ExeKaliBurr: uma Ferramenta Exploratória Auxiliar para o Levantamento de Informações em Pentests Web

Daniel R. Barros[1], **Saskya A. Pimenta**[1], **Lincoln S. Rocha** [1], **José M. Monteiro**[1]

[1]Laboratório de Sistemas e Bancos de Dados (LSBD)
Departamento de Computação (DC)
Universidade Federal do Ceará (UFC) – Fortaleza, CE – Brasil

daniel.rezende@lsbd.ufc.br, saskya.alves@lsbd.ufc.br

lincoln@dc.ufc.br, jose.monteiro@lsbd.ufc.br

Abstract. *The Pentest is one of the main approaches within the Offensive Security area, an important sector of Cybersecurity that seeks to improve the protection and reliability of virtual systems through proactive security checks. During the execution of a Pentest, the security professional carries out a series of steps to perform the procedures, and one of these steps is called the Information Gathering phase. This work proposes an exploratory tool capable of working together with security professionals to facilitate and automate the manual searches that are carried out during the execution of the Information Gathering phase, thus providing greater convenience during the completion of this stage.*

Resumo. *O Pentest ou Teste de Intrusão é uma das principais abordagens existentes dentro da área da Segurança Ofensiva, um importante setor da Segurança Cibernética, que busca aperfeiçoar a proteção e confiabilidade de sistemas virtuais por meio de técnicas proativas em verificações de segurança. Durante a execução de um Pentest, o profissional de segurança efetua uma série de etapas para a realização dos procedimentos, uma dessas etapas é chamada fase de Levantamento de Informações. Esse trabalho propõe uma ferramenta exploratória capaz de atuar em conjunto com os profissionais de segurança, para facilitar e automatizar as buscas manuais que são realizadas ao longo da execução do Levantamento de Informações, proporcionando assim uma maior praticidade durante a conclusão dessa etapa.*

1. Introdução

A Segurança Cibernética é uma área de grande importância no atual cenário tecnológico mundial, devido ao crescente número de ameaças virtuais e descobertas de vulnerabilidades em diversas tecnologias. Vulnerabilidades são definidas como fraquezas ou falhas em processos, componentes ou procedimentos que podem ser exploradas para causar violações de segurança e comprometer a integridade de sistemas virtuais [Force 2018]. Entender como defender as infraestruturas sensíveis não é suficiente, também torna-se necessário a criação de técnicas e ferramentas para atuar especificamente na área da Segurança Cibernética [Stuttard 2011].

Como posto [Walker 2013], os profissionais de segurança são responsáveis por garantir a proteção dos sistemas computadorizados contra diversos tipos de ataques virtuais, para isso são utilizadas estratégias e metodologias focadas no desenvolvimento de novas camadas de proteção introduzidas nesses sistemas, como é o exemplo do *Pentest*.

Segundo [Weidman 2014], um *Pentest* ou Teste de Intrusão, pode ser definido como uma simulação de ataques reais, destinada a avaliar os riscos e impactos associados às brechas de segurança em um sistema. Diferente de uma auditoria de segurança comum, onde o objetivo é o controle predefinido de ameaças e identificação das vulnerabilidades, a finalidade de um *Pentest* vai além, por conta da utilização de abordagens praticadas pelos atacantes, para não somente simular ações criminosas mas também explorá-las ao máximo. Podemos observar todas as etapas do *Pentest* na Figura 1.

