confidenciais da rede interna	ARP poisoning	5.5	6,25	3	5.875
9	Acesso à um ativo ou sistema por usuário não autorizado	Escalonamento de privilégios	6.53	6,66	9	6.595

4.2.4 *Saída*

O documento de saída desta atividade traz tabelas que organizam os riscos analisados, explicitando probabilidade e impacto.

4.3 Avaliação dos Riscos

Chegamos à última atividade do Processo de Avaliação de Riscos. As entradas incluem o documento da atividade anterior, a classificação e agrupamento dos riscos. Os mecanismos utilizados são os critérios de classificação e a matriz de riscos, organizados por meio de tabelas. A saída traz o documento final.

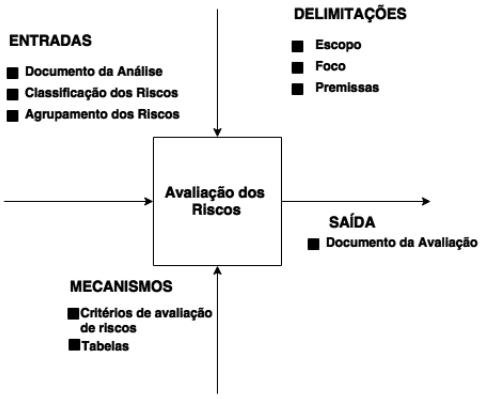

Figura 4.12: Atividade de Avaliação de Riscos de A+. Fonte: [6] - modificado

4.3.1 *Entradas*

Detalhamento das entradas da atividade.

Documento da Análise. Os documentos consolidando as informações à respeito dos riscos, como os incidentes relacionados, os ativos, a probabilidade de ocorrer aquele risco, e o impacto que o mesmo causa, irão auxiliar na elaboração da principal tabela: a matriz de riscos.

Classificação de Riscos. A classificação de riscos irá ordená-los de acordo com os valores obtidos pela média da probabilidade e do impacto. Esta classificação será feita seguindo os critérios de Avaliação de Riscos da tabela 3.1, exposta na seçao 3.1, e organizados na tabela matriz de riscos.

Agrupamento de Riscos. Os riscos semelhantes serão agrupados por meio de Análise teórica, ou seja, serão analisados de acordo com as suas características que envolvem atributos, incidentes e impactos semelhantes.

4.3.2 *Delimitações*

As delimitações desta atividade são, novamente, as mesmas do Estabelecimento do Contexto.

4.3.3 *Mecanismos*

Detalhamento dos mecanismos da atividade.

Tabela de Critérios de Avaliação. Com os valores de probabilidade e impacto, classificamos estes fatores de acordo com a tabela 3.1.

Análise Teórica. Neste mecanismo, o agrupamento de riscos será feito a partir de uma análise minuciosa a respeito de cada item que define os riscos finais. O valor da probabilidade do agrupamento permanece o mesmo dos riscos, apenas os impactos serão combinados.

Agrupamento 1. Aqui, os ataques XSS e SQL *injection* no site corporativo, foram agrupados por serem ameaças que possuem exploram vulnerabilidades parecidas, ambas envolvendo falta de validação e/ou *encoding* no código do *website*, incluindo banco de dados. Apesar do impacto do SQL *injection* ser maior, os dois causam mais danos se realizados em conjunto.

Agrupamento 2. Os ataques DHCP *Scope Exhaustion* e DHCP *Rogue Server* também foram agrupados. Além de partilharem de vulnerabilidades parecidas, envolvendo uma fraca política de segurança nas portas do roteador e ausência de DHCP *snooping*, são ameaças que exploram o mesmo protocolo. Também compartilham das mesmas fontes de ameaça e alvo (roteador).

Tabela Matriz de Riscos. Seguindo os critérios da tabela 3.2 juntamente com a tabela 4.10, construiu-se a matriz dos riscos identificados e avaliados.

