IPG Politécnico da Guarda
Escola Superior de Tecnologia e Gestão

RELATÓRIO DE ESTÁGIO

Curso Técnico Superior Profissional
em Cibersegurança

Rúben Jorge Abrantes dos Santos

julho | 2020

Escola Superior de Tecnologia e Gestão

Instituto Politécnico da Guarda

RELATÓRIO DE ESTÁGIO

RÚBEN SANTOS

RELATÓRIO PARA A OBTENÇÃO DO DIPLOMA DE TÉCNICO SUPERIOR PROFISSIONAL EM CIBERSEGURANÇA

JULHO 2020

Ficha de identificação

Estagiário:
Nome: Rúben Jorge Abrantes Dos Santos
Número de aluno: 1701443
Curso: Técnico Superior Profissional (TESP) em Cibersegurança
Morada: Rua Manuel Da Fonseca Nº6, 2º Esquerdo
E-mail: rubensantos995@hotmail.com

Entidade de estágio:
Nome: Unidade Local de Saúde da Guarda (ULSG)
Morada: Avenida Rainha Dona Amélia, Guarda
Código Postal: 6300-858
Telefone: 271 200 200
Fax: 271 223 104
Site: www.ulsguarda.min-saude.pt/
E-mail: secretariado.ca@ulsguarda.min-saude.pt

Supervisor/Tutor
Nome: Ricardo Mendonça Santos
Cargo: Diretor do Serviço de Sistemas e Tecnologias da Informação e Comunicações da Unidade Local de Saúde da Guarda (ULSG)
E-mail: ricardo.santos@ulsguarda.min-saude.pt

Docente Orientador:
Nome: José Carlos Coelho Martins Fonseca
Cargo: Diretor de Curso de Engenharia Informática
E-mail: josefonseca@ipg.pt

Escola:
Nome: Escola Superior de Tecnologia e Gestão
Morada: Avenida Dr. Francisco Sá Carneiro, Nº 50
Código Postal: 6300-559
Telefone: 271 220 120
Fax: 271 220 150
Site: www.estg.ipg.pt/
E-mail: estg-geral@ipg.pt

Agradecimentos

É com enorme orgulho, dedicação e desempenho que termino esta etapa da minha vida académica. Nada seria possível sem a ajuda e incentivo de todos os que percorreram este caminho comigo, a quem gostaria de agradecer por me ajudarem direta ou indiretamente nesta fase da minha vida e por me incentivarem a fazer melhor.

Em primeiro lugar, gostaria de agradecer ao Professor Doutor José Carlos Coelho Martins Fonseca por ter aceite ser meu orientador de estágio e por se disponibilizar sempre em me ajudar em qualquer momento.

Agradeço à minha namorada Cristiana Valério, por todo o apoio incondicional, pela paciência e compreensão ao longo de todo este percurso académico. Por acreditar em mim e nunca me deixar desistir mesmo com os desafios que foram surgindo.

À equipa do serviço de informática da ULSG, por terem sido prestáveis comigo durante estes meses, por me ajudarem nos momentos em que eu mais precisei e por me ensinarem sempre mais, aumentando assim as minhas capacidades e habilidades na área da informática.

Ao Engenheiro Ricardo Santos, gostaria de fazer um especial agradecimento pela sua disponibilidade e compreensão ao longo desta etapa. Agradeço ainda, por me orientar ao longo da realização do projeto de estágio e fazer com que ele se tornasse possível.

Agradeço ao Miguel Aguiar pela aprendizagem e conhecimento partilhado na área das impressoras, pelo companheirismo e amizade e por todas as experiências partilhadas ao longo deste percurso.

Ao Engenheiro Luís Domingos, agradeço a partilha de sabedoria e competências na área de redes de informática e por estar disponível para me ajudar a ultrapassar os obstáculos ao longo do projeto principal e ainda por fazer com que ele se tornasse possível.

Agradeço ao António Xavier pela aprendizagem e apoio demonstrado na área da rede informática, na comunicação informática e por me ensinar o funcionamento do Data Center da ULSG.

Agradeço ainda aos representantes das organizações que autorizaram e tornaram possível a realização do projeto do relatório.

Resumo

Este relatório dá a conhecer o que foi realizado durante o estágio na Unidade Local De Saúde da Guarda (ULSG). Este estágio teve uma duração de 750 horas, com início no dia 26 de fevereiro de 2020 e término no dia 23 de julho de 2020.

Tendo em vista alertar os funcionários da ULSG para os perigos da internet, para o estágio, propôs-se a realização de um ataque de engenharia social, na área do *phishing*. Este ataque consiste no envio de um e-mail malicioso para vários trabalhadores da ULSG. Este e-mail tem como tema a inscrição num concurso, no qual é obrigatório clicar no link que vai no e-mail para que o utilizador fique automaticamente inscrito. Esse link reencaminha o utilizador para um site falso que imita a página de *login* do Office que os utilizadores estão habituados a utilizar no serviço e no qual é preciso autenticar. Quando as credenciais de acesso são introduzidas, elas são enviadas para uma máquina controlada pelo atacante (neste caso, por mim). Quando o utilizador introduz as suas credenciais, é redirecionado para uma página que o avisa do perigo da utilização insegura da internet, dado que acabou de introduzir informações confidenciais num ataque de *phishing*. O intuito desta página é, não só alertar e mostrar ao utilizador os perigos do *phishing*, mas também ajudar no aumento do conhecimento já que inclui ainda inúmeras medidas de segurança a serem adotadas no mundo digital.

O teste com utilizadores reais ainda não foi possível realizar, por falta de autorização, no entanto foram realizados diversos testes que demonstram que o ataque funciona perfeitamente, conseguindo obter as credenciais de acesso e o redireccionamento.

Encontra-se na página "Anexo" um documento que elaborei com algumas medidas de segurança a adotar no mundo digital.

Durante o decorrer do estágio, e sempre que tal me era solicitado, também realizei ainda a reparação, configuração e instalação de diversos equipamentos informáticos, tais como impressoras, ecrãs e computadores.

Palavras-chave:

Engenharia Social, *Phishing*, Ataque, Credenciais de acesso.

Abstract

This report shows what was done during the internship at the Local Health Unit of Guarda (ULSG). This internship lasted 750 hours, starting on February 26, 2020 and ending on July 23, 2020.

In order to alert ULSG employees to the dangers of the internet, for the internship it was proposed to carry out a social engineering attack in the area of phishing. This attack consists of sending a malicious e-mail to several ULSG workers. This e-mail has as its theme the registration in a contest, in which it is mandatory to click on the link that goes in the e-mail so that the user is automatically registered. This link forwards the user to a fake website that imitates the Office login page that users are used to using the service and which they need to authenticate with. When access credentials are entered, they are sent to a machine controlled by the attacker (in this case, me). When the user enters his credentials, he is redirected to a page that warns him of the danger of unsafe use of the internet, since he has just entered confidential information in a phishing attack. The purpose of this page is not only to alert and show the user the dangers of phishing, but also to help increase knowledge since it also includes numerous security measures to be taken in the digital world.

The test with real users was not yet possible, due to lack of authorization, however several tests were performed that demonstrate that the attack works perfectly, managing to obtain the access credentials and the redirection.

There is a document on the "Attachment" page that I made with some security measures to be adopted in the digital world.

During the internship, and whenever requested, I also carried out the repair, configuration and installation of various computer equipment, such as printers, screens and computers.

Key-Words:

Social Engineering, Phishing, Attack, Access Credentials

Índice

Ficha de identificação i
Agradecimentos iii
Resumo v
Abstract vii
Índice de Figuras xi
Lista de Siglas e Acrónimos xiii
1. Introdução 1
1.1. Objetivos 1
1.2. Estrutura do relatório 2
2. Projeto desenvolvido 5
2.1. Engenharia Social 5
2.2 Arquitetura do sistema 6
2.3 Software utilizados 7
2.3.1. VirtualBox 7
2.3.2. Kali Linux 8
2.3.3. Social-Engineer Toolkit (SET) 9
2.3.4. Apache Web Server 10
2.3.5. GNU Nano 11
2.3.6. NotePad ++ 11
2.4 Implementação do projeto 12
2.4.1. Instalação do VirtualBox 13
2.4.2. Instalação do Kali Linux 14
2.4.3. Criação das páginas 16
2.4.4. Realização de testes 23
2.4.5. Inicio do ataque 26
3. Tema secundário de estágio 33
4. Conclusão 37
Anexo 38
Bibliografia 39

Índice de Figuras

Figura 1. Imagem ilustrativa da Arquitetura do Sistema 6
Figura 2. Imagem ilustrativa VirtualBox 8
Figura 3. Imagem ilustrativa Kali Linux 8
Figura 4. Imagem ilustrativa do Setoolkit 9
Figura 5. Imagem ilustrativa Apache 10
Figura 6. Imagem ilustrativa do uso do nano no index.html 11
Figura 7. Imagem ilustrativa NotePad++ 12
Figura 8. Imagem ilustrativa Instalação Oracle VM 13
Figura 9. Imagem ilustrativa meio da Instalação Oracle VM 13
Figura 10. Imagem ilustrativa fim da instalação Oracle VM 14
Figura 11. Imagem ilustrativa início da instalação Kali Linux 14
Figura 12. Imagem ilustrativa meio da instalação Kali Linux 15
Figura 13. Imagem ilustrativa fim da instalação Kali Linux 15
Figura 14. Imagem ilustrativa do Login Microsoft 1 16
Figura 15. Imagem ilustrativa do Login Microsoft 2 16
Figura 16. Imagem ilustrativa do Login Microsoft 3 17
Figura 17. Imagem ilustrativa de Opções Adicionais de Inicio de Sessão Microsoft 17
Figura 18. Imagem ilustrativa de Login Através do GitHub 18
Figura 19. Imagem ilustrativa do Index.html 18
Figura 20. Imagem ilustrativa obrigatório o uso do domínio no campo E-mail HTML 19
Figura 21. Preenchimento do campo Utilizador E-mail 19
Figura 22. Preenchimento com o formato do campo Utilizador E-mail certo 20
Figura 23. Preenchimento do campo Password 20
Figura 24. Imagem ilustrativa linha original do campo password 21
Figura 25. Imagem ilustrativa linha alterada do campo password 21
Figura 26. Imagem ilustrativa de Teste do index2.html 21
Figura 27. Imagem ilustrativa do index2.html início 22
Figura 28. Imagem ilustrativa do index2.html meio 22
Figura 29. Imagem ilustrativa do index2.html fim 23
Figura 30. Imagem ilustrativa do ficheiro ports.conf 23
Figura 31. Imagem ilustrativa do ficheiro 000-default.conf 24
Figura 32. Imagem ilustrativa do ficheiro set.config 24
Figura 33. Imagem ilustrativa problema cgi 25
Figura 34. Imagem ilustrativa import html 25
Figura 35. Imagem ilustrativa Alteração cgi para html 26
Figura 36. Imagem ilustrativa ativar Apache 26
Figura 37. Imagem ilustrativa verificar Apache 26
Figura 38. Imagem ilustrativa do setoolkit 27
Figura 39. Imagem ilustrativa primeiro menu setoolkit 27
Figura 40. Imagem ilustrativa segundo menu setoolkit 28
Figura 41. Imagem ilustrativa terceiro menu setoolkit 28
Figura 42. Imagem ilustrativa quarto menu setoolkit 29
Figura 43. Imagem ilustrativa endereço ip setoolkit 29
Figura 44. Imagem ilustrativa diretório index.html setoolkit 30
Figura 45. Imagem ilustrativa endereço url do index2.html setoolkit 30
Figura 46. Imagem ilustrativa do encurtador do link 30
Figura 47. Imagem ilustrativa E-mail 31
Figura 48. Imagem Ilustrativa Demonstração do ataque 31
Figura 49. Imagem ilustrativa do Data Center ULSG 33
Figura 50. Imagem ilustrativa Switchs 34
Figura 51. Imagem ilustrativa do Interior de um Bastidor 34

