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

Lucas Renan Meira dos Santos[1], **Carlo Marcelo Revoredo da Silva**[2]

[1]Campus Recife – Instituto Federal de Pernambuco (IFPE)

lrms@ifpe.edu.br

[2]Escola Politécnica de Pernambuco (POLI) – Universidade de Pernambuco (UPE)

cmrs@ecomp.poli.br

Abstract. *This work proposes to present the application Luner, a web system that identifies vulnerabilities in systems. Hackers who visualized data protection in pandemics and companies in the data protection role in pandemics consolidated a new notion of a data protection role in cities. These security incidents are in the availability, availability and confidentiality of applications and, consequently, financial loss for. Thus, it was proposed in this format a test application of a framework that emulates as consultancies through the* Network Mapper *(NMAP), has an exploration part integrated with Metasploit and that generates an article reports on the vulnerabilities. It will also be based on the database of informed data to pass to the attack and the time of two groups for your customer to fix such vulnerabilities, mitigating risks and protecting the tested system in question. As soon as possible, the risk of an attack occurring on the tested system.*

Resumo. *Este trabalho se proprõe a apresentar a aplicação Luner, um sistema web que identifica vulnerabilidades em sistemas. Visto que, os ataques hackers que surgiram a partir da pandemia e de um cenário ainda não consolidado de segurança da informação no Brasil, imprimiram uma nova noção do papel da proteção de dados nas empresas. Estes incidentes de segurança que comprometeram a disponibilidade,integridade e confidencialidade das aplicações e por consequência, perda financeira para empresas. Dessa forma, foi proposto neste artigo um framework de pentest através de uma aplicação que identifique as vulnerabilidades através do* Network Mapper *(NMAP), tenha uma parte de exploração integrada com o Metasploit e que gere relátorios sobre as vulnerabilidades encontradas. A aplicação Luner busca informar as vulnerabilidades encontradas baseada no banco de dados do Nmap Também será documentado passo a passo do pentest, e separado os usuários em dois grupos, o time de ataque e o time de defesa, havendo uma comunicação entre esses dois times para que seu cliente corrija as vulnerabilidades encontradas, mitigando riscos e protegendo o sistema testado em questão. Assim concluirmos que, a aplicação Luner, poderá facilitar o encontro de vulnerabilidades para serem corrigidas através de controles de segurança, diminuindo o risco de ocorrer algum ataque no sistema testado.*

1. Introdução

Atualmente, de acordo com um levantamento global feito pela [Bissell et al. 2021], constatou que houve um aumento de 31% de ataques cibernéticos em 2021 , se for comparado ao ano anterior. As aplicações estão sendo cada vez mais desenvolvidas nas nuvens e com isso, um maior número de clientes pode acessar a aplicação, trazendo um maior risco de sua aplicação ser alvo de ataque. Estudos de [Richabadas 2021] indicam que cerca de 54% de todos os ataques cibernéticos bloqueados em novembro e dezembro do ano passado foram a aplicativos da web e envolveram o uso de ferramentas automatizadas. Sendo 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 identifique essas vulnerabilidades antes de subir o ambiente em produção.

Desta maneira, uma das formas de se combater uma exploração automatica é detectar essas vulnerabilidades antes de serem exploradas, como a ISO 27001 exige no controle A.12.6.1 do Anexo A. Para se prevenir essa exploração, você pode identificar manualmente ou através de ferramentas para que essas vulnerabilidades em rede local sejam corrigidas, mas, identificar essas vulnerabilidades não corrigem a falha por si só, mas graças a identificação, o responsavel da implementação da medida de segurança irá corrigir a falha se necessário, e subir em produção, tomando a escolha certa para diminuir riscos e possíveis problemas financeiros e de imagem da empresa em questão.