Tabela 4.11: Matriz de Criticidade dos Riscos com Agrupamentos

Matriz de riscos (criticidade)				
IMPACTO	ALTO		6+7	2+3, 9, 10
	MÉDIO		5	1
	BAIXO		4, 8	
		BAIXO	MÉDIO	ALTO
	PROBABILIDADE			

Área Magenta - Riscos 9 e 10 e Agrupamento 1. Os riscos 9 e 10 são respectivamente Escalonamento de Privilégios e Engenharia social. A ameaça Engenharia Social foi incluída diretamente na matriz pois ela explora vulnerabilidades sociais, que não cabem na análise técnica realizada. Como citado na seção 2.7.3, é uma técnica de ataque utilizada para obter privilégios não autorizados sobre os ativos de rede e sistemas, explorando vulnerabilidades sociais de funcionários despreparados. Caso seja bem sucedido, será possível executar praticamente qualquer outro ataque aqui citado. Consequentemente, o risco 10 ficou no nível mais alto de criticidade bastando apenas uma reflexão de suas características. Já o risco 9, Escalonamento de Privilégios, ficou nesta posição da matriz porque também é um ataque muito prejudicial, que busca o acesso a agentes internos mal intencionados. As contas feitas na análise de riscos, resultou em um ataque com alta probabilidade de acontecer. Ambos os ataques são portas de entrada para outros, portanto eles se classificaram na mais séria posição da matriz de criticidade.

O agrupamento 1 (XSS + SQL *injection*) pode comprometer todos os pilares da segurança, alterando, apagando ou destruindo dados pessoais dos clientes, no banco de dados e no próprio *website*. Além disso, usuários externos podem realizá-los por meio da Internet, sendo bastante populares atualmente [31]. Por esses motivos, foram considerados críticos.

Área Vemelha - Risco 1 e Agrupamento 2. O risco 1, DDoS, recebeu essa posição na matriz por ter apresentado, através dos cálculos, altas chances de ser executado. Ademais, o nível de impacto obtido pelos cálculos foi médio, o que condiz com a realidade, visto que, na maioria das vezes, causa danos à disponibilidade e possivelmente a integridade dos dados, mas não compromete a confidencialidade.

O Agrupamento 2, DHCP *Scope Exhaustion* e DHCP *Rogue Server*, podem comprometer os três pilares da segurança. O agrupamento causou o aumento do impacto, classificado como alto.

Área Laranja - Risco 5. O risco 5, VLAN *Hopping*, apresenta probabilidade de execução média, pois exige que os agentes que os executem sejam internos, diminuindo a probabilidade de ataque. Também possuem impacto médio pois podem comprometer dois pilares da segurança.

Área Verde - Risco 4 e 8. Os riscos 4 e 8 são respectivamente MAC *Flooding* e ARP *Poisoning*. Assim como na área laranja, a probabilidade de execução desses ataques exige que sejam iniciados por atacantes internos da empresa, mas os impactos causados comprometem apenas um pilar da Segurança da informação e por isso são classificados como riscos de baixo impacto.

4.3.4 *Saída*

A saída desta atividade assim como de todo o Processo de Avaliação de Riscos é um documento onde se detalha todas as informações obtidas e organizadas à respeito de A+, desde o Estabelecimento do Contexto até o final do Processo de Avaliação de Riscos.

Com o entedimento de todos os itens expostos nesse documento, A+ poderá tomar decisões significativas nas políticas da empresa. Principalmente porque esse documento confirma as especulações das quais vem sofrendo, por conta das vulnerabilidades dos ativos de rede. De alguma forma, seus concorrentes estão tirando proveito disso.

4.4 Sugestões de Tratamento

Após gerar o documento final do Processo de Avaliação de Riscos, uma lista de sugestões de tratamento foi criada a respeito do que a empresa A+ poderia modificar para que seus riscos sejam amenizados ou até mesmo mitigados. Com referência à Matriz de criticidade (Tabela 4.11), as sugestões são:

Risco 1 - Ameaça DDoS. Um dos riscos mais sérios classificados neste trabalho, a sugestão é que A+ considere seguir tais instruções:

