Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GIANCARLO ROSA DE JESUS JUNIOR

ESTRATÉGIA DE ATAQUE EM AMBIENTE SIMULADO COM KALI LINUX

Assis/SP
2017

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GIANCARLO ROSA DE JESUS JUNIOR

ESTRATÉGIA DE ATAQUE EM AMBIENTE SIMULADO COM KALI LINUX

Projeto de pesquisa apresentado ao curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito à obtenção do Certificado de Conclusão.

Orientando(a): Giancarlo Rosa de Jesus Junior
Orientador(a): Prof. Douglas Sanches da Cunha

Assis/SP
2017

FICHA CATALOGRÁFICA

JUNIOR, Giancarlo Rosa de Jesus.

Estratégia de ataque em ambiente simulado com Kali Linux / Giancarlo Rosa de Jesus Junior. Fundação Educacional do Município de Assis – FEMA – Assis, 2017.

21p

1. Kali Linux. 2. Estratégia de ataque.

CDD: 001.6
Biblioteca da FEMA

ESTRATÉGIA DE ATAQUE EM AMBIENTE SIMULADO COM KALI LINUX

GIANCARLO ROSA DE JESUS JUNIOR

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Prof. Douglas Sanches da Cunha

Examinador: Prof. Fábio Eder Cardoso

Assis/SP
2017

RESUMO

Com o passar dos anos, nota-se que cada vez mais o ambiente empresarial necessita de uma boa segurança, podem-se afirmar isto analisando a evolução da tecnologia e investimento desta área ainda pouco valorizada. Ao decorrer desta monografia, será realizado um amplo estudo sobre o sistema operacional Kali Linux, deste modo, aplicando um estudo do porquê usar esta plataforma robusta e preparada, em seguida, a monografia mostrará a importância de aplicar a estratégia na invasão em um alvo, mostrando que não basta apenas buscar realizar a penetração sem que a mesma fosse bem elaborada. Por fim, a monografia mostrará a parte pratica dos estudos apresentados anteriormente, de forma que possa demonstrar cada etapa da estratégia de ataque e assim mostrar algumas das melhores ferramentas para cada objetivo. No final, será analisado que quando se trata de segurança nunca será afirmado que alguém está totalmente protegido.

Palavras-chave: Kali; Linux; Estratégia; Ataque; Segurança.

ABSTRACT

Over the years, we can notice that the corporative market needs a good security, we may state that by looking the evolution of the tecnology and investiment in this undervalued field. In this essay, it'l be made a broad study about Kali Linux and the reasons behind using this platform. Following this, the essay will show the importance of using invasion strategies on a target, showing that unplanned penetration testing is not enough. Finally, this essay will show the results of the aforementioned studies, in a way that it could demonstrate every step in a strategic digital invasion and the best tools for each objective. Concluding this, it'll be demonstrated how security is never absolute.

Keywords: *Kali; Linux; Strategy; Attack; Safety.*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. **INTRODUÇÃO**

Uma das áreas em destaque no mundo da tecnologia é a Segurança. Com o avanço da mobilidade, aumento de servidores e crescimento das integrações de rede as pessoas tendem a ficar mais vulneráveis. Por isso, o objetivo da monografia é criar uma estratégia de ataque em um servidor utilizando um ambiente simulado e o Kali Linux, para que então, pode-se obter conhecimento nesta área.

De acordo com *Offensive Security - Official Documentation*, o Kali Linux é uma distribuição Linux baseada em Debian com foco em teste de penetração avançado, contendo diversas ferramentas destinado a segurança da informação, como escaneador de portas, software para descobrir senhas, software para testar segurança em rede sem fio, entre outros.

O ambiente montado para realização dos estudos possuirá o seguinte cenário: área de ataque, área de defesa e servidor - interligados em uma mesma rede.

A formulação do ataque será dividida em cinco partes: o reconhecimento, avaliação do alvo, exploração, escalonamento de privilégios e manutenção do ponto de apoio.

O reconhecimento é onde tudo começa. Nesta etapa se realizara um estudo completo da rede e detectaram todos os possíveis alvos. Realizaram também o estudo pessoal do alvo, coletando informações sobre família, *hobbies* e afins. Isto ajudará quando precisar “quebrar” senhas pessoais de administrador. Este tópico é a base de toda a estratégia, pois com estas informações realizaram o escopo do trabalho.

Em seguida, será realizado a avaliação do alvo para coletar dados como avaliação das vulnerabilidades do alvo, possíveis fraquezas reais, informações de aplicações usadas e portas livres para acesso. Uma excelente fase de reconhecimento pode melhorar a precisão das vulnerabilidades, reduzindo o tempo da coleta de informações, dificultando assim, que a defesa possa detectar algum rastro deixado.

A fase de exploração é designada para explorar todas as vulnerabilidades encontradas na etapa anterior. Verificando, desta forma, se ela realmente é um ponto de acesso ou uma falsa vulnerabilidade deixada pela defesa, porém não será

invadido o alvo ainda, apenas obter mais informações. É nesta fase que analisaram todas possíveis vulnerabilidades e montaram uma estratégia de ataque.

Com o ataque ao servidor terão o acesso do mesmo, porém ainda não alcançarão o principal objetivo. Com este acesso terão a chance de visualizar o conteúdo público e recursos usados pelo servidor, mas também haverá outra função nesta fase de escalonamento de privilégios: usarão ferramentas para chegar ao ponto de terem um usuário *(login)* de administrador do servidor. Assim, poderão acessar os dados sensíveis, críticos e até mesmo a infraestrutura.

Como parte final, realizarão a manutenção do ponto de apoio. Organizara o acesso removendo vestígios de mensagens de erro gerado pelo esforço do acesso, mascarar esses canais e procurar outras falhas como novas contas de administração, túneis criptografados e outros canais de acesso à rede, caso o caminho principal seja descoberto pela defesa.

Atualmente pode-se observar um grande desenvolvimento na área da segurança da informação, principalmente nos campos de *pentest, hacker* ético, etc. Normalmente, esses profissionais trabalham com empresas focadas apenas em preparar a infraestrutura de segurança de servidores, porém, existem casos específicos em que as próprias empresas têm uma equipe especializada na área de segurança. Independente da forma de trabalhar, o objetivo é o mesmo: tentar invadir o servidor para que possa eliminar a vulnerabilidade encontrada, garantindo assim a segurança da empresa

1.1. **OBJETIVO**

A Segurança em TI é uma área de extrema importância. Por isso, neste projeto de pesquisa, será organizado alguns estudos de ataque em ambiente simulado, montando e realizando uma estratégia a fim de ter sucesso no acesso ao servidor protegido, além de adquirir mais conhecimento nesta importante área.

1.2. **PERSPECTIVA DE CONTRIBUIÇÃO**

Esperasse que este projeto de pesquisa contribua para o aprendizado dos alunos no ambiente simulado, bem como para os demais estudantes da área de tecnologia para que possam dar continuidade à pesquisa apresentada nesta Instituição.

1.3. **MOTIVAÇÃO**

A principal motivação para o desenvolvimento deste projeto de pesquisa foi a possibilidade de aprender mais sobre a Segurança, uma área que está crescendo e despertando o interesse de profissionais e empresas. Além disso, o tema apresentado é de suma importância para que consiga entender melhor como funciona todo esse “cenário”, especialmente para as pessoas que pretendem seguir a carreira na área.

1.4. **JUSTIFICATIVA**

Acreditasse que este estudo é fundamental e eficaz para os participantes do ambiente de ataque-defesa de um sistema. A intenção é adquirir conhecimento na área de Segurança, como funciona um ataque, como é realizado o estudo e criação das estratégias, e também visualizar como a defesa trabalha para impedir o acesso ao servidor.

1.5. **METODOLOGIA DE DESENVOLVIMENTO**

Para a elaboração deste trabalho de conclusão de curso será consultado livros e tutoriais sobre a realização de estratégias de ataque, afim de realizar as cinco fases da invasão ao servidor.

Para que possa ser usado as ferramentas adequadas para cada fase também será utilizado a consultar em artigos (sites especializados) que contenham as informações necessárias sobre cada ferramenta relacionada ao Kali Linux, pois este será o sistema operacional usado.

1.5.1. **RECURSOS**

Computador de ataque;

- Sistema Operacional Kali Linux**;**
- Infraestrutura de rede;
- Servidor de defesa;
- Servidor;
- Livros, tutoriais e sites sobre Kali Linux e suas ferramentas;

1.5.1. **RESUMO**

O Segundo capitulo será reservado para a pesquisa do sistema operacional Kali Linux, tais como suas propostas de trabalho, modelos de instalações finalizando com suas regras para a comunidade oficial, este capitulo mostrará as maneiras de instalações do sistema operacional, afim de demonstrar como dar os primeiros passos com a ferramenta.

Com a continuação da monografia será demonstrado no terceiro capitulo como são realizadas as invasões, tais como a demonstração de como conseguir realizar uma estratégia de ataque, dividindo-a em cinco etapas importantes na construção do sucesso da penetração em um alvo.

Em seguida, no quarto capitulo será demostrado a pesquisa anterior em pratica, mostrando algumas ferramentas ideais para cada fase dita no terceiro capitulo e analisando com cuidado cada informação colida com o desenvolvimento dos estudos.

2. **KALI LINUX**

Neste capitulo, será realizado um amplo estudo sobre o que é Kali Linux, como ele trabalha e como iniciar com o sistema operacional, desta forma demonstrando seus recursos e a maneira com quem a comunidade trabalha.

Segundo a introdução *what is* Kali Linux na documentação oficial, o Kali Linux é um sistema operacional elaborado para teste de segurança, tais como pesquisa de segurança, teste de penetração, engenharia reversa entre outras funções. Foi elaborada baseada em outras duas distribuições Linux, pode-se afirmar que sua base foi criada em cima da distribuição Debian, porém, o Kali Linux é uma evolução de outro sistema operacional com foco em segurança, chamado BackTrack, que por sua vez é baseado no sistema Ubuntu. Kali Linux foi desenvolvido e financiado por uma empresa líder em treinamentos e certificações na área de segurança da informação, Offensive Security, fundado no dia 13 de março de 2013.

2.1. **RECURSOS**

O Kali Linux é um sistema operacional baseado em Debian cujo seu núcleo é desenvolvido para a área da segurança. De acordo com a introdução ao Kali Linux escrito pela equipe da *Offensive Security* na documentação oficial, como diferencial o Kali Linux obtém os seguintes conteúdos:

- Mais de 600 ferramentas com o foco em invasão e auditoria de segurança, muitas das ferramentas do sistema BackTrack foi mantido pelo ótimo desempenho, porém outra ferramenta não se manteve pelo fato de duplicar funções dos demais programas.
- Compatível com o FHS, ou seja, o Kali Linux segue a estrutura de documentos e diretórios padrão do Linux, evitando assim dificuldade ao migrar para o sistema operacional.
- O *Kernel* do Kali Linux contém os patches de injeção mais recentes incluídos, para que possa sustentar um ataque ou estudo de rede.