Figura 52. Imagem ilustrativa do interior do computador utilizado no ataque 35
Figura 53. Imagem Ilustrativa Unidade de Imagem 35
Figura 54. Imagem ilustrativa Interior de Impressora Xerox 36

Lista de Siglas e Acrónimos

CPU	**C**entral **P**rocessing **U**nit
E-mail	**E**lectronic **M**ail
ESTG	**E**scola **S**uperior De **T**ecnologia e **G**estão
FTP	**F**ile **T**ransfer **P**rotocol
GNU	**G**NU is **N**ot **U**nix
GPL	**G**eneral **P**ublic **L**icense
Htaccess	**H**ypertext **A**ccess
HTML	**H**yper**T**ext **M**arkup **L**anguage
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol
HTTPS	**H**yper **T**ext **T**ransfer **P**rotocol **S**ecure
IP	**I**nternet **P**rotocol
IPG	**I**nstituto **P**olitécnico Da **G**uarda
IPv6	**I**nternet **P**rotocol **v**ersion **6**
PC	**P**ortable **C**omputer
PHP	**H**ypertext **P**reprocessor
RSE	**R**egisto de **S**aúde **E**letrónico
SET	**S**ocial-**E**ngineer **T**oolkit
SNS	**S**erviço **N**acional de **S**aúde
TI	**T**ecnologia da **I**nformação
ULS	**U**nidade **L**ocal De **S**aúde
ULSG	**U**nidade **L**ocal De **S**aúde Da **G**uarda
URL	**U**niform **R**esource **L**ocator
USB	**U**niversal **S**erial **B**us
WebDAV	**Web**-based **D**istributed **A**uthoring and **V**ersioning
WI-FI	**W**ireless **F**idelity

1. Introdução

O estágio curricular foi desenvolvido no serviço de informática da Unidade Local De Saúde da Guarda (ULSG) com o objetivo de conclusão do curso Técnico Superior Profissional em Cibersegurança através da Escola Superior de Tecnologia e Gestão (ESTG) do Instituto Politécnico da Guarda (IPG).

Como principal projeto de estágio, foi proposto a realização de um ataque de engenharia social na área do *phishing*. Este projeto teve como principal objetivo consciencializar as pessoas de que a engenharia social é cada vez mais uma realidade, alertando-as para o perigo deste crime e ajudando-as a protegerem-se, nomeadamente revelando várias maneiras de impedir o roubo de credenciais.

A engenharia social (que não é exclusivamente utilizada apenas através da informática) consiste em práticas utilizadas, para obter informações pessoais e importantes sem que as pessoas se apercebam, levando-as a revelarem credenciais de acesso inconscientemente. Um bom exemplo, são os roubos das credenciais de acesso a contas, sendo elas de redes sociais, sites do estado ou até mesmo do banco.

Phishing é uma das variantes da engenharia social, consistindo no envio de e-mails enganosos esperando que alguma vítima se identifique com esse e-mail ou que simplesmente por curiosidade entre no link do e-mail e preencha as credenciais pedidas, credenciais essas que serão enviadas para o computador do atacante.

1.1. Objetivos

O ataque de *phishing*, tem como principal objetivo a simulação de um concurso persuadindo as pessoas a entregarem as suas credenciais de acesso e o redireccionamento da vítima para um site falso que a informa do que foi feito e a ajuda a aprender mais sobre este tipo de ataques.

Para a realização deste projeto foram definidos os seguintes objetivos:

1) Criação de uma página de *Login* idêntica à original utilizada habitualmente pelos utilizadores da ULSG.
2) Realização de vários testes de ataque para verificar o seu funcionamento e corrigir os erros que irão surgir.
3) Envio do e-mail do falso concurso, com o link de acesso à página criada por mim.
4) Obtenção das credenciais de acesso das vítimas.
5) Redireccionamento para uma segunda página referindo que foi "hackeada" e contendo algumas medidas de prevenção.

A divulgação do concurso ocorreu através de e-mail e apenas aconteceu na rede interna da ULS da Guarda.

Tema secundário de estágio:

Para além do ataque realizei também inúmeras tarefas tais como:
Manutenção e reparação de:

- Impressoras
- Computadores
- Ecrãs
- Rede informática

Realizei ainda, ao longo do estágio, vários relatórios de abate e troca de equipamentos, entre outros.

1.2. Estrutura do relatório

Este relatório encontra-se organizado da seguinte maneira.

No Capítulo 1 encontra-se uma introdução, os objetivos do projeto de engenharia social a realizar e como é estruturado o relatório.

No Capítulo 2 encontram-se os programas utilizados e as várias etapas do projeto desenvolvido, tais como, a criação das páginas em html, testes feitos, correções de problemas de obstáculos que foram aparecendo ao longo deste projeto, entre outros.

No Capítulo 3 encontram-se algumas das atividades diárias realizadas por mim ao longo do percurso de estágio na ULSG.

No Capítulo 4 encontra-se a conclusão de tudo o que foi feito até ao final do estágio na ULSG.

2. Projeto desenvolvido

Este capítulo é constituído por algumas definições, relativamente ao ataque de engenharia social, tais como engenharia social e *phishing*, englobando ainda a arquitetura do sistema. Encontra-se também neste capítulo, informação sobre os software utilizados e a razão dessa mesma escolha. Por fim, apresenta-se a implementação do projeto e as respetivas etapas.

2.1. Engenharia Social

Engenharia Social é uma mistura de ciência, psicologia e arte. Embora seja incrível e complexa, também é muito simples (Social-engineer, s.d.).

É a arte de explorar a psicologia humana, em vez de técnicas de hacking, para obter acesso a edifícios, sistemas ou dados.

Um bom exemplo, em vez de tentar encontrar uma vulnerabilidade de software, um engenheiro social pode ligar para um funcionário e se passar por uma pessoa de suporte de TI, tentando induzi-lo a divulgar sua senha.

O hacker Kevin Mitnick ajudou a popularizar o termo 'engenharia social' nos anos 90. A engenharia social provou ser uma maneira muito bem-sucedida de um criminoso "entrar" na sua organização. Após um engenheiro social ter uma senha de um funcionário confiável, ele pode simplesmente fazer *login* e procurar dados confidenciais. Com um cartão ou código de acesso para entrar fisicamente numa instalação, o criminoso pode aceder aos dados, roubar ativos ou até prejudicar pessoas.

No artigo "Anatomia de um hack", um testador de penetração mostra como usou os eventos atuais, informações públicas disponíveis em sites de redes sociais e uma camisa da Cisco de US $ 4 que ele comprou numa loja de artigos usados para se preparar para a sua entrada ilegal. A camisa ajudou a convencer a receção do prédio e outros funcionários de que ele era funcionário da Cisco numa visita ao suporte técnico. Uma vez lá dentro, ele conseguiu dar entrada ilegal aos outros membros da equipa. Conectou ainda, várias pens USB carregadas de malware e invadiu a rede da empresa, tudo à vista de outros funcionários.

Estes tipos de ataques funcionam igualmente bem por e-mail, telefone ou rede social. O que todos os ataques têm em comum é que eles utilizam a natureza humana a seu favor, atacando a nossa ganância, medo, curiosidade e até o nosso desejo de ajudar os outros (Fruhlinger, 2019).

Os nove ataques de engenharia social mais comuns são, de acordo com (Terranovasecurity, s.d.):

- ***Phishing*:** Táticas que incluem e-mails enganosos, sites e mensagens de texto para roubar informações.
- **Spear *Phishing*:** O e-mail é usado para realizar ataques direcionados contra indivíduos ou empresas.
- **Baiting:** Ataque online ou físico de engenharia social que promete uma recompensa à vítima.
- **Malware:** As vítimas são levadas a acreditar que o malware está instalado no computador e que, se pagarem, o malware será removido.
- **Pretexting:** Usa identidade falsa para induzir as vítimas a dar informações.
- **Quid Pro Quo:** Depende de uma troca de informações ou serviços para convencer a vítima a agir.
- **Tailgating:** Depende da confiança humana para dar ao criminoso acesso físico a um edifício ou área segura.
- **Vishing:** Mensagens de voz urgentes convencem as vítimas de que precisam agir rapidamente para se proteger de prisões ou outros riscos.
- **Water-Holing:** Ataque avançado de engenharia social que infeta um site e os seus visitantes com malware.

O ataque de engenharia social utilizado na realização do projeto foi o ataque de *phishing* pedido pela direção do serviço de informática da ULSG. Foi escolhido este ataque por englobar um e-mail enganoso com a intenção de roubar as credenciais de acesso dos utilizadores da rede da ULSG.

2.2 Arquitetura do sistema

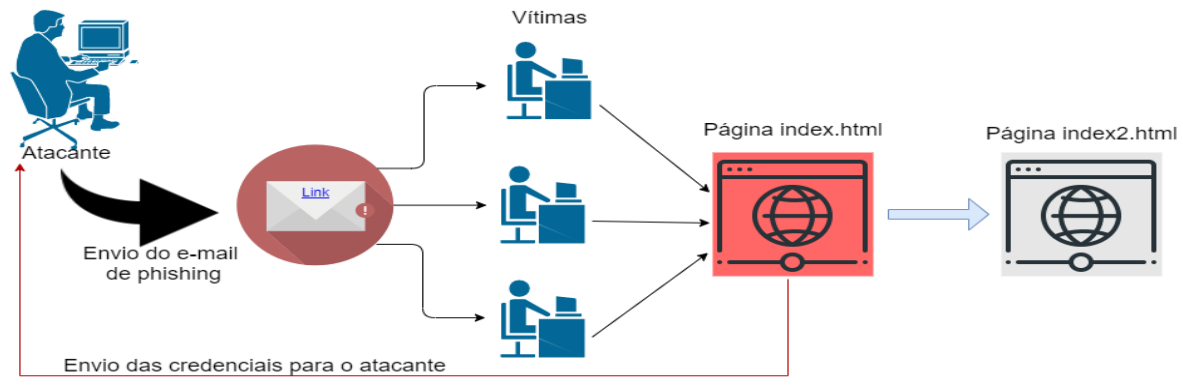

Figura 1. Imagem ilustrativa da Arquitetura do Sistema

A Figura 1 representa o projeto de ataque de engenharia social, que consiste no envio de um e-mail de phishing contendo um texto aliciante, com o tema de um concurso e um link para a máquina já pronta do atacante para receber as credenciais de acesso dos trabalhadores da ULSG e com as respetivas páginas em funcionamento (index.html e index2.html).
Seguidamente as vítimas, são direcionadas para um falso site de login (index.html), onde têm de iniciar sessão, depois de preencherem os campos com as credenciais de acesso, são enviadas para a máquina do atacante e as vítimas redirecionadas para uma segundo site (index2.html), onde irá dizer que nesse momento o atacante tem as suas credenciais, com o objetivo de assustar a vítima. Essa mesma página, terá também algumas medidas de prevenção no mundo digital.

2.3 Software utilizados

2.3.1. VirtualBox

Para a realização deste projeto foi utilizada uma máquina virtual e o software escolhido foi o VirtualBox da empresa Oracle na versão 6.1.10. O VirtualBox é um produto de virtualização x86 e AMD64 / Intel64 para uso corporativo e doméstico. Este não é apenas um produto de alto desempenho e rico em recursos para clientes corporativos, mas também a única solução profissional disponível gratuitamente como Software de Código Aberto sob os termos da GNU General Public License (GPL) versão 2.

Atualmente, é executado nos hosts Windows, Linux, Macintosh e Solaris e oferece suporte a um grande número de sistemas operacionais convidados, incluindo, sem limitação, o Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS / Windows 3.x, Linux (2.4, 2.6, 3.xe 4.x), Solaris e OpenSolaris, OS / 2 e OpenBSD. O host escolhido para a realização do ataque foi o Windows 10, pela praticidade e por ser o Windows utilizado no meu computador pessoal.