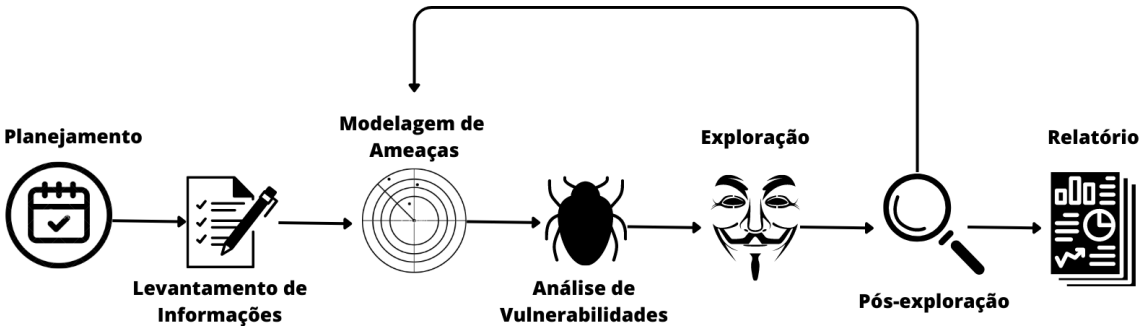

Figura 1. Etapas das atividades no *Pentest*

Este artigo apresenta o ExeKaliBurr, uma ferramenta exploratória focada na etapa do Levantamento de Informações. O ExeKaliBurr facilita a conclusão dessa etapa através da automatização dos processos de busca, resultando em uma maior praticidade para os profissionais de segurança durante a execução de um *Pentest*.

Os capítulos do estudo estão organizados da seguinte forma: A Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve a arquitetura e as principais funcionalidades do ExeKaliBurr. A Seção 4 expõe a implementação da ferramenta. A Seção 5 apresenta resultados obtidos em um experimento real. Por fim, detalhamos a demonstração planejada para o Salão de Ferramentas e considerações finais na Seção 6.

2. Trabalhos Relacionados

Em [Edwards 2019] é destacado a escassez de profissionais nas equipes *Red Team*, grupos compostos por especialistas focados na Segurança Ofensiva. Os autores relatam a necessidade da criação de uma ferramenta automatizada, para suprir a ausência desses profissionais. A proposta do trabalho descreve um simulador de *Pentest* completo, mas apresenta pré-requisitos para seu funcionamento, por se tratar de uma verificação de segurança na categoria *White Box*, cenário onde os especialistas já possuem informações e acesso livre ao sistema-alvo.

No trabalho realizado por [Laxmi Kowta et al. 2021], é feita uma análise sobre o Levantamento de Informações, com exemplos práticos da utilização de ferramentas exploratórias executadas separadamente. Os autores do trabalho descrevem a etapa do Levantamento de Informações como uma atividade primordial para a cadeia de processos em um *Pentest*, envolvendo a identificação e reconhecimento dos dados sensíveis.

Em paralelo aos trabalhos anteriores, o ExeKaliBurr apresenta alguns diferenciais em sua aplicação. Ao contrário da ferramenta proposta por [Edwards 2019], o ExeKaliBurr opera na categoria *Black Box*, onde não é necessário o conhecimento prévio de informações privilegiadas sobre o alvo analisado.

Da mesma forma que [Laxmi Kowta et al. 2021], o ExeKaliBurr trabalha com um conjunto de ferramentas exploratórias, porém ele é capaz de orquestrar essas ferramentas fazendo com que elas operem de forma sequencial e automatizada. A Tabela 1 exibe as características das ferramentas comparadas.

Ferramenta	Categoria	Modo de Execução	Completude do Pentest
Edwards 2019	*White Box*	Automatizada	Completo
Laxmi Kowta et al. 2021	*Black Box*	Manual	Parcial
ExeKaliBurr	*Black Box*	Automatizada	Parcial

Tabela 1. Comparações entre ferramentas

3. Arquitetura

Nessa Seção são exibidas as etapas e funcionalidades que compõe o esquema de execução do ExeKaliBurr. Na Figura 2 descrevemos todos os fluxos de funcionamento da ferramenta apresentada.