- Kali Linux é um sistema completamente personalizável, desta maneira podendo deixar sua parte gráfica de acordo com o gosto do usuário, ou até mesmo podendo optar pelo download de outras interfaces gráficas do Linux, como XFCE, LXDE, Mate entre outros.
- Para os usuários mais exigentes, a distribuição conta com a construção de *scripts* do *live-build* Debian, essencial para os usuários que pretende criar o Kali Linux ideal para o seu próprio tipo de trabalho, assim podendo controlar os repositórios que o sistema operacional depende e muitas outras configurações.
- Como hardware ARM (*Acorn RISC Machine*) estão se tornando cada vez maior no mercado por conta do seu tamanho e preço, a equipe do Kali Linux criou um suporte robusto, ate mesmo para esse tipo de hardware, desta forma criando um sistema operacional e repositórios próprios para os modelos ARM (Raspberry Pi, BeagleBone Black, Smartphone).

2.2. **INSTALAÇÃO KALI LINUX**

De acordo com a documentação oficial *category:* 3. *Installing* Kali Linux, um fato curioso sobre o Kali é sua usabilidade, segundo a documentação oficial o sistema não se trabalha sem um superusuário (*root*), exceto algumas ferramentas de invasão que tem opções de escalonamento de privilégios, para que se usufrua do sistema é necessário configurar uma senha do *root*. Caso a senha não seja informada, o sistema automaticamente coloca a senha do *root* como *“toor”*, sem as aspas.

Para a instalação do sistema operacional Kali Linux, primeiramente o passo a seguir é verifica a intenção do usuário, pois a uma variedade muito grande de instalação, como o objetivo do trabalho não é explicar a instalação do sistema operacional, listarei algumas possibilidades apenas, seguindo a documentação oficial do kali linux:

- Instalação comum em computadores;
- Instalação em máquinas virtuais, normalmente usados para testes de ferramentas específicas.
- Instalação em pendrive, este recurso tem como vantagem evitar a formatação e instalação do sistema em computadores, rodando então através de uma iso que contem no pendrive. É importante lembrar que esta maneira de usar o sistema operacional não armazenará os dados como *log* de penetração e outros arquivos na máquina, para que possa ter esse tipo de armazenamento, temos que configurar a persistência na instalação do Kali Linux no pendrive;

Além dessas formas, existem algumas diferenças da versão do sistema de acordo com a arquitetura utilizada, por exemplo, a arquitetura ARM contém uma versão específica para a instalação.

2.3. **COMUNIDADE**

Segundo a documentação do Kali Linux *category:* 3. Kali *Community Support*, notasse que a comunidade vem crescendo cada vez mais nos últimos anos, além disso, as pessoas que mantêm o sistema operacional criaram um grupo de autoajuda, com o nome de “evitando *bugs* no Kali Linux”. Esse grupo trabalha com pessoas que não contam com nenhum retorno financeiro, caso você tenha um problema no sistema operacional, eles pedem a liberdade de mexer no seu sistema para olhar o erro, desta forma, quando se resolve o problema automaticamente entram em contato com os desenvolvedores para que possam corrigir o erro relatado.

A equipe do Kali Linux demonstra que se importa com o usuário aprendiz, ou que busca informações sobre determinada ferramenta e estratégia de ataque, desta forma, o fórum oficial contém algumas regras como:

- A equipe que mantêm o fórum é bem rigorosa com a manipulação do Kali Linux, pois a mesma ferramenta que pode ser usado para estudar sobre segurança, invasão ou apenas obter a documentação de vulnerabilidade é a mesma ferramenta que pode ser usada para fins devastadores e ilegais, desta forma os profissionais que manter o fórum oficial é bem claro ao se referir que não permitem qualquer atividade ilegal ou dúvidas sobre isto no fórum.
- É proibido a divulgação de dados de rede de computadores ou qualquer ambiente que não seja de teste. Caso a equipe encontre alguma publicação deste tipo será excluída instantaneamente.
- Quando se publica alguma dúvida ou algo do tipo, o dono da publicação será responsável por qualquer ação relacionada ao seu post.

3. **ESTRATEGIA DE ATAQUE**

O capitulo a seguir, tem como principal foco realizar pesquisas e demonstrações de como realizar uma estratégia de ataque, apresentando os modelos de ataque e as fazes que terão que seguir para que os testes de penetração sejam realizados.

Quando falam que um determinado servidor sofreu um ataque, normalmente as pessoas relacionam o ocorrido a um determinado criminoso que, simplesmente ao acessar um computador e as ferramentas necessárias, realizou o ataque para roubar informações ou até mesmo na intenção de simplesmente encerrar determinada função do servidor. As pessoas tem isso em mente porque é comum visualizar em filmes esta maneira de ataque: a imagem de uma pessoa que em poucos minutos consegue realizar o ataque a um servidor com muita importância. Na realidade, não é desta forma que ocorrem os ataques. Eles precisam ser muito bem elaborados, com diversas etapas e na maioria das vezes com uma ou mais equipes trabalhando com o mesmo objetivo, cada um com uma determinada função diferente, segundo o livro *Web Penetration Testing With* Kali Linux.

3.1. **MODELOS DE TESTE**

O teste de segurança ou ataque contém alguns modelos de invasão, diferenciados em teste de caixa preta, teste de caixa branca e teste de caixa cinza, com base no livro *Web Penetration Testing With* Kali Linux a seguir será explicado um pouco mais desses modelos.

- O teste de caixa preta se resume aos ataques que não contém nenhuma ou pouquíssima informação do alvo. Este teste costuma ser mais específico para que o invasor consiga achar uma maior variedade de vulnerabilidade, porém a porcentagem de erro ou a chance da defesa do servidor encontrar o ataque é muito maior, pois consequentemente sem as informações de infraestrutura de rede, por exemplo, o ataque acaba sendo menos camuflado e os testes para a penetração no servidor mais visíveis.

- O teste de caixa branca tem a função de ser mais específico em uma única função do servidor, contendo o reconhecimento do alvo muito maior que o teste de caixa-preta, e normalmente não tem apenas as informações da empresa, mas sim, da vida pessoal de quem administra a mesma. E isto a torna ideal para testar vulnerabilidades específicas e documentá-las posteriormente.
- O teste de caixa cinza é o mais usado em ataques e teste de segurança. Trata-se de uma união do teste de caixa preta e caixa branca contendo mais informações úteis do alvo ao mesmo tempo em que realiza uma varredura para encontrar o máximo de vulnerabilidade possível. Esta opção acaba sendo a mais utilizada, pois quando se trata de um invasor em um alvo qualquer, coleta-se a informação antes de efetuar o ataque, fugindo da opção do teste de caixa preta. E quando falamos dos profissionais em segurança, estas pessoas acabam fazendo os mesmos testes para simular um ataque verdadeiro, realizando assim o teste de caixa cinza também.

3.2. **FORMULAÇÃO DO ATAQUE**

Para que se possa realizar um ataque de maneira organizada precisasse passar por algumas etapas: o reconhecimento, avaliação do alvo, exploração, escalonamento de privilégios e manutenção do ponto de apoio. Apesar de todos os ataques precisarem destas etapas, não tem uma regra ou nome específico para cada uma. O estudo das etapas está sendo realizado segundo o livro *Web Penetration Testing With* Kali Linux, de Joseph Muniz e Aamir Lakhami.

O processo de reconhecimento serve para que possa coletar o máximo de informações do alvo. Considerasse está uma das etapas principais, pois caso não seja realizada a coleta o ataque acabou sem ao menos começar. Logo, para que se possa ter sucesso na formulação de um ataque, é de extrema importância uma coleta de dados bem-sucedida. Conforme o estudo, os testes de caixa-preta requerem uma atenção maior nesta etapa, pois os dados não são fornecidos como no teste de caixa branca.

Entre as opções para se coletar o reconhecimento, o atacante usará pesquisas realizadas na internet sobre o alvo, os recursos de monitoramentos, coletas de informações de pessoas e processos, digitalizações para obter endereços IP e sistemas utilizados pelo alvo, bem como engenharia social através de serviços como *help desk* e outros meios.

Como dito anteriormente, o reconhecimento é o primeiro passo para elaborar o ataque, independente se realmente realiza um ataque ou apenas confirmasse um determinado dado ou vulnerabilidade. Através dos dados colhidos posteriormente os atacantes traçarão as estratégias em vulnerabilidades mais fáceis para chegar ao objetivo, pois irão conter uma documentação do alvo, como exemplo quais portas são utilizadas para os serviços prestados, onde é hospedado, etc.

O sistema operacional Kali Linux, oferece uma categoria de ferramentas chamada coleta de informações. Nesta categoria encontram o que precisa para realizar o reconhecimento (Joseph Muniz; Aamir Lakhani, 2013, p.17).
Após esta etapa precisasse conter as seguintes informações:

- Alvo (s) identificado (s);
- Tipos de sistemas usados;
- Portas usadas;
- Serviços em execução;
- Informações de engenharias social;
- Descoberta de documentos;

Quando finalizasse o reconhecimento, conterão os relatórios de dados do alvo com suas possíveis vulnerabilidades, então é a hora de chegar ao próximo passo: a avaliação do alvo. Neste momento, o invasor deve saber o suficiente do alvo para que possa testar cada vulnerabilidade encontrada na fase anterior. Com isso, concluísse a fase de análise do objetivo.

Com a fase de reconhecimento, obtenha-se uma avaliação do alvo mais elaborada porque os invasores podem ir direto às vulnerabilidades encontradas. Caso não seja feita com eficiência a etapa anterior, o invasor deve procurar as vulnerabilidades por ferramentas de escâner de rede. O problema em usar estas ferramentas é que elas

são fáceis de ser detectadas pela defesa do alvo. Porém, se utilizar uma ferramenta para investigar uma vulnerabilidade específica, as chances de defesa existentes no alvo para identificar o ataque são menores.

Esta etapa pode ser realizada por ferramentas, conforme explicado anteriormente. O sistema operacional Kali Linux contém um grupo de ferramentas próprias para esta tarefa, mas também pode ser realizada manualmente ficando a critério do invasor (Joseph Muniz; Aamir Lakhani, 2013, p.18).

Após esta etapa, deverá ter as seguintes informações:

- Analise das fraquezas do objetivo;
- Identificar e priorizar as vulnerabilidades do objetivo;
- Descoberta de documentos;

O próximo passo é a exploração. Esta etapa é vinculada a documentação da etapa anterior, pois agora podem saber se as vulnerabilidades são reais ou algo criado pela defesa para enganar um suposto ataque. Vale lembrar que ainda não realizaram a penetração do objetivo. Apenas uma investigação em cada vulnerabilidade para torná-las reais ou não.