Mediante as informações, faz-se necessário aplicação destes controles para diminuir riscos e potenciais incidente 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 também de 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 pentester compartilhe informações entre si, resolvendo o problema da falta de informação sobre as fraquezas do seu sistema. O pentester ficará responsável para a validação se as vulnerabilidades encontradas no sistema web são 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 os números de serviços disponibilizados nesta, serviço aqui no artigo 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, podemos ver na Figura ref-fig:quantosites.webp, um tipo de serviço que é o web site em 2021 tem mais de 1,88 bilhões disponivéis 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.

Diante de um avanço tecnológico percebido em todo o mundo, também surgiram

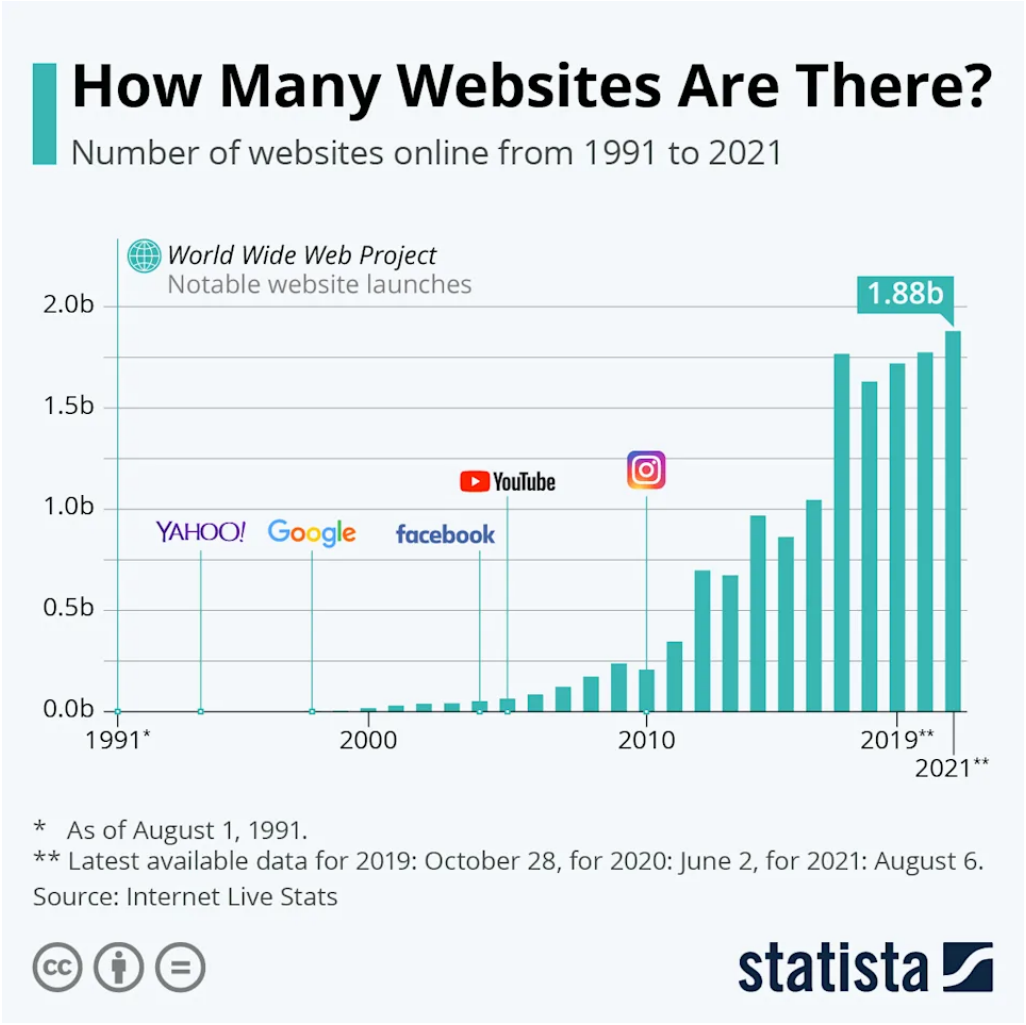

Figure 1. Aumento exponencial de sites na internet

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 seguranças adequados a 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, todos esses ataques são feitos por Crackers que não possuem vinculos com as empresas. Mas, 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 *Network Mapper* 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 torna 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.