O VirtualBox é desenvolvido ativamente com lançamentos frequentes e possui uma lista cada vez maior de recursos, sistemas operacionais convidados suportados e plataformas em que é executado. É também um esforço da comunidade apoiado por uma empresa dedicada: todos são incentivados a contribuir, enquanto a Oracle garante que o produto sempre atenda aos critérios de qualidade profissional (Virtualbox, s.d.).

Este software foi escolhido com base no conhecimento já adquirido anteriormente acerca deste e devido à sua utilização ao longo do meu percurso académico. A Figura 2 mostra o VirtualBox com o Kali Linux já instalado.

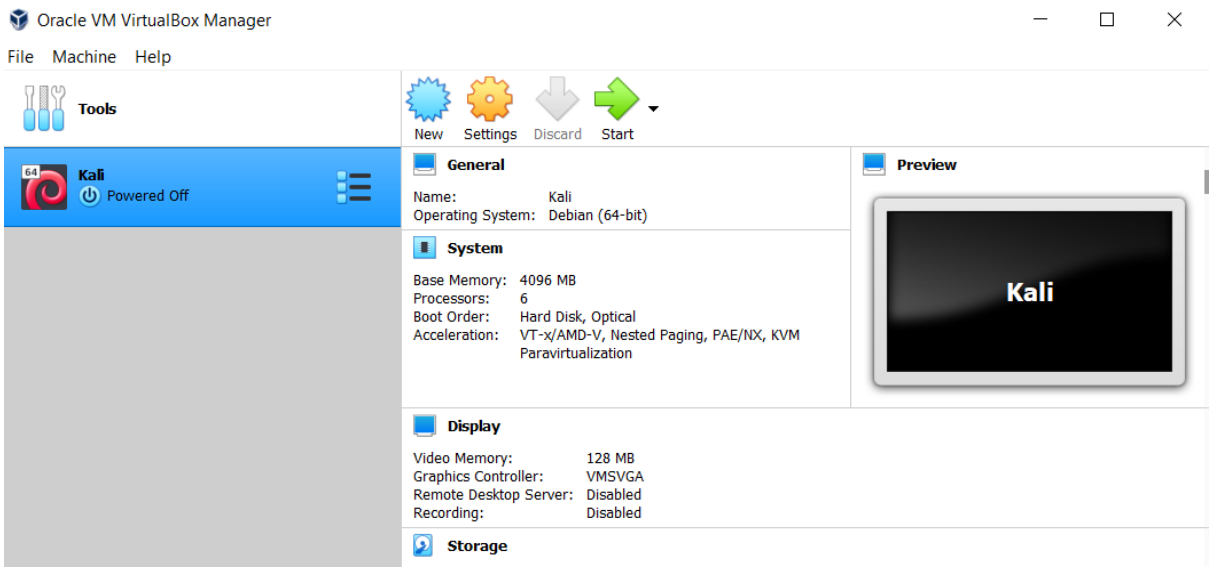

Figura 2. Imagem ilustrativa VirtualBox

2.3.2. Kali Linux

No VirtualBox anteriormente referido e no projeto final foi utilizado o sistema operativo Kali na versão 2020.1, sendo uma distribuição Linux.

O Kali Linux é um projeto de código aberto que é mantido e financiado pela Offensive Security, uma fornecedora de serviços de treino e teste de penetração de classe mundial em segurança da informação. Além do Kali Linux, o Offensive Security também mantém o Exploit Database e o curso on-line gratuito, Metasploit Unleashed (Kali, s.d.).

O sistema operativo Kali na versão 2020.1 foi escolhido por ser uma distribuição Linux com o qual já realizei vários projetos anteriormente em contexto académico. Essa utilização permitiu-me adquirir bastante conhecimento e segurança, aumentando assim a minha capacidade de utilização do sistema. A Figura 3 mostra o ambiente de trabalho no Kali Linux na versão acima referida.

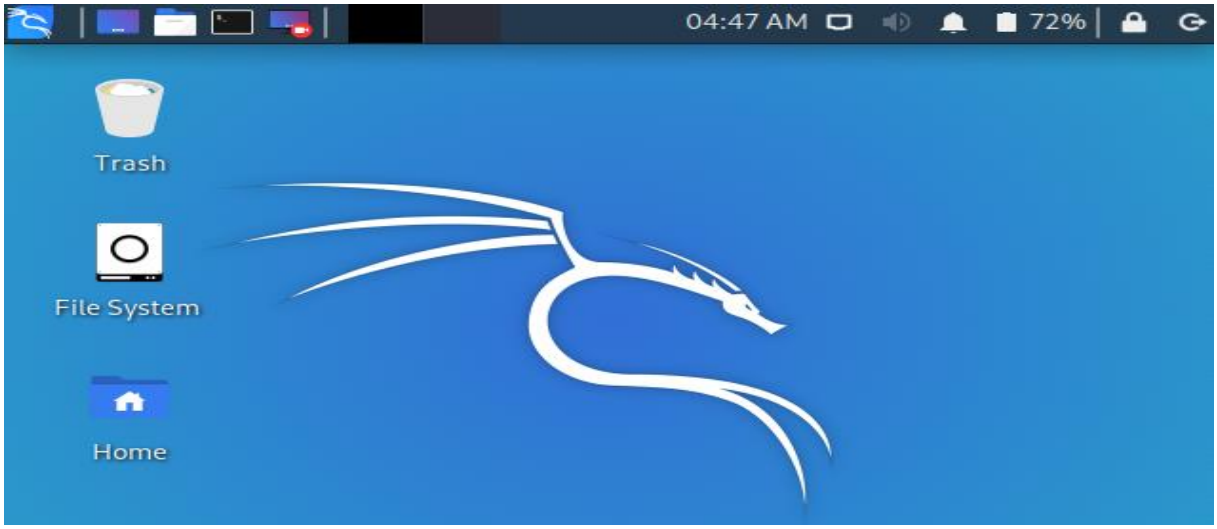

Figura 3. Imagem ilustrativa Kali Linux

2.3.3. Social-Engineer Toolkit (SET)

O software de engenharia social escolhido para este projeto foi o Social-Engineer Toolkit. O Social-Engineer Toolkit (SET) foi criado e escrito por Dave Kennedy, fundador da TrustedSec. É uma ferramenta de código aberto orientada a Python, destinada a testes de penetração em torno da Social-Engineering.

Foi apresentado em conferências de larga escala, incluindo Blackhat, DerbyCon, Defcon e ShmooCon. É o padrão para testes de penetração de engenharia social e apresenta forte suporte na comunidade de segurança.

O Social-Engineer Toolkit (SET) visa promover ataques tecnológicos avançados num ambiente do tipo de engenharia social. A TrustedSec acredita que a engenharia social é um dos ataques mais difíceis de proteger e, atualmente, um dos mais prevalentes (Trustedsec, s.d.).

Optei por escolher este software, por ser um dos principais softwares de engenharia social no sistema operativo Kali Linux. Ao longo do meu percurso académico foi um dos softwares abordados, aumentando a minha compreensão e o meu conhecimento acerca deste. A Figura 4 mostra a página inicial do software.

Figura 4. Imagem ilustrativa do Setoolkit

2.3.4. Apache Web Server

O software Web Server utilizado para as páginas web customizadas que foram utilizadas durante o ataque foi o Apache.

O Apache é o servidor web de plataforma aberta mais popular que existe e também um dos mais antigos, tendo o seu primeiro lançamento em 1995.

É usado por grandes empresas como Cisco, IBM, Salesforce, General Electric, Adobe, VMware, Xerox, LinkedIn, Facebook, Hewlett-Packard, AT & T, Siemens, eBay, entre outras.

O apache web server foi o software escolhido por já ter alguma experiência com este, devido à sua utilização ao longo do curso. A Figura 5 mostra a ativação e o status do software.

Alguns dos recursos do Apache são:

- Htaccess
- IPv6
- FTP
- HTTP/2
- Perl, Lua e PHP
- Limitação de largura de banda
- WebDAV
- Balanceamento de carga
- Reescrita de URL
- Acompanhamento de sessão
- Geolocalização baseada em endereço IP

(Santos, 2019)

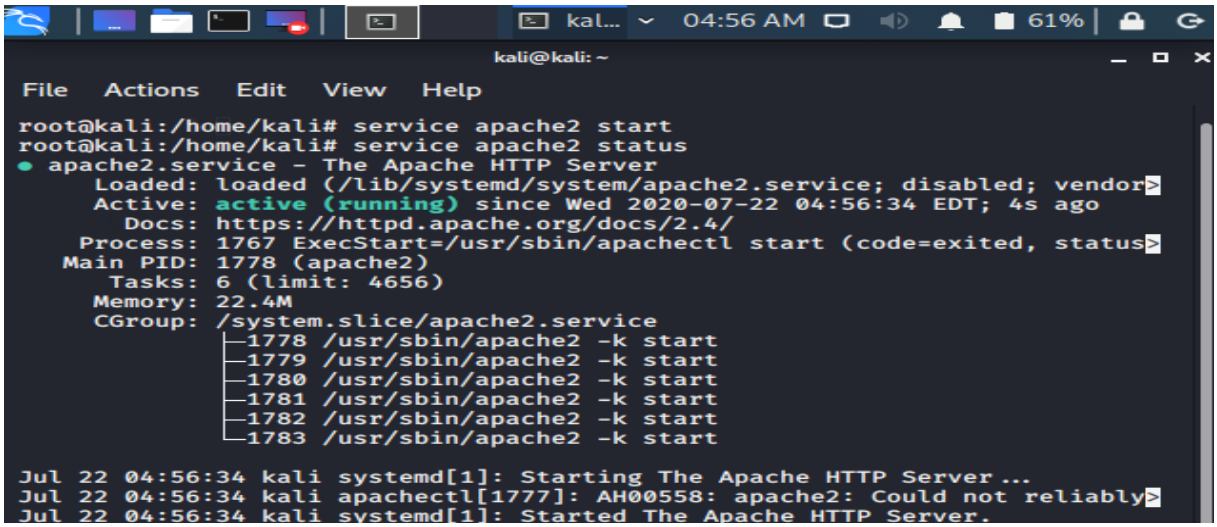

Figura 5. Imagem ilustrativa Apache

Editores de texto utilizados:

2.3.5. GNU Nano

O editor utilizado no sistema operativo Kali Linux para edição das páginas html foi o GNU nano.

O GNU nano é um editor de texto de linha de comando de fácil utilização para sistemas operacionais Unix e Linux. Ele inclui toda a funcionalidade básica de um editor de texto comum, como destaque de sintaxe, vários buffers, pesquisa e substituição por suporte a expressões regulares, verificação ortográfica, codificação UTF-8 e muito mais.

Foi lançado como software livre por Chris Allegretta em 1999. O nano tornou-se parte do Projeto GNU em 2001 (Linuxize, 2019).

A escolha deste, deve-se ao facto de mais uma vez ser um software de edição bastante utilizado durante algumas aulas e de ser um editor de texto bastante simples na sua utilização que o sistema operativo Kali Linux faculta. Foi usado principalmente para a programação da página index.html, como se verifica na Figura 6.

