Análise de Vulnerabilidades em domínios

Raissa Rinaldi Yoshioka[1], Carlos Alberto da Silva[2]

[1]Curso de Bacharelado em Engenharia de Computação – Faculdade de Computação (FACOM)
[2]Faculdade de Computação (FACOM)
Universidade Federal de Mato Grosso do Sul (UFMS).
Av. Costa e Silva, s/n. - Bairro Universitário - CEP 79070-900 - Campo Grande - MS.

raissa.r.yoshioka@ufms.br, carlos.silva@ufms.br

Abstract. *This research aims to deepen knowledge in information security, highlighting the importance of vulnerability analysis and risk assessment in virtual environments. The Nmap and Nuclei tools present in the Kali Linux operating system were used to carry out testing and analysis of vulnerabilities in multiple sub-domains belonging to the same entity. This article presents the pentesting results and the vulnerabilities found.*

Resumo. *Esta pesquisa objetiva o aprofundamento do conhecimento em segurança da informação, destacando a importância da análise de vulnerabilidades e avaliação de riscos nos ambientes virtuais. Foram utilizadas as ferramentas Nmap e Nuclei presentes no sistema operacional Kali Linux para realizar os pentestings e análise das vulnerabilidades em múltiplos sub-domínios pertencentes a uma mesma entidade. O presente artigo apresenta os resultados dos pentestings e as vulnerabilidades encontradas.*

1. Introdução

Com o avanço da internet, serviços *web* vem crescendo de modo exponencial nos últimos anos e o tópico de segurança da informação têm entrado cada vez mais em destaque. A Segurança da Informação é uma área muito ampla, destinada a compreender e aprimorar estratégias e ações para proteger dados confidenciais, englobando a proteção tanto de ambientes digitais quanto físicos. Um termo que, por muitas vezes, pode ser confundido com segurança da informação é a chamada cibersegurança, que compreende exclusivamente a proteção de ativos digitais, atuando na antecipação e resposta efetiva contra ameaças cibernéticas.

Os princípios fundamentais em segurança da informação para manter os dados e ativos protegidos, segundo [Hintzbergen et al. 2018], são definidos como: confidencialidade, disponibilidade e integridade, onde confidencialidade se refere aos limites em termos de quem pode obter que tipo de informação, disponibilidade trata de a informação estar disponível sempre que necessário e integridade se refere a ser correto e consistente com o estado ou informação pretendida.

Esta pesquisa surge de um estudo de caso, ou experiência prática, realizada entre os meses de maio e junho de 2024, onde foi realizada uma análise de cibersegurança em múltiplos sub-domínios pertencentes a uma mesma entidade. Ao longo desta pesquisa, foram abordados aspectos fundamentais da execução de *pentesting* associados à descoberta e identificação de vulnerabilidades, por meio de ferramentas e técnicas utilizadas por agentes maliciosos para encontrar e explorar essas vulnerabilidades.

O resultado deste trabalho visa não apenas colaborar com o conhecimento acadêmico em relação à segurança da informação e cibersegurança, mas também, com uma avaliação dos riscos, que contribuirão para orientar e determinar as ações corretivas a fim de implementar as proteções contra as ameaças, destacando a importância de que a avaliação do risco deve ser repetida de modo periódico para tratar qualquer mudança de *hardware* e/ou *software* capaz de influenciar os riscos da segurança dos domínios analisados.

2. Conceitos Básicos

A fim de facilitar o entendimento e compreensão ao longo do artigo, esta seção é destinada a esclarecer conceitos básicos, metodologias e técnica que foram utilizadas ao longo da pesquisa em segurança computacional.

É apresentado o conceito de *google dorking*, que consiste em uma técnica de pesquisa onde é usado o buscador do Google para encontrar informações sensíveis e ocultas que podem não estar disponíveis por meio de consultas de pesquisa padrão.