A medida que a surge a necessidade de as empresas pensarem em segurança digital, também é importante realizaçáó de testes de seguranças. 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 relatorio.

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.

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

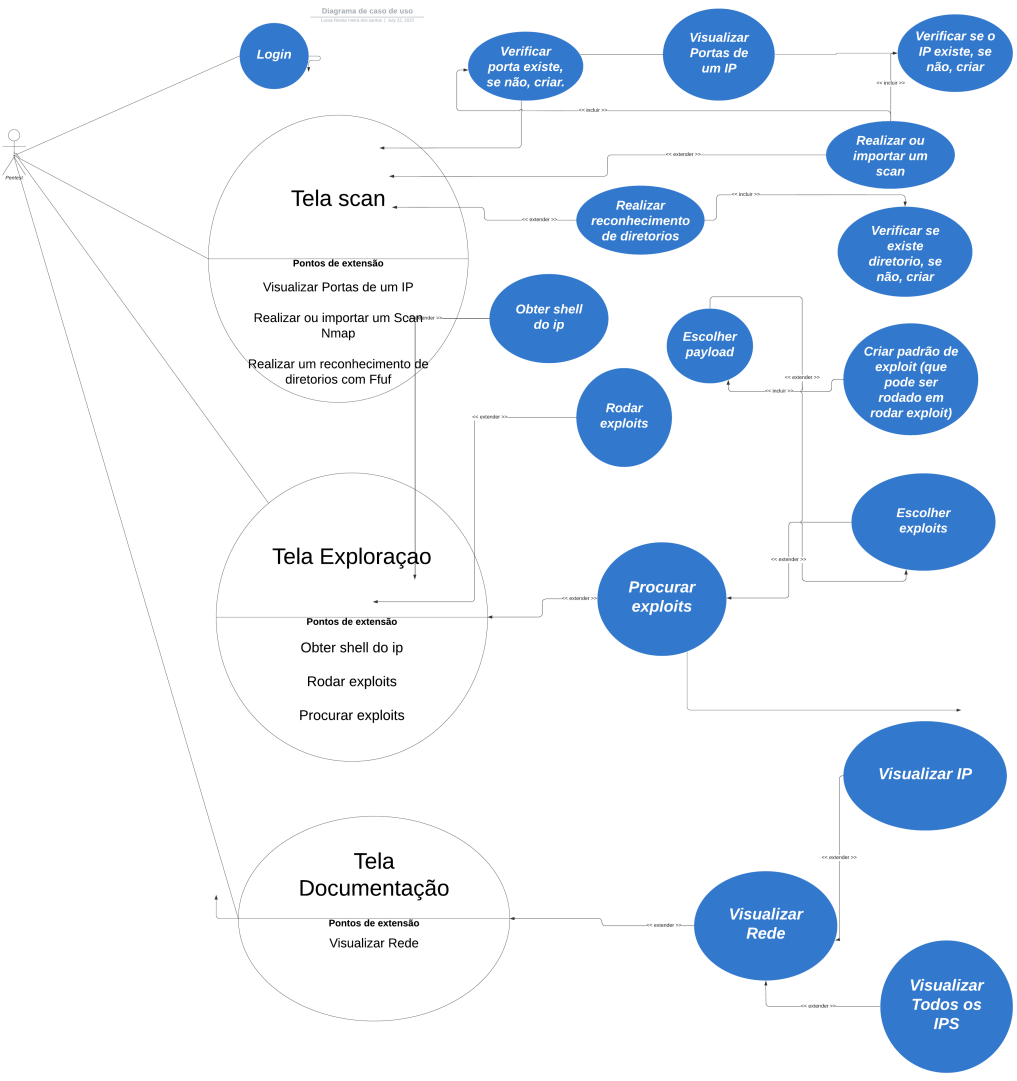

Figure 2. Diagrama de casos de uso da aplicação

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: Diretorios. 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 para realizar a exploração de uma vulnebilidade, 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 intuítivos, mostrando a quantidade de vulnerabilidades e portas abertas encontradas no sistema.