Para que posam garantir sucesso nesta fase, dependesse muito das etapas anteriores, afinal a maioria dos *exploits* são criados para vulnerabilidades específicas e não genéricas, e caso sejam executadas de maneira incorreta, podem gerar consequências indesejáveis. A melhor estratégica adotada é conseguir um grupo de vulnerabilidades e assim estudar a melhor maneira de formular um ataque.

Aqui o objetivo será: através das vulnerabilidades conseguir alguma credencial do alvo (Joseph Muniz; Aamir Lakhani, 2013, p.19).

Nesta etapa deverá conter:

- Exploração das vulnerabilidades;
- Capturar dados não autorizados;
- Explorar mais sistemas e aplicações;
- Descoberta de documentos;

Entrando na fase de escalonamento de privilégios o invasor tem que ter em mente que a exploração realizada anteriormente não garante o objetivo da penetração ainda, pois esta etapa tem muitas limitações. Com o escalonamento de privilégios seguirão para etapa em que poderão obter itens críticos como infraestrutura, senhas, etc.

O escalonamento de privilégios tem por objetivo agir na descoberta de senhas, progredindo até chegar em um acesso do administrador. Neste trajeto ainda se realiza muitas coletas de informações. Ressaltando que em nenhum momento os invasores param de procurar documentos. Com esta etapa não é diferente, e o Kali Linux contém um arsenal completo de ferramentas para realizar a tarefa necessária (Joseph Muniz; Aamir Lakhani, 2013, p.19).

A seguir, os itens necessários para finalizar a etapa de escalonamento de privilégios:

- Obter acesso superior do objetivo;
- Obter informações de senhas de usurário;
- Obter acesso a outros sistemas;
- Descoberta de documentos;

Por fim, o invasor tem a manutenção do ponto de apoio que se resume em um suporte a penetração. Com o esforço gerado para que possa alcançar o objetivo, naturalmente se acumula algumas sujeiras no alvo. O foco aqui é eliminar essas sujeiras para que a defesa não possa suspeitar do ataque. Da mesma maneira que existem ferramentas para que possam realizar o objetivo de ataque, também existem ferramentas para que a defesa possa investigar qualquer tipo de sujeira gerada e assim detectar um ataque. Então, o dever é garantir que o rastro seja apagado e assim concluir criando outras maneiras de invasão do alvo, para que, acaso a defesa consiga fechar o acesso principal, o invasor tem outros caminhos para continuar com o objeto (Joseph Muniz; Aamir Lakhani, 2013, p.20).

Com isso o invasor deve realizar:

- Criar várias maneiras de acesso ao alvo;
- Remover provas de esforço da penetração;
- Injetar dados falsos (se precisar);
- Esconder caminhos de invasão com criptografia;
- Descoberta de documentos;

4. **TESTE DE ATAQUE COM PFSENSE**

Para conclusão do estudo realizado, este capitulo terá a pratica dos capítulos anteriores, contendo imagens do sistema operacional Kali Linux e logo após a descrição do que foi realizado na imagem. Também será demonstrado algumas ferramentas próprias para cada faze da estratégia de ataque.

4.1. **RECONHECIMENTO**

Para iniciar o estudo sobre a estratégia de ataque, primeiramente será realizado a fase de reconhecimento. O foco aqui é conhecer e avaliar o alvo, como base do estudo de reconhecimento será utilizado a referência do livro *Web Penetration Testing With* Kali Linux.

Para que possa iniciar os testes no ambiente simulado, será realizado a instalação do sistema operacional Xubuntu e logo após a configurar do serviço https. Com essa configuração poderam alocar um site rodando Localhost. Assim, realizando o teste primeiramente em cima deste serviço e sistema operacional.

Como ponto de partida, será analisado o alvo. Até agora sabemos que é um site, logo, concluísse que certamente as portas que contém um serviço será a 443 (Https) ou 80 (Http).

Para gerar conhecimento, quando o alvo é um site, pode-se usufruir de diversas ferramentas online para a coleta de informações. No ambiente, não será possível a utilização destas ferramentas porque o ambiente simulado contém um site teste rodando em *Localhost*, porém, será demonstrado brevemente a utilização de algumas ferramentas.

4.1.1. **WAYBACK MACHINE**

Segundo o livro *Web Penetration Testing With* Kali Linux com e evolução da internet todos os sites sofrem com um processo de atualização, isto é, troca de versão do site. Esta ferramenta pode armazenar o histórico de projetos de milhares de sites. Ou seja, se caso o invasor queira obter o conhecimento de como era o site em versões passadas para saber de vulnerabilidades que talvez não foram corrigidas com novas versões, este site será uma ótima ferramenta para o reconhecimento, no site do Wayback Machine podemos obter alguns exemplos de como usufruir da ferramenta.

Em seguida, será mostrado a utilização da ferramenta começando pela pesquisa do site alvo:

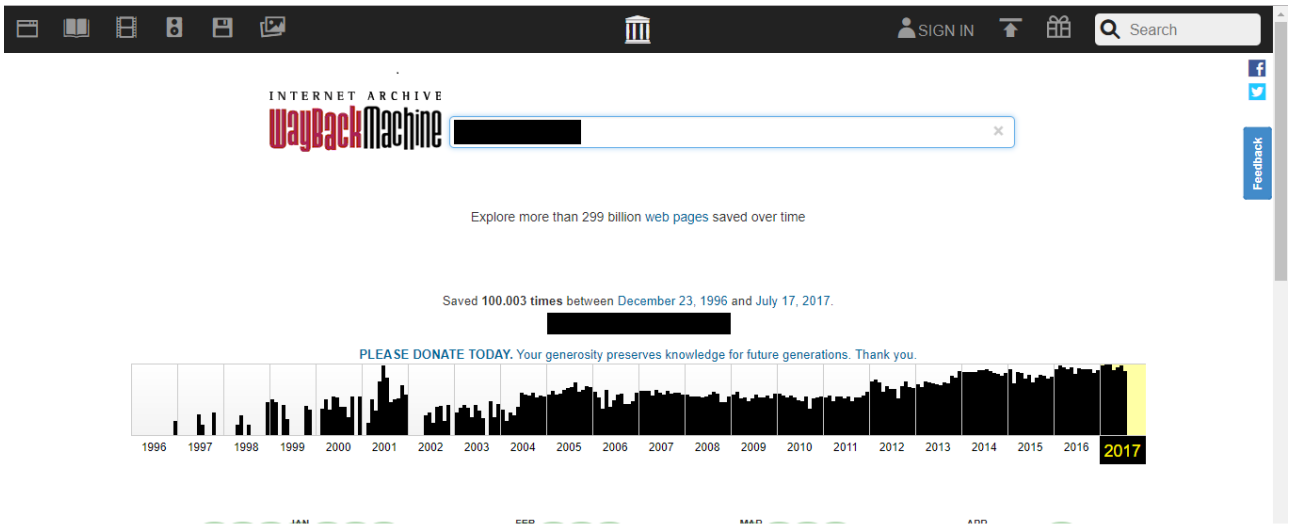

Figura 1- Wayback Machine (Pesquisa), Fonte: Elaborado pelo autor.

Pode-se observar que na tela inicial da ferramenta, necessita que o usuário informe o site alvo, seguido pelo ano, mês e dia em que se pretende colher as informações do alvo.

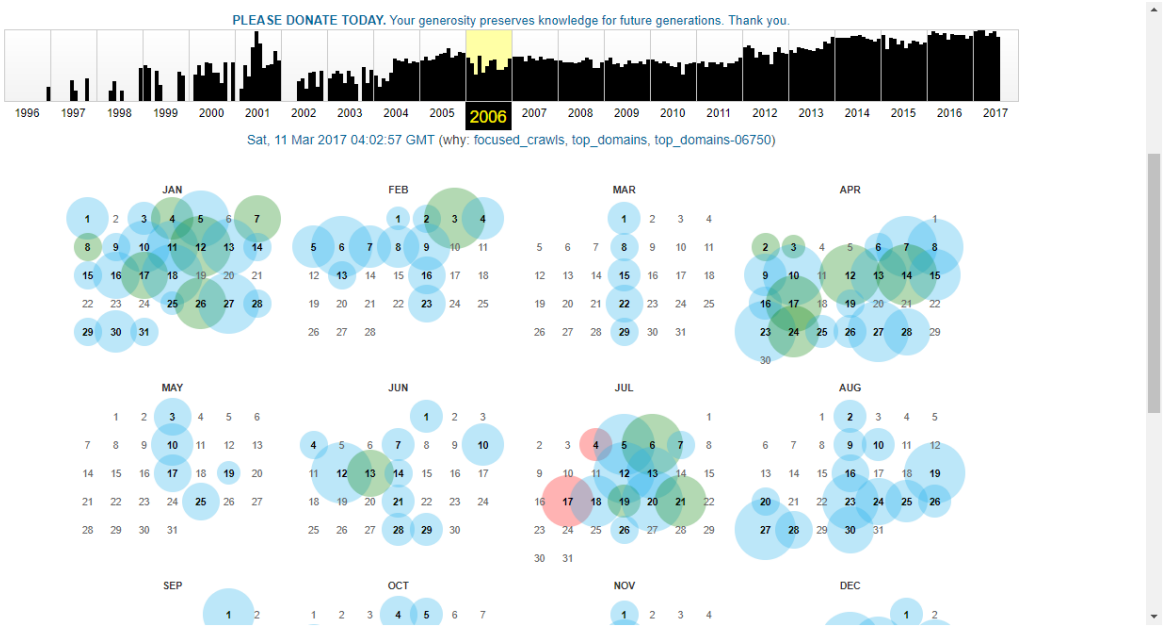

Figura 2- Wayback Machine (Escolha de período), Fonte: Elaborado pelo autor.

Na imagem a cima, houve uma demonstração da maneira em que o site se comporta quando se informa as informações da data desejada, para que se possa obter o download especifico, necessitasse que o usuário realize a ação de clicar no dia que se deseja obter a versão do site.

4.1.2. **ROBOTS.TXT**

Segundo a documentação oficial do robots.txt no próprio site da ferramenta, o robots.txt no caso não se encaixa no termo de ferramenta, pois ele é um arquivo de configuração que alguns sites contêm. Alguns sites precisam esconder determinadas páginas ou arquivos de mecanismos de busca, também conhecido como robôs web. Logo, esse arquivo na raiz do projeto serve para que os mecanismos de busca não consigam enxergar determinado conteúdo da página. Este recurso acaba sendo extremamente interessante para que o invasor possa obter conhecimento sobre o conteúdo que o alvo pretender esconder.

