CENTRO UNIVERSITARIO ASSIS GURGACZ

Gustavo Henrique Esser

Analise de Malware baseados em cenários reais da mitigação a prevenção

Cascavel

2018

CENTRO UNIVERSITARIO ASSIS GURGACZ

Gustavo Henrique Esser

Analise de Malware baseados em cenários reais da mitigação a prevenção

Projeto de pesquisa apresentado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação pelo Centro Universitário da Fundação Assis Gurgacz.

Professora Orientadora: Elaine De Oliveira Zanini

Cascavel

2018

SUMÁRIO

1 INTRODUÇÃO 1
1.1 ASSUNTO / TEMA 2
1.2 PROBLEMA DE PESQUISA 2
1.3 OBJETIVOS DA PESQUISA 2
1.3.1 Objetivo Geral 2
1.3.2 Objetivos Específicos 2
1.4 JUSTIFICATIVA 3
2 FUNDAMENTAÇÃO TEÓRICA 3
2.1 DADO E INFORMAÇÃO 4
2.2 REDES DE COMPUTADORES 4
2.3 SEGURANÇA DA INFORMAÇÃO 6
2.3.1 Política de Segurança 7
2.3.2 Ameaças e Vulnerabilidades 8
2.4 SOLUÇÕES E TECNOLOGIA 9
3 ENCAMINHAMENTO METODOLÓGICO 10
3.1 CARACTERIZAÇÃO GERAL DA PESQUISA 10
3.1.1 Local de realização da pesquisa 11
3.2 ETAPAS DO DESENVOLVIMENTO DA PESQUISA 11
3.3 COLETA DE DADOS 11
3.3 CRONOGRAMA 12
4 REFERENCIAS 12

1 INTRODUÇÃO

Por volta da década de 1970, surgia o que hoje conhecemos como a internet. A sua pioneira ARPANET, foi a primeira rede operacional de computadores à base de comutação de pacotes, o seu objetivo final era interligar alguns departamentos e instituições dos Estados unidos para realizarem uma troca de dados e informações, mas como o seu tráfego era totalmente em texto puro surgiam na época as primeiras falhas de segurança da informação. Nesta época os engenheiros não se preocupavam com os protocolos de segurança da informação e com isso a internet herdou a insegurança dos dados e informações (ERIBERTO, 2013).

Com o aumento diário de dispositivos conectados à rede mundial de computadores e também devido a nova revolução conhecida como a Internet das Coisas (*Internet of Things – IoT*), o número de invasões e infecções teve aumento significativo (CARRARETTO, 2016). Segundo o CERT.BR – Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, em 2017 ocorrerem o total de 833.775 incidentes reportados apenas no País, em contrapartida os investimentos em soluções de segurança e também *appliances* como *Firewall*, IDS (Sistema de detecção de intrusão), IPS (Sistema de prevenção de intrusão), SIEM (Gerenciamento e Correlação de Eventos de Segurança) cresceram no mesmo período. De acordo com a PWC Brasil - PricewaterhouseCoopers houve um aumento em 40% em investimentos na área de segurança da informação. Isso ocorre devido os cibercriminosos que atuam no Brasil estão entre os que aplicam os golpes mais sofisticados. Neste meio tempo um termo conhecido como *malware* ficou em destaque.

A palavra *malware* normalmente carrega com sigo o sinônimo de invasão, danificação, roubo de informações. Segundo Vieira (2014), o *malware* não se refere apenas a um artefato malicioso, mas a um conjunto de vários tipos diferentes que podem ser definidos em um vírus, um *worm* e um *rootkit*. Porém o termo não é recente, é do final dos anos 60 e inícios dos anos 70, quando os *mainframes* estavam dominando as grandes corporações e centro de pesquisas. Surgindo os denominados *rabbits* conhecido por ser o primeiro malware, que se espalhava por uma rede e gerava cópias de si mesmo, prejudicando o desempenho fazendo com que o computador trave.

