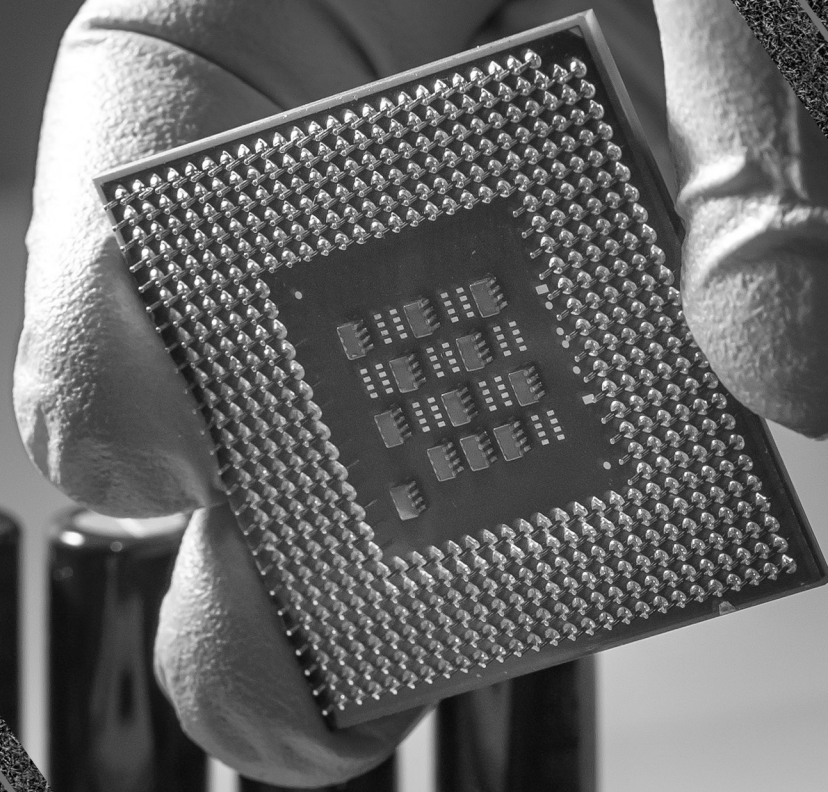


João Dallamuta
Henrique Ajuz Holzmann
Marcelo Henrique Granza
(Organizadores)

**Engenharia Elétrica
e de Computação:
Atividades Relacionadas com
o Setor Científico e Tecnológico**

Atena
Editora

Ano 2020



João Dallamuta
Henrique Ajuz Holzmann
Marcelo Henrique Granza
(Organizadores)

**Engenharia Elétrica
e de Computação:
Atividades Relacionadas com
o Setor Científico e Tecnológico**

2020 by Atena Editora

Copyright © Atena Editora

Copyright do Texto © 2020 Os autores

Copyright da Edição © 2020 Atena Editora

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira

Diagramação: Camila Alves de Cremo

Edição de Arte: Lorena Prestes

Revisão: Os Autores



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição *Creative Commons*. Atribuição 4.0 Internacional (CC BY 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

Conselho Editorial

Ciências Humanas e Sociais Aplicadas

Profª Drª Adriana Demite Stephani – Universidade Federal do Tocantins

Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas

Prof. Dr. Alexandre Jose Schumacher – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso

Profª Drª Angeli Rose do Nascimento – Universidade Federal do Estado do Rio de Janeiro

Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná

Prof. Dr. Antonio Gasparetto Júnior – Instituto Federal do Sudeste de Minas Gerais

Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília

Prof. Dr. Carlos Antonio de Souza Moraes – Universidade Federal Fluminense

Profª Drª Cristina Gaio – Universidade de Lisboa

Profª Drª Denise Rocha – Universidade Federal do Ceará

Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia

Prof. Dr. Edvaldo Antunes de Farias – Universidade Estácio de Sá

Prof. Dr. Eloi Martins Senhora – Universidade Federal de Roraima

Prof. Dr. Fabiano Tadeu Grazioli – Universidade Regional Integrada do Alto Uruguai e das Missões

Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná

Prof. Dr. Gustavo Henrique Cepolini Ferreira – Universidade Estadual de Montes Claros

Profª Drª Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice

Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense

Profª Drª Keyla Christina Almeida Portela – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso

Profª Drª Lina Maria Gonçalves – Universidade Federal do Tocantins

Prof. Dr. Luis Ricardo Fernandes da Costa – Universidade Estadual de Montes Claros

Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte

Prof. Dr. Marcelo Pereira da Silva – Universidade Federal do Maranhão

Profª Drª Miranilde Oliveira Neves – Instituto de Educação, Ciência e Tecnologia do Pará

Profª Drª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa

Profª Drª Rita de Cássia da Silva Oliveira – Universidade Estadual de Ponta Grossa

Profª Drª Sandra Regina Gardacho Pietrobon – Universidade Estadual do Centro-Oeste

Profª Drª Sheila Marta Carregosa Rocha – Universidade do Estado da Bahia

Prof. Dr. Rui Maia Diamantino – Universidade Salvador

Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará

Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

Prof. Dr. William Cleber Domingues Silva – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

Ciências Agrárias e Multidisciplinar

Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano
Prof. Dr. Antonio Pasqualetto – Pontifícia Universidade Católica de Goiás
Prof. Dr. Cleberton Correia Santos – Universidade Federal da Grande Dourados
Profª Drª Daiane Garabeli Trojan – Universidade Norte do Paraná
Profª Drª Diocléa Almeida Seabra Silva – Universidade Federal Rural da Amazônia
Prof. Dr. Écio Souza Diniz – Universidade Federal de Viçosa
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul
Prof. Dr. Fágner Cavalcante Patrocínio dos Santos – Universidade Federal do Ceará
Profª Drª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Júlio César Ribeiro – Universidade Federal Rural do Rio de Janeiro
Profª Drª Lina Raquel Santos Araújo – Universidade Estadual do Ceará
Prof. Dr. Pedro Manuel Villa – Universidade Federal de Viçosa
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará
Profª Drª Talita de Santos Matos – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Tiago da Silva Teófilo – Universidade Federal Rural do Semi-Árido
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

