Luner: um mecanismo para detecção de vulnerabilidades em serviços de rede

Luner: a mechanism for detecting vulnerabilities in network services

Lucas Renan Meira dos Santos
lrms2@discente.ifpe.edu.br
Marco Antonio de Oliveira Domingues
marcodomingues@recife.ifpe.edu.br
Carlo Marcelo Revoredo da Silva
cmrs@ecomp.poli.br

RESUMO

O trabalho proposto apresenta a aplicação **Luner**, um sistema web que tem como objetivo identificar vulnerabilidades em sistemas. Com o surgimento de ataques hackers durante a pandemia e a falta de consolidação da segurança da informação no Brasil, torna-se evidente a importância da proteção de dados nas empresas. Esses incidentes comprometem a disponibilidade, integridade e confidencialidade das aplicações, resultando em perdas financeiras para as empresas. Nesse contexto, o artigo propõe um framework de pentest (teste de penetração) por meio de uma aplicação que utiliza o *Network Mapper* (*NMAP*) para identificar vulnerabilidades. Além disso, o sistema integra a exploração de vulnerabilidades usando o Metasploit e gera relatórios detalhados sobre as vulnerabilidades encontradas. A aplicação **Luner** busca informar as vulnerabilidades com base no banco de dados do Nmap. O trabalho também documenta um passo a passo do pentest, dividindo os usuários em dois grupos: equipe de ataque e equipe de defesa. Esses dois times se comunicam para que o cliente possa corrigir as vulnerabilidades encontradas, mitigando riscos e protegendo o sistema testado.

Palavras-chave: Teste de intrusão, Framework, Segurança da informação

ABSTRACT

This paper aims to present the application **Luner**, a web system that identifies vulnerabilities in systems. Considering the hacker attacks that have emerged during the pandemic period and an still unsettled scenario of information security in Brazil, it is possible to perceive a new notion of the role of data protection in companies. These security incidents compromise the availability, integrity, and confidentiality of applications and, consequently, result in financial losses for the companies. Thus,

Instituto Federal de Pernambuco. Campus Recife. Curso de Análise e desenvolvimento de sistemas .
15 de Junho de 2023.

this article proposes a pentest framework through an application that identifies vulnerabilities using *Network Mapper (NMAP*), integrates an exploitation component with *Metasploit*, and generates reports on the vulnerabilities found. The **Luner** application aims to inform about the vulnerabilities found based on the *Nmap* database. The pentest process will also be documented step by step, and users will be divided into two groups: the attack team and the defense team, with communication between these two teams so that the client can correct the vulnerabilities found, mitigating risks and protecting the tested system.

Keywords: Pentest, Framework, CyberSecurity

1 INTRODUÇÃO

Atualmente, de acordo com um levantamento global feito pela (ACCENTURE, 2021), constatou-se que houve um aumento de 31% de ataques cibernéticos em 2021, se for comparado com o ano anterior. Também tem crescido a escolha pelo ambiente em nuvem para desenvolvimento de aplicações e, com isso, aumenta o número de clientes com acesso à aplicação, gerando um maior risco de sua aplicação ser alvo de ataque. Estudos de (TUSHAR RICHABADAS, 2021) indicam que cerca de 54% de todos os ataques cibernéticos bloqueados em novembro e dezembro de 2020 foram a aplicativos da web e envolveram o uso de ferramentas automatizadas. Nesse contexto, torna-se importante a identificação de vulnerabilidades em serviços de fácil detecção pelos atacantes, pois, essas serão as primeiras a serem exploradas e utilizadas por esses atacantes, necessitando de uma aplicação automatizada que as identifique antes de serem incorporadas ao ambiente em produção.

Desta maneira, o combate à exploração automática de vulnerabilidades é essencial para garantir a segurança cibernética, e a ISO 27001 destaca a importância desse controle no Anexo A, seção A.12.6.1. Existem diversas abordagens para prevenir essa exploração, sendo duas delas a identificação manual de vulnerabilidades em redes locais e a utilização de ferramentas automatizadas. Cada uma dessas abordagens tem suas próprias vantagens e desvantagens, conforme discutido no artigo “Automated versus Manual Approach of Web Application Penetration Testing”, apresentado na 11ª Conferência Internacional sobre Tecnologias de Computação, Comunicação e Redes (ICCCNT) em 2020.

Os testes manuais têm a vantagem de identificar vulnerabilidades ainda desconhecidas, graças à criatividade e experiência dos testadores humanos. Essa abordagem é essencial para revelar falhas únicas que podem não ser detectadas por ferramentas automatizadas. No entanto, os testes manuais podem ser demorados e caros, o que pode ser impraticável em ambientes de grande escala.

Por outro lado, as ferramentas automatizadas, como o caso mencionado do *EternalBlue*, têm a capacidade de identificar vulnerabilidades conhecidas em larga escala e de maneira eficiente, tornando-se uma escolha valiosa em termos de velocidade e cobertura. No entanto, essas ferramentas não conseguem identificar vulnerabilidades novas e desconhecidas.