A seguir será demonstrado o robots.txt da rede social *Facebook:*

```
# Notice: Crawling Facebook is prohibited unless you have express written
# permission. See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: Applebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /hashtag/
Disallow: /l.php
Disallow: /live/
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /sharer/

User-agent: baiduspider
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /hashtag/
Disallow: /l.php
Disallow: /live/
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /sharer/

User-agent: Bingbot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /hashtag/
```

Figura 3- Robots.txt, Fonte: Elaborado pelo autor.

4.1.3. **ENGENHARIA SOCIAL**

Outra técnica que o invasor pode utilizar é a Engenharia Social. De acordo com o livro *Web Penetration Testing with Kali Linux*, de Joseph Muniz e Aamir Lakhami, todas as empresas contém algum tipo de Facebook, Linkedin, blog ou qualquer rede social. A Engenharia Social acontece quando o atacante se aproveita de ferramentas de marketing para então colher informações da empresa e ficar informado sobre o conteúdo que futuramente terá em mãos. Outro local em que podem realizar a Engenharia Social é os helpdesk, que boa parte das empresas contém. Neste ambiente os invasores podem tirar algumas informações que podem ser valiosas futuramente.

Conforme o atacante colhe mais informações de um alvo, aos pouco vão se familiarizando com o seu foco e rotinas. Quando visualizam uma simples postagem de contratação de funcionários, obtém-se uma grande variedade de informações

como o cargo que o funcionário vai exercer, salário, serviços que o futuro funcionário deverá saber, com quais ferramentas irá trabalhar (por exemplo, linguagem c++, Java, banco de dados Oracle, ferramentas para aplicações *web* ou *mobile*). Com certeza essas informações serão as mais valiosas que os invasores conseguiram, pois caso o foco seja uma empresa de criação de *software* saberão que eles usam a linguagem PHP em sistemas de rotina interna, podendo realizar uma ampla pesquisa e saber quais vulnerabilidades essas ferramentas contêm. Assim já terá um ponto de partida para realizar a próxima fase.

4.1.4. **LOCALIZAÇÃO**

De acordo com o livro *Web Penetration Testing with Kali Linux*, de Joseph Muniz e Aamir Lakhami, quando o atacante deseja realizar uma estratégia de ataque não podem deixar de obter nenhuma informação. Sabendo que a segurança cibernética é um conceito em que boa parte das pessoas não julgam como importante, até o momento de acontecer algo a elas. Com base nessas informações, pode-se até avaliar fisicamente um local para então poderem ter uma base da segurança existente no local. Quando usarem a ferramenta *Google Maps* e olharem como é o local do alvo, podem ter o conhecimento de como é feita a segurança física, e então tirar como base o investimento feito em segurança da empresa. Sabendo que deduzir uma informação é um pouco perigoso, pois devem ter em mente que isto é só uma base. Afinal, uma empresa pode não ter um investimento bom na segurança física, porém na cibernética pode ser um dos lugares mais seguros encontrados. Deste modo, devem aproveitar ao máximo a informação sem esquecer que ela é uma simples dedução.

4.1.5. **SHODAN**

De acordo com a documentação oficial do Shodan, certamente essa ferramenta, se não for o melhor meio de captar informação, está entre as melhores. Com o Shodan

o invasor pode obter informações de equipamentos que se conectam a internet, pois este site armazena esses dados e mostra através de uma busca.

Para demonstrar um breve exemplo, será realizado a busca com o nome “Windows XP”, que retornou com o seguinte resultado:

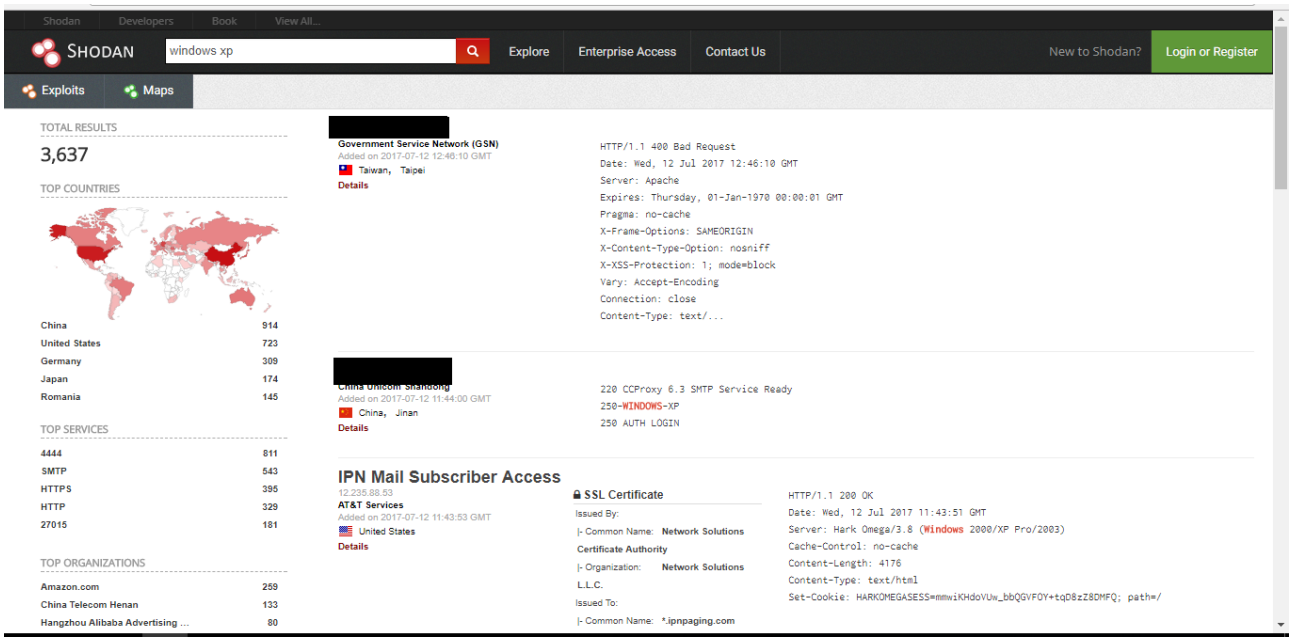

Figura 4- Shodan, Fonte: Elaborado pelo autor.

Pode-se observar que o Shodan trouxe informações muito valiosa como o IP do computador, o serviço usado, a tecnologia do servidor, a data da última conexão entre outras informações que, de acordo com a pesquisa, pode ser o suficiente para que possam ter informações da base de um determinado local. Com o Shodan pode-se obter o IP de câmeras, e assim, com ferramentas especificas, ter acesso a visibilidade dessas câmeras.

4.1.6. **GOOGLE HACKING**

Todos os dias, diversas pessoas usufruem das pesquisas da *Google*, e nos dias de hoje isto não é novidade. Mas o que muitas pessoas não sabem é que através do motor de busca do *Google* os hackers podem obter informações muito poderosas de

servidores ou serviços mal configurados. O objetivo até o momento não é demonstrar o funcionamento da ferramenta, porém com uma breve busca por aprendizado, qualquer pessoa consegue usufruir desse recurso, de acordo com o livro *Web Penetration Testing with Kali Linux.*

4.1.7. **HTTTACK**

Uma ferramenta frequentemente usada para fins de teste, porém quando o invasor está na prática não é muito indicada, o HTTrack de acordo com o livro *Web Penetration Testing with Kali Linux*, é uma ferramenta que permite que possam clonar um site específico junto com seus diretórios, e o interessante dessa ferramenta é que podem obter o conteúdo de um site e criar ferramentas personalizadas para um alvo especifico. Porém, como ela é uma ferramenta de varredura, não se tem o controle dela no alvo, e desta forma a ação efetuada fica mais fácil de ser detectada.

4.2. **AVALIAÇÃO DO ALVO**

Segundo o livro *Web Penetration Testing With* Kali Linux, com o decorrer das etapas, a próxima fase em que o invasor deve entrar é a avaliação do alvo. Nesta etapa conseguira as futuras vulnerabilidades de acordo com as informações colhidas na fase de reconhecimento.

Para iniciar a avaliação do alvo, primeiro o invasor deve ter em mente qual será o objetivo da invasão. No estudo elaborado, será realizado o teste de caixa preta. Como dito anteriormente, os testes de caixa preta são utilizados quando não se tem muita informação do alvo. Deste modo, como apenas realizamos um estudo de algumas ferramentas e não colocamos em prática em nosso ambiente simulado na fase de reconhecimento, consideramos que este teste é o que melhor se encaixa em nossa estratégia.

Iniciando com o teste de detecção de vulnerabilidades, será usado a ferramenta Nmap.

4.2.1. **NMAP**

De acordo com a documentação oficial no próprio site do Nmap, a ferramenta pode ajudar em diversas tarefas. Com ele o invasor pode descobrir *host* ativos ou não, descobrir portas abertas, serviços em execução e enviar alguns scripts já prontos. O interessante da ferramenta é que o invasor pode ter bastante informações sem muito esforço.

A seguir, será demonstrado o primeiro teste realizado em no ambiente simulado:

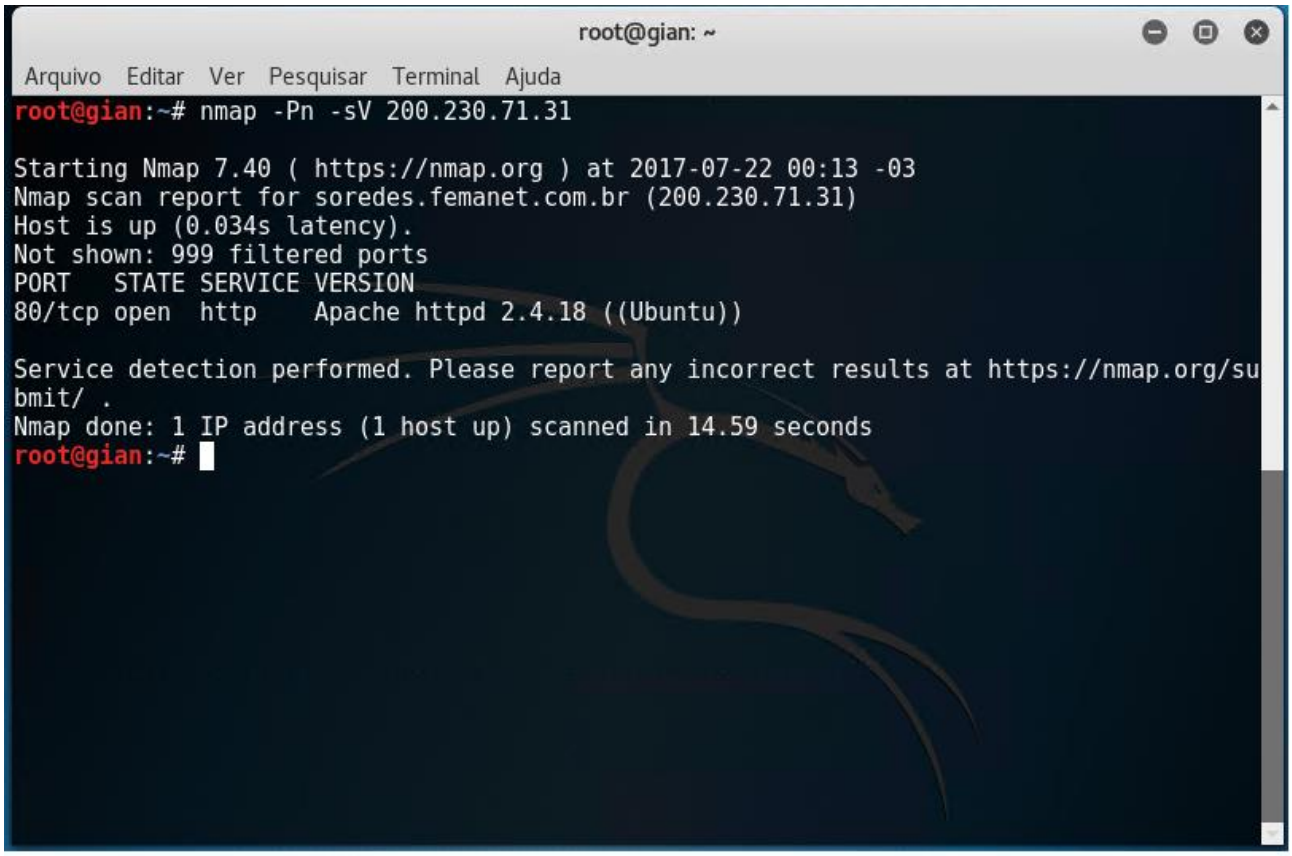

Figura 5 - Nmap –sV, Fonte: Elaborado pelo autor.

Na imagem acima, pode-se observar que ao passar o comando especificando o IP do alvo, o NMAP respondeu com o serviço ativo e se a porta está aberta ou não.

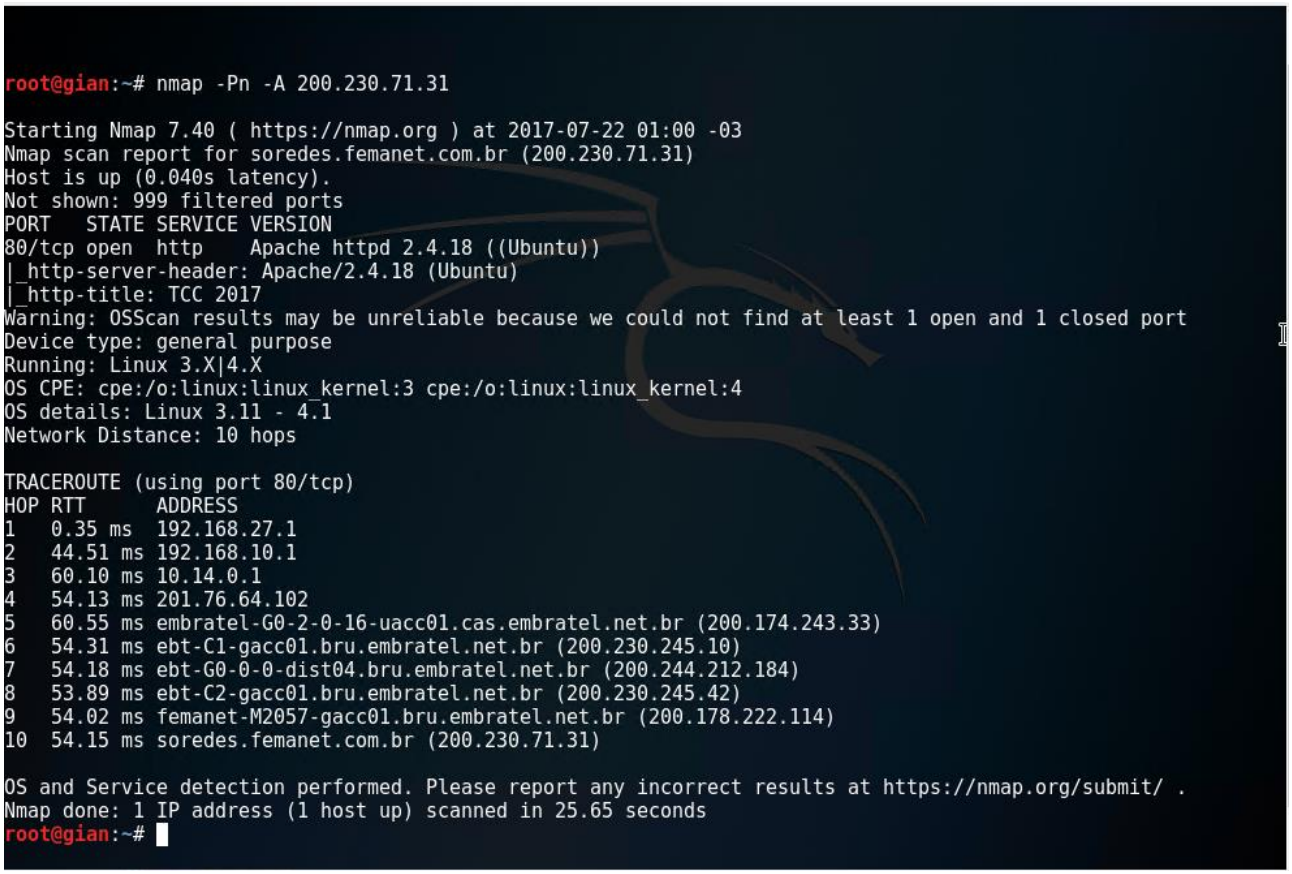

Figura 6 - Nmap –A, Fonte: Elaborado pelo autor.

De acordo com o comando executado, podem notar que se obteve algumas informações importantes, por exemplo, agora o invasor pode ter conhecimento que existe a porta 80 aberta, rodando o serviço http com o Apache 2.4.18 no sistema operacional Ubuntu. Esta informação sobre a versão da ferramenta do alvo é de extrema importância, pois a partir deste momento o invasor pode focar em pesquisas para vulnerabilidades de um único serviço e versão, reduzindo assim o tempo de verificação de portas realmente abertas para elaboração de estratégias. Sabendo que no ambiente simulado existe um arquivo no serviço http com o título Tcc 2017, além do caminho realizado pelo teste até chegar no Ip específico (Traceroute).

A seguir será demostrado a mesma ferramenta, porém usando a parte gráfica. Quando se usa o Nmap com a parte gráfica, a ferramenta passa a chamar Zenmap.

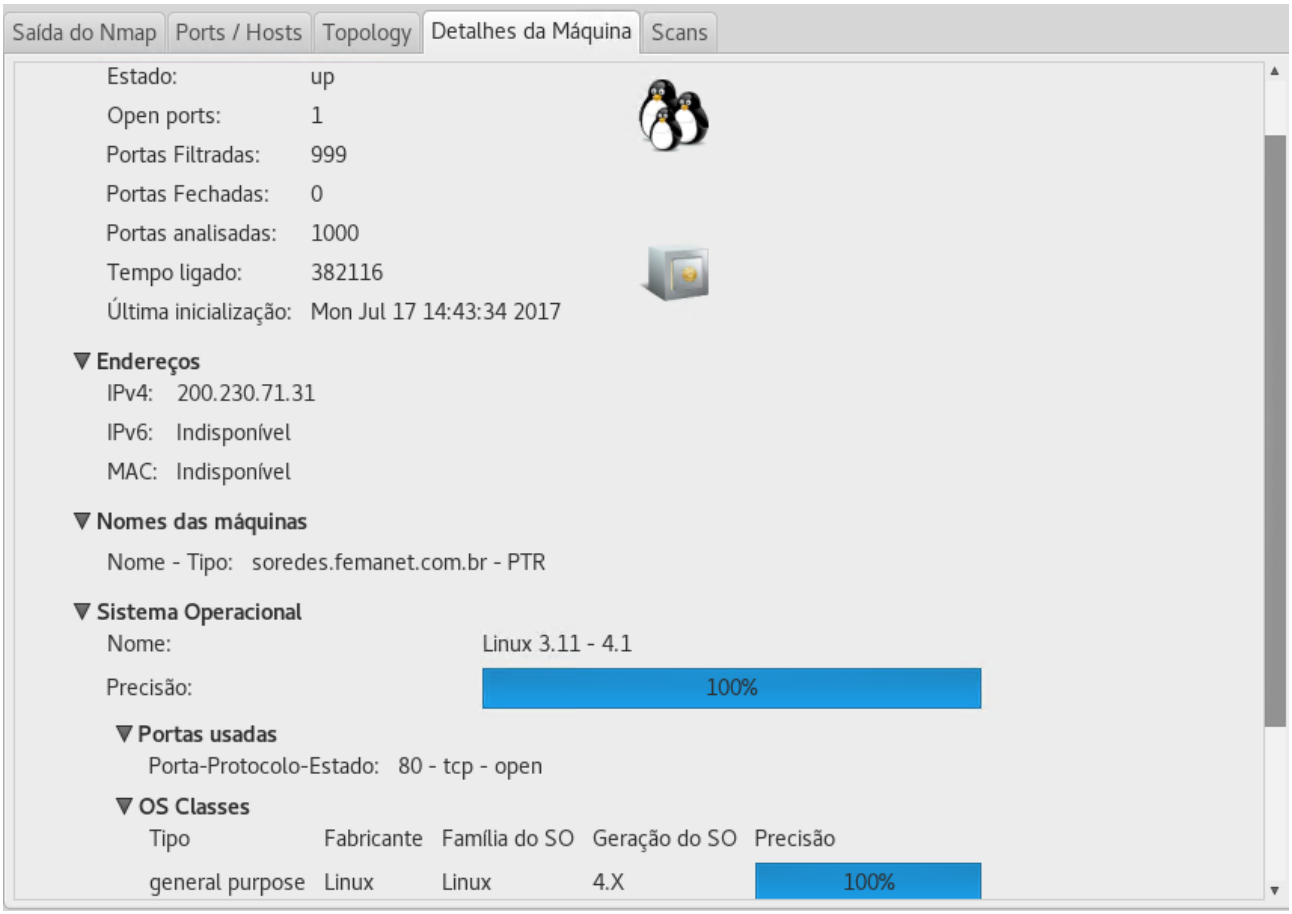

Figura 7 – Zenmap, Fonte: Elaborado pelo autor.

