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

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*

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação: Camila Alves de Cremo
Edição de Arte: Lorena Prestes
Revisão: Os Autores

Atena Editora
Ano 2020

Atena Editora
Ano 2020

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

E57 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.

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

1. Ciência da computação – Pesquisa – Brasil. 2. Engenharia elétrica – Pesquisa – Brasil. I. Dallamuta, João. II. Holzmann, Henrique Ajuz. III. Granza, Marcelo Henrique.

CDD 623.3

Elaborado por Maurício Amormino Júnior – CRB6/2422

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

Atena Editora
Ano 2020

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 porem 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 espirito de parceria.

Boa leitura

João Dallamuta
Henrique Ajuz Holzmann
Marcelo Henrique Granza

SUMÁRIO

CAPÍTULO 10

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 coorporativas. 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 coorporativa 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 I 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 ARPNET, 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 (*Masschusetss 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].

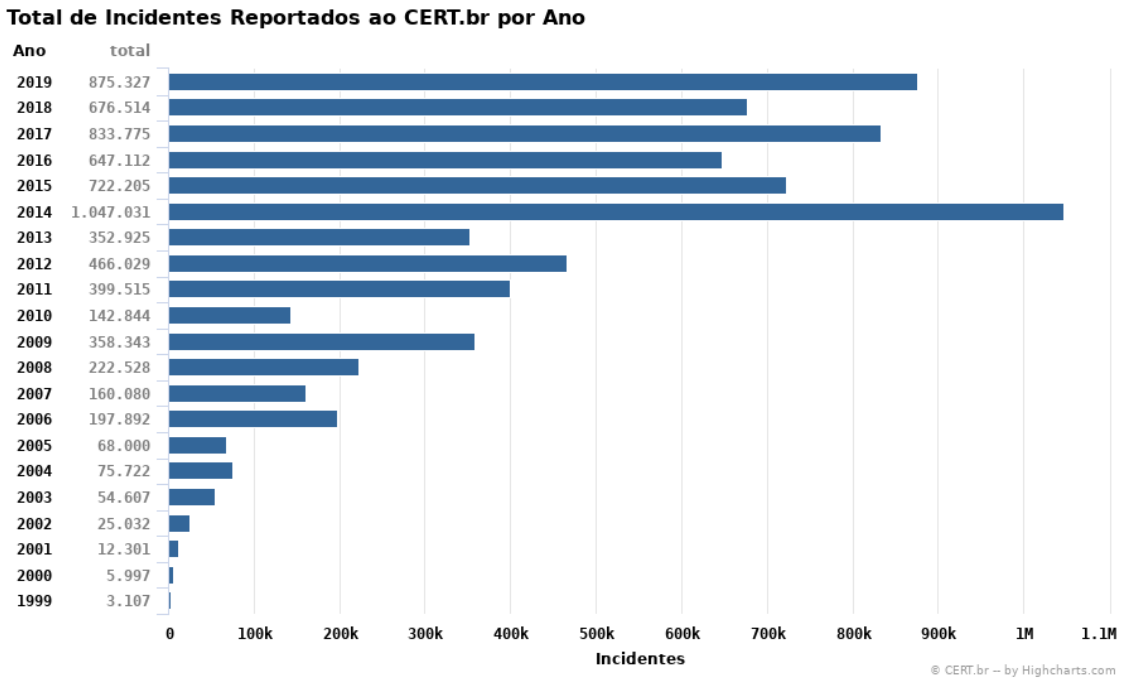

Figura 1. Total de Incidentes Reportados ao CERT.br por Ano [cert.br 2020].

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-repudio)**: 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 contribuí 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].