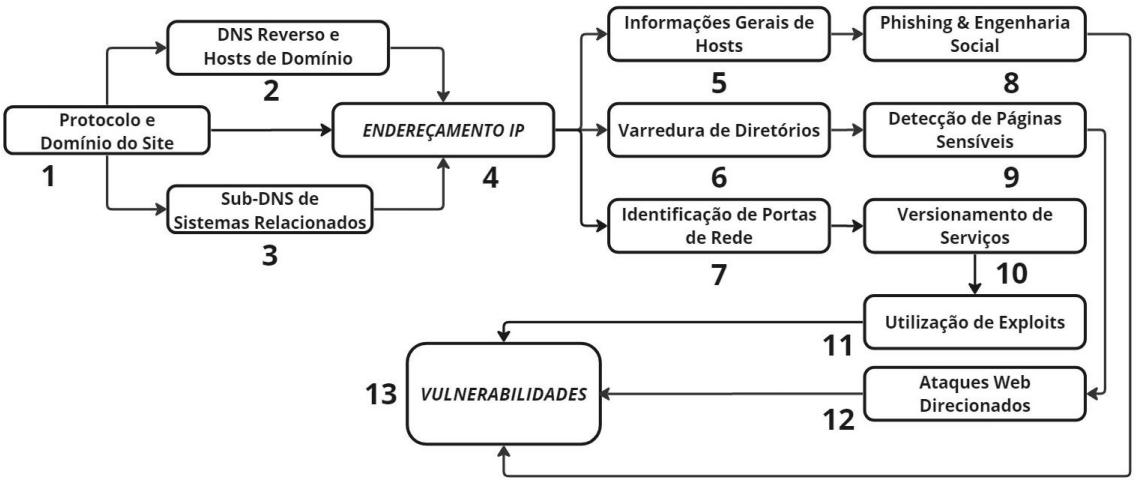

Figura 2. Fluxo de processos no Levantamento de Informações do ExeKaliBurr

A partir do protocolo de comunicação e nome de domínio do site, apontados pela etapa 1 da Figura 2, o ExeKaliBurr desencadeia seu *pipeline* de exploração iniciando varreduras em busca de mais informações sobre o alvo determinado. A ferramenta inicia com pesquisas relacionadas a identificação de endereços *IP* (*Internet Protocol*), enumeração de *DNS* (*Domain Name System*) e sub-sistemas integrados ao alvo analisado, como visto nas etapas 2, 3 e 4 da Figura 2.

Após obter informações a respeito dos endereçamentos *IP* vinculados ao alvo, o ExeKaliBurr segue com explorações mais profundas abordando três principais tópicos, para analisar possíveis vulnerabilidades não detectadas. Os tópicos mencionados são:

1. **Detecção de Serviços em Portas de Rede:** Um método para identificar e obter as versões das tecnologias específicas que estão sendo executadas na infraestrutura do alvo. Cenário onde um agente malicioso poderia capturar essas informações e a partir delas, realizar abordagens para explorar falhas nesses serviços.

Fluxo de exploração $\{1, 4, 7, 10, 11, 13\}$ descrito pela Figura 2.

2. **Varredura de Diretórios Ocultos:** Funcionalidade que tem como objetivo, revelar todas as páginas e diretórios ocultos relacionados ao sistema-alvo. Através dessa ação, um agente malicioso pode adquirir novas superfícies de ataque ao encontrar páginas que não devem ser acessadas por usuários comuns, como painéis de *login* de funcionários ou serviços para transmissão de arquivos do sistema. Fluxo de exploração $\{1, 4, 6, 9, 12, 13\}$ descrito pela Figura 2.

3. **Vazamento Impróprio de Informações:** Caso em que um atacante, por sua vez, muda a forma de atuação e redireciona suas abordagens para focar nos funcionários e administradores do serviço. Esses tipos de ataques podem ser caracterizados por golpes de *Engenharia Social* ou *Spear Phishing*, como descritos por [Dewan et al. 2014]. Quando o agente malicioso busca obter informações privilegiadas através de dados básicos verdadeiros que podem ser descobertos por meio do Levantamento de Informações. Fluxo de exploração $\{1, 4, 5, 8, 13\}$ descrito pela Figura 2.

4. Implementação

Nessa Seção iremos abordar os detalhes da implementação do ExeKaliBurr, para descrever os métodos e softwares que foram utilizados na construção das funcionalidades e dos fluxos de exploração existentes na ferramenta.