4.3. **EXPLORAÇÃO**

Após o tempo investido em reconhecimento e avaliação do alvo, certamente o invasor chegou em um ponto onde consegue obter diversas informações como os serviços usados, portas abertas, etc. Agora o objetivo será começar a construir a estratégia de ataque. Primeiramente pode-se iniciar priorizando o futuro ataque que irão usar, e para isto devem escolher qual tipo de serviço e em quais portas irão priorizar o ataque, segundo o livro *Web Penetration Testing with Kali Linux*.

No ambiente simulado, contem um excelente *firewall* (Pfsense), onde até o momento pode-se coletar apenas a informação do serviço http. Com isso, o atacante deve elaborar estratégias para usufruir de recursos que usam como alvo a porta 80 (porta destinada ao serviço http).

4.3.1 **METASPLOIT**

Segundo o livro *Web Penetration Testing With* Kali Linux, uma das ferramentas mais utilizada e conhecida na segurança da informação é o *Metasploit,* que contém em sua estrutura a utilidade para todas etapas de um teste, desde o início para conhecer um alvo, até o momento da invasão.

De acordo com sua documentação oficial o *Metasploit* é um *framework* que trabalha com scripts onda de acordo com o comando dado e realiza determinada tarefa. Os scripts encontrados dentro da ferramenta dividem-se em *Exploits, Auxiliary, Payloads, Nops, Encoders* e *Post*.

- Os *Exploits* são scripts criados para explorarem determinada vulnerabilidade do alvo. Na versão do Kali Linux mais recente contem disponível 1639 *Exploits*.
- Os scripts de *Auxiliary* serve para testar se determinado *Exploits* irá funcionar em determinada situação. Quando se trabalha com estratégia de ataque, esse tipo de script acaba sendo extremamente importante, pois em certo momento, dependendo do ataque, o invasor não quer deixar rastro, apenas testar se determinada ferramenta irá executar corretamente.
- Se consultar a documentação oficial da ferramenta, será observado que os *Payloads* equivalem a *Sockts*, ou seja, a API responsável em fazer com que a aplicação se comunique com a camada de transporte.
- Os *Nops* são responsáveis em garantir o bom funcionamento dos *Payloads* de forma que disponibilizem o necessário para os scripts trabalharem de maneira correta.

- *Encoders* tem uma função de extrema importância. Com este script pode-se mudar o código executado para que a defesa do alvo não consiga decifrar que aquele programa em execução é um vírus.
- Os *Post* são responsáveis pelos pós penetração no alvo. Sua função é manter o vínculo ao alvo para que depois da invasão ainda tenhamos contato com a vítima.

A seguir, será demonstrado a execução de alguns *scripts* pertencente a fase de exploração no ambiente simulado.

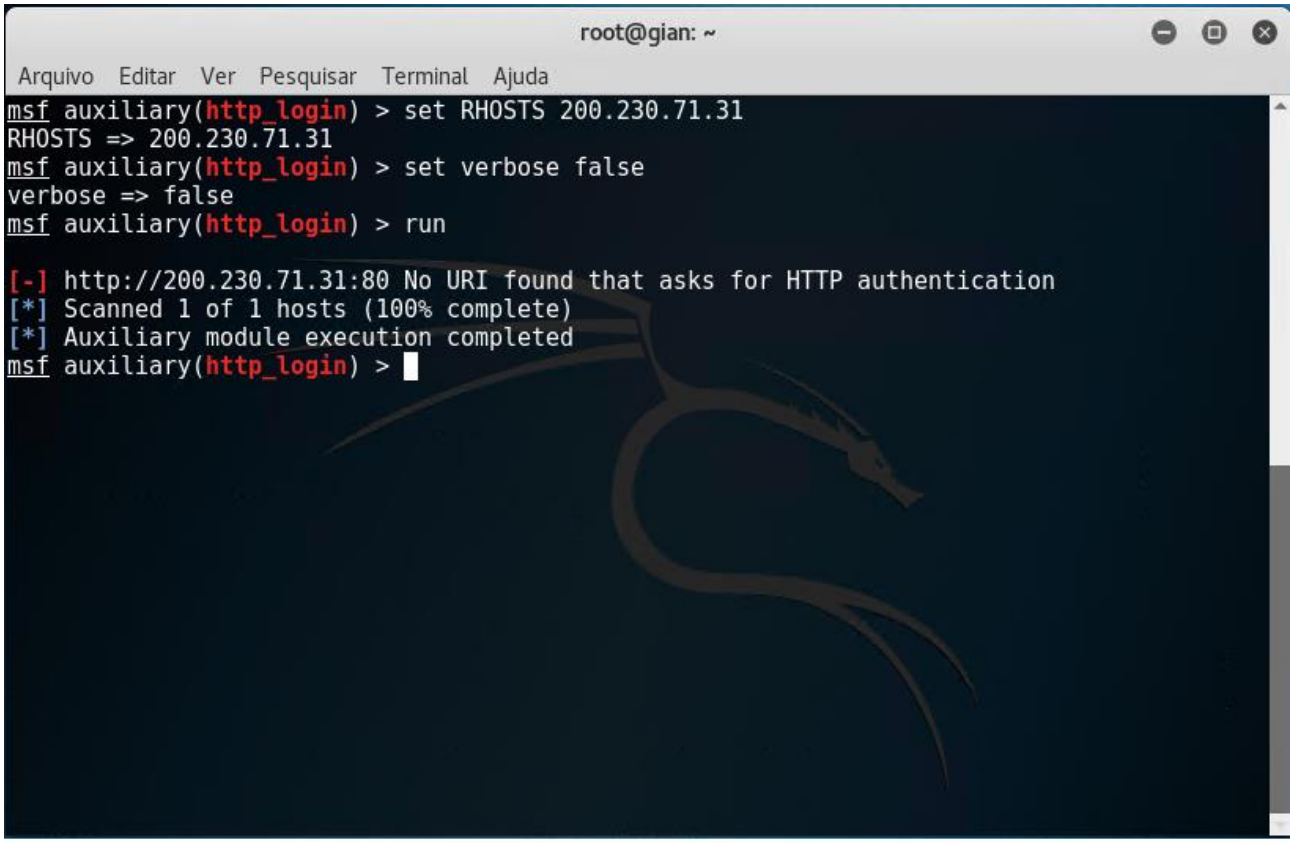

Figura 8 – Metasploit http login, Fonte: Elaborado pelo autor.

No exemplo acima, utilizasse um *script* do tipo *Auxiliary* com nome de Http_login. Este script realiza um scanner no alvo em cima da porta 80 como padrão, e seu objetivo é adquirir alguma senha relacionada ao protocolo Http. Como pode-se ver, não se obteve nenhuma senha.

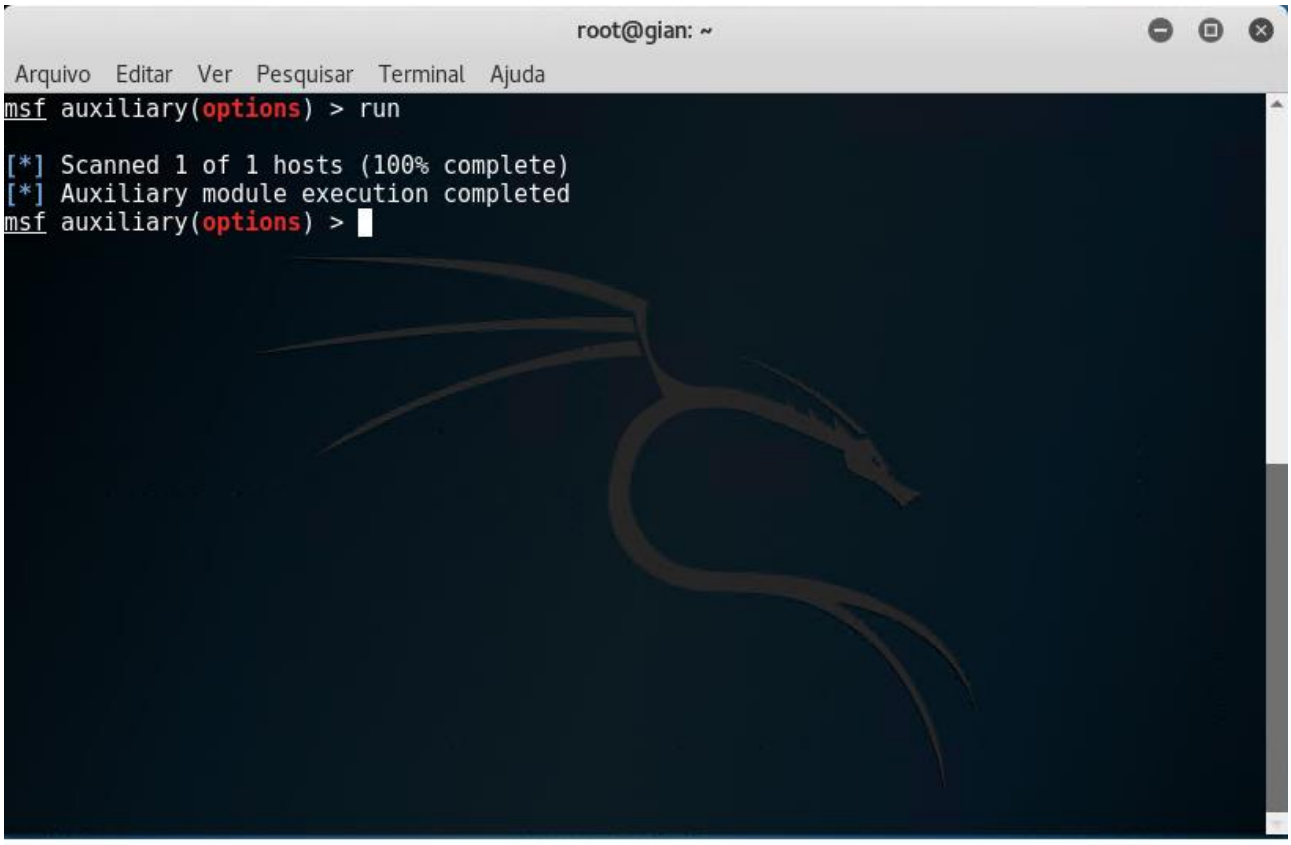

Figura 9 – Metasploit options, Fonte: Elaborado pelo autor.

Como podemos ver, foi realizado mais um teste onde não se obteve o resultado que se espera. Desta vez, foi utilizado um *script* onde o foco era conseguir toda informação existente sobre a aplicação do serviço http, ou seja, o objetivo deste teste era saber sobre o site existente no ambiente simulado.