Ciências Biológicas e da Saúde

Prof. Dr. André Ribeiro da Silva – Universidade de Brasília
Profª Drª Anelise Levay Murari – Universidade Federal de Pelotas
Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás
Prof. Dr. Edson da Silva – Universidade Federal dos Vales do Jequitinhonha e Mucuri
Profª Drª Eleuza Rodrigues Machado – Faculdade Anhanguera de Brasília
Profª Drª Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina
Profª Drª Eysler Gonçalves Maia Brasil – Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Prof. Dr. Ferlando Lima Santos – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Fernando José Guedes da Silva Júnior – Universidade Federal do Piauí
Profª Drª Gabriela Vieira do Amaral – Universidade de Vassouras
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria
Profª Drª Iara Lúcia Tescarollo – Universidade São Francisco
Prof. Dr. Igor Luiz Vieira de Lima Santos – Universidade Federal de Campina Grande
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará
Prof. Dr. Luís Paulo Souza e Souza – Universidade Federal do Amazonas
Profª Drª Magnólia de Araújo Campos – Universidade Federal de Campina Grande
Prof. Dr. Marcus Fernando da Silva Praxedes – Universidade Federal do Recôncavo da Bahia
Profª Drª Mylena Andréa Oliveira Torres – Universidade Ceuma
Profª Drª Natiéli Piovesan – Instituto Federaci do Rio Grande do Norte
Prof. Dr. Paulo Inada – Universidade Estadual de Maringá
Profª Drª Renata Mendes de Freitas – Universidade Federal de Juiz de Fora
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

Ciências Exatas e da Terra e Engenharias

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto

Prof. Dr. Alexandre Leite dos Santos Silva – Universidade Federal do Piauí
Prof. Dr. Carlos Eduardo Sanches de Andrade – Universidade Federal de Goiás
Prof^a Dr^a Carmen Lúcia Voigt – Universidade Norte do Paraná
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Prof. Dr. Juliano Carlo Rufino de Freitas – Universidade Federal de Campina Grande
Prof^a Dr^a Luciana do Nascimento Mendes – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Prof. Dr. Marcelo Marques – Universidade Estadual de Maringá
Prof^a Dr^a Neiva Maria de Almeida – Universidade Federal da Paraíba
Prof^a Dr^a Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

Conselho Técnico Científico

Prof. Me. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo
Prof. Me. Adalberto Zorzo – Centro Estadual de Educação Tecnológica Paula Souza
Prof. Me. Adalto Moreira Braz – Universidade Federal de Goiás
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba
Prof. Me. André Flávio Gonçalves Silva – Universidade Federal do Maranhão
Prof^a Dr^a Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico
Prof^a Dr^a Andrezza Miguel da Silva – Universidade Estadual do Sudoeste da Bahia
Prof. Dr. Antonio Hot Pereira de Faria – Polícia Militar de Minas Gerais
Prof^a Ma. Bianca Camargo Martins – UniCesumar
Prof^a Ma. Carolina Shimomura Nanya – Universidade Federal de São Carlos
Prof. Me. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro
Prof. Ma. Cláudia de Araújo Marques – Faculdade de Música do Espírito Santo
Prof^a Dr^a Cláudia Taís Siqueira Cagliari – Centro Universitário Dinâmica das Cataratas
Prof. Me. Daniel da Silva Miranda – Universidade Federal do Pará
Prof^a Ma. Daniela da Silva Rodrigues – Universidade de Brasília
Prof^a Ma. Dayane de Melo Barros – Universidade Federal de Pernambuco
Prof. Me. Douglas Santos Mezacas – Universidade Estadual de Goiás
Prof. Dr. Edwaldo Costa – Marinha do Brasil
Prof. Me. Eduardo Gomes de Oliveira – Faculdades Unificadas Doctum de Cataguases
Prof. Me. Eliel Constantino da Silva – Universidade Estadual Paulista Júlio de Mesquita
Prof. Me. Euvaldo de Sousa Costa Junior – Prefeitura Municipal de São João do Piauí
Prof^a Ma. Fabiana Coelho Couto Rocha Corrêa – Centro Universitário Estácio Juiz de Fora
Prof. Dr. Fabiano Lemos Pereira – Prefeitura Municipal de Macaé
Prof. Me. Felipe da Costa Negrão – Universidade Federal do Amazonas
Prof^a Dr^a Germana Ponce de Leon Ramírez – Centro Universitário Adventista de São Paulo
Prof. Me. Gevair Campos – Instituto Mineiro de Agropecuária
Prof. Dr. Guilherme Renato Gomes – Universidade Norte do Paraná
Prof. Me. Gustavo Krahl – Universidade do Oeste de Santa Catarina
Prof. Me. Helton Rangel Coutinho Junior – Tribunal de Justiça do Estado do Rio de Janeiro
Prof^a Ma. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia
Prof. Me. Javier Antonio Albornoz – University of Miami and Miami Dade College
Prof^a Ma. Jéssica Verger Nardeli – Universidade Estadual Paulista Júlio de Mesquita Filho
Prof. Me. Jhonatan da Silva Lima – Universidade Federal do Pará
Prof. Me. José Luiz Leonardo de Araujo Pimenta – Instituto Nacional de Investigación Agropecuaria Uruguay
Prof. Me. José Messias Ribeiro Júnior – Instituto Federal de Educação Tecnológica de Pernambuco

Profª Ma. Juliana Thaisa Rodrigues Pacheco – Universidade Estadual de Ponta Grossa
 Profª Drª Kamilly Souza do Vale – Núcleo de Pesquisas Fenomenológicas/UFPA
 Profª Drª Karina de Araújo Dias – Prefeitura Municipal de Florianópolis
 Prof. Dr. Lázaro Castro Silva Nascimento – Laboratório de Fenomenologia & Subjetividade/UFPR
 Prof. Me. Leonardo Tullio – Universidade Estadual de Ponta Grossa
 Profª Ma. Lilian Coelho de Freitas – Instituto Federal do Pará
 Profª Ma. Liliani Aparecida Sereno Fontes de Medeiros – Consórcio CEDERJ
 Profª Drª Lívia do Carmo Silva – Universidade Federal de Goiás
 Prof. Me. Lucio Marques Vieira Souza – Secretaria de Estado da Educação, do Esporte e da Cultura de Sergipe
 Prof. Me. Luis Henrique Almeida Castro – Universidade Federal da Grande Dourados
 Prof. Dr. Luan Vinicius Bernardelli – Universidade Estadual do Paraná
 Prof. Dr. Michel da Costa – Universidade Metropolitana de Santos
 Prof. Dr. Marcelo Máximo Purificação – Fundação Integrada Municipal de Ensino Superior
 Prof. Me. Marcos Aurelio Alves e Silva – Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
 Profª Ma. Marileila Marques Toledo – Universidade Federal dos Vales do Jequitinhonha e Mucuri
 Prof. Me. Ricardo Sérgio da Silva – Universidade Federal de Pernambuco
 Prof. Me. Rafael Henrique Silva – Hospital Universitário da Universidade Federal da Grande Dourados
 Profª Ma. Renata Luciane Polsaque Young Blood – UniSecal
 Profª Ma. Solange Aparecida de Souza Monteiro – Instituto Federal de São Paulo
 Prof. Me. Tallys Newton Fernandes de Matos – Faculdade Regional Jaguaribana
 Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)	
E57	<p>Engenharia elétrica e de computação [recurso eletrônico] : atividades relacionadas com o setor científico e tecnológico 1 / Organizadores João Dallamuta, Henrique Ajuz Holzmann, Marcelo Henrique Granza. – Ponta Grossa, PR: Atena, 2020.</p> <p>Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-65-5706-167-1 DOI 10.22533/at.ed.671200207</p> <p>1. Ciência da computação – Pesquisa – Brasil. 2. Engenharia elétrica – Pesquisa – Brasil. I. Dallamuta, João. II. Holzmann, Henrique Ajuz. III. Granza, Marcelo Henrique.</p> <p style="text-align: right;">CDD 623.3</p>
Elaborado por Maurício Amormino Júnior – CRB6/2422	