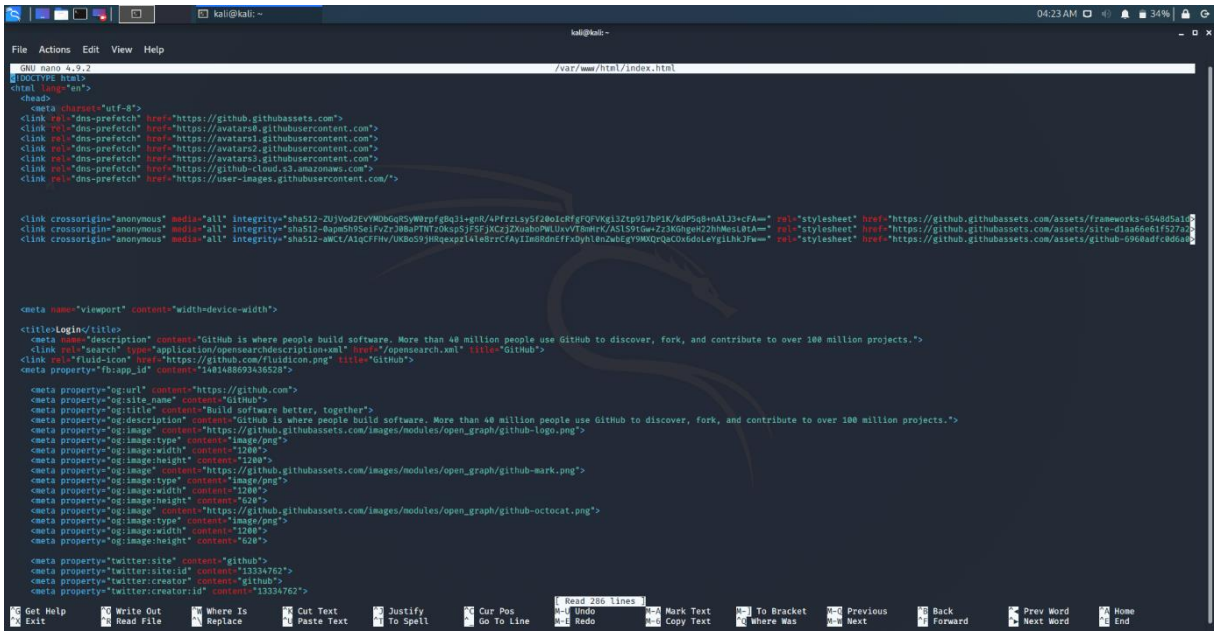

Figura 6. Imagem ilustrativa do uso do nano no index.html

2.3.6. NotePad ++

O editor utilizado no sistema operativo Windows 10 para edição das páginas html foi o NotePad ++.

O Notepad ++ é um editor de código-fonte gratuito e funciona como substituição do bloco de notas que suporta vários idiomas. Executando no ambiente MS Windows, o seu uso é regido pela Licença GPL (General Public License).

Baseado no poderoso componente de edição Scintilla, o Notepad ++ é escrito em C ++ e usa a API e o STL Win32 puros. Ao otimizar o maior número possível de rotinas sem perder a facilidade de uso, o Notepad ++ tenta reduzir as emissões mundiais de dióxido de carbono. Utilizando menos energia da CPU, o PC pode acelerar e reduzir o seu consumo de energia, resultando num ambiente mais verde (Notepad, s.d.).

Foi escolhido este editor de texto para conseguir editar as páginas html, sem ter de iniciar o Kali Linux na máquina virtual, sendo este editor muito mais completo e melhor para edição de linguagens de programação, do que o simples bloco de notas facultado pelo sistema operativo, Windows 10. Foi usado principalmente para a programação da página index.html, como se verifica na Figura 7.

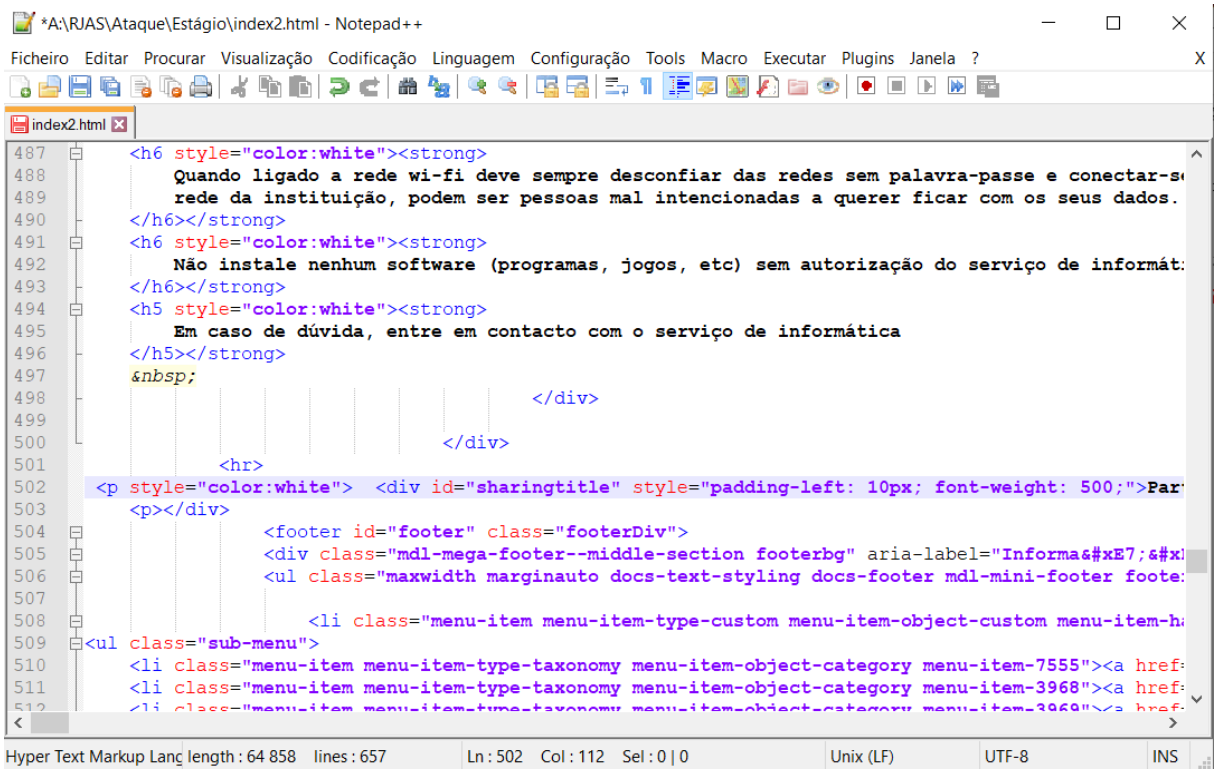

Figura 7. Imagem ilustrativa NotePad++

2.4 Implementação do projeto

Depois de organizar as ideias e decidir quais os softwares a serem utilizados, dei início ao desenvolvimento do projeto.

2.4.1. Instalação do VirtualBox

Instalação do software

VirtualBox no meu computador pessoal.

A Figura 8 **representa o início da instalação**

Figura 8. Imagem ilustrativa Instalação Oracle VM

A Figura 9 **representa o meio da instalação**

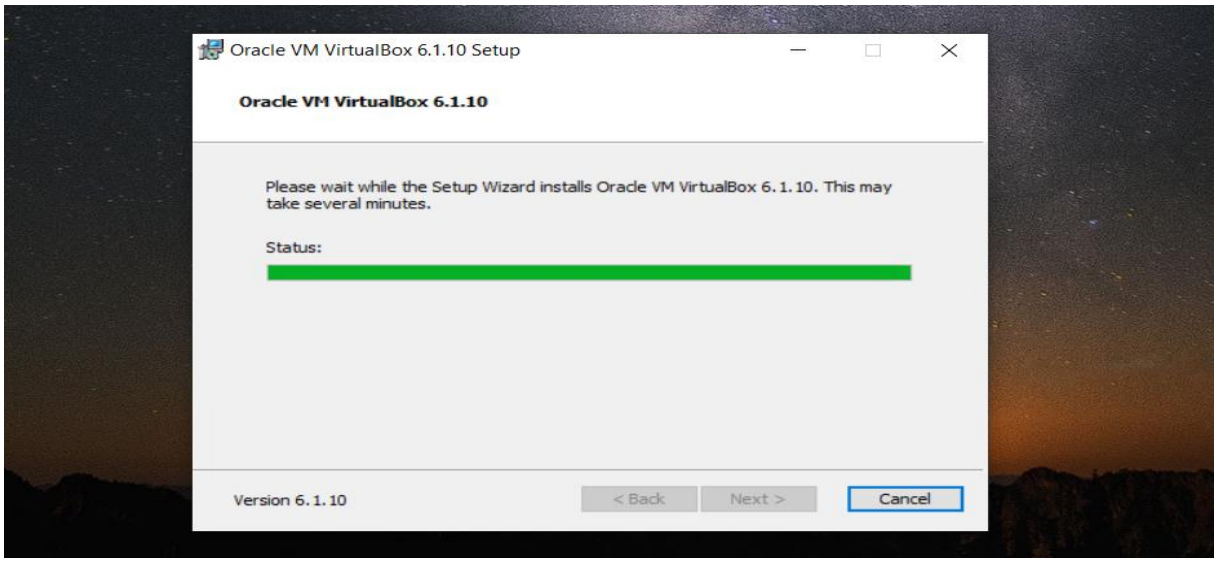

Figura 9. Imagem ilustrativa meio da Instalação Oracle VM

A Figura 10 **representa instalação concluída**

Figura 10. Imagem ilustrativa fim da instalação Oracle VM

Após a instalação concluída passei ao próximo passo.

2.4.2. Instalação do Kali Linux

Instalação do sistema operativo Kali Linux na máquina virtual anteriormente instalada.

A Figura 11 **representa o início da instalação do sistema operativo Kali Linux.**