É importante ressaltar que a identificação das vulnerabilidades, seja de forma manual ou automatizada, não corrige a falha por si só. No entanto, essa

identificação é o primeiro passo para que os responsáveis pela segurança possam tomar as medidas necessárias para mitigar os riscos. Isso inclui a correção das vulnerabilidades quando necessário e a implementação de medidas de segurança adequadas. Essas ações são cruciais para reduzir os riscos, evitar problemas financeiros e proteger a imagem da empresa.

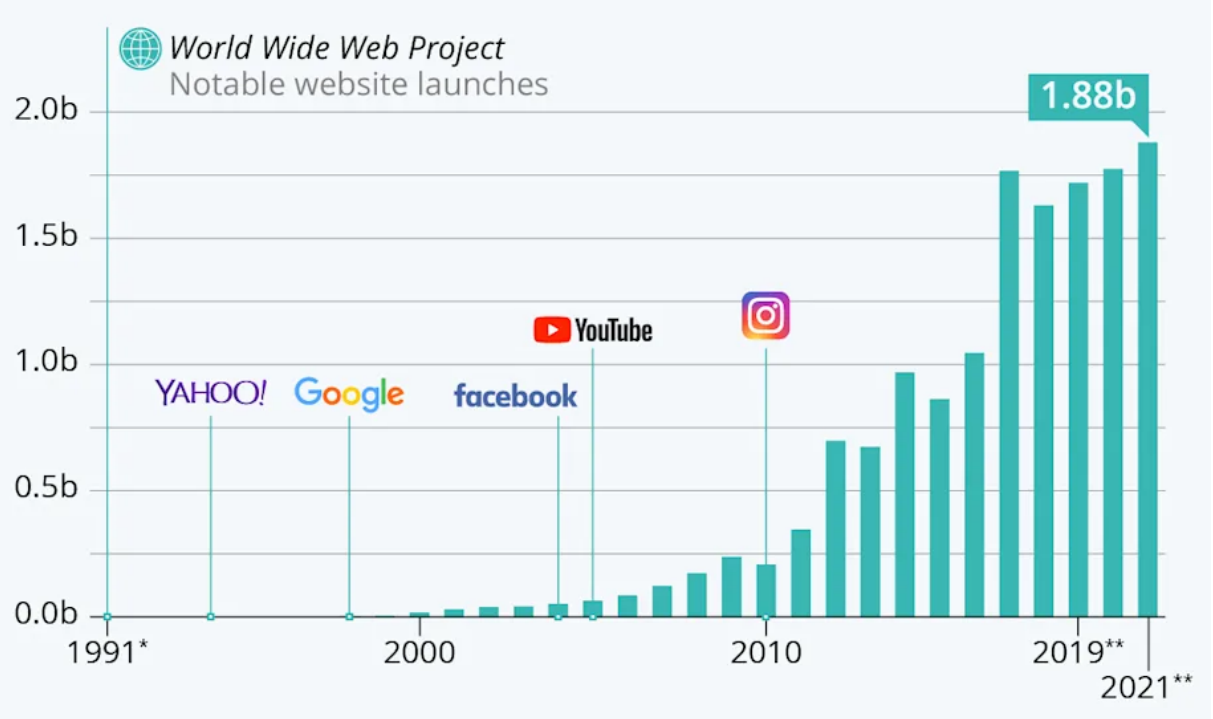
Em resumo, a combinação de testes manuais e automatizados desempenha um papel fundamental na prevenção da exploração de vulnerabilidades. Cada abordagem tem suas vantagens e desvantagens, e a escolha da melhor estratégia depende das necessidades específicas da organização e do ambiente em questão. O objetivo final é fortalecer a segurança cibernética e reduzir os riscos associados a possíveis explorações de vulnerabilidades.

Mediante as informações, faz-se necessário aplicação destes controles para diminuir riscos e potenciais incidentes de segurança que são explorados através de vulnerabilidades em serviços. O artigo em questão apresenta um sistema web, nomeado de **Luner**, com o objetivo de encontrar vulnerabilidades, gerar relatórios com base nas vulnerabilidades encontradas, e catalogar o passo a passo da exploração. A aplicação também pode ser utilizada em equipe ou sozinho, para que algum analista de segurança mais experiente ajude um menos experiente ou o grupo de pentest compartilhe informações entre si, resolvendo o problema da falta de informação sobre as fraquezas do seu sistema. O pentester ficará responsável pela validação se as vulnerabilidades encontradas no sistema web forem reais ou não. O sistema foi implementado utilizando as linguagens Python, HTML, CSS, Javascript, XML e JSON, permitindo a um usuário realizar testes de segurança em aplicações de sua escolha. O restante desse artigo é organizado da seguinte maneira: Trabalhos correlatos a proposta, visão geral da proposta arquitetura do sistema, prova de conceito, paradigmas na resolução do sistema e a conclusão.