A evolução da tecnologia facilitou muito em ambas as partes, tanto atacantes quanto defensores, porém o custo elevado de soluções de segurança da informação para as

corporações tem deixado os atacantes em vantagem. Com isso o propósito deste trabalho é elevar o grau de maturidade em segurança da informação nas organizações.

1.1 ASSUNTO / TEMA

O tema desta pesquisa é a análise de *Malware* baseados em cenários reais da mitigação a prevenção e abordará a construção e a execução de uma arquitetura de segurança totalmente open source para diversos tipos de ambientes computacionais, buscando identificar e correlacionar ameaças de segurança da informação.

1.2 PROBLEMA DE PESQUISA

Analisar, prevenir e correlacionar incidentes de segurança da informação em ambientes de *data center* de alta disponibilidade sem afetar os 3 pilares da segurança a disponibilidade, integridade e a confidencialidade.

Como uma arquitetura de segurança da informação pode contribuir para minimizar os riscos do negócio ?

1.3 OBJETIVOS DA PESQUISA

1.3.1 Objetivo Geral

Construir de forma escalável e dinâmica um ambiente de monitoramento para análise, prevenir, correlacionar e mitigar os possíveis vetores de ataques em uma infraestrutura real de *Data Center* baseados em normas de segurança informação.

1.3.2 Objetivos Específicos

a) Fornecer uma solução de arquitetura de segurança totalmente open source de forma escalável e dinâmica.

b) Analisar e correlacionar os eventos de segurança coletados para detectar ataques no ambiente monitorado.

c) Validar os princípios de compliance internacionais e nacionais alinhados a estratégia de segurança.

d) Verificar a conformidade com as normas ISO27001 e PSI-DSS e gestão de incidentes de segurança.

e) Identificar principais vantagens e desvantagens das soluções utilizadas.

f) Avaliar a viabilidade da continuidade da gestão do processo.

1.4 JUSTIFICATIVA

Há necessidade de uma solução Open Source para área de operação e prevenção tendo em vista que no mercado existe soluções *Security Information and Event Management* (SIEM), porém, o custo elevado dificulta as empresas a adquirem soluções eficientes para seus ambientes de data center ou backbones. e estas tecnologias não são escaláveis. com isso o objetivo e fornecer toda arquitetura de segurança necessária para implantar e gerenciar um ambiente sem ter custo elevados com *appliances* e todo está arquitetura de forma escalável e dinâmica.

Segundo a SANS *Institute* (2016), as organizações precisam de conhecimentos técnicos para tomar decisões. Os riscos de segurança da informação que os departamentos de Tecnologia da informação (TI) e InfoSec estão enfrentando devem obter uma compreensão da operação, para comunicar com eficiência os responsáveis da organização e gerenciar os riscos. O objetivo de uma segurança da informação bem-sucedida e estratégica e encontrar soluções que gerenciem riscos e criem valor para o organização.

Desta forma abordaremos uma arquitetura de soluções *open source* voltadas a segurança da informação de fim a fim, apresentando na prática um ambiente construído para analisar o tráfego de rede à procura dos problemas e das anomalias de segurança.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados os temas de análise de *malware* baseado em um cenário real de *data center*, utilizando tecnologias para monitoramento, prevenção e correlação de softwares maliciosos. Consequentemente aumentando o nível de segurança da informação na organização e verificando a conformidade com a Política de Segurança da Informação (PSI).

2.1 DADO E INFORMAÇÃO

Atualmente é impossível falarmos de segurança da informação sem mencionar o que é dado e informação. Eles são as bases para que a segurança exista tanto nos ambientes corporativos como também individuais.