Figura 11. Imagem ilustrativa início da instalação Kali Linux

A Figura 12 **representa o meio da instalação do sistema operativo Kali Linux.**

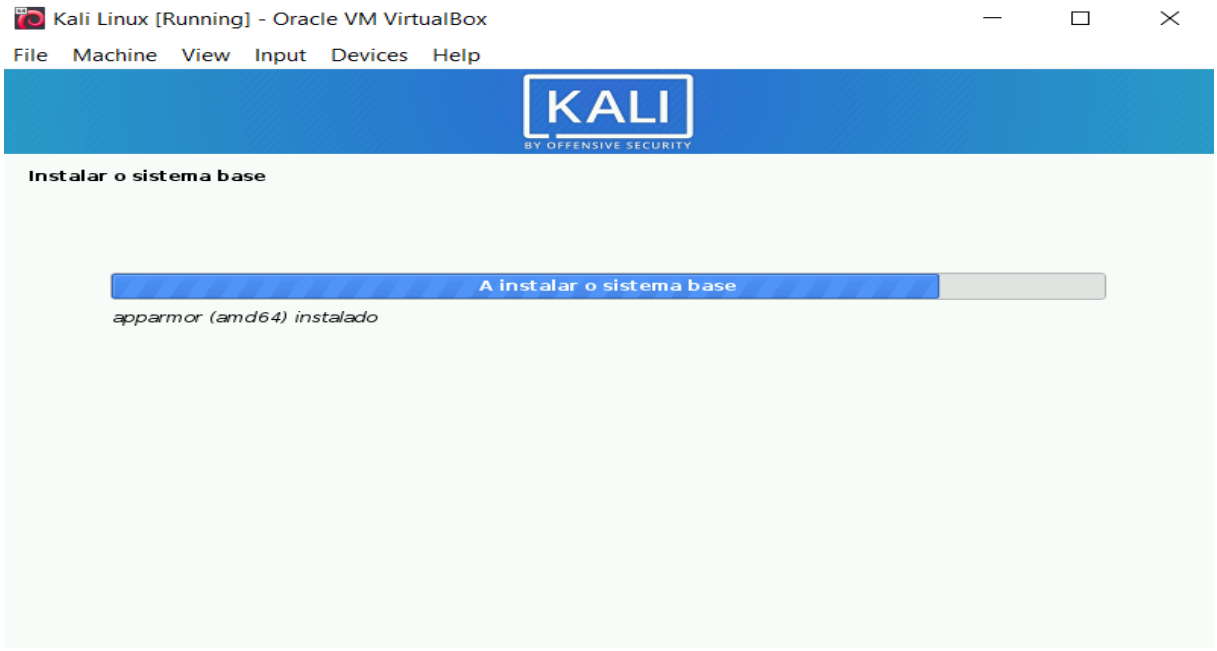

Figura 12. Imagem ilustrativa meio da instalação Kali Linux

A Figura 13 **representa instalação concluída.**

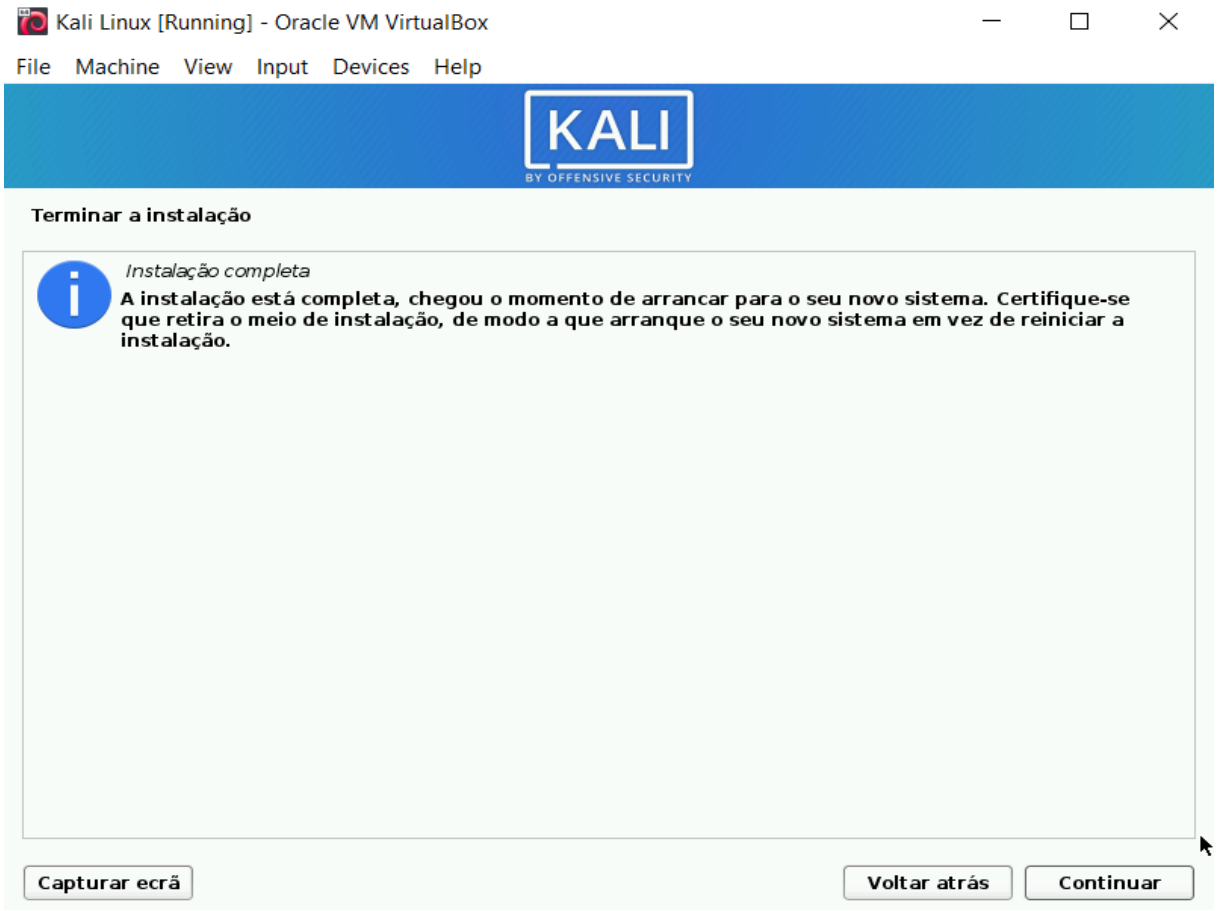

Figura 13. Imagem ilustrativa fim da instalação Kali Linux

Após a instalação de todos os softwares concluída, foquei-me na realização do ataque.

2.4.3. Criação das páginas

Página index.html

Depois de ter os softwares necessários prontos, comecei a procurar soluções de temas para a página inicial de *login*.

A ideia era simular uma página de *login* de e-mail da empresa Microsoft, mas surgiu o primeiro obstáculo.

As credenciais no site não eram pedidas simultaneamente. Primeiro era pedido o e-mail, depois tinha de clicar em seguinte e era então pedido a palavra-passe, em páginas distintas, como se pode ver nas seguintes imagens na Figura 14 e Figura 15, respetivamente.

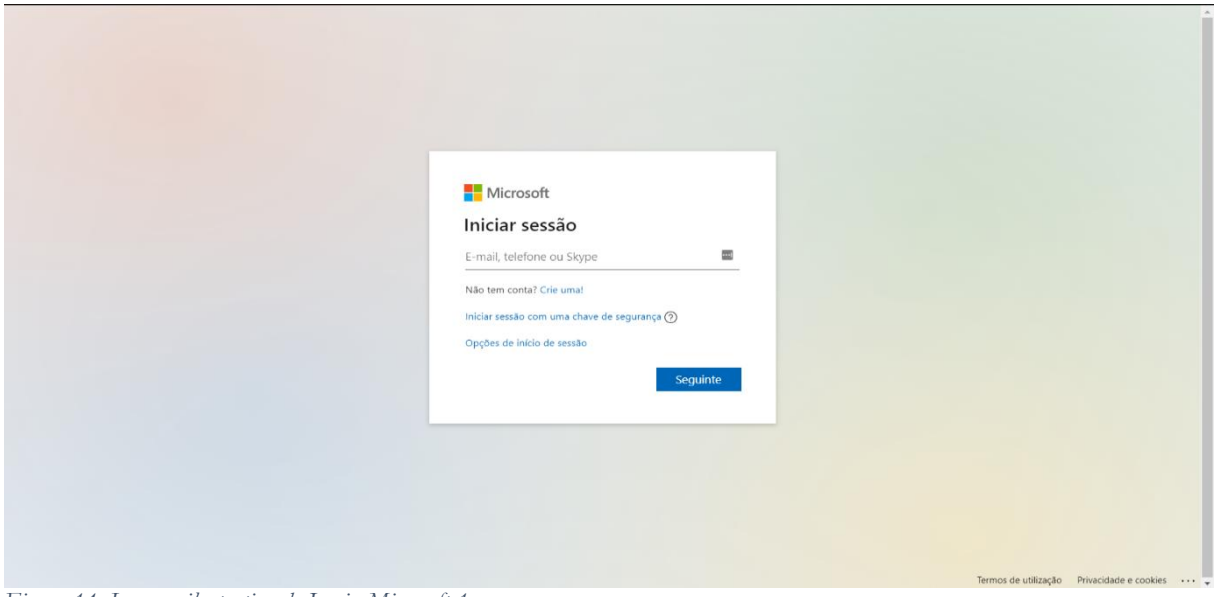

Figura 14. Imagem ilustrativa do Login Microsoft 1

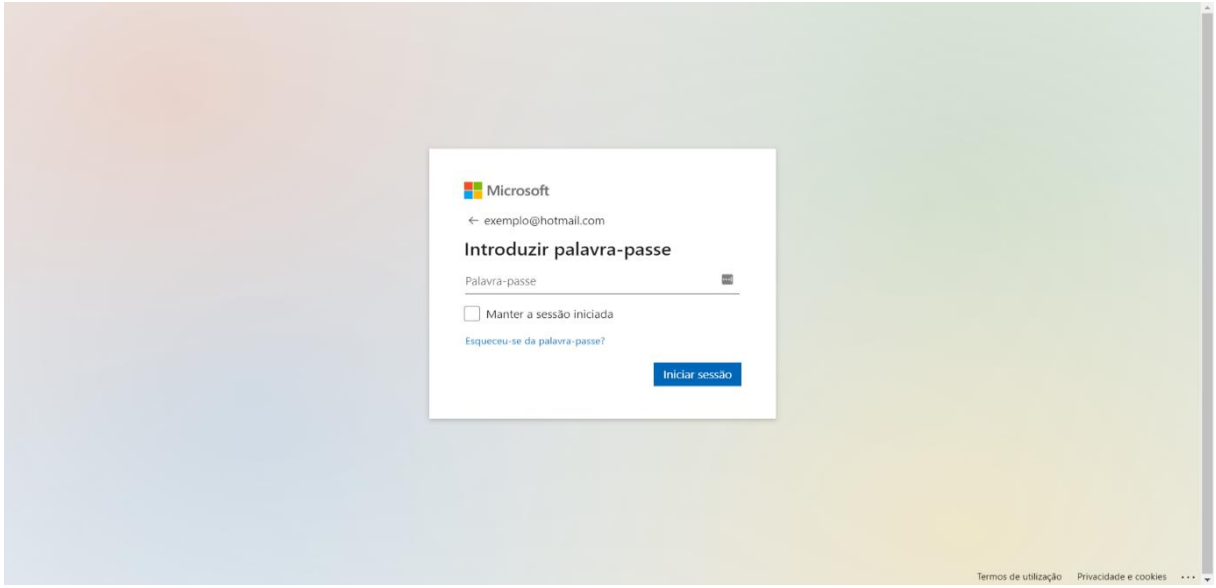

Figura 15. Imagem ilustrativa do Login Microsoft 2

Depois notei que estava presente outras opções de início de sessão, como se verifica na Figura 16.

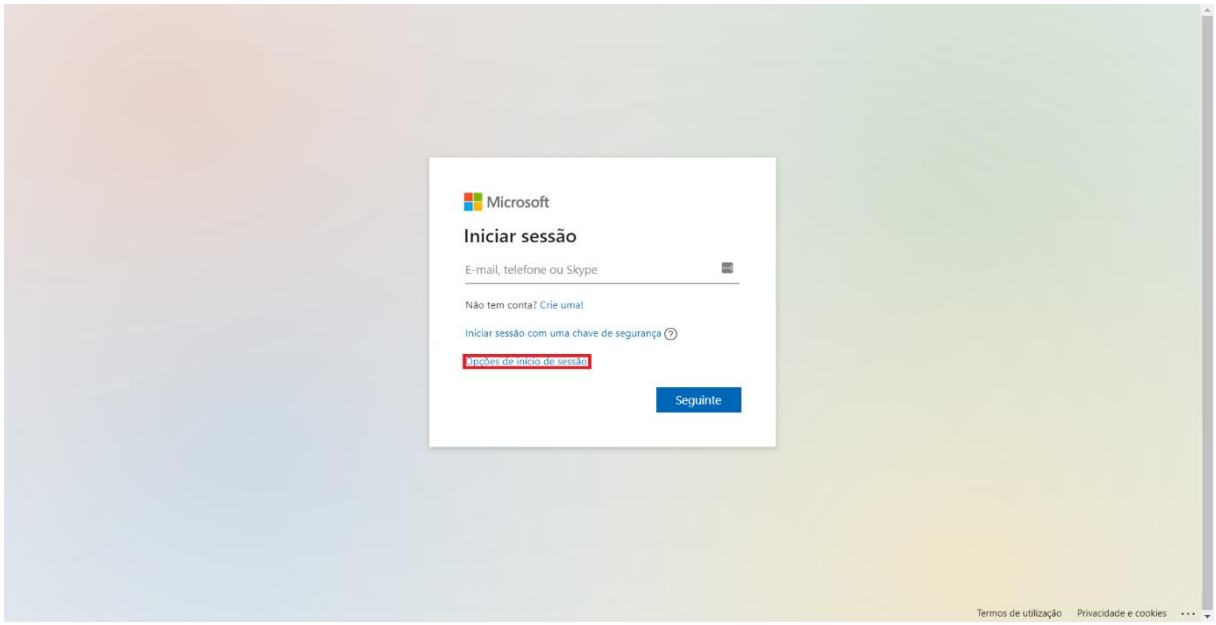

Figura 16. Imagem ilustrativa do Login Microsoft 3

Estavam presentes as seguintes opções adicionais de *Login*, como se verifica na Figura 17.