2 CONTEXTUALIZAÇÃO

Com a popularização da internet e da tecnologia, aumentou também o número de serviços disponibilizados nesta; um serviço está relacionado a uma porta aberta no servidor que troca informação com um cliente através da rede. Um exemplo do aumento exponencial de serviços em todo o mundo pode ser visto na Figura 1, que ilustra um tipo de serviço que é o web site. Em 2021, havia mais de 1,88 bilhões disponíveis na internet, sem contar com web sites disponibilizados na intranet de empresas e em redes locais, como, por exemplo, o serviço oferecido por roteadores para acessar o painel administrativo do mesmo.

Figura 1 – Aumento exponencial de sites na internet



Fonte: World Wide Web Project (2021)

Diante do avanço tecnológico percebido em todo o mundo, também surgiram formas de atacar esses serviços disponibilizados nas intranets ou na internet, uma dessas formas é um ciberataque, que é qualquer tentativa de impedir o cumprimento das propriedades da segurança informação, isto é, atacar a disponibilidade, integridade e confidencialidade de algum sistema. Quando a aplicação não aplica os controles de segurança adequados à proteção desses ataques, ela está vulnerável e essa vulnerabilidade deixa o ambiente exposto para possíveis invasões.

Todos esses ataques podem causar danos financeiros e na reputação da empresa alvo e são feitos por c*rackers* que não possuem vínculos com as empresas. Por outro lado, também existem profissionais da segurança da informação, que sabem trabalhar com essas mesmas ferramentas dos hackers, que o exemplo é um analisador de vulnerabilidades, mas que fazem isso para identificar e alertar a empresa sobre suas vulnerabilidades e formas de correção.

A aplicação desenvolvida nesse trabalho utilizará o *NMAP* para identificação de vulnerabilidades e utilizará o Metasploit como framework de exploração de alvos.

2.1 TRABALHOS RELACIONADOS

O autor [SANTOS and Soares 2018] cita conceitos de segurança e a importância da segurança da informação para as empresas, demonstrando a tendência do aumento dos incidentes de segurança com o passar dos anos no Brasil: através dos dados reportados ao CERT.br, em 1999 ocorreram somente 3107 casos enquanto em 2017 ocorreram 833775 incidentes. A pesquisa teve como resultado que com o aumento da tecnologia e a importância desta, ataques virtuais se tornam lucrativos, seja para extorquir ou roubar dinheiro e por isso a necessidade de as empresas pensarem em segurança digital. E para começar a implementar a segurança digital,

nada melhor do que começar com a política de segurança, onde é uma declaração formal da alta diretoria da organização, definindo o papel da Segurança da Informação dentro de uma organização e sendo adequada a sua organização em questão.

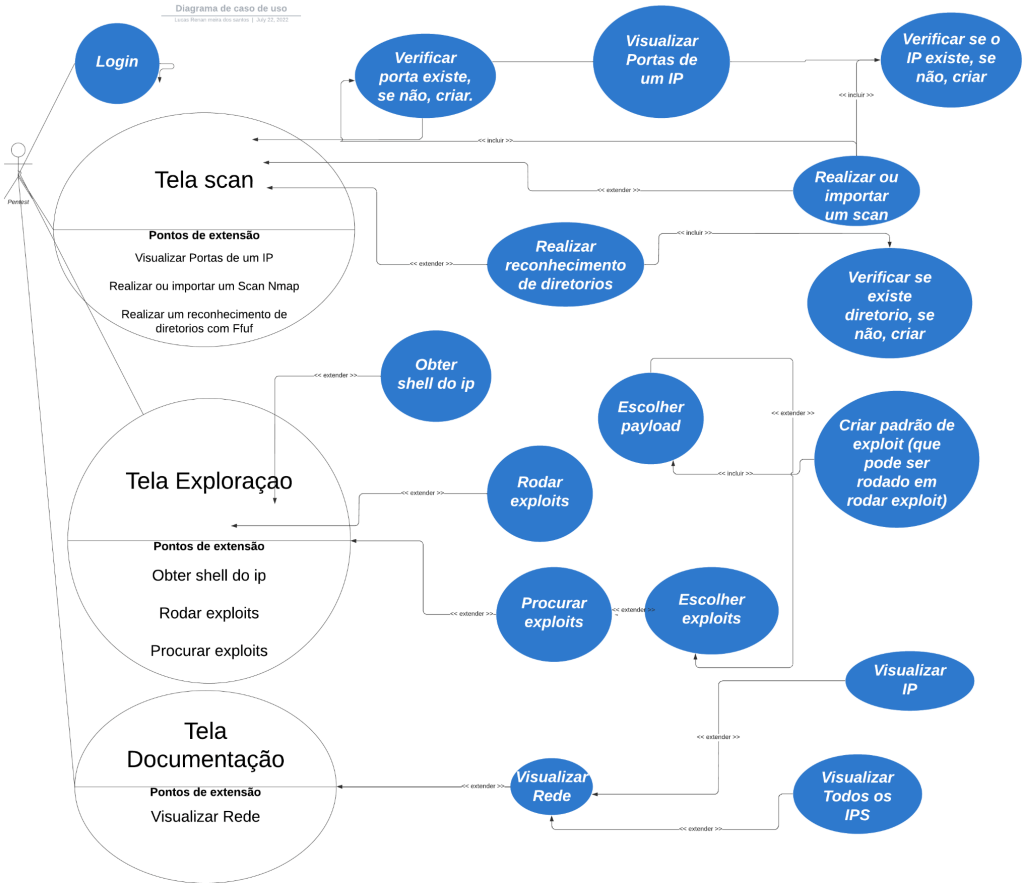
À medida que surge a necessidade de as empresas pensarem em segurança digital, também é importante a realização de testes de segurança. O artigo de [dos Santos MARTINS and CARDOSO 2018] detalha com etapas e processos bem definidos de testes de segurança para garantir que as vulnerabilidades sejam identificadas e aplicados os controles de segurança de acordo com a vulnerabilidade e necessidade do sistema.