Conforme a definição de Chiavenato (2008), os dados servem como base para a formar uma informação. Um dado nada mais é do que índice ou um registro. Existem técnicas *hackers* que vão coletando pequenos dados pela internet, sejam estes dados de uma organização ou indivíduo, quando classificados, armazenados e relacionados entre si, os dados permitem a obtenção da informação. Conforme definição da INFOSEC INSTITUTE (2016), a técnica é denominada como *information gathering* conhecida por ser a primeira fase na realização de um teste de intrusão.

A informação e a organização dos dados que tem como objetivo transmitir significado e a compreensão. Atualmente a informação é arma estratégica em qualquer empresa e também é um recurso de vital importância nas organizações. Conforme Cesar (2013), a segurança da informação é um recurso que tem por finalidade proteger as informações e garantir que a continuidade do negócio ocorra sem incidentes e vazamentos.

Entretendo qualquer dado ou informação que esteja de alguma forma ligado a tecnologia, ele trafega através das redes de computadores que discutiremos abaixo.

2.2 REDES DE COMPUTADORES

Para falarmos sobre segurança da informação, é necessário conhecer os conceitos e toda história das redes de computadores.

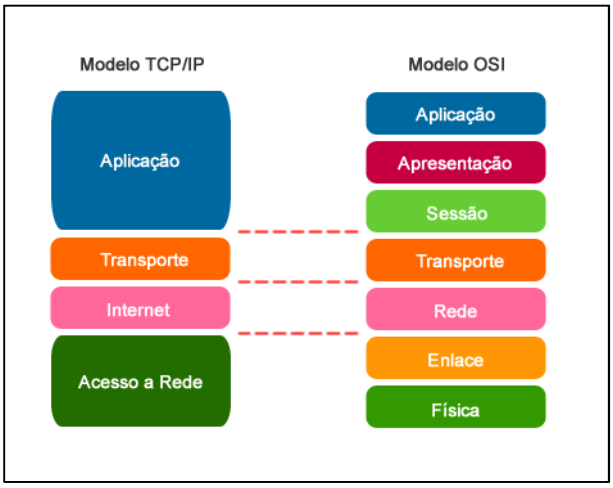
> "Na década de 1960, existiam muitos computadores de grande porte, conhecidos como mainframes, espalhados pelos centros de pesquisas dos Estados Unidos. Havia um profundo desejo de interligar essas maquinas. Um dos problemas foi que computadores de fabricantes diferentes não podiam se comunicar, uma vez que não havia um padrão até o momento estabelecido, já em 1967, a ARPA (Advanced Research and Projects Agency) apresentou um projeto intitulado ARPANET. A ideia era simples interligar tudo ao computador central, com capacidade para entender todos os outros computadores. Este computador central recebeu o nome de *Interface Message Processor* (IMP). O IMP ficou conhecido como o pai dos roteadores de rede moderno"(ERIBERTO, 2013, pág. 21).

Conforme Tanenbaum (2011) define que redes de computadores ou *network* é um grupo de sistemas de computadores interligados por qualquer meio físico capaz de trocar informações. Já Kurose (2014, pág. 3) discorda do termo rede de computadores, ele acredita que o termo está começando a se tornar um tanto desatualizado, pois muitos equipamentos não tradicionais estão sendo ligados a internet.

Para compreendermos melhor as redes de computadores temos que compreender os protocolos de redes, conforme definido na ciência da computação, um protocolo é uma convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais. De maneira simples, um protocolo pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação. O protocolo utilizado nas redes comutadores atuais e o TCP/IP que tem como base o modelo OSI o TCP/IP e muito utilizado por possuir sua arquitetura aberta e qualquer fabricante pode adotar o protocolo sem custo, ele acabou-se transformando em um protocolo universal (LINO, 2015).

A arquitetura do TCP/IP, como é possível verificar na Figura 1 é um protocolo de quatro camadas que utiliza como referência as 7 camadas do modelo OSI.

Figura 1: Arquitetura TCP/IP



Fonte: Gustavo Henrique Esser, adaptado de Lino (2015)

Conforme a Figura 1 o modelo TCP/IP baseia-se nas seguintes camadas:
Camada de Acesso a rede ou Acesso aos Meios: Esta é a camada inferior da arquitetura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI.