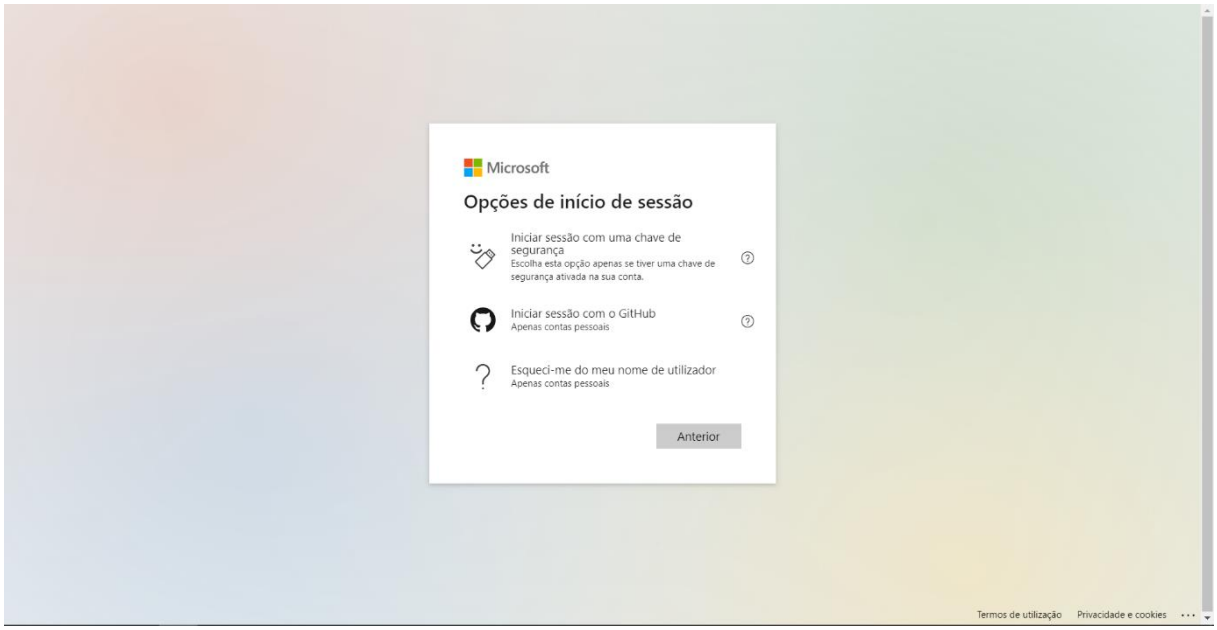

Figura 17. Imagem ilustrativa de Opções Adicionais de Inicio de Sessão Microsoft

Ao ver a opção do GitHub, representada na Figura 18, ponderei em aproveitar a página e modificar o código HTML, para ficar como pretendia.

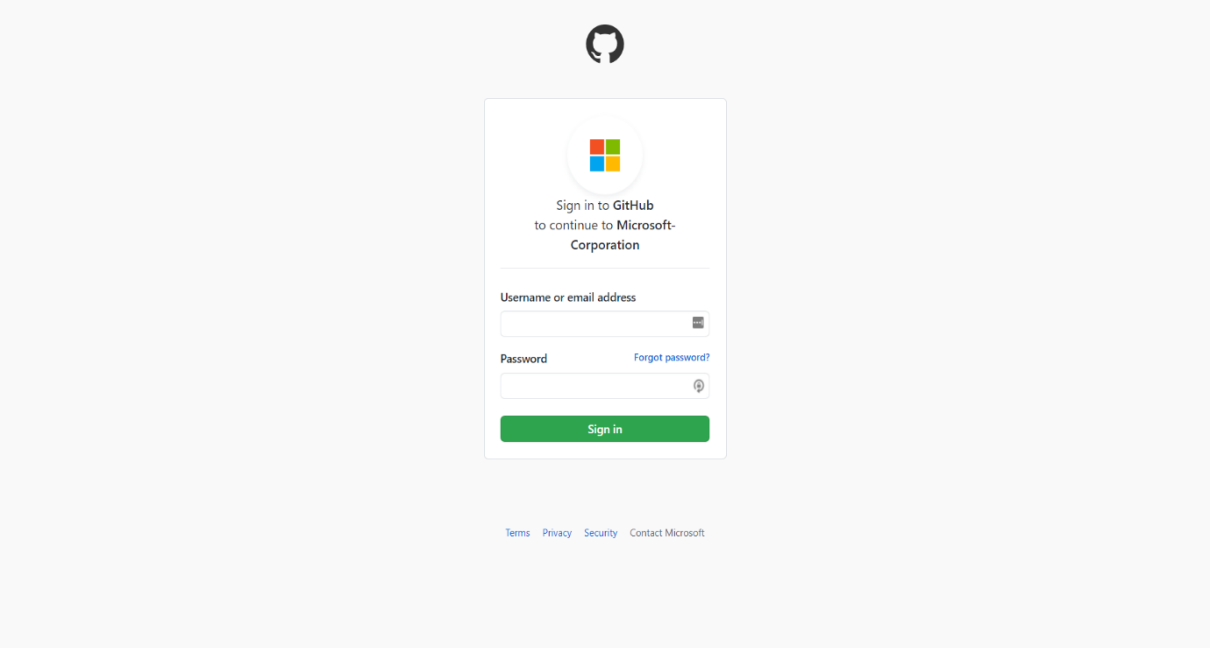

Figura 18. Imagem ilustrativa de Login Através do GitHub

Alterei o código original do ficheiro index.html que se encontra no diretório:
`/var/www/html/`

Após a alteração, visualmente, ficou da seguinte forma, como se verifica na Figura 19.

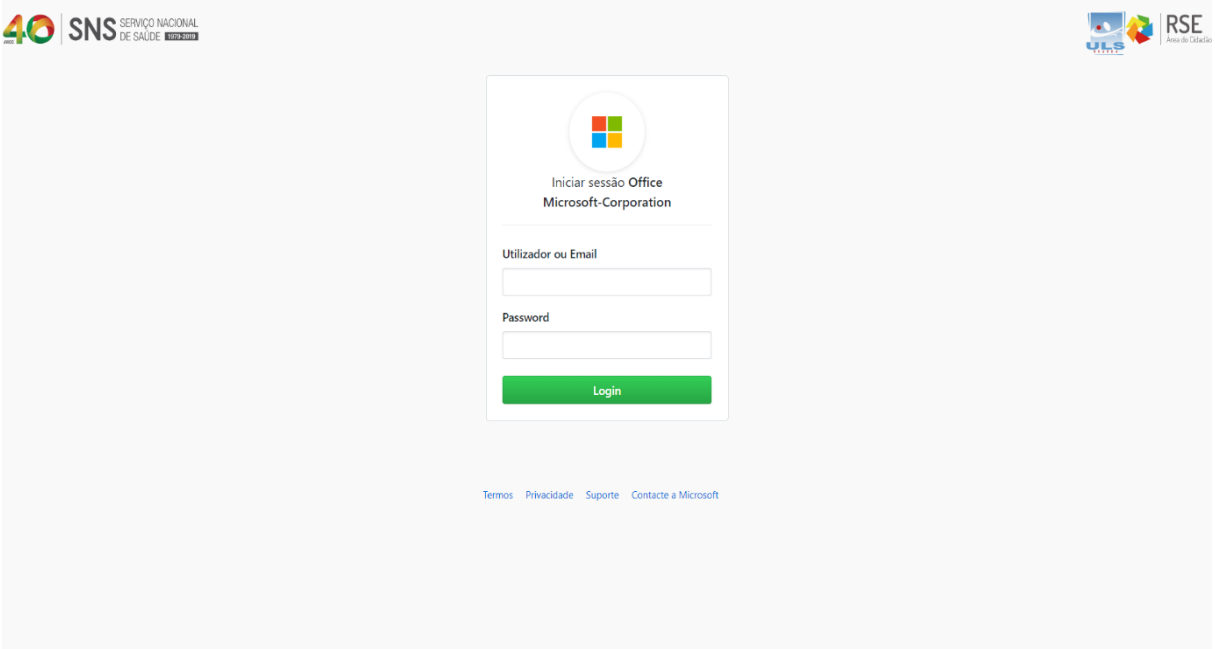

Figura 19. Imagem ilustrativa do Index.html

A página representada na Figura 19 contém hiperligações totalmente funcionais, tanto nos "Termos", "Privacidade", "Suporte" e "Contacte a Microsoft", como nos logotipos da SNS, ULS e RSE e respetivos textos, informando o que irá acontecer caso clique nas imagens.

Como solução para os utilizadores serem forçados a inserir as suas credenciais de acesso, no campo de e-mail programei para ser obrigatório ter o domínio de e-mail utilizado na ULSG (@ulsguarda.min-saude.pt) e no campo palavra-passe, apenas garantir que o campo não fica vazio. Como se pode verificar nas linhas 210 e 214, respetivamente, da Figura 20.

```
206        <label for="login_field">
207          Utilizador ou Email
208        </label>
209        <input type="text" name="login" id="login_field" class="form-control input-block" tabindex="1" autocapitalize="off" autc
210        required pattern="\S+.*[@][u][l][s][g][u][a][r][d][a][.][m][i][n][-][s][a][u][d][e][.][p][t]"/>
211    <label for="login_field">
212    Password
213    </label>
214        <input type="password" name="" id="sempassword" class="form-control form-control input-block" tabindex="2" required/>
```

Figura 20. Imagem ilustrativa obrigatório o uso do domínio no campo E-mail HTML

A Figura 21 mostra o preenchimento do campo "Utilizador ou Email" obrigatório.

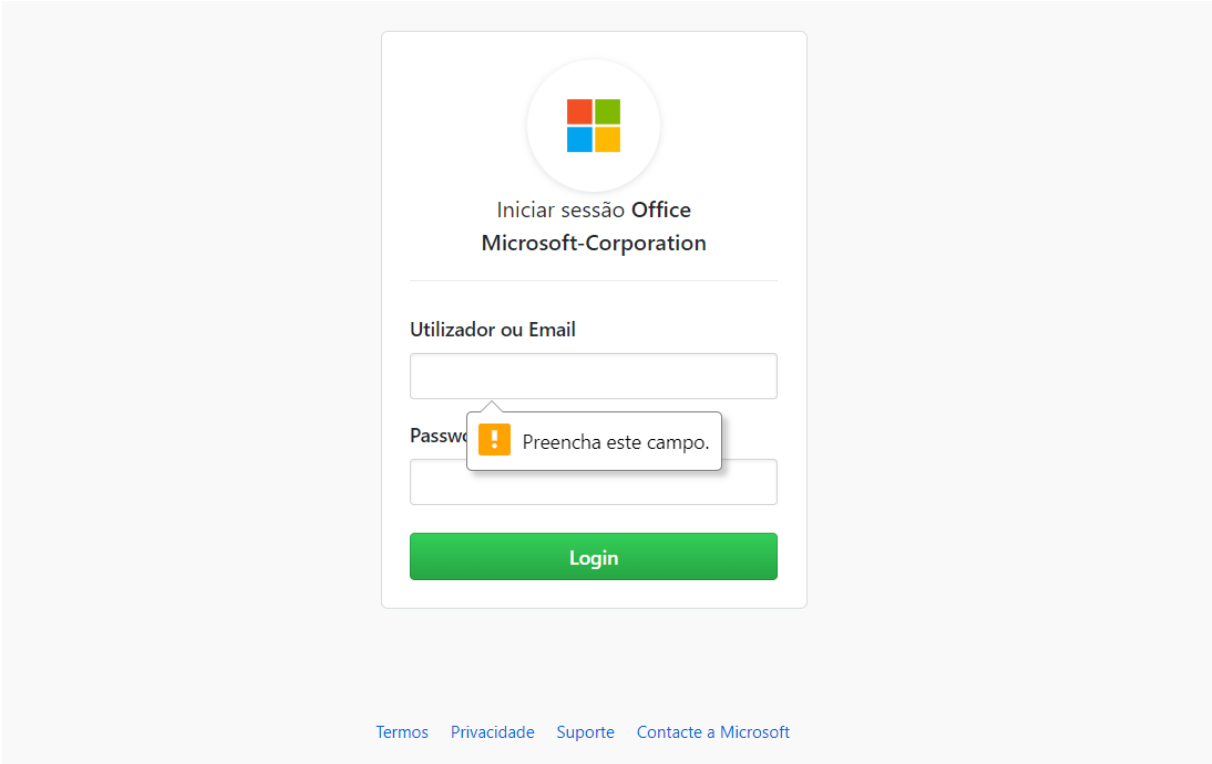

Figura 21. Preenchimento do campo Utilizador E-mail

A Figura 22 mostra o preenchimento do campo "Utilizador ou Email" com o formato certo, ou seja (Texto+@ulsguarda.min-saude.pt).