Este artigo [Pavan and Guardia 2016], demonstra a importância de um pentest para garantir um aumento da segurança das aplicações corporativas, também foi uma das bases para a criação do **Luner**, onde ele consegue facilmente entrar na parte da descoberta, novas descobertas, ataque e relatório.

3 VISÃO GERAL

Por ser uma aplicação web, várias pessoas poderiam trabalhar em conjunto a invasão de um sistema com o **Luner** de qualquer lugar, supondo que o alvo esteja na rede do **Luner** ou na internet e que o usuário tenha um navegador instalado em seu computador.

Figura 2 – Diagrama de casos de uso da aplicação



O software está organizado de forma que A Figura 2 ilustra a arquitetura e o diagrama de casos de uso do **Luner**. Tendo 3 módulos principais: Identificação, Exploração e documentação.

O módulo de identificação é o responsável por identificar e encontrar através do *NMAP*: IPs, Portas, Sistemas operacionais, e Vulnerabilidades dos Sistemas e através do ffuf: Diretórios. Também dá para descobrir de qual linguagem de programação, servidor web e afins é feita o alvo em questão, através de uma funcionalidade do whatweb, dá para realizar testes de SQL injection através de uma funcionalidade do Sqlmap e buscar por novos paths através de um script que lê o site em busca de novas referências.

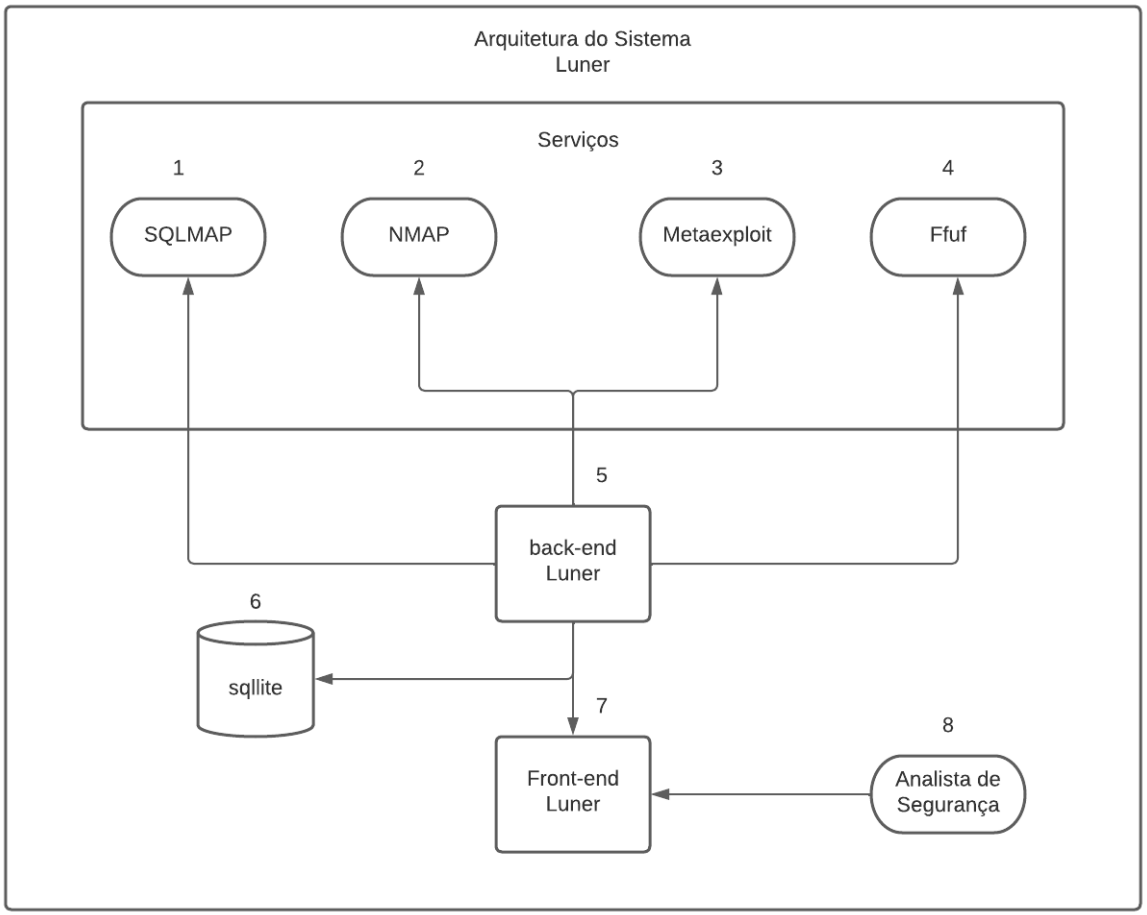
O módulo de exploração é responsável por realizar a exploração de uma vulnerabilidade, ele está integrado com o Metasploit e caso a vulnerabilidade seja explorada, possibilita uma web shell, onde o utilizador do sistema pode tirar prints para comprovar a invasão do sistema.