Camada Internet: A camada Internet, também conhecida como de Rede ou Internetwork, é equivalente à camada 3 do Modelo OSI. Os protocolos IP e ICMP (ping) estão presentes nesta camada.
Camada de Transporte: A camada de Transporte equivale à camada 4 do Modelo OSI. Seus dois principais protocolos são o TCP e o UDP.
Camada de Aplicação: A camada superior é chamada de camada de aplicação equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos são: HTTP, FTP, Telnet, DNS e SMTP.

2.3 SEGURANÇA DA INFORMAÇÃO

De acordo com a norma ISO/IEC27002 (2005, pág. 16), "a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Já segundo a autora Diana (2013) "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados de acordo com as necessidades em questão, a fim de garantir a segurança da informação".

Para a norma ISO/IEC27002 (2005, pág. 16), "a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Os princípios básicos quem regem de segurança da informação abrangem basicamente os seguintes pilares: confidencialidade, integridade e disponibilidade (CID), e tem como base a norma ISO/IEC 27002 que aborda os atributos básicos da informação, também chamado de princípios básicos da segurança da informação por alguns autores e especialistas da área podemos entendê-los da seguinte maneira:

A segurança da informação baseia-se nos seguintes princípios os três se destacam:

- **Confidencialidade** – Define que somente pessoas que tenham as permissões corretas devem acessar e ao mesmo tempo impede que outros, não autorizados, a vejam.

- **Integridade** – Define que a informação mantenha-se intacta, precisa e util.
- **Disponibilidade** – Disponível para acesso quando necessário sem infringir os dois pilares acima.

Para Rocha (2008) quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente.

2.3.1 Política de Segurança

Para implantar um projeto de segurança da informação em uma organização é preciso estabelecer as diretrizes, mecanismo de segurança, políticas e procedimentos, ferramentas de proteção e autenticação, e a sua relação custo benefício. A política de segurança serve como base para definir e para adotar os padrões e como será montado a estrutura.

Para Dantas (2001), pode-se definir a política de segurança é como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações. Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras pré-estabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir. A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por exemplo a indisponibilidade do serviço, furto ou até mesmo a perda de informações. As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pela experiência tem que irá dar continuidade na gestão do processo.

Para elaborar uma política de segurança na organização para Ferreira e Araújo (2008), deve-se formar um comitê de segurança da informação, constituído por profissionais de diversos departamentos, como informática, jurídico, engenharia, infraestrutura, recursos humanos e outro que for necessário. Este comitê e responsável por estabelecer e também evangelizar os procedimentos na organização.

Para a elaboração desta política, deve-se levar em conta a norma ISO/IEC 17799 que divide nos seguintes controles:

1- Análise/Avaliação e tratamento da Informação;

2- Política de Segurança da informação;

3- Organizando a Segurança da Informação;

4- Gestão de Ativos;

5- Segurança em Recursos Humanos;

6- Segurança Física e do Ambiente;

7- Gerenciamento das Operações e Comunicações;

8- Controle de Acesso;

9- Aquisição, Desenvolvimento, Manutenção da Segurança de Sistemas;

10- Gestão de Incidentes de Segurança da Informação;

11- Gestão da Continuidade do Negócio;

12- Conformidade.

Segundo a NBR ISO/IEC27002 (2005, pág. 8), "é recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia da política".

2.3.2 Ameaças e Vulnerabilidades

Segundo Rocha (2008), a ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação a confidencialidade, integridade ou disponibilidade. O impacto de um incidente de segurança e medido pelas consequências que ela pode causar ao negócio.

Podemos definir que *malwares* são uma ameaça que se aproveita das vulnerabilidades de aplicações. Conforme foram surgindo foram identificadas determinadas características e funcionalidades comuns em certos grupos de malwares e assim criaram-se categorias para distingui-los. Veremos abaixo os *malwares* mais comuns e identificados facilmente.