Atena Editora
 Ponta Grossa – Paraná - Brasil
www.atenaeditora.com.br
 contato@atenaeditora.com.br

APRESENTAÇÃO

Não há padrões de desempenho em engenharia elétrica e da computação que sejam duradouros. Desde que Gordon E. Moore fez a sua clássica profecia tecnológica, em meados dos anos 60, a qual o número de transistores em um chip dobraria a cada 18 meses - padrão este válido até hoje – muita coisa mudou. Permanece porém a certeza de que não há tecnologia na neste campo do conhecimento que não possa ser substituída a qualquer momento por uma nova, oriunda de pesquisa científica nesta área.

Produzir conhecimento em engenharia elétrica e da computação é, portanto, atuar em fronteiras de padrões e técnicas de engenharia. Algo desafiador para pesquisadores e engenheiros.

Neste livro temos uma diversidade de temas nas áreas níveis de profundidade e abordagens de pesquisa, envolvendo aspectos técnicos e científicos. Aos autores e editores, agradecemos pela confiança e espírito de parceria.

Boa leitura

João Dallamuta
Henrique Ajuz Holzmann
Marcelo Henrique Granza

SUMÁRIO

CAPÍTULO 1	1
DESENVOLVIMENTO DE UMA INTERFACE PARA ESTUDO EM CONTROLE DE UM ROBÔ MÓVEL DE EQUILÍBRIO DINÂMICO	
Alex Sandro Garefa Guyllherme Emmanuel Tagliaferro de Queiroz Luis Antonio Bassora Flavio Eduardo Tapparo	
DOI 10.22533/at.ed.6712002071	
CAPÍTULO 2	17
ROBÔ PARA INSTALAÇÃO DE SINALIZADORES AVIFAUNA	
Bruno Monteiro Costa Máique! Bruno de Andrade Rezende Waldir Alves Diniz Ricardo de Souza Marcelo Clécio Paula da Silva	
DOI 10.22533/at.ed.6712002072	
CAPÍTULO 3	26
PROSPECTOS PARA A EVOLUÇÃO DA INTERFACE HUMANO-COMPUTADOR EM CENTROS DE CONTROLE DE ENERGIA ELÉTRICA	
Luiz Corrêa Lima	
DOI 10.22533/at.ed.6712002073	
CAPÍTULO 4	40
PROJETO CANAÃ - IRRIGADOR AUTOMÁTICO PARA O AGRONEGÓCIO	
André Kroupa Eldon Moura Cláudio Matheus da Costa Comin Rogério Luis Spagnolo da Silva	
DOI 10.22533/at.ed.6712002074	
CAPÍTULO 5	54
PAINEL DE BORDO - UMA INÉDITA PLATAFORMA COMPUTACIONAL EM UTILIZAÇÃO NO NOVO CENTRO DE OPERAÇÃO DA CEMIG-D	
Tiago Vilela Menezes Bruno Henrique da Silva Carlos Jose de Andrade Huliton Paz de Oliveira Marco Aurélio da Silva Fereda Odimar José Bezerra Lima Rafael Carneiro Motta	
DOI 10.22533/at.ed.6712002075	
CAPÍTULO 6	69
PARADIGMAS DAS TECNOLOGIAS 5G NA AUTOMAÇÃO DE SISTEMAS VERTICAIS NA INDÚSTRIA 4.0	
Daniel Rodrigues Ferraz Izario João Luiz Brancalhona Filho Yuzo Iano Karine Mendes Siqueira Rodrigues Ferraz Izario	
DOI 10.22533/at.ed.6712002076	

CAPÍTULO 7	81
DATA REGENERATION 2R IN OPTICAL COMMUNICATION NETWORK BASED ON MACH-ZEHNDER INTERFEROMETER WITH ACOUSTIC-OPTICAL FILTER AND HIGHLY NON-LINEAR PHOTONIC CRYSTAL FIBER	
Fabio Barros de Sousa Fiterlinge Martins de Sousa Jorge Everaldo de Oliveira Elizabeth Rego Sabino Marcos Benedito Caldas Costa	
DOI 10.22533/at.ed.6712002077	
CAPÍTULO 8	95
PROJETO DE UMA ANTENA PATCH PLANAR UTILIZANDO A SUPER FÓRMULA DE GIELIS	
Elder Eldervitch Carneiro de Oliveira Pedro Carlos de Assis Júnior	
DOI 10.22533/at.ed.6712002078	
CAPÍTULO 9	108
UMA CONTRIBUIÇÃO NA AVALIAÇÃO DE MODELOS DE SATISFAÇÃO DO CLIENTE PARA OS SERVIÇOS DE COMUNICAÇÕES MÓVEIS COM EQUAÇÕES ESTRUTURAIS	
Gutembergue Soares da Silva André Pedro Fernandes Neto Fred Sizenando Rossiter Pinheiro Antonio Salvio de Abreu	
DOI 10.22533/at.ed.6712002079	
CAPÍTULO 10	130
ATAQUES E DESCOBERTA DE VULNERABILIDADES EM REDES CORPORATIVAS	
Roger Robson dos Santos Jackson Mallmann	
DOI 10.22533/at.ed.67120020710	
CAPÍTULO 11	139
MODELO MATEMÁTICO PARA CONSOLIDAÇÃO DE MÁQUINAS VIRTUAIS	
Alexandre Henrique Teixeira Dias Luiz Henrique Andrade Correia	
DOI 10.22533/at.ed.67120020711	
CAPÍTULO 12	151
CAPTURE THE FLAG: MÉTODO DE APRENDIZADO PARA A DISCIPLINA DE FORENSE COMPUTACIONAL EM UMA UNIVERSIDADE PÚBLICA	
Carlos Eduardo de Barros Santos Júnior Ana Clara Nobre Mendes Jhonattan Carlos Barbosa Cabral Juliana Barbosa dos Santos Erick de Oliveira Silva Pedro Henrique Rodrigues Emerick	
DOI 10.22533/at.ed.67120020712	
CAPÍTULO 13	157
A METODOLOGIA EPRI PARA AVALIAÇÃO DE RISCOS CIBERNÉTICOS NAS INFRAESTRUTURAS CRÍTICAS E SUA RELAÇÃO COM A NORMA IEC 62443-2-1	
Luiz Augusto Kawafune Campelo	