Nesta pesquisa, são mostradas as vulnerabilidades confirmadas e é utilizado com frequência o termo CVE, do inglês *Common Vulnerabilities and Exposures*, que trata de um identificador utilizado para catalogar as vulnerabilidades individuais, com o intuito de facilitar o rastreamento e a referência de diferentes vulnerabilidades. Ao analisar cada vulnerabilidade, foram levados em consideração dois padrões relevantes para a área, sendo eles: o *CVSS (Common Vulnerability Scoring System)*, que, de acordo com [IBM 2024], é utilizado para classificar a severidade e o risco de segurança do sistema em relação à vulnerabilidade específica, seguindo uma escala de zero a dez, a fim de priorizar a correção de falhas com base na criticidade relacionada; e o *EPSS (Exploit Prediction Scoring System)*, que é utilizado para realizar a estimativa da probabilidade, entre o valor de zero a 100%, de exploração de uma determinada vulnerabilidade dentro de um período de 30 dias.

3. Metodologia

A metodologia abordada nesta pesquisa contou com a combinação entre uma técnica chamada Teste de Caixa Preta, ou ainda Teste Funcional, em que, de acordo com [Delamaro et al. 2007] é levado em consideração apenas o ponto de vista do usuário, sem nenhum conhecimento de estrutura interna ou de como a implementação foi realizada, juntamente com a elaboração de um plano teste, com o intuito de enumerar as diferentes falhas e vulnerabilidades encontradas. Com isso, os seguintes passos foram aplicados para o plano teste:

1. Realizar o planejamento, sendo definido o escopo e o domínio onde seriam realizados os *pen-testings*, bem como a instalação do Kali Linux (sistema operacional com foco em segurança e várias ferramentas inclusas em seu pacote);
2. Coleta de informações, com a utilização da técnica *google dorking*, para encontrar endereços de sub-domínios inclusos no domínio analisado e possíveis informações ocultas na rede, bem como análise manual dos *sites*;
3. Análise dos sub-domínios, utilizando ferramentas automatizadas como Nmap [Nmap 2024] e Nuclei [Nuclei 2024] em busca de mais informações dos sub-domínios;
4. Pesquisa sobre as vulnerabilidades, a fim analisar as falhas e determinar quais se encaixavam nas especificações de cada *web site* verificado, além de classificar a severidade de acordo com os padrões *CVSS (Common Vulnerability Scoring System)* e *EPSS (Exploit Prediction Scoring System)*;
5. Revisão e observação geral, onde foi realizada uma análise das vulnerabilidades e falhas encontradas utilizando fontes como *NVD (National Vulnerability Database)* [NVD 2024], *CVEdetails* [CVEdetails 2024], *Tenable* [Tenable 2024e] e *Qualys Threat Protection* [Qualys 2024], que são especializados na classificação e descrição de vulnerabilidades conhecidas.

4. Ferramentas

As ferramentas utilizadas nesta pesquisa foram o sistema operacional Kali Linux [Linux 2023], o hipervisor VirtualBox [Oracle 2023], responsável pela criação do ambiente de máquina virtual (VM) onde o sistema operacional Kali Linux foi instalado e, então, as ferramentas Nmap e Nuclei, que vêm integrados na distribuição do Kali Linux.

4.1. Kali Linux

O Kali Linux é uma distribuição Linux de código aberto, baseada no sistema operacional Debian, capaz de rodar em várias plataformas, oferece amplo suporte para dispositivos e está disponível em [Linux 2023].

Essa distribuição possui centenas de ferramentas que permite aos usuários executar *pentesting* avançado e auditoria de segurança, bem como tarefas, como exemplo, de análise forense de computadores, engenharia reversa e detecção de vulnerabilidades.

4.2. Ferramenta Nmap

Nmap é uma ferramenta de código aberto para escaneamento de rede e auditorias de segurança, cuja principal função, de acordo com [Lyon 2009], é realizar uma varredura em portas *TCP (Transmission Control Protocol)*, onde a resposta para essa varredura pode ser classificada como os estados: *open* (aberta), *closed* (fechada), *filtered* (filtrada), *unfiltered* (não filtrada) ou uma combinação entre dois estados, como por exemplo *open / filtered* e *closed / filtered*. A ferramenta, ainda segundo [Orebaugh and Pinkard 2008] segue principalmente quatro técnicas básicas:

- **Mapeamento de rede**, que se trata do envio de mensagens para um host onde uma resposta será gerada se o host estiver ativo;
- **Escaneamento de portas**, realiza o envio de mensagens para uma porta específica a fim de determinar se ela está ativa;
- **Detecção de serviço e versionamento**, faz o envio de mensagens criadas especialmente para portas ativas com o intuito de gerar respostas que indicarão o tipo e a versão do serviço em execução;
- **Detecção de sistema operacional**, realiza o envio de mensagens criadas especificamente para um host ativo a fim de gerar determinadas respostas que indicarão o tipo de sistema operacional em execução no host.