A base para efetuar a implementação do ExeKaliBurr foi o sistema operacional Kali Linux[1], uma distribuição GNU/Linux baseada na arquitetura Debian. A partir disso foi possível desenvolver um programa em *Shell Script*, utilizado para orquestrar os recursos e softwares que vieram nativos da versão 2023.2 no sistema Kali Linux. Os processos e ferramentas utilizadas na criação do ExeKaliBurr são:

- **1** - Fase inicial da execução, inserção dos parâmetros nome de domínio do site e protocolo de comunicação cliente/servidor utilizado (*http* ou *https*).
- **2 e 3** - Explorações recursivas via *DNS Reverso* e *Sub-DNS*, para verificar a existência de sistemas relacionados ao alvo principal. Os softwares *DNSRecon* e *DNSMap* são utilizados nessa etapa.
- **4** - Descoberta de endereçamentos *IP* relacionados ao site alvo. Ferramentas utilizadas foram *WhatWeb* e *Host*.
- **5 e 8** - Coleta de informações gerais. Dados como nomes de proprietários, empresas ou funcionários, e-mails de contato, informações específicas que podem ser utilizadas como base para ataques maliciosos. Os buscadores de dados utilizados nesse passo foram *WhatWeb*, *WhoIs* e *CURL*.
- **6, 9 e 12** - Investigação de diretórios por meio de verificações *Brute Force* em possíveis páginas *Web*, utilizando os softwares *DIRB* e *GoBuster* para a detecção páginas ocultas suscetíveis à falhas de segurança.
- **7, 10 e 11** - Identificação e versionamento dos serviços que estão sendo utilizados pela infraestrutura do alvo, procedimento realizado pela ferramenta *NMAP*.

[1] https://www.kali.org/

Detecção de possíveis falhas de segurança através da utilização de vulnerabilidades conhecidas e documentadas (*Exploits*), estratégia muito utilizada nos casos onde o sistema analisado possui serviços desatualizados em execução.

5. Experimentos

Nessa Seção iremos descrever a aplicabilidade do ExeKaliBurr em um cenário real e em seguida, apresentar alguns resultados obtidos através da utilização da ferramenta. Por meio dessa abordagem, iremos demonstrar o potencial da ferramenta durante a realização do processo de Levantamento de Informações.

5.1. Alvo de Exploração

Para realização dos experimentos, foi selecionado o sistema *Web* pertencente a uma empresa de grande porte, no ramo de comércio varejista e mercadorias em geral, uma rede de supermercados. Segundo dados públicos[2], a empresa em questão possui um faturamento anual de aproximadamente quinhentos milhões de reais. A rede conta com mais de dezesseis lojas espalhadas por cinco cidades, com cada uma possuindo cerca de cinco mil funcionários. Os principais motivos que influenciaram na escolha desse alvo foram:

- A ausência do protocolo de segurança *https* em sua página principal;
- A existência de uma política que promove a coleta constante de dados sensíveis relacionados aos clientes das lojas, a empresa incentiva seus consumidores a cederem seus dados pessoais em troca de promoções e ofertas nos produtos da marca. Essa prática pode expor os consumidores a golpes cibernéticos em casos de ataques e vazamentos de informações.

Portanto, podemos considerar um elevado grau de importância em utilizar nossa ferramenta para realizar uma investigação, por se tratar de um processo de auditoria numa empresa de grande porte. E também, pelos riscos que poderiam afetar milhares de consumidores dessa marca, ao levarmos em consideração um possível cenário de quebra de segurança. Logo, com os resultados encontrados pelo Levantamento de Informações, podemos analisar as possíveis vulnerabilidades presentes no sistema-alvo do experimento.

5.2. Resultados

Durante a execução dos experimentos foi utilizado uma *Sandbox*, um ambiente controlado e isolado onde é possível executar programas e avaliar os softwares de forma segura. Como verificado em [Mulholland 2018], o ato individual da realização de um Levantamento de Informações não infringe nenhum parâmetro específico na Lei Geral de Proteção de Dados (LGPD). Também é importante ressaltar que as ações executadas não foram intrusivas, as informações obtidas consistem apenas em metadados sem nenhum impacto prejudicial ao alvo de exploração e esses dados foram eliminados após o teste.

Ao finalizar a execução do ExeKaliBurr, a ferramenta gera um relatório no formato *.txt*, contendo informações relacionadas as funcionalidades descritas na Seção 3. Um pequeno trecho do relatório de exploração é apresentado na Figura 3, onde foi feita uma breve anonimização das informações diretamente relacionadas ao alvo de exploração.

[2]https://econodata.com.br/

Figura 3. Fragmento do relatório de exploração

A Tabela 2 apresenta os demais tópicos de exploração e um resumo dos resultados obtidos, descrevendo as informações contidas no relatório do ExeKaliBurr. Por questões de limitação textual, não foi possível apresentar todos os dados encontrados durante a exploração, porém nessa breve amostragem são destacados alguns dos pontos críticos encontrados no sistema-alvo.