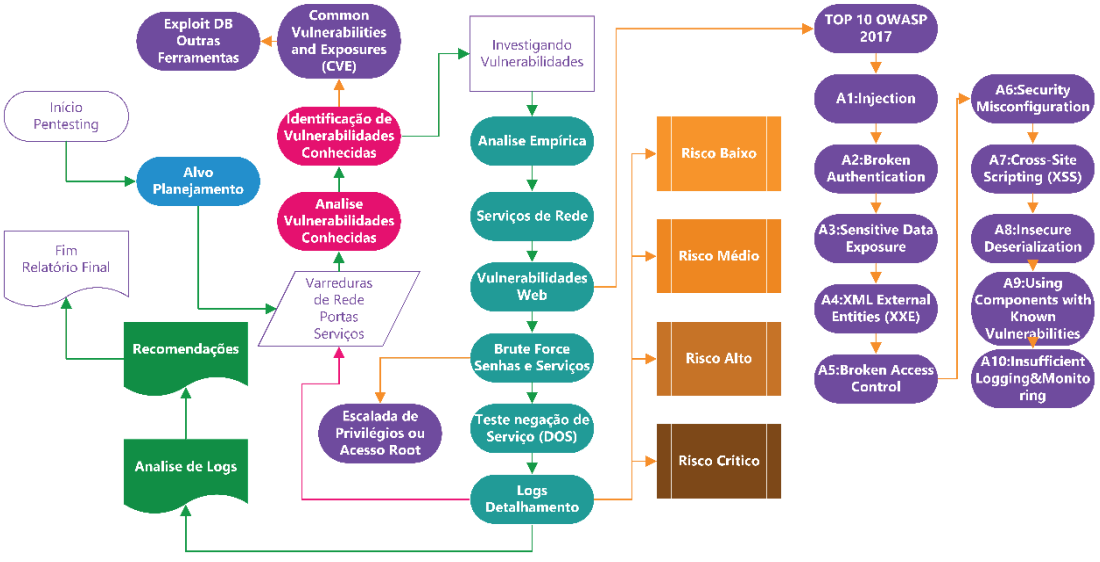

Figura 2. Etapas de *Pentesting*

3 I 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.

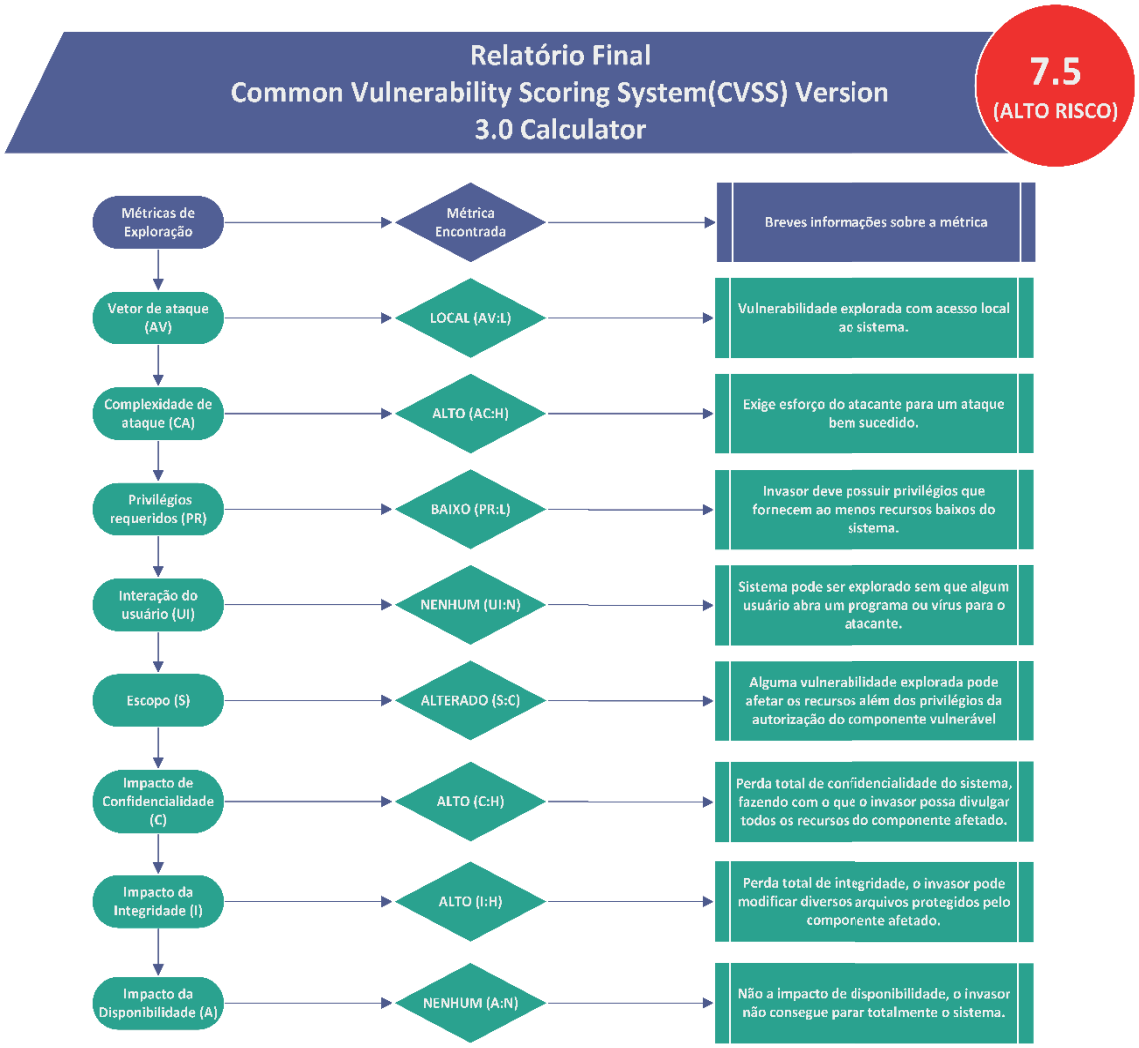

Figura 3. Relatório final CVSS

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 gravida das vulnerabilidades encontradas. Esta pontuação consiste em representar as vulnerabilidades como (baixa, média, alta e crítica), podendo assim ajudar as organizações de como avalizar 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 adotas 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 I 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 coorporativa, 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

A

C

D

E

F

I

L

M

N

O

P

R

S

T


Atena
Editora
2020