A ferramenta Nmap possui uma extensa comunidade de contribuidores, com o objetivo de melhorar a ferramenta e suas funcionalidades a cada nova versão e está disponível em [Nmap 2024].

4.3. Ferramenta Nuclei

Nuclei é uma ferramenta para escaneamento direcionado, que pode ser configurável com base em *templates* que oferecem grande extensibilidade e facilidade de uso, a ferramenta está disponível em [Nuclei 2024].

Esta ferramenta é utilizada, em sua maioria, para enviar solicitações entre alvos usando como base um modelo que leva a um mínimo de falsos positivos e sendo possível realizar diferentes varreduras em um grande número de hosts e em uma variedade de protocolos, incluindo *TCP (Transmission Control Protocol)*, *DNS (Domain Name System)* e *HTTP (Hipertext Transfer Protocol)*.

Com *templates* flexíveis, todos os tipos de verificações de segurança podem ser modelados com o Nuclei, que é uma ferramenta de código aberto e possui uma grande comunidade de contribuidores.

5. Resultados Obtidos

Ao longo desta seção será discorrido acerca das vulnerabilidades identificadas, apresentando detalhes sobre CVEs específicas e severidades relacionadas, bem como a falta de algumas configurações cruciais encontradas nos sub-domínios testados. Para fins de sigilo, nenhum dado viável para identificação da empresa será divulgado.

5.1. Vulnerabilidades Confirmadas

Este tópico trata da apresentação das vulnerabilidades identificadas ao longo do estudo prático realizado, destacando que as vulnerabilidades informadas são aquelas que são esclarecidamente confirmadas por dependerem de um estado obrigatório na aplicação e não foram inclusas as vulnerabilidades que dependem de múltiplos fatores, como módulos ou configurações específicas.

Como já foi citado anteriormente, ao realizar a análise das vulnerabilidades, esta pesquisa seguiu dois padrões comuns em relação à CVEs, sendo eles o *CVSS*, que segue uma escala de zero a dez para priorizar a correção de falhas com base na criticidade relacionada, em que zero é a classificação mais baixa e dez a mais crítica, e o *EPSS*, que calcula a probabilidade, de zero a 100%, de uma determinada vulnerabilidade ser explorada dentro de um período de 30 dias.

Por meio da ferramenta Nmap [Nmap 2024] foi possível encontrar as versões das aplicações utilizadas nos múltiplos sub-domínios analisados e, em alguns deles, foram encontradas diferentes versões desatualizadas do Apache, que é um servidor HTTP que atualmente tem sua versão mais recente como 2.4.62 [Apache 2024], também foram encontradas versões desatualizadas do OpenSSH, que é uma ferramenta de conectividade para login remoto utilizando o protocolo SSH, criptografando o tráfego de informações na rede, cuja versão mais recente consta como a 9.8p1 [OpenSSH 2024].

No total, houveram cinco vulnerabilidades confirmadas e a Tabela 1 mostrada a seguir apresenta as vulnerabilidades encontradas, juntamente com seus respectivos códigos CVE e valores de *CVSS* e *EPSS* relacionadas a cada uma.

Tabela 1. Tabela das Vulnerabilidades Confirmadas

Objeto	Vulnerabilidade	Código CVE	CVSS	EPSS
Apache	Denial of Service (DoS) issue in HTTP/2	CVE-2023-43622	Alto	0,06
	Security Update for module HTTP/2	CVE-2024-27316	Alto	0,46
OpenSSH	Potential information leak	CVE-2016-20012	Médio	0,59
	SSH Attack Surface	CVE-2023-48795	Médio	96,57
	SSH Unexpected Code Execution Vulnerability	CVE-2023-51385	Crítico	0,27

Vale ressaltar que, como todas as CVEs confirmadas nessa pesquisa são conhecidas, suas respectivas soluções também são conhecidas e, a seguir, será explicado brevemente do que cada vulnerabilidade informada na Tabela 1 trata:

- **CVE-2023-43622**: essa vulnerabilidade afeta o protocolo HTTP/2 e torna o ativo suscetível a um ataque *DDoS (Distributed Denial of Service)*, ou ataque de negação de serviço distribuído, que acontece pelo envio infinito de *frames* até resultar no esgotamento de recursos e sobrecarga do servidor;
- **CVE-2024-27316**: referente ao protocolo HTTP/2, torna o ativo suscetível a um ataque *DoS (Denial of Service)*, ou ataque de negação de serviço, que ocorre pelo envio infinito de *frames* para a aplicação até levar ao esgotamento de memória e interrupção de serviços *online*;
- **CVE-2016-20012**: essa vulnerabilidade está relacionada ao protocolo SSH e pode levar a um potencial vazamento de informações, pois permite descobrir se uma informação de login na aplicação é válida ou não;
- **CVE-2023-48795**: referente ao protocolo SSH, essa vulnerabilidade ficou conhecida como Ataque Terrapin, e acontece pelo fato de possibilitar, dependendo de um estado específico da aplicação, a redução do protocolo SSH e levar ao acesso não autorizado à informações confidenciais;
- **CVE-2023-51385**: essa vulnerabilidade afeta o protocolo SSH e torna o ativo suscetível a um *shell injection*, que basicamente permite a execução de comandos do sistema operacional no servidor que executa a aplicação, possivelmente comprometendo os dados da aplicação.

5.2. Falta de Cabeçalhos de Segurança Web

Durante o escaneamento dos sub-domínios testados nesta pesquisa, a ferramenta Nuclei [Nuclei 2024] encontrou a falta de diversos cabeçalhos de segurança HTTP *(HTTP Security Headers)*. Muitos desses cabeçalhos servem para proteger usuários e servidores *web* de atacantes maliciosos.

Dentre os diversos cabeçalhos em falta, que possuem uma grande importância nos sub-domínios, é importante destacar esses quatro listados abaixo, pois a falta desses cabeçalhos culminam em *CVSS* de severidades média ou baixa:

- **Content Security Policy** [Tenable 2024a] é um padrão de segurança em domínios *web*, que fornece mecanismos para que os *websites* possam restringir o conteúdo ao qual os navegadores têm acesso e serve para reduzir ataques do tipo *cross-site-scripting (XSS)*, onde um agente malicioso manipula um site vulnerável para que retorne *scripts* maliciosos aos usuários, obtendo acesso a informações confidenciais retidas pelo navegador;
- **Strict Transport Security Policy** [Tenable 2024b] é um cabeçalho que serve para instruir o navegador a se comunicar apenas por meio do *HTTPS*, que é mais seguro que o *HTTP*, por encapsular os dados e evitar ataques de interceptação entre cliente e servidor;
- **X-Frame-Options** [Tenable 2024d] é um cabeçalho utilizado para indicar se um navegador deve, ou não, ser permitido para renderizar uma página em um *frame* ou *iframe*, evitando ataques como *clickjacking*, que é uma técnica para levar um usuário na *web* a clicar em algo diferente do indicado, possibilitando a revelação de informações confidenciais;
- **X-Content-Type-Options** [Tenable 2024c] é um cabeçalho do tipo resposta usado pelo servidor para indicar quais os tipos de formatos de mensagens que devem ser seguidos sem alteração, cuja falta deixa o ativo vulnerável a ataques como *cross-site scripting (XSS)*.

5.3. Resumo das Vulnerabilidades Confirmadas por Domínio

Com o objetivo de não identificar os domínios fisicamente, será adotado apenas a nomenclatura de D1 para o Domínio 1, até D8 para o Domínio 8 analisado. Na Tabela 2, é apresentado o resultado das vulnerabilidades por domínio.