O módulo de documentação, responsável por gerar relatórios para os clientes. Demonstrando todos os resultados que foram encontrados, através de gráficos intuitivos, mostrando a quantidade de vulnerabilidades e portas abertas encontradas no sistema.

Para implementação, foi utilizada a linguagem python com o framework Django. O código fonte está disponível online https://github.com/lucasrenaa/luner, bem como os scripts para identificação das vulnerabilidades.

4 Arquitetura Luner

Figura 3 – Arquitetura **Luner**



Na Figura 3 vemos a arquitetura **Luner**, a arquitetura é separada em módulos, no módulo de serviço, estão apresentados serviços externos que é necessário para a utilização do sistema. Nesses serviços, são fornecidas ferramentas como: Sqlmap que possibilitam a realização de teste de SQL Injection nos parâmetros detectados do sistema; *NMAP* que permite o descobrimento de computadores e vulnerabilidades nos serviços; Metasploit que fornece a possibilidade de exploração do sistema alvo e por fim, *Fuzz Faster U Foo (FFUF)* enumerando os diretórios do alvo em questão.

Em seguida é apresentado o módulo de back-end que faz a conexão com todos esses serviços, processando as informações recebidas e agregando ao sistema, ele também armazena essas informações em um banco de dados no SQLite.

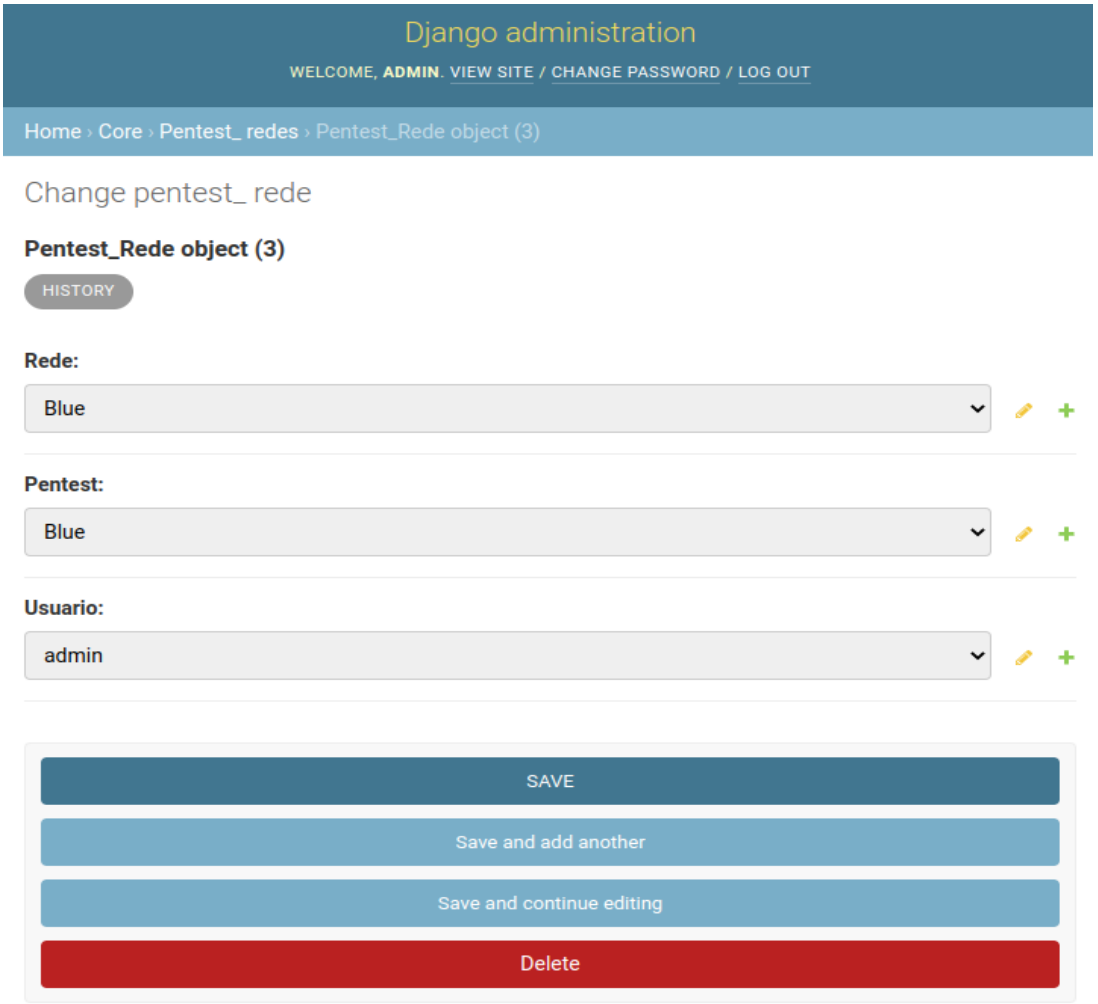
O back-end processa as informações do banco de dados, e resulta em no front-end, através da requisição do usuário ao sistema por meio do protocolo HTTP e que pode ser atualizado por uma biblioteca para o modo com HTTPS. As ferramentas que compõem o back-end são: A linguagem de programação python, o framework de desenvolvimento web Django.