CAPÍTULO 14	170
ANÁLISE DA PERFORMANCE DO MRE E SEUS IMPACTOS COMERCIAIS – PROPOSTA DE REVISÃO DA REGULAÇÃO	
João Carlos Mello Leonardo Calabro Vinicius Ragazi David Daniela Souza Luiz Laércio Simões Machado Junior Renato Mendes	
DOI 10.22533/at.ed.67120020714	
CAPÍTULO 15	190
DESENVOLVIMENTO DE SOFTWARE PARA INCLUSÃO EDUCACIONAL DE PESSOAS COM DEFICIÊNCIA MOTORA	
Felipe Massayuki Quiotoqui Italo Rodrigues da Silva	
DOI 10.22533/at.ed.67120020715	
CAPÍTULO 16	200
SISTEMAS IMUNOLÓGICOS ARTIFICIAIS APLICADOS AO DIAGNÓSTICO DE CÂNCER DE MAMA	
Gustavo da Silva Maciel Wagner Kenhiti Nakamura Júnior Luiz Francisco Granville Gonçalves Leonardo Plaster Silva Simone Silva Frutuoso de Souza Fábio Roberto Chavarette Fernando Parra dos Anjos Lima	
DOI 10.22533/at.ed.67120020716	
CAPÍTULO 17	213
AVALIAÇÃO DE TECNOLOGIAS NÃO INVASIVAS DE MEDIÇÃO DE GLICOSE EM HUMANOS	
Leanderson André Pedro Bertemes Filho	
DOI 10.22533/at.ed.67120020717	
CAPÍTULO 18	224
ENTENDIMENTO DOS CONTROLES E POSSÍVEIS CONFLITOS DE PRIVACIDADE NAS REDES SOCIAIS ONLINE	
Talita de Souza Costa Marbilia Possagnolo Sérgio Regina Marin	
DOI 10.22533/at.ed.67120020718	
CAPÍTULO 19	236
MODELAGEM DE PROBLEMA ELETROSTÁTICO UTILIZANDO ELEMENTOS FINITOS	
Julia Grasiela Busarello Wolff Pedro Bertemes Filho	
DOI 10.22533/at.ed.67120020719	

CAPÍTULO 20	252
SISTEMA DE MONITORAÇÃO DE CULTURA CELULAR <i>IN VITRO</i> VIA BIOIMPEDÂNCIA ELÉTRICA: REGRAS DE PROJETO	
Kaue Felipe Morcelles	
Pedro Bertemes Filho	
DOI 10.22533/at.ed.67120020720	
SOBRE OS ORGANIZADORES	265
ÍNDICE REMISSIVO	266

ATAQUES E DESCOBERTA DE VULNERABILIDADES EM REDES CORPORATIVAS

Data de aceite: 01/06/2020

Data da submissão: 10/03/2020

Roger Robson dos Santos

Programa de Pós-Graduação em Informática
(PPGIa)

Pontifícia Universidade Católica do Paraná (PUC-PR)

Curitiba - PR – Brasil

<http://lattes.cnpq.br/3797351864330209>

Jackson Mallmann

Instituto Federal Catarinense – Jardim Maluche
Brusque - SC

<http://lattes.cnpq.br/4046837503511326>

RESUMO: O avanço da tecnologia é um dos problemas para o surgimento de vulnerabilidades em redes de computadores corporativas. Este crescimento não é acompanhado pelas empresas que não investem e nem se preocupam com a segurança. O nosso estudo foca em conhecer o processo de uma atividade pentesting do tipo gray box em uma rede de computadores corporativa simulada, com serviços e vulnerabilidades dos dias atuais. Assim mostramos as empresas um incentivo para que possam investir em segurança e para que profissionais da área se interessem

em buscar conhecimentos de segurança ao desenvolverem seus sistemas.

PALAVRAS-CHAVE: CyberSegurança, pentest, redes corporativas, ataques de rede, segurança da informação

ABSTRACT: The advancement of technology is one of the problems for the emergence of vulnerabilities in corporate computer networks. This growth is not accompanied by companies that do not invest or worry about security. Our study focuses on knowing the process of a gray box pentesting activity on a simulated corporate computer network, with services and vulnerabilities of the present day. Thus, we show companies an incentive so that they can invest in security and for professionals in the area to be interested in seeking security knowledge when developing their systems.

KEYWORDS: CyberSecurity, pentest, corporate networks, network attacks, information security

1 | INTRODUÇÃO

A informática, ferramenta muito utilizada para auxiliar trabalhos diários das empresas, capaz de prover uma conectividade e comunicação entre pessoas da própria empresa e de fora. Seu grande crescimento

na usabilidade e aplicabilidade das redes de computadores, tem se tornado cada dia mais frequentes vulnerabilidades de segurança em equipamentos de informática, sendo que muitos fabricantes desconhecem e dificilmente resolvem estes problemas. Com esse crescimento, torna-se indispensável a utilização de mecanismos de segurança conhecidos como, *Antivírus*, *Firewall*, Políticas de Segurança, Análise de Riscos e Vulnerabilidades, Backup, *Firewall* de Aplicação Web (WAF), Detecção de Intrusão (IDS), Sistema de Prevenção de Intrusão (IPS), sendo essas grandes aplicações de segurança na área de redes e servidores.

Com o passar dos anos diversas técnicas na segurança de sistemas foram descobertas, e com isso tem tido um aumento nas pesquisas que envolvem identificação de anomalias na rede, muitas destas pesquisas visam melhorar técnicas de segurança utilizadas pelas empresas.

Neste trabalho temos como foco em conhecer uma visão geral na segurança da informação encontrando soluções que possibilitem um sistema mais confiável e seguro para seus usuários, além como atacantes descobrem e se aproveitam destas vulnerabilidades.