1. Comprar um novo *Firewall* em *hardware*. Apesar do *Firewall* em *software* ser uma solução, aquele em *hardware* ainda assim oferece mais recursos. Em relação ao *firewall* em *hardware*, existe uma maior garantia de segurança para a empresa;
2. Configurar o *firewall* com uma política de *whitelist*;
3. Implementar um processo de monitoramento constante nas requisições ao servidor;

Risco 2 + 3 - Agrupamento 1. Esse risco está altamente relacionado ao website do *e-commerce* e banco de dados, ou seja, pode prejudicar as vendas e reputação da empresa. As sugestões são:

1. Implantar sintaxe *escaping* no código, especificamente nas entradas dos usuários [33];
2. Uso de declarações prontas e com *ueries* parametrizadas [34];
3. Uso de *Stored Procedures* [34];

Risco 4 - Ameaça MAC *Flooding*. Apesar de não ter um impacto tão sério, esse risco indica uma fonte de ameaça interna, o que compromete a credibilidade de seus funcionários. A sugestão para esse risco é:

1. Implementar uma política de segurança de porta dos *switches* que, por exemplo, limita o número de endereços MAC por porta.

Risco 5 - Ameaça Vlan Hopping. Esse risco, se executado corretamente, pode acarretar em outros para os equipamentos de rede, ou até mesmo para os servidores. Então, é importante implementar melhorias de prevenção nesse aspecto.

1. Novamente, implementar uma política de segurança de porta nos *switches*;
2. Desabilitar o protocolo DTP nos *switches*;
3. Não utilizar a Vlan 1 como *default*.

Risco 6 + 7 - Agrupamento 2. Este agrupamento possui médio impacto, mas pode afetar um ativo de redes custoso: o roteador. Para previnir isso, as sugestões são:

1. Habilitar DHCP *Snooping*;
2. Implementar políticas de portas no roteador.

Risco 8 - Ameaça Escalonamento de Privilégios. Um dos mais sérios riscos presentes, a sugestão é instruir os funcionários da área de TI a seguir tais políticas:

1. Sempre armanezar senhas dos equipamentos e a topologia da rede de maneira segura;
2. Permitir entrada apenas de pessoas autorizadas na sala de equipamentos;
3. Nunca deixar os computadores e equipamentos sozinhos com a sessão iniciada sem que alguém esteja utilizando;
4. Mudar periodicamente as senhas, revisar todas os *logins* e senhas autorizados ao acesso dos ativos;
5. Criar uma política de análise de *logs* por meio de *scripts*; [35]
6. Monitorar os *logs* periodicamente em busca de atividades suspeitas; [35]
7. Implantação de um sistema de gerenciamento e monitoramento de Redes.

Risco 9 - Ameaça ARP Poisoning. Apesar de ser um risco de baixo impacto, ainda pode ser perigoso pois representa uma ameaça à confidencialidade. Para amenizar os efeitos desse ataque, a sugestão é:

1. Instalar o protocolo SSL no servidor com intuito de proteger os dados contra *sniffers*, apesar de não impedir o ataque em si, ele se torna inútil pois obterá dados criptografados.

Risco 10 - Ameaça Engenharia Social. Este é o risco mais grave para a empresa, pois, a partir desse ataque, é possível executar outros subsequentes. Além disso, envolvem aspectos emocionais e sociais dos seres humanos, muito mais difíceis de compreender e controlar do que o dos ativos de rede. O recomendado é:

1. Instruir os funcionários de toda a empresa através de treinamentos e palestras à respeito do que é engenharia social, esclarecer o quão sério é esta ameaça, ensiná-los a reconhecê-lo e quais medidas tomar quando ocorrer.

Foram citadas aqui algumas possíveis soluções para as vulnerabilidades da A+. Existem diversas outras soluções, envolvendo, por exemplo, a implementação de novas tecnologias, como virtualização e redes definidas por software. Fica a critério da empresa selecionar as medidas de tratamento com melhor custo-benefício. Ressaltamos que as sugestões de tratamento podem favorecer o surgimento de novas situações de risco, explorando agora outras vulnerabilidades. Por isso, o Processo de Avaliação de Riscos não deve ser realizada apenas uma única vez, e sim ser parte integrante da empresa.