- Vírus: É um dos mais antigos porem tem se tornado um termo genérico para descrever os tipos de malwares.
- Worm: Similar ao vírus porem se replica pela rede sem a necessidade da ação do usuário.
- Cavalo de troia: Com base na mitologia grega, e um programa que executa um trojan escondido no meio de uma aplicação sem o conhecimento do usuário.

- Backdoor: Código malicioso que se instala no computador para permitir o acesso remoto do atacante. Permite ao atacante se conectar e executar comandos no computador infectado sem que o administrador perceba.
- Bot/Botnet: Também conhecida como exército de zumbis, é uma rede composta por um grande número de computadores que foram infectados.
- Rootkit: Malware designado para ocultar sua presença e de outros códigos maliciosos no sistema operacional.
- Ransoware: Restringe o acesso ao sistema operacional de seu computador e pede que um resgate em criptomoedas (ACADEMIA DE AMEAÇAS ONLINE AVAST, 2018).

As ameaças que acabamos de conhecer são apenas algumas no meio de milhares que estão na internet. Segundo o CERT.BR – Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo.

2.4 SOLUÇÕES E TECNOLOGIA

Atualmente em uma infraestrutura de redes, existem diversas soluções de tecnologia para construímos um ambiente capaz de prefinir invasões. Abaixo iremos apresentar os principais conceitos e termos utilizados.

Sistema de detecção de intrusos (IDS) é um sistema de detecção de intrusão que possibilita a coleta e o uso de informações dos diversos tipos de ataques em prol da defesa de toda uma infraestrutura de rede (PANDINI, 2017) .

Os sistemas IDS são constituídos:

• Sensores: que geram os eventos e alarmes de segurança da informação;

• Console: que controla os sensores, e monitora os eventos e alertas;

• Motor: utiliza as regras de segurança para gerar os alertas a partir dos eventos de segurança.

O Sistema de prevenção de intrusão (IPS) é um software de prevenção de intrusão. fornece as políticas e normas para o tráfego de rede, juntamente com um sistema de detecção de intrusão para alertar os administradores de sistema (CELESTE, 2016).

Abaixo iremos apresentar as características do Sistema de prevenção de intrusão :
O posicionamento em corte na rede do IPS e não apenas à escuta na rede para o IDS (tradicionalmente posicionado como um *sniffer* na rede).

A possibilidade de bloquear imediatamente as intrusões e independentemente do tipo de protocolo de transporte utilizado e sem reconfiguração de um equipamento terceiro. O que induz que o IPS é constituído em como nativo numa técnica de filtragem de pacotes e meios de bloqueio (*drop connection, drop offending packets, block intruder*).

Sistema de Detecção de Intrusão na Rede (NIDS) e responsável por monitorar e analisa todo o tráfego no segmento da rede. Consiste em um conjunto de sensores que trabalha detectando atividades maliciosas na rede, como ataques baseados em serviço como *portscans*, entre outros métodos de ataque (SANTOS, 2010).

Sistemas de Detecção de Intrusão baseados em Host (HIDS) monitora e analisa informações coletadas de um único Host (Máquina). Não observa o tráfego que passa pela rede, seu uso volta-se a verificação de informações relativas aos eventos e registros de logs e sistema de arquivos (permissão, alteração, etc.).

3 ENCAMINHAMENTO METODOLÓGICO

3.1 CARACTERIZAÇÃO GERAL DA PESQUISA

O procedimento desta pesquisa é classificado como um estudo de caso com pesquisa bibliográfica e exploratória, quanto a natureza da pesquisa caracteriza-se como pesquisa qualitativa Conforme definição do INSPER “um estudo de caso quando não se tem uma solução pré-definida, exigindo empenho do aluno para identificar o problema, analisar evidências, desenvolver argumentos lógicos, avaliar e propor soluções ”.