Nosso objetivo neste trabalho, será apresentar diversos métodos e técnicas utilizadas por um *pentester*, em um teste de *Gray Box*, a fim, de identificar vulnerabilidades em redes corporativas conhecendo breves informações limitadas sobre a rede e os serviços existentes.

Junto ao auxílio do sistema operacional *Kali Linux*, vamos simular a realização de testes de intrusão utilizando de ferramentas como *NMAP*, *WPScan*, *Burp Suite*, *Hydra*, *Dig*, *Metasploit* e muito mais em um ambiente que emula uma rede corporativa real, para melhor entendimento foi criado na Figura 2 todos os passos necessários para realização dos testes.

A motivação para realização deste trabalho, está em demonstrar como um atacante identifica vulnerabilidades em uma rede corporativa e quais medidas são necessárias para se prevenir, tornando seu ambiente mais seguro e confiável.

2 | FUNDAMENTAÇÃO TEÓRICA

Para facilitar o entendimento referente aos estudos de caso que foram realizados, será descrito uma breve história da internet com alguns aspectos necessários para melhor compreensão, abordando também as ferramentas, técnicas e algoritmos utilizados no trabalho. Além disso será também efetuado uma análise empírica entre eles, tendo como intuito selecionar as melhores técnicas de segurança da informação.

2.1 Introdução a História da Internet

A internet, uma ferramenta que se tornou dependência na vida das pessoas, seja

para lazer, trabalho, a internet nunca foi algo planejado, ela surgiu durante a Guerra Fria nos Estados Unidos cobrindo a necessidade de comunicação entre bases americanas em 1945. Quando se iniciou, ela se chamava ARPANET, nome derivado da empresa que a desenvolveu (*Advanced Research and Projects Agency*), desta forma garantir a comunicação entre os soldados americanos, caso o pentágono fosse atingido pela Ex-União Soviética (Atualmente Rússia) [Staling 2006].

Logo adiante, membros da MIT (*Massachusetts Institute of Technology*) tiveram uma ideia, converter toda a linguagem da ARPANET para uma linguagem mais humana, com isso desencadeou os primeiros mestres da informática, conhecidos como *Hackers*, que foram capazes de criar e desenvolver os primeiros compiladores da época até chegar os atuais compiladores [Staling 2006].

Com o passar dos anos começaram a nascer problemas de invasões em redes de internet nas organizações, com isso em 1994 a IAB (*Internet Architecture Board*) iniciou a emissão de relatórios de arquitetura de internet. Mostrando que havia a necessidade de melhorar a segurança da internet [Staling 2006].

2.2 Incidentes Relatados no Brasil

O CERT.br (Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil) um Grupo de Resposta a Incidentes de Segurança para internet no Brasil mantido pela NIC.br, do Comitê Gestor da internet no Brasil. Tem como objetivo atuar no tratamento de incidentes e na conscientização sobre os problemas de segurança. Na figura 1 apresenta-se um gráfico dos incidentes reportados pela CERT.br [cert.br 2020].

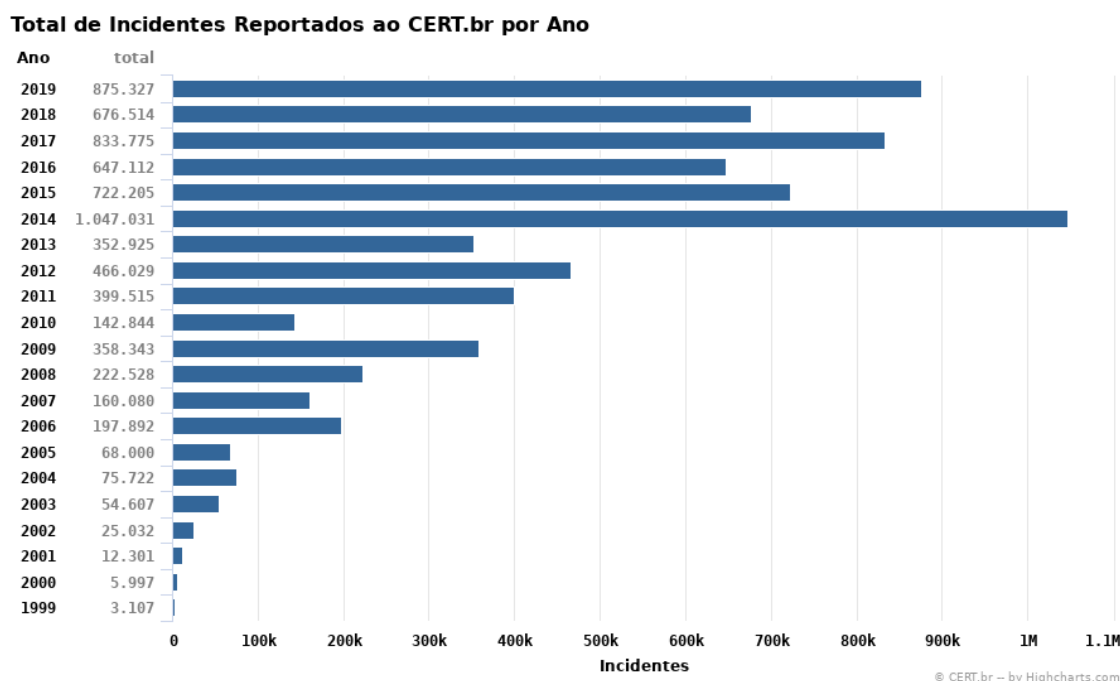


Figura 1. Total de Incidentes Reportados ao CERT.br por Ano [cert.br 2020].

2.3 São Pilares da Segurança da Informação

São pilares da segurança da informação.

- **Confidencialidade:** Garantir que as informações trocadas dentro do sistema de informação sejam confidenciais. (Roubo de banco de dados é uma violação) [Landwehr et al. 2011].
- **Disponibilidade:** Visa garantir que seu sistema esteja sempre disponível a quem interessa. Exemplos de ataques DDOS, faxineira na tomada [Yahya et al. 2015].
- **Integridade:** Garantir que todos os dados trafegados estejam íntegros e originais aos que foram enviados. Exemplo um banco enviando dinheiro para outro banco (um atacante do meio poderia alterar as informações) [Yahya et al. 2015].
- **Autenticidade:** Visa garantir que tal informação foi autêntica por tal usuário. Exemplo, você assina digitalmente um e-mail ou documento e vai pertencer a você. Você assina e garante que é sua [Landwehr et al. 2001].
- **Irretratabilidade (Não-repúdio):** Você não pode negar um ato que você fez. Fizer algo e alguém for investigar não terá como negar que você fez aquela coisa. Exemplo: Chaves autenticação, chaves criptografia, logs. (Enviar um e-mail no nome de outra pessoa de forma que você não vai ser descoberto) [Yahya et al. 2015].