Capítulo 5

Conclusões

Encerrado o Processo de Avaliação de Riscos, concluímos o projeto observando o sucesso dos objetivos específicos. Para atingir o primeiro objetivo, foi necessário obter experiência na área de Gestão de Riscos por meio de leitura e estudo de normas internacionais e livros, bem como a aplicação deste assunto aos ativos de rede. O segundo objetivo demandou aplicação dos conhecimentos adquiridos na área de gestão para se realizar o Processo de Avaliação de Riscos em uma empresa fictícia. Na atividade de Identificação, refletimo sobre como abordar problemas técnicos de redes de forma que as vulnerabilidades fossem identificadas por meios de recursos do *Moodle* (fóruns e questionários). Na atividade de Análise, foi necessário a instalação das configurações do GNS3 e ativos virtualizados que pudessem simular um ambiente vulnerável e seus efeitos. Na etapa de Avaliação, consolidamos o Processo chegando a matriz de criticidade de Riscos.Para alcançarmos o terceiro objetivo, instalamos o *Moodle* em ambiente virtualizado e estudamos seus conceitos para customizá-lo de forma que apoiasse as atividades do Processo. O uso do *plugin* H5P se mostrou eficiente para esse fim. O quarto objetivo foi alcançado através de pesquisas formas de mitigação dos riscos analisados e sugestões de como aplicá-las.

O sucesso dos objetivos específicos nos leva a concluir que o projeto alcançou seu objetivo principal, o qual era realizar o Processo de Avaliação de ativos de rede apoiado pelo *Moodle*. Mostrando assim que o *Moodle* customizado pode ser uma ferramenta útil para a Gestão de Riscos, podendo até mesmo solucionar um dos problemas que muitas empresas enfrentam, pouca disponibilidade de ferramentas de Gestão de Riscos *open source*.

Como sugestão de trabalhos futuros a quem se interessar pela continuidade do assunto, propomos a realização da Gestão de Riscos completa em um ambiente corporativo real, tendo como foco os ativos de rede e considerando outras ameaças não abordadas neste projeto. Além disso, a natureza *open source* do *Moodle* torna possível o desenvolvimento de *plugins* que automatizem e facilitem o Processo. Um desenvolvimento de tal magnitude exige muito estudo e provavelmente uma grande equipe para realizá-lo.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] PWC. **Turnaround and Transformation in Cybersecurity**. Disponível em <http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf>. Acesso em Junho de 2017.

[2] RUPPERT, Brad. **SANS Institute InfoSec Reading Room**: Protecting Against Insider Attacks. 2009. Disponível em: <https://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168>. Acesso em Junho de 2017.

[3] Batista Ribas de Moura, J. **Desenvolvimento e Implementação do Sistema de Avaliação de Riscos com Software Livre "Moodle"no Conselho Administrativo de Recursos Fiscais do Ministério da Fazenda**. Tese (Qualificação de Mestrado) — Universidade de Brasília, 2016

[4] INTERNATIONAL STANDARD FOR ORGANIZATION. **ISO/IEC 27000**: Information technology — Security techniques — Information security management systems. 2009

[5] INTERNATIONAL STANDARD FOR ORGANIZATION. **ISO/IEC 31000**: Risk Management - Principles and guidelines. 2009.

[6] CHAPMAN, Robert J. **Simple Tools and Techniques for Enterprise Risk Management**. 2 ed. Wiley, 2011

[7] REFSDAL, Atle; SOLHAUG, Bjørnar; STØLEN, Ketil. **Cyber-Risk Management**. 1 ed. Pearson, 2015

[8] INTERNATIONAL STANDARD FOR ORGANIZATION. **ISO/IEC 9001**: Quality management systems – Requirements. 2008.

[9] VYNCKE,Eric; PAGEN, Christopher. **LAN Switch Security**: What Hackers Know About Your Switches. Cisco Press 2007.

[10] LAMMLE, Todd. **CCNA Routing and Switching Study Guide**. 1 ed. Sybex, 2013

[11] ALBUQUERQUE, R. d. O. Material disciplinar: Segurança de Redes - Universidade de Brasília. 2016.