O front-end recebe as informações do back-end e as exibe para o Analista de Segurança. Ferramentas que compõem o Front-end são: A linguagem de marcação de texto HTML para renderizar os textos na tela, CSS para estilizar as páginas, A linguagem de programação Javascript para o funcionamento dinâmico das páginas, e o framework Bootstrap para auxiliar em estilos no projeto.

5 Prova de conceito (Proof of concept - POC)

O ambiente de teste selecionado para esta prova de conceito é o "Blue - TryHackMe", uma plataforma que disponibiliza servidores vulneráveis para estudantes e profissionais de segurança praticarem e aprimorarem suas habilidades na exploração de vulnerabilidades em sistemas. Neste cenário, concentramos nossos esforços em um servidor Windows vulnerável à infame falha do EternalBlue.

Figura 4 – Finalização da configuração da Rede

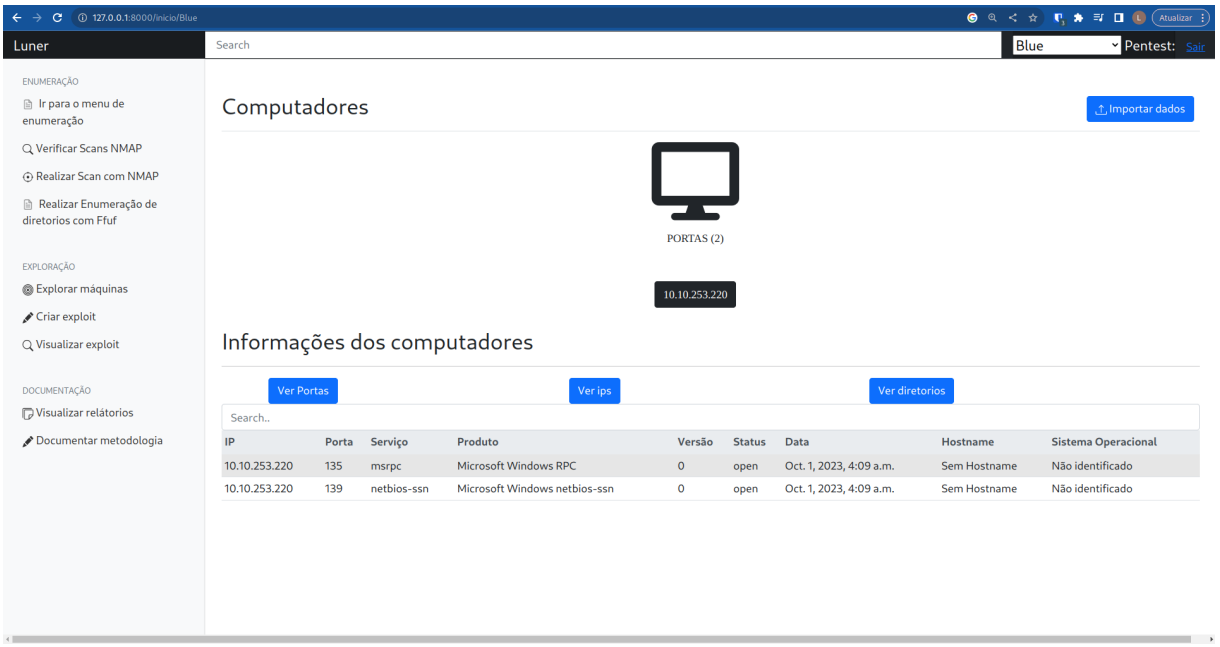


O *EternalBlue* é um exploit de ataque cibernético que foi originalmente desenvolvido pela Agência de Segurança Nacional (NSA) dos Estados Unidos. Sua divulgação ocorreu quando o grupo de hackers conhecido como Shadow Brokers o tornou público em 14 de abril de 2017. Essa vulnerabilidade tornou-se um elemento-chave em vários tipos de ataques, resultando em danos financeiros

superiores a 1 bilhão de dólares em mais de 65 países. Hackers aproveitaram essa vulnerabilidade tanto para a exploração inicial quanto para a movimentação lateral dentro de sistemas comprometidos.

O objetivo desta prova de conceito é demonstrar a capacidade de executar comandos remotamente no sistema alvo e mapear as vulnerabilidades identificadas, a fim de gerar um relatório detalhado.

Figura 5 – Scan Realizado, alvo com 2 portas abertas, pode-se ver o computador de forma gráfica e intuitiva, e os serviços e produtos também na visualização da tela de enumeração.