Para implementação, foi utilizada a linguagem python com o framework Django. Ó código fonte está disponivel online em ”https://github.com/LUCASRENAA/Luner”. Os scripts para identificação das vulnerabilidades

4. Arquitetura Luner

Na Figura 3 vemos a arquitetura Luner, a arquitetura é separada em modulos, no modulo de serviço, estão apresentadas serviços externos que é necessário para a utilização do sistema. Nesses serviços, são fornecidos ferramentas como: Sqlmap que possibilitam a realização de teste de SQLInjection nos parametros 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 Fool (ffuf) enumerando os diretorios do alvo em questão.

Em seguida é apresentado o modulo 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 SqlLite.

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 para a prova de conceito é o ”Blue - TryHackMe”,TryHackMe é uma plataforma onde disponibiliza servidores vulneraveis para estudantes e profissionais

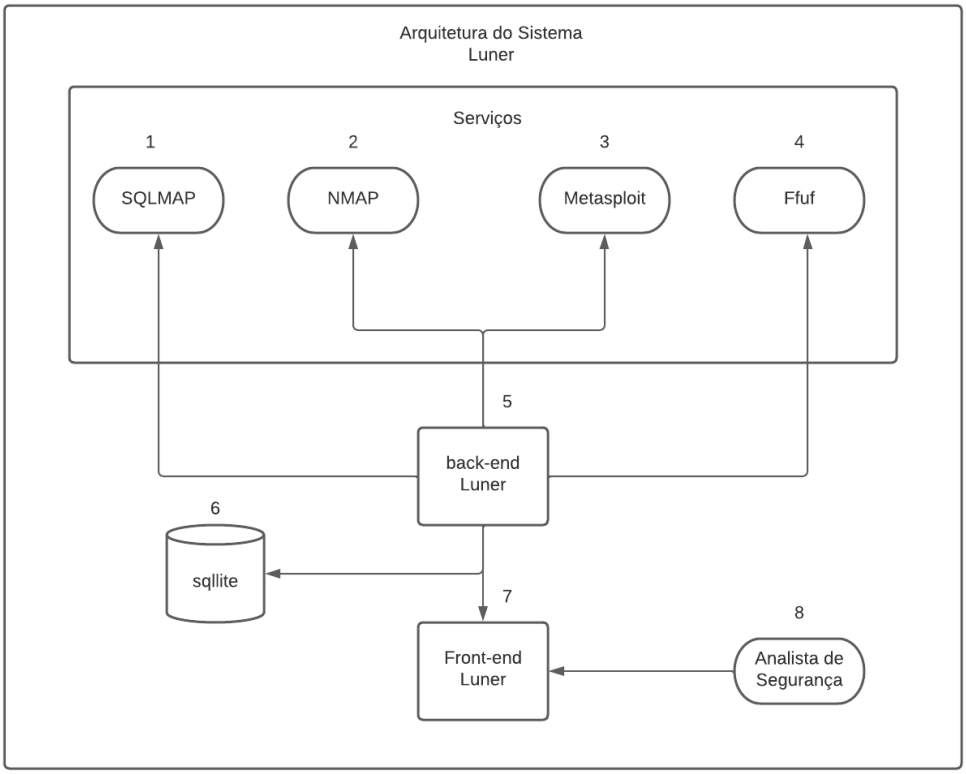

Figure 3. Arquitetura Luner

de segurança aprenderem a explorar vulnerabilidades em sistemas. Esse servidor em questão é um Windows Server vulneravél a famosa falha do EternalBlue. EternalBlue é um exploit de ataque cibernético desenvolvido pela Agência de Segurança Nacional (NSA) dos Estados Unidos da América. Foi divulgado (”vazado”) pelo grupo de hackers Shadow Brokers em 14 de abril de 2017. Essa falha foi explorada em diversos tipos de ataques e no total foi gerado mais de 1 bilhão de dolares em prejuízo em mais de 65 países, hackers usando essa falha tanto para exploração inicial tanto para movimento lateral.