[12] CIAMPA, Mark. **CompTIA Security+ Guide to Network Security Fundamentals**. 5 ed. Cengage Learning, 2015

[13] KUROSE, James; ROSS, Keith W. **Computer Networking**: a top-down approach. 6 ed. Companion Website: Pearson, 2013.

[14] CISCO PRESS. **VLANs and Trunking**. Disponível em <http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>. Acesso em Junho de 2017.

[15]CISCO. **Cisco Networking Academy**. Disponível em <http://www.cisco.com/c/en/us/

training -events/resources/networking-academy.html>. Acesso em Junho de 2017.

[16]SEBRAE. **Lei geral das micro e pequenas empresas**. Disponível em <http://www.sebrae.com.br/sites/PortalSebrae/artigos/entenda-as-diferencas-entre-microempresa

pequena-empresae-mei,03f5438af1c92410VgnVCM100000b272010aRCRD>. Acesso em Junho de 2017.

[17]SECNET. **Estatíticas do e-commerce no Brasil em 2017**. Disponível em <https://www.secnet.com.br/blog/e-commerce-no-brasil-2016>. Acesso em Junho de 2017.

[18]OWASP. **OWASP Risk Rating Methodology**. Disponível em <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology> acesso em Junho de 2017.

[19] MOODLE. **About Moodle**. Disponível em <https://docs.moodle.org/32/en/About_Moodle>. Acesso em Junho de 2017.

[20] UNB-APRENDER. **Institucional**. Disponível em <http://aprender.unb.br/index.php/iinstitucional > acesso em Junho de 2017.

[21] TECH TARGET. **Definition–LAMP**. Disponível em <http://searchenterpriselinux.tech

target.com/definition/LAMP > acesso em Junho de 2017.

[22] H5P. **Home page**. Disponível em <https://h5p.org>. Acesso em Junho de 2017.

[23] APPEAR.IN. **Home page**. Disponível em <https://appear.in>. Acesso em Junho de 2017.

[24] GNS3. **What is GNS3?** Disponível em <https://gns3.com/software/>. Acesso em Junho de 2017.

[25] CISCO. **Cisco History Timeline**. Disponível em <http://video.cisco.com/detail/videos/thought-leadership/video/4147229068001/cisco-history-timeline>. Acesso em Junho 2017

[26]FIREEYE. **FireEye Advanced Threat Report**. Disponível em <http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf>. Acesso em Junho de 2017.

[27] YERSINIA. **Home page**. Disponível em <http://www.yersinia.net/index.htm>. Acesso em Junho de 2017.

[28] ETTERCAP. **Home page**. Disponível em <https://ettercap.github.io/ettercap/>. Acesso em Junho de 2017.

[29] WIRESHARK. **About Wireshark**. Disponível em <https://www.wireshark.org/>. Acesso em Junho de 2017.

[30] KALI LINUX TUTORIALS. **Macof**. Disponível em <http://kalilinuxtutorials.com/macof/>. Acesso em Junho de 2017.

[31] OWASP. **Top 10 2017**. Disponível em <https://www.owasp.org/index.php/Top_10_2017-Top_10>. Acesso em Junho de 2017.

[32] UNIVERSITY OF ILLINOIS. **Project reports**. Disponível em <http://citebm.business.illinois.edu/TWC\%20Class/Project_reports_Spring2006/Business\%20Risk\%20Management/Manzoor/Audit\%20Checkilist.pdf>. Acesso em Junho de 2017.

[33] OWASP. **XSS (Cross Site Scripting) Prevention Cheat Sheet**. Disponível em < https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet>. Acesso em Junho de 2017.

[34] OWASP. **SQL Injection Prevention Cheat Sheet**. Disponível em <https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>. Acesso em Junho de 2017.

[35] RNP. **Os Logs como Ferramenta de Detecção de Intrusão**. Disponível em <http://memoria.rnp.br/newsgen/9905/logs.html>. Acesso em Junho de 2017.