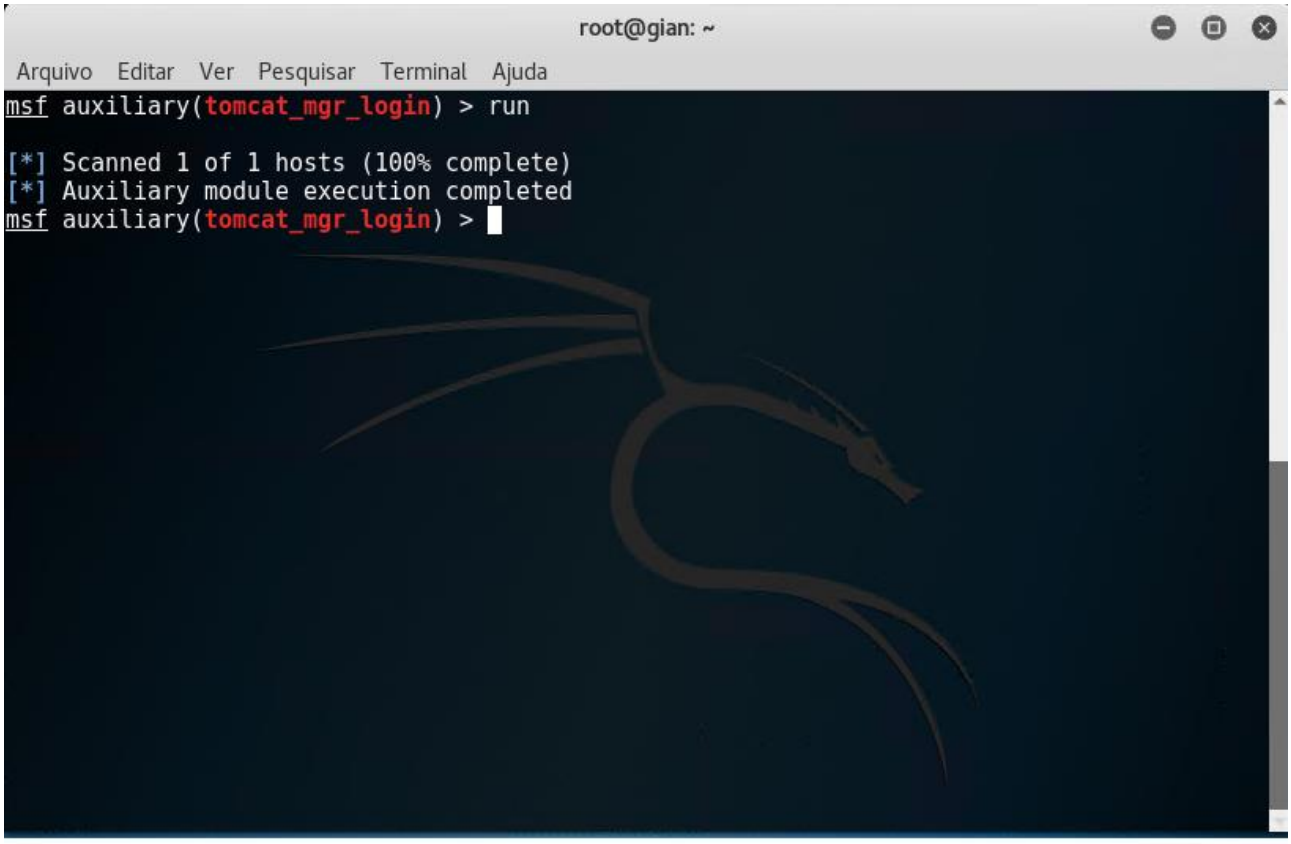

Figura 10 – Metasploit tomcat mgr login, Fonte: Elaborado pelo autor.

O teste realizado acima, foi o primeiro teste com “força bruta” (intensidade) utilizado. O *script* busca se conectar com a ferramenta *Tomcat* do alvo utilizando “força bruta”. Em seu banco de dados, possui um dicionário de palavras chave para quebrar senhas. A partir deste ponto, o *script* trabalha para tentar se conectar com o *Tomcat*. Porém, pode-se notar que não foi obtido o resultado desejado.

4.4. **ESCALONAMENTO DE PRIVILÉGIOS**

De acordo com o livro *Web Penetration Testing with Kali Linux*, saindo da fase onde verificamos se a possível vulnerabilidade é real, o invasor entrará no momento de realizar a penetração no alvo. O escalonamento de privilégios é o momento onde pode-se usar diversas ferramentas de ataque no alvo para a penetração. No

ambiente de teste, de acordo com as ferramentas usadas, já foi possivel detectar que a porta 80 está aberta. Neste caso, as opções mais usadas contra esse serviço são ataques DDos, Cross-site scripting e SQL injection:

- Ataque DDos ou negação de serviço, geralmente são realizados em sites onde o propósito é de simplesmente derrubar o serviço do ar. Os ataques DDos funciona com várias requisições enviadas ao site alvo, desta forma sobrecarregando o servidor e derrubando a aplicação. Na grande maioria das vezes, esse tipo de ataque é usado apenas para derrubar a aplicação rapidamente para que depois ela consiga restabelecer como antes, porém, quando ela volta ao normal precisa reiniciar suas ferramentas internas e é nesta hora que o objetivo do atacante é alcançado; após o servidor se reiniciar, ferramentas poderão detectar logins e senhas, e assim o objetivo do atacante será alcançado.

- O ataque de Cross-site *scripting*, está crescendo cada dia mais. Este recurso é quando o atacante consegue ter acesso ao site alvo e injeta *scripts* na página para que usuários da mesma possam ser, de certa forma, infectados. Nos deparamos com esse tipo de ataque todos os dias, na maioria das vezes são aquelas páginas cheias de anúncios.

- Ataques do tipo SQL *injection* é uma maneira mais simples de se efeituar um ataque, mas ela é um pouco complexa em relação ao estudo que necessita ter em cima da aplicação alvo. O ataque se resume em falhas na aplicação, seja *web* ou local. Deste modo o atacante consegue efetuar uma injeção de SQL e obter os dados necessários.

Para concluir a fase de escalonamento de privilégios, será realizado o ataque do tipo DDos com a ferramenta *Slowloris*.

Nativamente, esta ferramenta não vem instalada no Kali Linux. Entretanto, sua instalação é simples. Como o objetivo do trabalho não é a demonstração da ferramenta e sim o estudo do ataque, não abordaremos o procedimento de instalação da ferramenta.

4.4.1 **SLOWLORIS**

A ferramenta *Slowloris* permite realizar teste de negação de serviço. Para que possa usufruir deste recurso devesse passar o IP do alvo, a porta de destino o tempo de saída para envio de pacotes e a quantidade de pacotes enviados. A seguir será demonstrado o teste realizado:

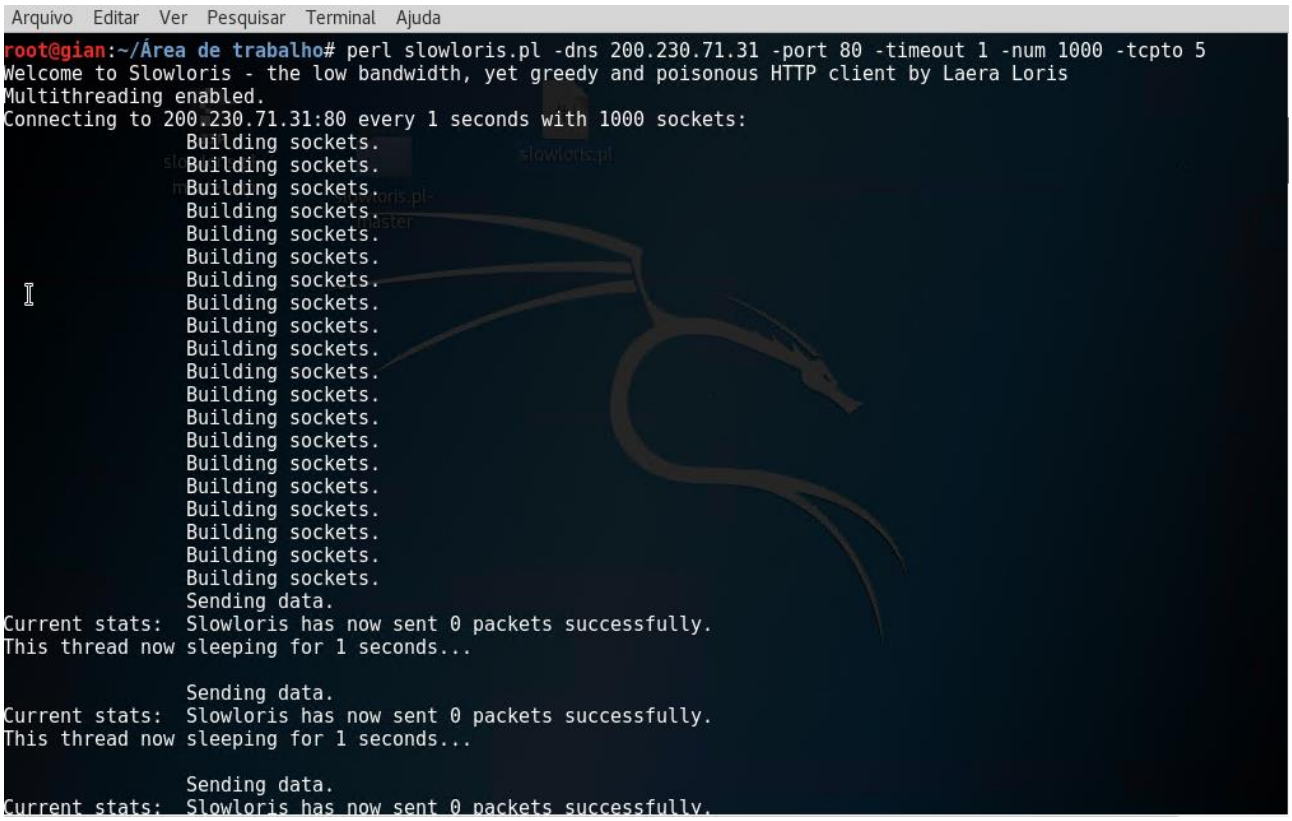

Figura 11 – Slowloris, Fonte: Elaborado pelo autor.

Como pode-se observar, após um período de tempo os envios de pacotes sofrem uma perda, isto pode acontecer por alguns motivos. O primeiro deles pode ser pelo fato da ferramenta não aguentar realizar tantas requisições durante muito tempo, e após alguns segundos retorna com o normal. O segundo pode ser a falta de resposta do servidor, isto pode ocorrer para que ele consiga se proteger porque a defesa reconhece várias requisições realizadas do mesmo Ip e assim pode bloquear o Ip temporariamente.