Será uma pesquisa bibliográfica e exploratória, porque busca implementar algo de que se tem pouco conhecimento, e também é pouco explorado. A bibliografia tem como objetivo servir como base para a construção da proposta do tema Analise de *Malware* baseados em cenários reais da mitigação a prevenção.

A pesquisa exploratória, segundo Severino (2007), busca apenas encontrar informações sobre um objeto determinado, delimitando assim um campo de trabalho, explorando as condições de manifestação desse objeto.

Segundo o INSTITUTO PHD (2015) a pesquisa qualitativa está mais relacionada no levantamento de dados sobre as motivações de um grupo, em compreender e interpretar determinados comportamentos, a opinião e as expectativas dos indivíduos de uma população. É exploratória, portanto não tem o intuito de obter números como resultados, mas *insights* – muitas vezes imprevisíveis – que possam nos indicar o caminho para tomada de decisão correta sobre uma questão-problema.

3.1.1 Local de realização da pesquisa

A pesquisa será realizada no *data center* da Brascloud localizado na cidade de Cascavel (PR), que possui uma arquitetura hiper convergente e segue os padrões de design *Open Compute Project* (OCP) utilizado por empresas globais como Google e Facebook.

3.2 ETAPAS DO DESENVOLVIMENTO DA PESQUISA

O estudo tem como objetivo elaborar uma arquitetura de segurança da informação aplicados a ambientes de *data center.* Estabelecendo de forma escalável e dinâmica um ambiente de monitoramento para analisar, prevenir, correlacionar e mitigar os possíveis *malwares* em uma infraestrutura.

A pesquisa será dívida em 03 fases sendo elas, a primeira fase será o levantamento teórico e prático, a segunda fase e analise do ambiente onde será implementado, e a terceira fase será a implantação das ferramentas e documentação de toda a arquitetura e implementação que será utilizada no projeto, disponibilizada de forma gratuita através da maior plataforma de códigos e projetos *opensource* do mundo o GitHub.

3.3 COLETA DE DADOS

A coleta de dados ocorrera através das ferramentas que serão os pilares deste projeto, através dos instrumentos de coletas iremos processar estes dados e informações nas ferramentas, mediante análise profunda iremos conseguir demonstrar relatórios e gráficos de como o ambiente funciona com a arquitetura de segurança.

3.3 CRONOGRAMA

ATIVIDADE	ANO 2018											
MESES	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Definição problema, objetivos e justificativa.		X										
Descrição da metodologia				X	X							
Fundamentação teórica				X	X	X	X	X				
Protocolo do projeto						X						
Banca de defesa do projeto							X					
Implantação							X	X	X	X		
Documentação								X	X	X		
Considerações finais										X		
Protocolo do artigo											X	
Banca de defesa do artigo											X	

4 REFERENCIAS

FILHO, João Eriberto Mota. Análise de trafego em redes tcp/ip: Utiliza tcpdump na análise de tráfegos em qualquer sistema operacional. 1 ed. São Paulo: Novatec, 2013. 416 p.

O GLOBO. Investimento em segurança da informação cresce mais no país. Disponível em: <https://oglobo.globo.com/economia/negocios/investimento-em-seguranca-da-informacao-cresce-mais-no-pais-17645471>. Acesso em: 08 abr. 2018.

Cert.br O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Disponível em: https://www.cert.br/stats/incidentes/ Acesso em: 08 abril 2018.

VIEIRA, Luiz. Análise de Malwares com Software Livre. O maior evento integrado das ciências forenses da América Latina, [S.L], jan. 2012. Disponível em: <http://www.iccyber.org/sites/default/files/Análise de Malwares com Software Livre.pdf>. Acesso em: 09 abr. 2018.

EARNEST, Wesley. Investing in Information Security: A Case Study in Community Banking. SANS Institute InfoSec Reading Room, [S.L], ago. 2016.