2.4 Invasores e Profissionais da Segurança da Informação

Hackers são pessoas que constroem ferramentas que auxiliam e facilitam o trabalho dos usuários, normalmente os *hackers* costumam ter uma ideia de que o acesso à rede da internet deve ser ilimitado com o objetivo do autoconhecimento, em meio a isso *hackers* cometem crimes de invasões, com o intuito de corrigir problemas que os técnicos de informática das organizações desconhecem, ajudando os mesmos, a evitar ataques por meio de *crackers*, podemos dizer que o *hacker* é o profissional que mais contribui para que os pilares da segurança da informação não sejam quebrados, mas sim, renovados a cada dia [Marques 2010] .

Crackers, estes são opostos dos *hackers*, eles têm apenas o entendimento utilizado para o mal, utilizam suas habilidades técnicas e ferramentas com intuito de destruir uma rede, piratear programas, jogos e construção de vírus capazes de destruir todas as informações de uma rede, podemos dizer que o *crackers* são os principais responsáveis por encontrar vulnerabilidades, afim de tentar quebrar os pilares da segurança da informação [2010].

Quando falamos de serviços de segurança, podemos dar como exemplo o serviço de autenticação de dados, onde os dados durante a comunicação são assegurados que a entidade ao qual estamos se comunicando, realmente é aquela que se afirma ser. Outro grande serviço importante é o controle de acesso. Ele impede que o uso não autorizado de algum recurso dentro da organização trabalhe com a instrução de Confidencialidade, ou seja, ela assegura que não haja divulgação dos dados não autorizados garantindo a

proteção de dados durante a conexão e mesmo em uma conexão de um arquivo local [Stalling 2006].

2.5 Tipos de Pentest (Testes de intrusão)

Iremos abordar técnicas capazes de identificar vulnerabilidades de rede através de testes de intrusão, para melhor entendimento dessas técnicas precisamos entender quais os tipos de *pentesting* podem ser utilizados.

- **Black Box (Caixa Preta):** O *pentester* não tem ideia do que ele vai encontrar durante o teste, ele irá buscar coletar informações sobre o sistema ou a rede alvo. O principal motivo deste teste é que o *pentester* só sabe os resultados que ele pode esperar, mas não sabe como irá chegar até eles, lembrando que neste teste não serão examinados nenhum código fonte apenas a intrusão propriamente dita na rede [Jimenez 2016].
- **White Box (Caixa Branca):** Neste teste, o *pentester* já tem ideia sobre o sistema que ele irá testar, pois lhe será fornecido uma gama de informações sobre o sistema e a rede (detalhes de SO, endereços de IP, códigos fontes, aplicações etc.). Desta vez o *pentester* irá simular um ataque por uma fonte interna. O teste consiste em examinar códigos fontes e fluxos de dados, caminhos, loops e entres outros na rede da empresa [Gutmann et al. 2010].
- **Gray Box (Caixa Cinza):** O *pentester*, desta vez possui algumas informações parciais ou limitadas sobre detalhes da rede e aplicações de sistema. Pode desta vez efetuar um ataque externo afim de obter acesso ilegítimo a diversos documentos da infraestrutura da rede da organização [Rahimpour et al. 2017].

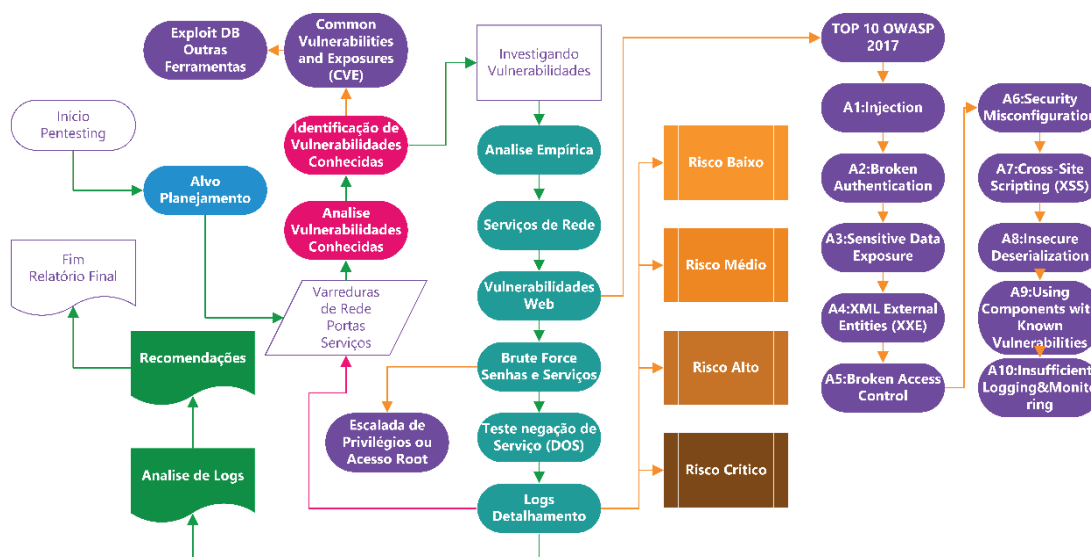


Figura 2. Etapas de Pentesting

3 | MÉTODO PROPOSTO

Em nossa proposta será realizado a procura por *tokens* em um sistema que simula uma rede computadores corporativa, ao qual teremos que utilizar diversos métodos e técnicas para buscar e encontrar esses *tokens*, visto que, eles estão escondidos em

serviços de redes encontrados no ambiente alvo.

3.1 Ambiente Teste

A realização dos nossos testes ocorreu no ambiente teste “*Pentestit – Penetration Testing Laboratories*” utilizando “*Test Lab V.12*”, que apresenta 16 *tokens* para procurar, sendo eles *Mail, DNS, Helpdesk, Users, Repository, SIEM, Site, My, API, User API, Image, VPN, DB, AD, Admin e Reverse*.

A *Pentesti*, é um laboratório que emula a infraestrutura de uma rede corporativa real com o objetivo de aprimorar as habilidades em um processo de *pentesting*. Os laboratórios possuem as vulnerabilidades recentes mais conhecidas cobrindo as áreas de segurança de rede, segurança de sistemas operacionais e aplicativo. O ambiente é construído para realização de testes em *Gray Box*, onde os participantes têm a informação sobre a infraestrutura de rede em forma de esquema e uma descrição de texto.