Antes de realizarmos o teste no ambiente de trabalho, o site estava no ar normalmente, como pode-se observar:

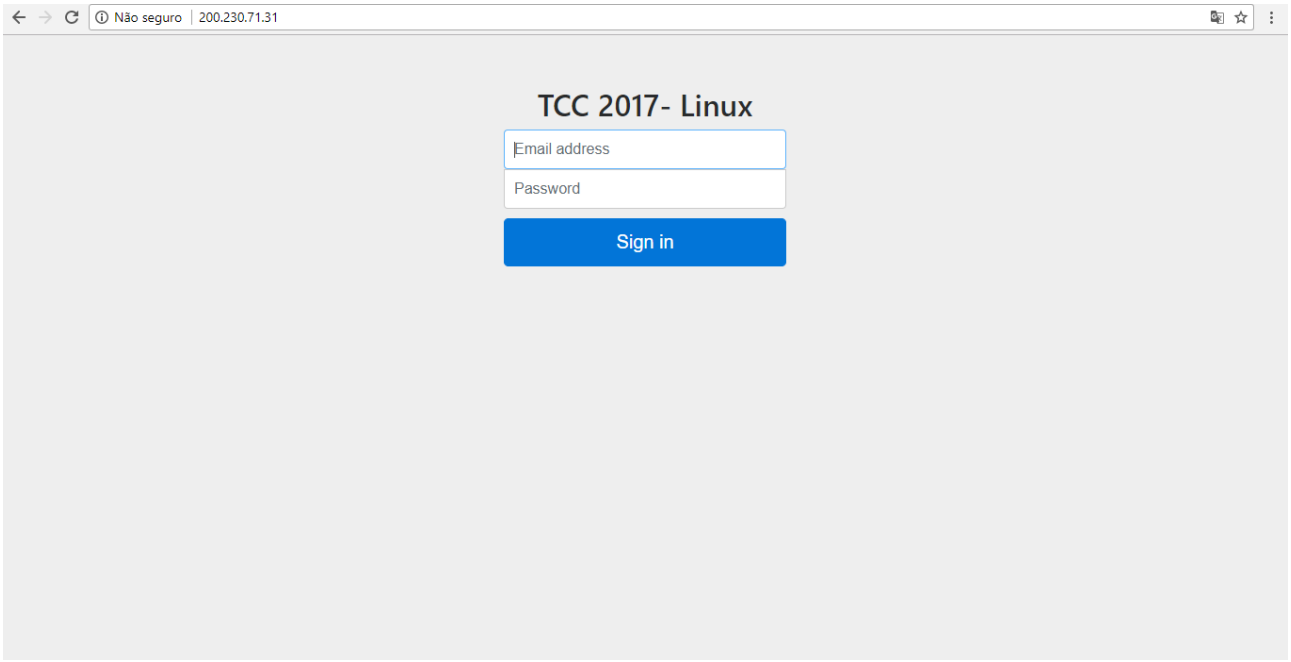

Figura 12 – Site ambiente simulado (Up), Fonte: Elaborado pelo autor.

Após a utilização do ataque de negação de serviço pode-se observar que o site não está mais no ar, ou seja, o objetivo de derrubar o mesmo foi concluído, como próximo passo, o invasor pode trabalhar com *scripts* para tentar colher senhas e *logins* quando o site tentar voltar para o ar.

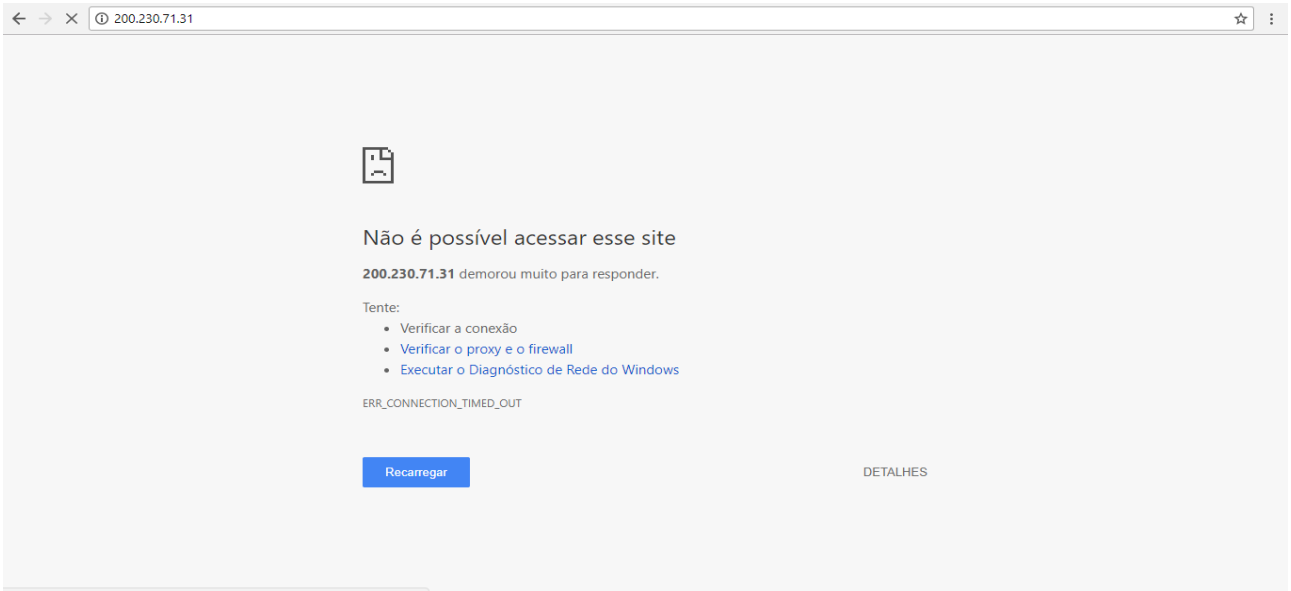

Figura 13 – Site ambiente simulado (Off), Fonte: Elaborado pelo autor.

5. **CONCLUSÃO**

De acordo com o desenvolvimento da pesquisa realizada e apresentada nesta monografia, pode-se afirmar que a importância da segurança da informação é imprescindível para a preservação dos dados de uma empresa, órgãos ou até mesmo para os nossos dados pessoais, pois trata-se de algo muito valioso e que precisa ser preservado. E esta afirmação ficou extremamente visível para todos os integrantes do ambiente simulado. Em cada livro ou artigo que fundamentaram o estudo e pesquisa, a maioria enfatiza, logo no início, sobre a importância de conseguir proteger seus dados ao máximo. É fato que ninguém está totalmente protegido, porém com este estudo pode-se observar diversos métodos para obter o êxito desejado, protegendo assim ao máximo a informação.

Ao decorrer da monografia, pode-se afirmar que a meta em conseguir realizar um estudo sobre como é feito um ataque e, com isso, entender a maneira que é realizada a estratégia por trás de uma invasão, foi concluída satisfatoriamente. Pode-se notar que não basta ter as ferramentas certas sem que aconteça uma elaboração sobre como invadir. Observar-se que os teste apresentados no trabalho, foram positivos em sua maioria, pois um ataque é feito, na maioria das vezes, com base nas falhas. Porém, para que possa realizar uma melhor apresentação dos estudos foi demonstrado todas as tentativas de acertos sem necessariamente expor os testes que se obteve falhas.

Assim, pode-se observar que em todo o tempo depararam com diversas ferramentas e atualizações que possam garantir a segurança da informação, e que da mesma maneira centenas de ferramentas e estratégias são criadas para “burlar” ou de certa forma passar pela defesa. Fato este que contribui para a justificativa e conclusão deste estudo, ou seja: para proteger os nossos dados pessoais ou empresariais, informações tão valiosas, é realmente indispensável a atualização do sistema de segurança, e isto deve ser um compromisso. Afinal, nunca estaram totalmente seguros.

No segundo capitulo apresentado nesta monografia, foi desenvolvido o estudo do sistema operacional Kali Linux. O estudo elaborado teve como objetivo compreender a importância de se usar o sistema operacional ideal para a invasão, pois, pode-se

afirmar que as ferramentas usadas ao decorrer do projeto também são usadas em outros sistemas operacionais, assim como o Windows, porém não se pode negar que a utilização de uma plataforma que propõe ao usuário final toda sustentabilidade que necessita uma invasão faz a diferença.

O terceiro capitulo, teve como objetivo a demonstração de como realmente é feito um ataque, se tratando de que não se pode somente usar uma ferramenta e invadir o alvo, com o estudo apresentado pode-se afirmar que, a invasão sobre um alvo é semelhante a um jogo de tabuleiro, onde qualquer jogada pode ser a última, desta forma, a pesquisa apresentada teve como objetivo demonstrar estratégias para que então o ataque possa ser bem estruturado.

Por fim, o quarto capitulo teve como objetivo a demonstração da pratica sobre as pesquisas realizadas no segundo e terceiro capitulo, assim, demonstrando diversas ferramentas para cada fase dita na estratégia de ataque.

5. **TRABALHO FUTURO**

A monografia apresentada não terá uma continuação, porém, espera-se que possa servir para estudos futuros na área da segurança da informação, podendo haver uma continuação na parte pratica das pesquisas realizadas e expandindo teste em arquitetura ARM, pois é uma tecnologia que tem ganho espaço nos dias de hoje.

REFERÊNCIAS

ROBOTS.TXT. the/robots.txt. Disponível em

< Http://www.robotstxt.org/robotstxt.html>. Acesso em: 12 maio. 2017.

METASPLOIT.

< Https://www.metasploit.com/>. Acesso em: 13 jun. 2017.

MUNIZ; LAKHANI, JOSEPH; AAMIR. *Web Penetration Testing With* Kali Linux, Birmingham; Mumbai: Packt publishing, 2013.

Nmap. *Nmap Security Scanner*. Disponível em

< https://nmap.org/>. Acesso em: 30 maio. 2017.

OFFENSIVE SECURITY. *What is* Kali Linux?. Disponível em:

< Http://docs.kali.org/introduction/what-is-kali-linux >. Acesso em: 04 mar. 2017.

OFFENSIVE SECURITY. *Category: 03. Installing* Kali Linux. Disponível em

< Http://docs.kali.org/category/installation>. Acesso em: 04 mar. 2017.

OFFENSIVE SECURITY. *Category: 07.* Kali *Community Support*. Disponível em

< Http://docs.kali.org/category/community >. Acesso em: 04 mar. 2017.

OFFENSIVE SECURITY. *Scanner HTTP Auxiliary Modules*. Disponível em

< Http://docs.kali.org/category/community >. Acesso em: 04 mar. 2017.

WAYBACK MACHINE.

< Https://archive.org/web/ >. Acesso em: 09 maio. 2017.