Tabela 2. As Vulnerabilidades Confirmadas por Domínios

Código CVE	Vulnerabilidade	D1	D2	D3	D4	D5	D6	D7	D8
CVE-2023-43622	Denial of Service (DoS) issue in HTTP/2	X							
CVE-2024-27316	Security Update for module HTTP/2	X							
CVE-2016-20012	Potential information leak	X	X	X	X	X	X	X	X
CVE-2023-48795	SSH Attack Surface		X		X		X		
CVE-2023-51385	SSH Unexpected Code Execution				X				

6. Conclusão

Esta pesquisa buscou demonstrar os aspectos fundamentais para a segurança da informação, apresentando vulnerabilidades e falhas encontradas com a utilização de técnicas e ferramentas disponíveis para qualquer um. Foi realizada uma análise utilizando os resultados de um estudo prático e, como foi utilizada a técnica de pentesting de caixa preta, em que não havia nenhum conhecimento sobre a implementação realizada dentro de cada aplicação analisada, é possível que hajam outras falhas e vulnerabilidades além das destacadas neste artigo. Este estudo não só contribuiu para colaborar com o conhecimento acadêmico na área de segurança da informação, mas também destacou a importância de que sejam realizadas análises periódicas em busca de vulnerabilidades a fim de manter a segurança de qualquer empresa ou instituição, compreendendo a necessidade de manter os três príncipios fundamentais da segurança da informação: a confidencialidade, a integridade e a disponibilidade.

Este trabalho é apenas o começo de uma jornada constante em busca de ambientes *webs* com mais proteções e garantias contra ataques maliciosos, permitindo, assim, aprender e aprimorar a cada novo avanço da internet e de serviços *web*.

Referências

[Apache 2024] Apache (2024). Apache http server project. https://httpd.apache.org/download.cgi. Acessado em 17 julho de 2024.

[CVEdetails 2024] CVEdetails (2024). Cvedetails. https://www.cvedetails.com/. Acessado entre maio e junho de 2024.

[Delamaro et al. 2007] Delamaro, M. E., Maldonado, J. C., and Jino, M. (2007). *Introdução ao Teste de Software*. Elsevier Editora Ltda., Rio de Janeiro, RJ.

[Hintzbergen et al. 2018] Hintzbergen, J., Hintzbergen, K., Smulders, A., and Baars, H. (2018). *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. BRASPORT Livros e Multimídia Ltda., Rio de Janeiro, RJ.

[IBM 2024] IBM (2024). Commons vulnerability score (cvss). https://www.ibm.com/docs/en/qradar-on-cloud?topic=vulnerabilities-common-vulnerability-scoring-system-cvss. Acessado em julho de 2024.

[Linux 2023] Linux, K. (2023). Kali linux. https://www.kali.org/. Acessado em novembro de 2023.

[Lyon 2009] Lyon, G. F. (2009). *Exame de Redes com Nmap*. Editora Ciência Moderna Ltda, Rio de Janeiro, RJ.

[Nmap 2024] Nmap (2024). Nmap. https://www.kali.org/tools/nmap/. Acessado em maio de 2024.

[Nuclei 2024] Nuclei (2024). Nuclei. https://www.kali.org/tools/nuclei/. Acessado em maio de 2024.

[NVD 2024] NVD (2024). National vulnerability database. https://nvd.nist.gov/vuln. Acessado entre maio e junho de 2024.

[OpenSSH 2024] OpenSSH (2024). Openssh. https://www.openssh.com/. Acessado em 17 julho de 2024.

[Oracle 2023] Oracle (2023). Oracle vm virtualbox. https://www.virtualbox.org/. Acessado em outubro de 2023.

[Orebaugh and Pinkard 2008] Orebaugh, A. and Pinkard, B. (2008). *Nmap in the Enterprise: Your Guide to Network Scanning*. Syngress Publishing, Burlington, MA.

[Qualys 2024] Qualys (2024). Threat protection. https://threatprotect.qualys.com/. Acessado entre maio e junho de 2024.

[Tenable 2024a] Tenable (2024a). Missing content security policy. https://www.tenable.com/plugins/was/112551. Acessado em julho de 2024.

[Tenable 2024b] Tenable (2024b). Missing http strict transport security policy. https://www.tenable.com/plugins/was/98056. Acessado em julho de 2024.

[Tenable 2024c] Tenable (2024c). Missing 'x-content-type-options' header. https://www.tenable.com/plugins/was/112529. Acessado em julho de 2024.

[Tenable 2024d] Tenable (2024d). Missing 'x-frame-options' header. https://www.tenable.com/plugins/was/98060. Acessado em julho de 2024.

[Tenable 2024e] Tenable (2024e). Tenable. https://www.tenable.com/. Acessado entre maio e julho de 2024.