O objetivo do teste é conseguir realizar comandos remotamente no alvo através do sistema, e mapear as vulnerabilidades encontradas no sistema, gerando um relátorio para o alvo.

A realização dos testes foi feita no sistema operacional Kali linux. Para funcioanr em outros ambientes, precisará ter o NMAP instalado e acessível via path do sistema.

Para começar a realizar o pentest, teremos que criar uma rede como veremos na Figura 4 no painel administrativo, pois, essa configuração foi criada para que haja separação entre cada pentest, caso você faça mais de 1 e com isso, os seus alvos da rede 1 e da rede 2 não estarão visíveis para qualquer rede ou usuário do sistema, e também para que, caso você trabalhe em equipe, consiga fazer que outros analistas consigam visualizar o seu pentest e realizarem scans juntos. O teste em questão será realizado de forma individual.

Feito a criação da rede, o próximo passo é realizar um scan, você pode tanto

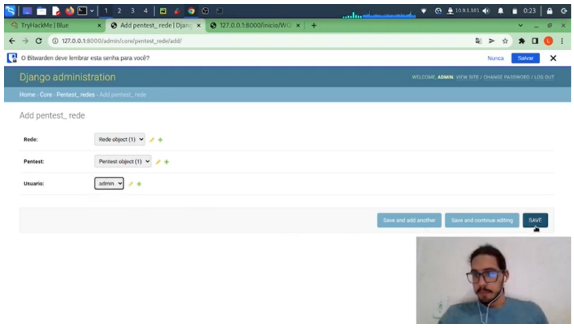

Figure 4. Finalizando configuração de rede

importar uma saída do NMAP com xml ou rodar no próprio sistema.

Depois da finalização do scan, que vemos na Figura 5, pode verificar quais são as portas abertas do alvo e os seus serviços.

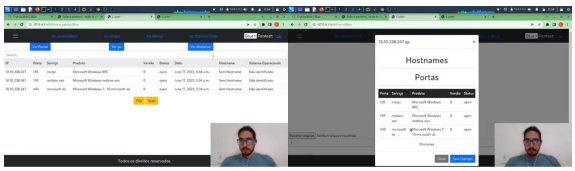

Figure 5. Scan realizado, alvo com 3 portas abertas, do lado esquerdo está em formato de tabelas isolado na aba de tabelas e do lado direito está na visualização rápida da tela inicial

No próximo passo na tela de documentação, escolha a rede que você criou para fazer o pentest, aqui na prova de conceito é a rede Blue, como observa-se na Figura 6.

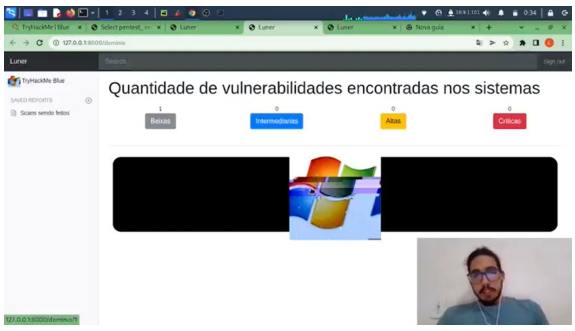

Figure 6. Tela de documentação

Observa-se que existem dois gráficos e um aqui mostra que foi encontrado uma vulnerabilidade no sistema, veja na Figura 7 e em baixo, observa-se na Figura 8 que a vulnerabilidade encontrada que é o EternalBlue

Na aba de vulnerabilidades depois que você clica no IP alvo, aparece as vulnerabilidades encontradas pelo scan NMAP, como na Figura 9, encontra-se a vulnerabilidade do EternalBlue, para explorar-la, iremos para a tela de Exploração.