Tópico de Exploração	**Quantidade**	**Descrição dos Dados**
Identificação de Endereço IP	7	Mail Exchange (MX)
Scanner de Portas de Redes	10	Pure-FTPd, OpenSSH 7.4 (protocol 2.0), Apache httpd, Dovecot pop3d, Dovecot imapd, Exim smtpd 4.95.
Varredura de Diretórios	11	Diretórios ocultos sem bloqueio de *Status*
Informações Gerais do Domínio	12	Apache, Boostrap, Frame, Google Analytics, HTML5, HTTPServer, JQuery, Meta Author, Open Graph Protocol, Script, Uncommon Headers, X-UA-Compatibles
DNS Reverso do Domínio	254	IP vinculados ao alvo analisado
Sub-DNS & Sistemas Integrados	9	Domínios vinculados ao alvo analisado
Sub-DNS & Sistemas Integrados	10	IP vinculados ao alvo analisado

Tabela 2. Dados contidos no relatório de exploração

Após a análise desses dados, podemos identificar serviços desatualizados e a existência de páginas sensíveis entre os diretórios ocultos, informações descobertas pelas etapas de *Scanner de Portas de Redes* e *Varredura de Diretórios* respectivamente.

A Figura 4 apresenta um fragmento de pesquisa na plataforma *Exploit-DB*[3], um banco de dados de vulnerabilidades conhecidas e documentadas, juntamente a um exemplo de página oculta pertencente ao alvo. Esses são alguns dos principais pontos críticos vulneráveis no sistema, que possivelmente estão suscetíveis a ataques e explorações.

Portanto, foi possível estabelecer um paralelo entre algumas das falhas de segurança existentes e as dez principais vulnerabilidades conhecidas, descritas pela organização segurança OWASP - *Open Web Application Security Project*.

[3]https://www.exploit-db.com/

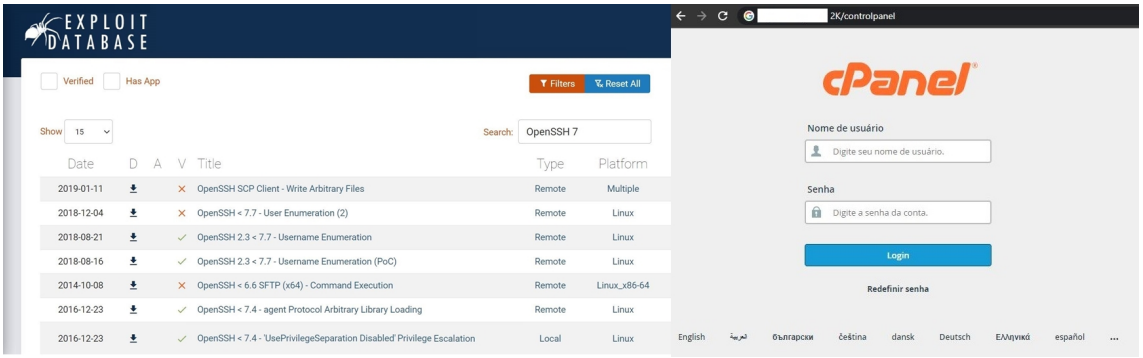

Figura 4. Principais exemplos de vulnerabilidades encontradas

- **`OWASP Top 10 A01_2021 – Broken Access Control:`** Fluxo $\{1, 4, 6, 9, 12, 13\}$ da Figura 2. Vulnerabilidade ocorre quando não são implementadas corretamente as políticas de controle de acesso, autenticação ou autorização, permitindo que usuários mal-intencionados iludam as restrições e acessem informações ou funcionalidades indevidamente.
- **`OWASP Top 10 A03_2021 – Injection:`** Fluxo $\{1, 4, 6, 9, 12, 13\}$ da Figura 2. Falha de segurança que acontece quando os dados fornecidos por um usuário não são devidamente validados ou sanitizados, antes de serem utilizados em uma consulta a um banco de dados, em comandos do sistema operacional ou em outros pontos sensíveis da aplicação.
- **`OWASP Top 10 A05_2021 – Security Misconfiguration:`** Fluxo $\{1, 4, 7, 10, 11, 13\}$ da Figura 2. Ocorre devido a falha em configurações inseguras por padrão, configurações desatualizadas, permissões incorretas, políticas de segurança mal definidas ou outras práticas inadequadas de configuração.
- **`OWASP Top 10 A07_2021 – Identification and Authentication Failures:`** Fluxo $\{1, 4, 5, 8, 13\}$ da Figura 2. Quando ocorrem falhas na identificação e autenticação, como acessos não autorizados a informações ou recursos sensíveis, comprometimento de contas de usuários legítimos, violando privacidade, entre outros cenários.