Os testes foram conduzidos utilizando o sistema operacional Kali Linux. Para replicar esses testes em outros ambientes, é necessário que o utilitário NMAP esteja devidamente instalado e acessível através do PATH do sistema.

Para iniciar o processo de pentest, a primeira etapa envolve a configuração de uma rede, conforme ilustrado na Figura 4 no painel administrativo. Essa configuração foi criada com a finalidade de proporcionar segregação entre diferentes testes. Caso múltiplos testes sejam realizados, essa configuração garante que os alvos da "Rede 1" e "Rede 2" não estejam visíveis para outros usuários ou redes. Além disso, possibilita a colaboração entre analistas, permitindo que eles visualizem e conduzam análises conjuntas. Vale ressaltar que o teste em questão foi conduzido de forma individual.

Após a criação da rede, a próxima etapa consiste na realização de um escaneamento. Isso pode ser realizado através da importação de um resultado do NMAP no formato XML ou executando um escaneamento diretamente no sistema. Após a conclusão do escaneamento, como ilustrado na Figura 5, é possível identificar quais portas estão abertas no alvo e quais serviços estão sendo executados.

Na etapa seguinte, na tela de documentação, é necessário selecionar a rede previamente configurada para conduzir o pentest. Neste exemplo, utilizamos a rede "Blue", conforme indicado na Figura 6. Os resultados desta etapa revelam a

presença de vulnerabilidades, como evidenciado em um dos gráficos da Figura 7. Mais especificamente, podemos observar a identificação da vulnerabilidade conhecida como EternalBlue.

Figura 6 – Tela de documentação

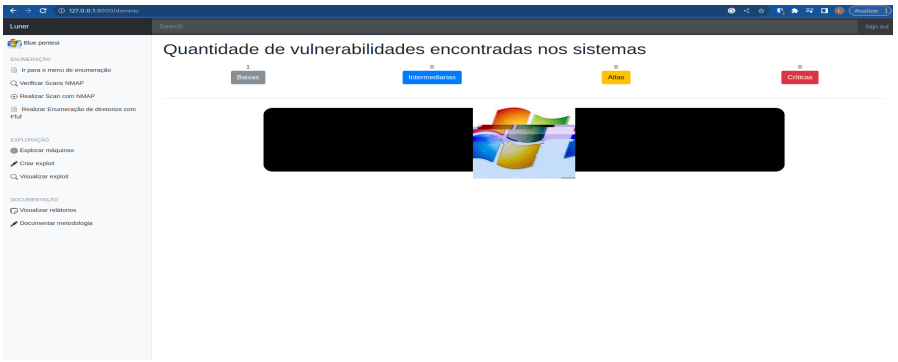


Figura 7 – Gráficos

A tela de exploração, após a execução do exploit, apresenta o computador alvo pronto para exploração. Ao clicar no endereço IP do alvo, é possível enviar comandos, como o "ipconfig", para verificar o estado do sistema, conforme demonstrado na Figura 9, à direita. O objetivo desta prova de conceito é claramente estabelecido: identificar vulnerabilidades, explorar a falha e gerar relatórios abrangentes sobre essas vulnerabilidades.

Esta prova de conceito oferece uma visão prática das etapas envolvidas na detecção e exploração de vulnerabilidades, bem como na documentação e relato dos resultados, contribuindo para uma compreensão mais profunda da segurança cibernética.