CHIAVENATO, Idalberto. Administração nos novos tempos. São Paulo: Campus, 2000.

INFOSEC INSTITUTE. Introduction to information gathering. Disponível em: <https://resources.infosecinstitute.com/information-gathering/#gref>. Acesso em: 12 mai. 2018.

PROFISSIONAIS TI. Politica de segurança da informação: definição, importância, elaboração e implementação. Disponível em: <https://www.profissionaisti.com.br/2013/06/politica-de-seguranca-da-informacao-definicao-importancia-elaboracao-e-implementacao/>. Acesso em: 12 mai. 2018.

FILHO, João Eriberto Mota. Análise de trafego em redes tcp/ip: Utiliza tcpdump na análise de tráfegos em qualquer sistema operacional. 1 ed. São Paulo: Novatec, 2013. 21 p.

TANENBAUM, Andrew Stuart. Redes de computadores. 4 ed. Rio de Janeiro: Elsevier, 2003. 947 p.

KUROSE, Jim; ROSS, Keith. Redes de computadores e a internet: uma abordagem top-down. 6 ed. São Paulo: Pearson Education do Brasil, 2013. 634 p.

OLANCA, Ricardo Lino. Administração de redes Linux: Conceitos e praticas na administração de redes em ambientes Linux. 1 ed. São Paulo: Novatec, 2015. 256 p.

MUNDO DA ROBÓTICA. Protocolo (ciência da computação). Disponível em: <https://mundodarobotica.wordpress.com/2011/06/11/protocolo-ciencia-da-computacao/>. Acesso em: 12 mai. 2018.

LYRA, Mauricio Rocha. Segurança e auditoria em sistemas de informação. 1 ed. Rio de Janeiro: Ciência Moderna, 2008. 253 p.

FAQ INFORMATICA. Protocolo tcp/ip, como funciona e quais as suas camadas. Disponível em: <https://faqinformatica.com/o-que-e-o-tcpip-e-as-camadas/>. Acesso em: 12 mai. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT)– Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT,2003.

PROFISSIONAIS TI. Política de segurança da informação – introdução ao desenvolvimento. Disponível em: <https://www.profissionaisti.com.br/2013/03/politica-de-seguranca-da-informacao-introducao-ao-desenvolvimento/>. Acesso em: 19 mai. 2018.

DANTAS, Marcus Leal. Segurança da informação: Uma abordagem focada em gestão de riscos. 1 ed. Olinda: Livro Rápido – Elógica, 2011. 155 p.

FREITAS,F;ARAUJO, M. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: Guia prático para elaboração e implementação. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT)– Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT,2003.

AVAST. Academia de ameaças online. Disponível em: <https://www.avast.com/pt-br/c-online-threats>. Acesso em: 16 jun. 2018.

CERT.BR. Códigos maliciosos (malware). Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 16 jun. 2018.

OSTEC. Ids: história, conceito e terminologia. Disponível em: <https://ostec.blog/seguranca-perimetro/ids-o-que-e-e-principais-conceitos>. Acesso em: 16 jun. 2018.

THALLITACELESTE. Firewall, nids, hids, ids e ips. Disponível em: <https://thallitaceleste.blogspot.com/2015/03/firewall-nids-hids-ids-e-ips.html>. Acesso em: 16 jun. 2018.

INSPER. O que é um estudo de caso. Disponível em: <https://www.insper.edu.br/casos/estudo-caso/>. Acesso em: 23 jun. 2018.

INSTITUTO PHD. Pesquisa quantitativa e pesquisa qualitativa: entenda a diferença. Disponível em: <https://www.i.com.br/pesquisa-quantitativa-e-pesquisa-qualitativa-entenda-a-diferenca/>. Acesso em: 23 jun. 2018.

BRASCLOUD. A brascloud. Disponível em: <https://www.brascloud.com.br/a-brascloud>. Acesso em: 23 jun. 2018.