4 | ETAPAS DE PENTEST GRAY BOX

Com ajuda do fluxograma apresentado na Figura 2, relatamos que os testes de *Gray Box* serão conduzidos a partir da identificação do alvo (Empresa em questão) junto a um planejamento, com isso uma sondagem e varredura de portas será usado para identificação de serviços executando nesta rede alvo, em nosso caso, o nosso ambiente teste *Test Lab V.12*.

Com a descoberta de portas de serviços, vamos explorar as vulnerabilidades conhecidas, que podem ser encontradas no *site* do *Common Vulnerabilities and Exposures (CVE)* [CVE 2020], um *site* que apresenta as principais vulnerabilidades. Após a descoberta dos serviços conhecidos, a partir de agora será necessário analisarmos mais a fundo os serviços restantes e investigarmos possíveis vulnerabilidades. Caso seja encontrado uma vulnerabilidade que possibilite acesso ao sistema, será necessário agora repetir os processos a partir do processo de varreduras de portas. A OWASP [OWASP 2020], uma comunidade *online* que cria e disponibiliza de forma gratuita metodologias, artigos, ferramentas, documentação e tecnologias de segurança para aplicações web, pode nos apresentar os TOP 10 de vulnerabilidades web conhecidas, tornando uma ótima ferramenta a investigação de vulnerabilidades encontradas durante nossos testes.

Com o processo anterior realizado, agora é hora de colocar um grau de risco para cada vulnerabilidade como por exemplo: risco baixo (Serviços desatualizados, sistema operacional sem reiniciar etc.), médio (Listagem de diretórios, Falta de proteção conta *brute-forcing*, página de administração aberta etc.), alto (Criptografia de senhas em MD5, Página de login sem Criptografia SSL, *Cross-site Scripting (XSS)* etc.) ou crítica (*SQL Injection, Shell Upload*). Com os riscos identificados, será necessária uma avaliação dos logs em busca de outros possíveis problemas e assim avaliar as recomendações de

mudança para o sistema.

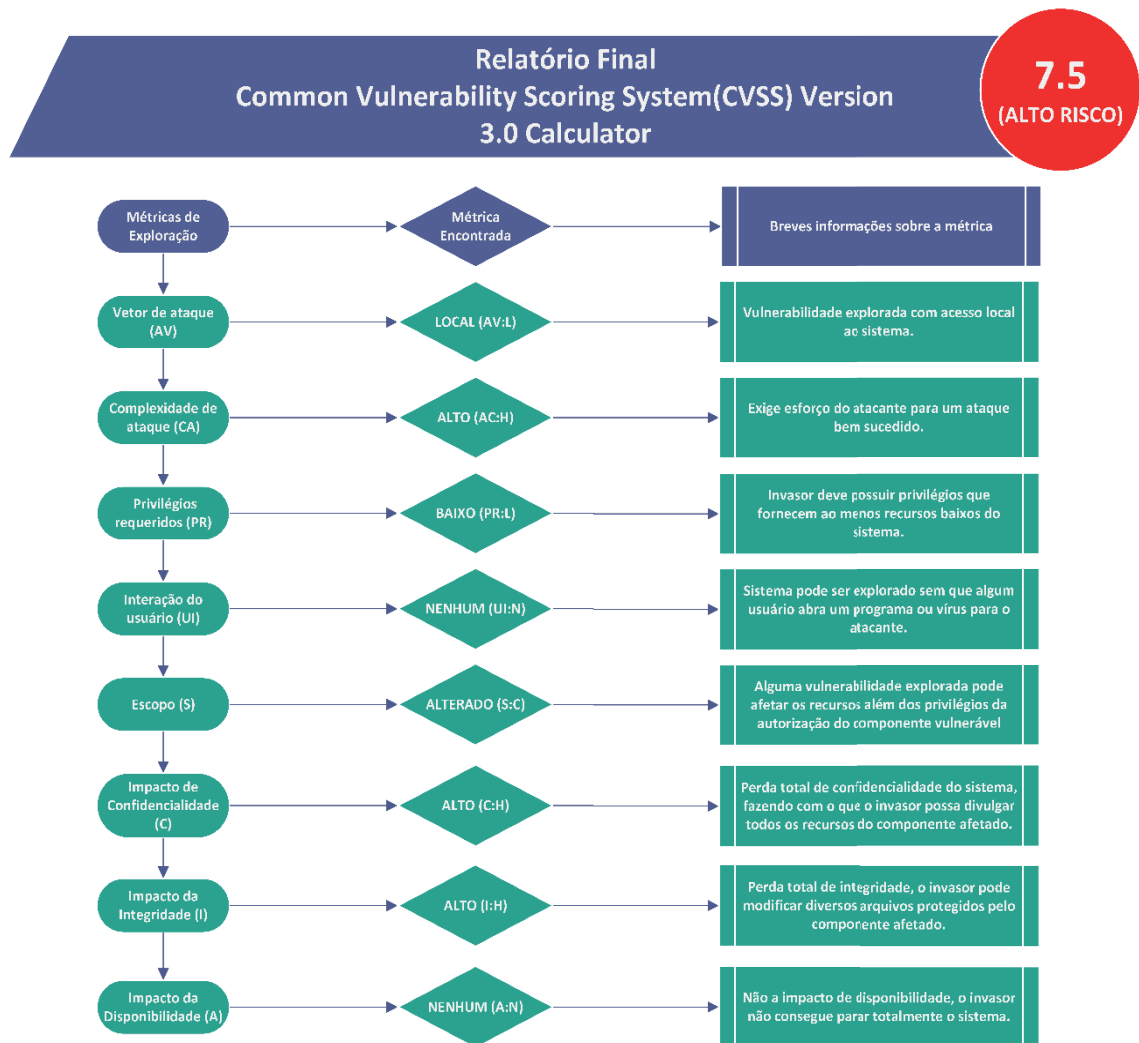


Figura 3. Relatório final CVSS

Por fim elaborar o relatório final com intuito de identificar e catalogar todas as vulnerabilidades envolvidas no sistema, irregularidades, possíveis abordagens de melhorias e resoluções de problema, para isso utilizaremos o *Common Vulnerability Scoring System (CVSS)*, um relatório que produz uma pontuação numérica que reflita a gravidade das vulnerabilidades encontradas. Esta pontuação consiste em representar as vulnerabilidades como (baixa, média, alta e crítica), podendo assim ajudar as organizações de como avaliar e priorizar adequadamente o processo de gerenciamento de suas vulnerabilidades. Na Figura 3 apresenta-se o relatório que foi construído durante o projeto.