Figura 8 – EternalBlue detectado

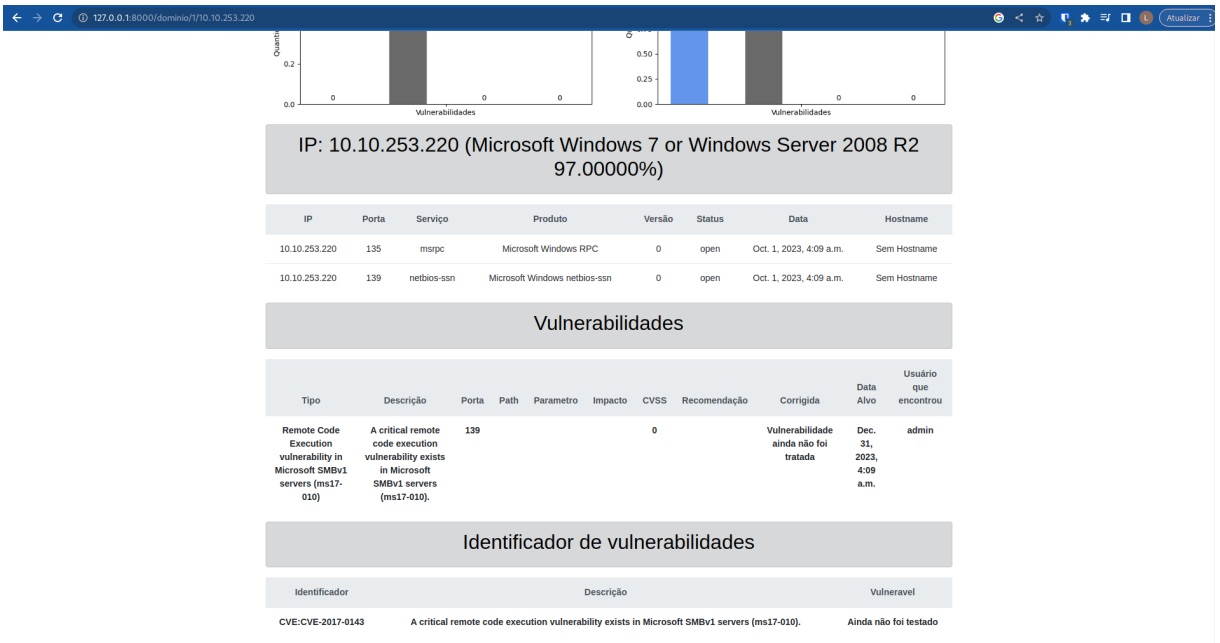
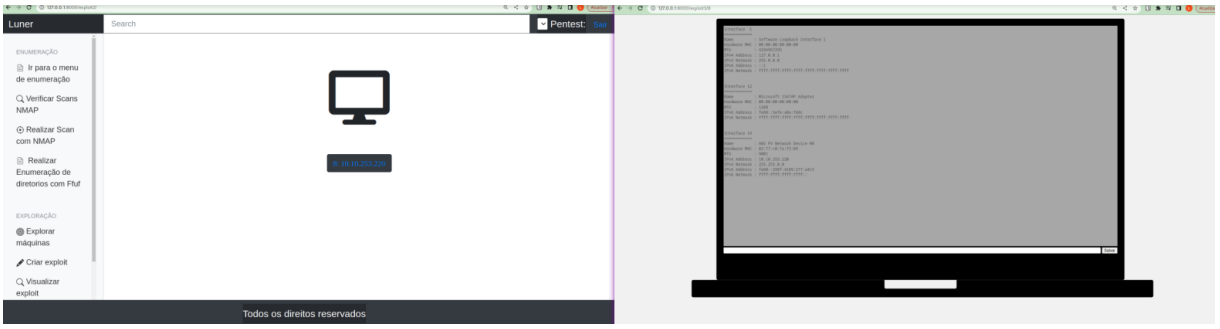


Figura 9 – No lado esquerdo da figura, o alvo sistema conseguiu obter sua shell e no lado direito o analista de segurança já consegue enviar comandos remotamente através da tela de computador do sistema



6 CONCLUSÃO

A análise de vulnerabilidades é eficiente para a descoberta de vulnerabilidades. Entretanto, **Luner** ainda não consegue identificar todas as vulnerabilidades, o banco de dados está restrito aos scripts do *NMAP*.

Portanto, uma boa parte de vulnerabilidades podem ser encontradas de forma manual ou com outros scripts recém-divulgados na Internet, mas não serão encontrados por **Luner**. Para resolver esse problema, a aplicação teria que ter uma forma de criar e adicionar novos scripts, mas para resolver esse caso de uma forma mais simples, foi colocado uma opção de importar novas vulnerabilidades que foram descobertas manualmente. Mas, normalmente os crackers sem experiência, optam por scripts automatizados e divulgados a muito tempo na internet para tentar realizar suas invasões. E a aplicação consegue muito bem identificar essas vulnerabilidades comuns nos seus relatórios como podemos ver na prova de conceito do EternalBlue.

A ferramenta conseguiu descobrir a vulnerabilidade no ambiente de teste da TryHackMe e conseguiu gerar um relatório. Recomenda-se que os analistas de

segurança tentem explorar o ambiente manualmente e catalogar a vulnerabilidade no sistema, caso tenha encontrado alguma e o sistema gerará o relatório normalmente. Como trabalho futuro, pretende expandir o Luner para vários scans já automatizados, com área para buscar banco de dados, ou scans personalizados para web e que não precise o usuário fazer o scan e automaticamente informar se conseguiu shell do alvo ou não, também desejo criar uma imagem docker para fácil utilização de qualquer pessoa através da imagem.

REFERÊNCIAS

SINGH, Navneet; MEHERHOMJI, Vishtasp; CHANDAVARKAR, B. R. Automated versus manual approach of web application penetration testing. In: 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020. Kharagpur, India: IEEE, 2020. p. 1-6. DOI: 10.1109/ICCCNT49239.2020.9225385.

SANTOS MARTINS, H. e CARDOSO, F. E. Teste de vulnerabilidades em sistemas web. Disponível em: https://cepein.femanet.com.br/BDigital/arqPics/1811550301P887.pdf

PAVAN, P. V. A. e GUARDIA, H. C. Pentest para auditoria de segurança de rede em ambientes corporativos. Revista TIS, v. 4, n. 2, 2016.

SANTOS, E. E. d. e SOARES, T. M. M. K. Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações. Faculdade de Tecnologia de Americana.

ACCENTURE. How aligning security and the business creates cyber resilience State of Cybersecurity Resilience 2021. [S.l.: s.n.].

TUSHAR RICHABADAS. Threat Spotlight: Automated attacks on web applications.