Sendo assim, um atacante que seguir os passos descritos por algum dos fluxos apresentados será capaz de gerar um grande impacto ao sistema do serviço analisado. Podendo resultar em prejuízos financeiros para a empresa, além da descredibilidade pela ineficiência do sistema de defesa que deveria respaldar esses serviços sensíveis em cenários críticos como os descritos pelo estudo. Essas detecções são exemplos de explorações automatizadas possibilitadas graças a utilização do ExeKaliBurr, assim a ferramenta se mostra eficaz em auxiliar uma das etapas presentes no processo de *Pentest*.

6. Considerações Finais

Demonstração. O código fonte, documentação e instruções de instalação estão disponíveis no repositório do ExeKaliBurr[4]. A demonstração da ferramenta será realizada através de um ambiente disponibilizado por um dispositivo próprio dos autores. As funcionalidades da ferramenta serão apresentadas através dos seguintes passos:

[4]https://github.com/ExeKaliBurr/ExeKaliBurr

(i) definição de um alvo de exploração; (ii) demonstração da utilização da ferramenta, com exceção de etapas que envolvem processos de *Brute Force*; (iii) apresentação dos resultados da execução; (iv) interpretação e discussão das possíveis vulnerabilidades apontadas.

Conclusão. Através desse estudo foi possível avaliar a capacidade do ExeKaliBurr em coletar informações sigilosas a partir de dados públicos conhecidos, por meio da utilização estratégica e coordenada de softwares *Open Source*. A ferramenta se mostrou eficaz na automatização da etapa do Levantamento de Informações no processo de *Pentest*, sendo capaz de concluir atividades que tradicionalmente são realizadas de forma manual pelos profissionais de segurança, proporcionando assim agilidade e praticidade para o usuário. Com isso, algumas informações aparentemente protegidas puderam ser expostas, antecipando o risco da utilização dessas brechas de segurança por agentes maliciosos. A partir dos experimentos realizados, foi possível demonstrar a eficiência da ferramenta para mitigar os impactos associados a falhas de segurança em um sistema *Web* real.

Como trabalhos futuros, podemos destacar: (a) inclusão de funcionalidades para geração de relatórios interativos e em formato *.pdf*; (b) aumento na performance e desempenho do ExeKaliBurr; (c) inclusão e automatização das próximas etapas que compõem o processo de *Pentest*.

Agradecimentos

Este trabalho foi parcialmente financiado pela Lenovo, como parte de seu investimento em P&D pela lei de informática.

Referências

Dewan, P., Kashyap, A., and Kumaraguru, P. (2014). Analyzing social and stylometric features to identify spear phishing emails. In *2014 apwg symposium on electronic crime research (ecrime)*, pages 1–13. IEEE.

Edwards, P. L. (2019). *Cyber Automated Red Team Tool*. PhD thesis, Monterey, CA; Naval Postgraduate School.

Force, J. T. (2018). Risk management framework for information systems and organizations. *NIST Special Publication*, 800:37.

Laxmi Kowta, A. S., Bhowmick, K., Kaur, J. R., and Jeyanthi, N. (2021). Analysis and overview of information gathering & tools for pentesting. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–13.

Mulholland, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, 19(3):159–180.

Stuttard, Dafydd; Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Wiley.

Walker, M. (2013). *Certified Ethical Hacker Practice Exams*. McGraw-Hill Osborne Media.

Weidman, G. (2014). *Penetration Testing: A Hands-on Introduction to Hacking*. Novatec.