Conforme a Figura 3, podemos observar as métricas adotadas pelo CVSS, onde podemos identificar as métricas de exploração e baseado na resposta geramos um *Score* da rede em questão, em nosso trabalho, nosso laboratório teste apresentou uma nota de 7.5 de risco, considerada Alto Risco segundo o CVSS.

5 | CONSIDERAÇÕES FINAIS

Com a realização de uma análise de intrusão em uma rede corporativa em testes de *pentest*, podemos identificar uma metodologia eficaz no processo de *pentest* do tipo *Gray Box* utilizando nosso processo no fluxograma apresentado na Figura 2. Destacamos ainda a utilização de uma ferramenta gratuita, o *Kali Linux*, composto por diversas ferramentas capazes de auxiliar em nosso projeto, a fim de obter informações sobre vulnerabilidades.

Podemos destacar que nenhuma aplicação está perfeitamente segura e livre de ataques, mas com o uso de técnicas ou testes de intrusão (*Pentesting*) diversas destas vulnerabilidades podem ser encontradas e superadas, evitando ataques que visam minar a integridade e confiabilidade dos dados que eles manipulam.

É importante trabalhar com um risco reduzido e segurança dentro da organização, garantindo integridade de arquivos, visto que o avanço da tecnologia tem gerado diariamente inúmeras vulnerabilidades de segurança de rede.

O objetivo deste trabalho foi demonstrar um estudo de métodos de intrusão de redes (*Pentesting*) em uma rede de computadores corporativa, convencendo as empresas da necessidade de segurança em suas organizações.

REFERÊNCIAS

Cert.br 2020 “Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil”. Available at [<https://www.cert.br>].

CVE 2020 “Common Vulnerabilities and Exposures”. Available at [<https://cve.mitre.org/>].

CVSS 2020 “Common Vulnerability Scoring System SIG”. Available at [<https://www.first.org/cvss/>].

Gutmann, Peter; Naccache, David; Palmer, Charles C. (2010) – “Opportunities in White-Box Cryptography”. IEEE Computer and Reliability Societies.

Jimenez, Rina Elizabeth Lopez de. (2016) “Pentesting on Web Applications using Ethical – Hacking”.

Kali Linux 2020 “Penetration Testing and Ethical Hacking Linux Distribution”. Available at [<https://www.kali.org>].

Landwehr, Carl E. (2001) “Computer security”.

Marques, Glenio Leitão Filho (2010) – “Hackers e Crackers na internet: as duas faces da moeda”.

OWASP 2020 “The Open Web Application Security Project”. Available at [<https://www.owasp.org>].

PENTESTIT 2020 “Penetration Testing Laboratories”. Available at [<https://lab.pentestit.ru>].

Rahimpour, Ebrahim; Rashtchi, Vahid; Aghmasheh, Reza (2017) – “Parameters Estimation of Transformers Gray Box Model”

Stalling, Willian. (2006) “Criptografia e segurança de redes”, vol. 4.

Yahya, Fara; Walters, Robert J.; Wills, Gary B. (2015) "Analysing Threats in Cloud Storage". World Congress on Internet Security (WorldCIS-2015), pp. 44–48.

ÍNDICE REMISSIVO

SÍMBOLOS

5G 69, 70, 71, 73, 74, 75, 76, 77, 78, 79, 95, 96

A

Antenas de microfita 95, 96, 107

Ataques de rede 130

Automação 2, 40, 59, 69, 70, 71, 72, 73, 74, 75, 79, 80, 159, 163, 167, 168, 260

C

Chave 2, 17, 26, 37, 40, 54, 69, 74, 75, 82, 96, 108, 130, 139, 151, 157, 170, 190, 201, 213, 216, 224, 236, 253

Computação 95, 129, 139, 140, 141, 152, 153, 156, 190, 192, 198, 200, 211, 260

Comunicação 1, 4, 5, 14, 22, 23, 24, 28, 36, 57, 69, 70, 71, 74, 76, 77, 81, 95, 96, 97, 99, 102, 106, 111, 112, 121, 122, 124, 130, 132, 133, 226, 260

Controle 1, 2, 3, 4, 5, 9, 15, 16, 23, 24, 26, 27, 29, 32, 33, 34, 36, 38, 40, 41, 47, 49, 50, 51, 52, 54, 55, 58, 64, 65, 73, 75, 77, 133, 158, 159, 163, 165, 166, 167, 168, 225, 227, 228, 234, 253, 256, 261, 264

CyberSegurança 130

D

Desempenho 4, 34, 57, 58, 68, 69, 75, 82, 95, 99, 106, 109, 112, 113, 114, 117, 120, 122, 123, 125, 139, 142, 144, 145, 149, 153, 170, 171, 172, 174, 175, 176, 188, 202, 203, 209, 215, 261

Dinâmico 1, 2, 3, 4, 5, 6, 15, 252

E

Equação polar 96, 97, 98, 99

Equilíbrio 1, 2, 3, 4, 5, 142, 171, 172, 173, 175

F

Fauna 17, 18, 25

Filtro de Kalman 1, 2, 5, 10, 12, 14, 15

I

Indicadores 18, 37, 55, 69, 76, 77, 117, 141, 199

Informação 27, 28, 29, 32, 36, 58, 62, 67, 77, 111, 121, 130, 131, 133, 135, 151, 152, 153, 154, 156, 193, 199, 210, 222, 224, 225, 227, 235, 254, 255

Irrigação 40, 41, 45, 46, 47, 50, 52, 53

L

LQR 1, 2, 5, 10, 13, 14, 15

M

Máquinas virtuais 139, 141, 142, 143, 144

Migração 139, 141, 142, 143, 144, 145, 148, 252

N

Nuvem 139, 140, 141, 142, 145

O

Osmose 40, 41, 43, 44, 45, 49, 51, 52

P

Pentest 130, 134, 135, 137

Programação linear inteira mista
139

Proteção 17, 134, 135, 172, 173, 179, 187

R

Redes corporativas 130, 131

Robô 1, 3, 4, 5, 6, 9, 15, 17, 18, 21, 22, 23, 24

S

Segurança 21, 22, 24, 25, 30, 34, 60, 64, 72, 73, 75, 130, 131, 132, 133, 135, 137, 151, 152, 153,
156, 158, 159, 160, 161, 164, 167, 168, 175, 177, 188, 193, 211, 235

Sem fio 41, 70, 71, 79, 95, 96, 97, 99, 102, 106

Simulink 1, 2, 3, 4, 5, 14, 15, 16

Sinalizador avifauna 17, 18

Sistemas verticais 69, 70

Super fórmula de Gielis 95, 96

T

Topologia distribuída 69, 77

 **Atena**
Editora

2 0 2 0