Na tela de exploração depois de rodar o exploit, encontra-se o computador pronto para exploração

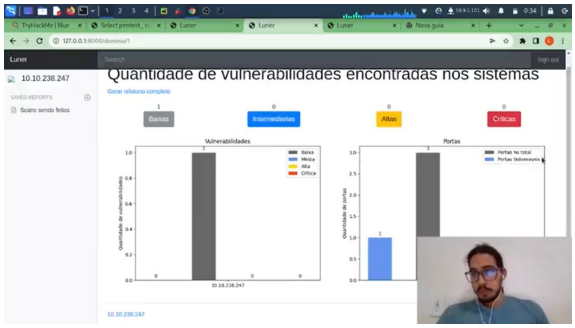

Figure 7. Gráficos

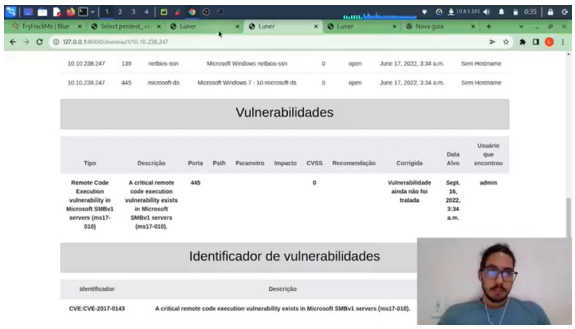

Figure 8. EternalBlue Detectada

Depois de clicar no IP do alvo, envia-se um comando de ipconfig para verificar se tudo está ok, como podemos ver na Figura 9 no lado direito, onde o comando é rodado e consegue-se o objetivo deste artigo que é, identificar as vulnerabilidades, explorar a falha e gerar relátorios sobre essas vulnerabilidades.

6. Conclusão

A análise de vulnerabilidades são eficientes para 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 será encontrado 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 experiências, 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 relatorios 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 relátorio. Recomenda-se que os analistas de segurança tente explorar o ambiente manualmente e catalogar a vulnerabilidade no sistema, caso tenha encontrado alguma e o sistema gerará o relátorio normalmente. Como trabalho futuro, pretendo 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

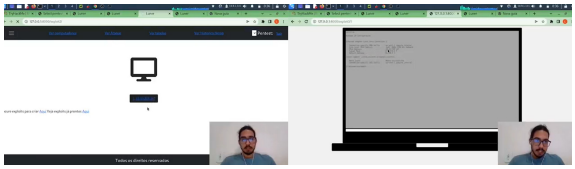

Figure 9. No lado esquerdo da figura, o alvo sistema conseguiu obter sua shell e no lado direito o analista de segurança já consegue enviar comandos remotamentes através da tela de computador do sistema

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.

References

Bissell, K., Jacky Fox, R. M. L., and Cin, P. D. (2021). Estado da resiliência da cibersegurança 2021. *Accenture*.

dos Santos MARTINS, H. and CARDOSO, F. E. (2018). Teste de vulnerabilidades em sistemas web. *"https://cepein.femanet.com.br/BDigital/arqPics/1811550301P887.pdf"*.

Pavan, P. V. A. and Guardia, H. C. (2016). Pentest para auditoria de segurança de rede em ambientes corporativos. *Revista TIS*, 4(2).

Richabadas, T. (2021). Threat spotlight: Automated attacks on web applications. *Barracuda Networks*.

SANTOS, E. E. d. and Soares, T. M. M. K. (2018). Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações. *Faculdade de Tecnologia de Americana*.