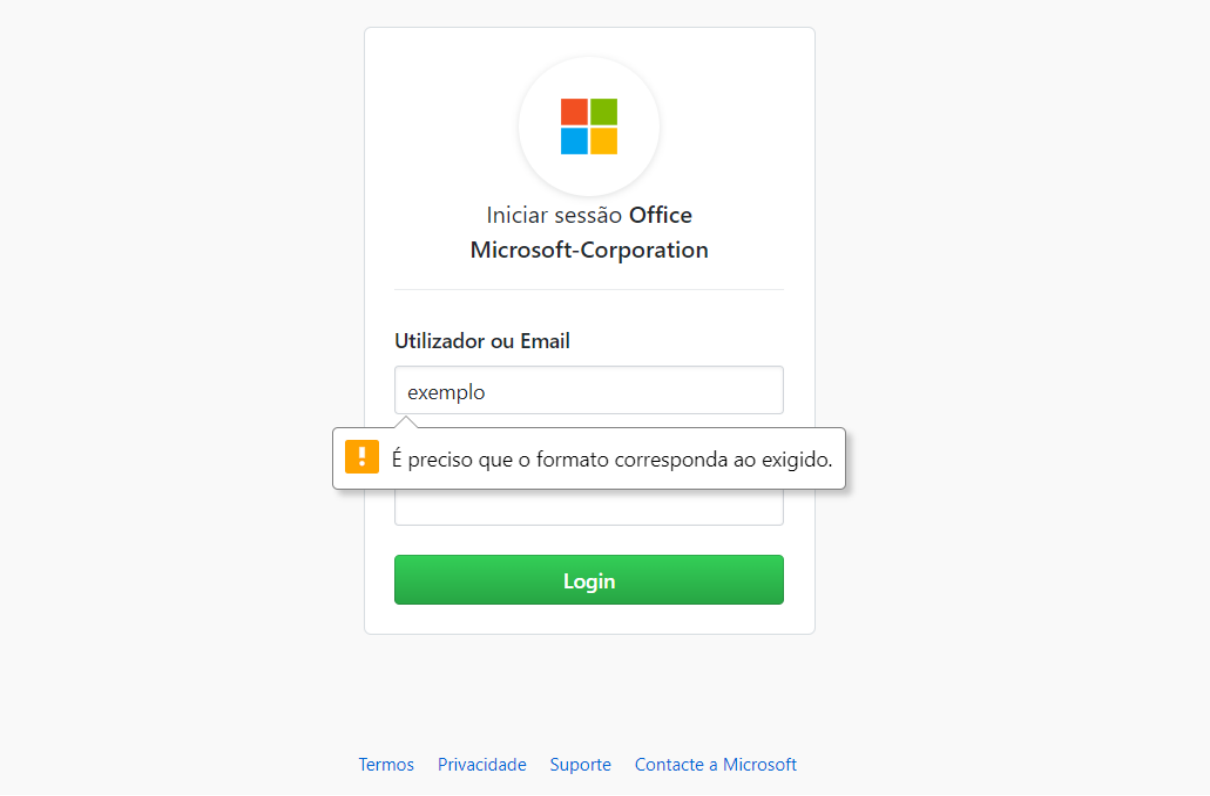

Figura 22. Preenchimento com o formato do campo Utilizador E-mail certo

A Figura 23 mostra o preenchimento do campo "Password" obrigatório.

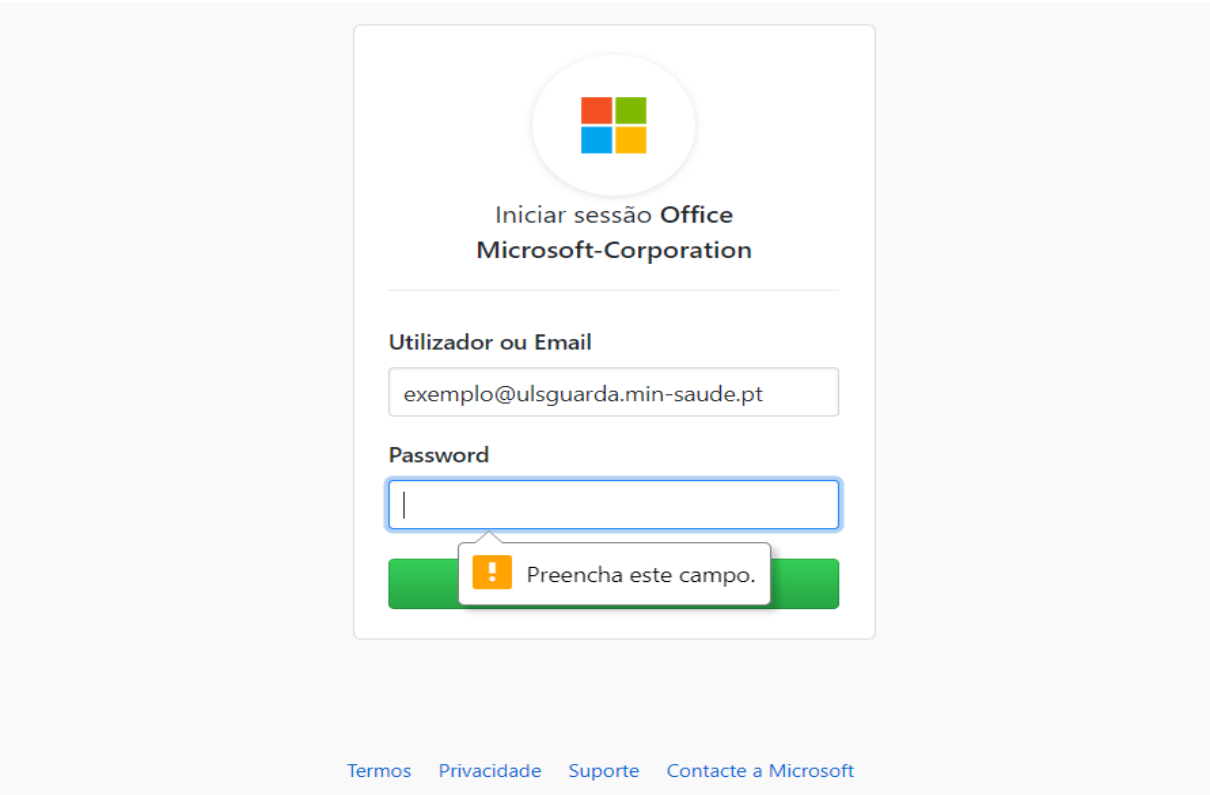

Figura 23. Preenchimento do campo Password

Após o problema anterior resolvido, surgiu outro, as entidades de cibersegurança, tiveram como preferência a não captação da palavra-passe por haver vítimas que mesmo assim, depois do susto, não iriam mudar as suas palavras-passe.
Para isso a solução que me ocorreu, foi alterar o id do campo palavra-passe, para assim o software SET não reconhecer o campo.

Originalmente a linha do campo palavra-passe estava como na Figura 24.

```
Password
</label>
<input type="password" name="" id="password" class="form-control form-control input-block" tabindex="2" required/>
```

Figura 24. Imagem ilustrativa linha original do campo password

Depois de alterado o id de "password" para "sempassword", como mostra a Figura 25, o software SET não reconheceu o campo, como inicialmente tinha pensado.

```
Password
</label>
<input type="password" name="" id="sempassword" class="form-control form-control input-block" tabindex="2" required/>
```

Figura 25. Imagem ilustrativa linha alterada do campo password

Página index2.html

Depois da página index.html estar pronta, precisei de outra página na qual iria ser utilizada como segunda página, index2.html. Esta página redirecionava as vítimas após fazerem *Login* e teve como principal objetivo assustar as vítimas e ainda destacar algumas medidas de segurança no mundo digital.

O primeiro passo foi criar a página index2.html através do editor nano no diretório: `/var/www/html/`

No início programei apenas uma página simples para conseguir ir para a parte mais importante que era o ataque em si, como se pode verificar na Figura 26, depois de ter sucesso no ataque continuei a página index2.html.

Voce foi hackeado

Neste momento temos as suas credeciais de acesso

Figura 26. Imagem ilustrativa de Teste do index2.html

Após o ataque ter ocorrido, o aspeto da minha página index2.html foi o seguinte:

A Figura 27, representa topo da página index2.html.

Figura 27. Imagem ilustrativa do index2.html início

A Figura 28 representa o meio da página index2.html.

Figura 28. Imagem ilustrativa do index2.html meio

A Figura 29 representa o fim da página index2.html.

Figura 29. Imagem ilustrativa do index2.html fim

2.4.4. Realização de testes

Depois de instalado o software necessários e as páginas index.html e index2.html prontas, foi dado início às tentativas de ataque.

Era essencial que o index.html funcionasse através do Setoolkit e o index2.html funcionasse através do Apache por ambas serem páginas html customizadas.

Logo no início surgiu o problema de ambos os softwares usarem a mesma porta, porta essa que é a 80, responsável pelo protocolo http.

Para resolver esse problema consultei um site (Cezar, 2018) para saber como mudar a porta utilizada pelo Apache para a porta 4444 em dois ficheiros.

A Figura 30 representa o ficheiro ports.conf que se encontra no diretório:

`/etc/apache2/`

```
  GNU nano 4.9.2                                    /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 4444

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```

Figura 30. Imagem ilustrativa do ficheiro ports.conf

A Figura 31 representa o ficheiro 000-default.conf que se encontra no diretório:

/etc/apache2/sites-enabled/

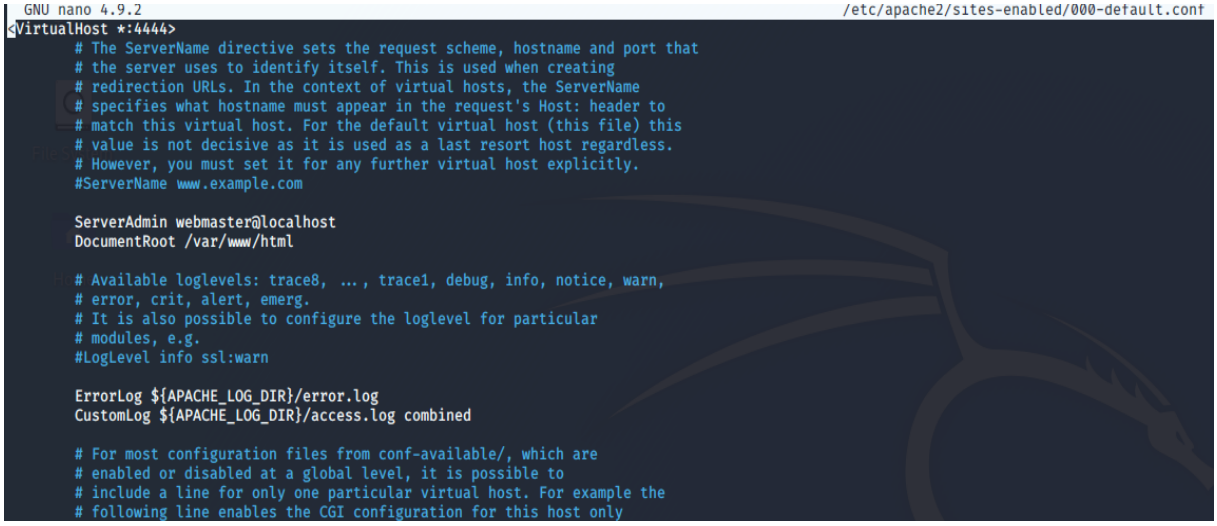

Figura 31. Imagem ilustrativa do ficheiro 000-default.conf

Após a resolução do problema percebi que por alguma razão o software setoolkit, dentro da rede ULSG, não funcionava com a porta 80.

Decidi mudar a porta 80 do software setoolkit para 8080 com a ajuda da consulta de um website (ghost, 2017).

Para isso, editei a web_port do ficheiro set.config, como se pode ver na Figura 32,que se encontra no diretório:

/etc/setoolkit/set.config

Figura 32. Imagem ilustrativa do ficheiro set.config

Mais tarde, acabou por dar problema e voltei ao mesmo ficheiro para repor a porta para 80.

Depois de resolvidos os problemas anteriormente referidos, surgiu outro, causado pela versão do sistema operativo que foi utilizada.

A Figura 33 mostra o problema.

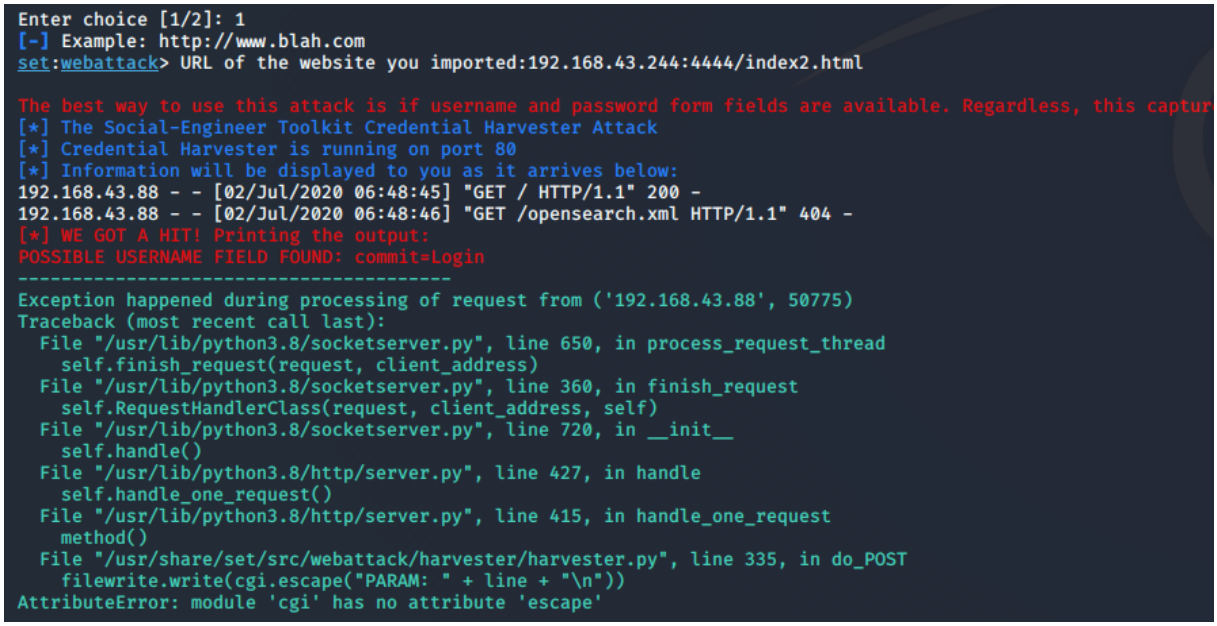

Figura 33. Imagem ilustrativa problema cgi

Consultei vários sites e encontrei a solução num deles (neorampage, 2020).

A solução do problema foi ir ao ficheiro harvester.py no diretório:

`/usr/share/set/src/webattack/harvester/`

acrescentar import html no inicio do ficheiro e mudar cgi.escape para html.escape.

A Figura 34 mostra o acréscimo de import html.

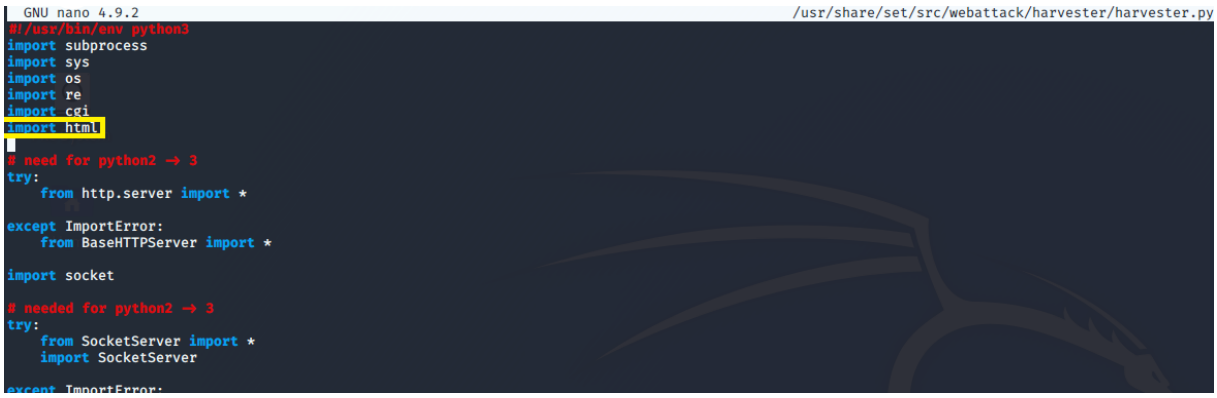

Figura 34. Imagem ilustrativa import html

A Figura 35 mostra a alteração de cgi.escape por html.escape.

```
            # not an exact science
            log_password = check_config("HARVESTER_LOG_PASSWORDS=")
            if log_password.lower() == "on":
                print(bcolors.RED + "POSSIBLE PASSWORD FIELD FOUND: " + line + "\r" + bcolors.GREEN)
            else:
                line = ""
            counter = 1
        filewrite.write(html.escape("PARAM: " + line + "\n"))
        filewrite2.write(line + "\n")
        # if a counter hits at 0 then print this line
        if counter == 0:
            print("PARAM: " + line + "\r")
        # reset counter
        counter = 0
```

Figura 35. Imagem ilustrativa Alteração cgi para html

2.4.5. Inicio do ataque

Ativar o serviço apache2

O primeiro passo do ataque é dar início ao serviço apache2, **para isso digitei o comando:**

`service apache2 start`

Como mostra a Figura 36.

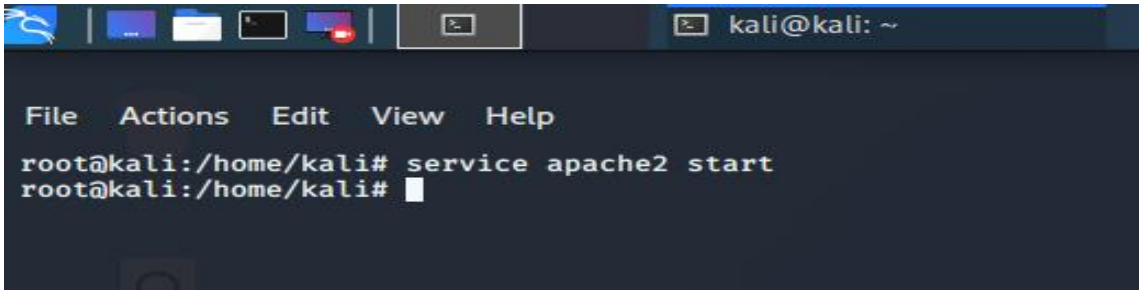

Figura 36. Imagem ilustrativa ativar Apache

Após o passo anterior, verifiquei se realmente o serviço estava a funcionar.

Para isso digitei o comando:

`service apache2 status`

Como mostra a Figura 37.

```
root@kali:/home/kali# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2020-07-03 05:01:31 EDT; 2min 56s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1716 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1727 (apache2)
      Tasks: 6 (limit: 4656)
     Memory: 19.2M
     CGroup: /system.slice/apache2.service
             ├─1727 /usr/sbin/apache2 -k start
             ├─1728 /usr/sbin/apache2 -k start
             ├─1729 /usr/sbin/apache2 -k start
             ├─1730 /usr/sbin/apache2 -k start
             ├─1731 /usr/sbin/apache2 -k start
             └─1732 /usr/sbin/apache2 -k start

Jul 03 05:01:31 kali systemd[1]: Starting The Apache HTTP Server...
Jul 03 05:01:31 kali apachectl[1726]: AH00557: apache2: apr_sockaddr_info_get() failed for kali
Jul 03 05:01:31 kali apachectl[1726]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1.
Jul 03 05:01:31 kali systemd[1]: Started The Apache HTTP Server.
root@kali:/home/kali#
```

Figura 37. Imagem ilustrativa verificar Apache

Entrei no programa setoolkit com o comando:

`setoolkit`

Como mostra a Figura 38.

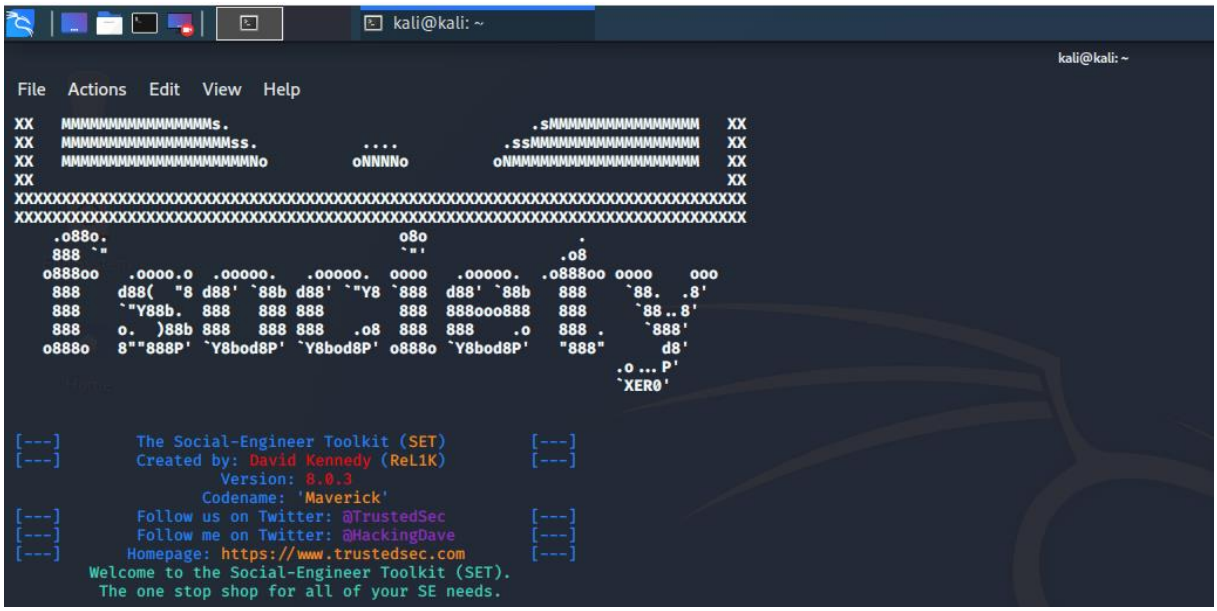

Figura 38. Imagem ilustrativa do setoolkit

Selecionei a primeira (1º) opção (Social-Engineering Attacks), como pode ser vista na Figura 39**, digitando 1.**

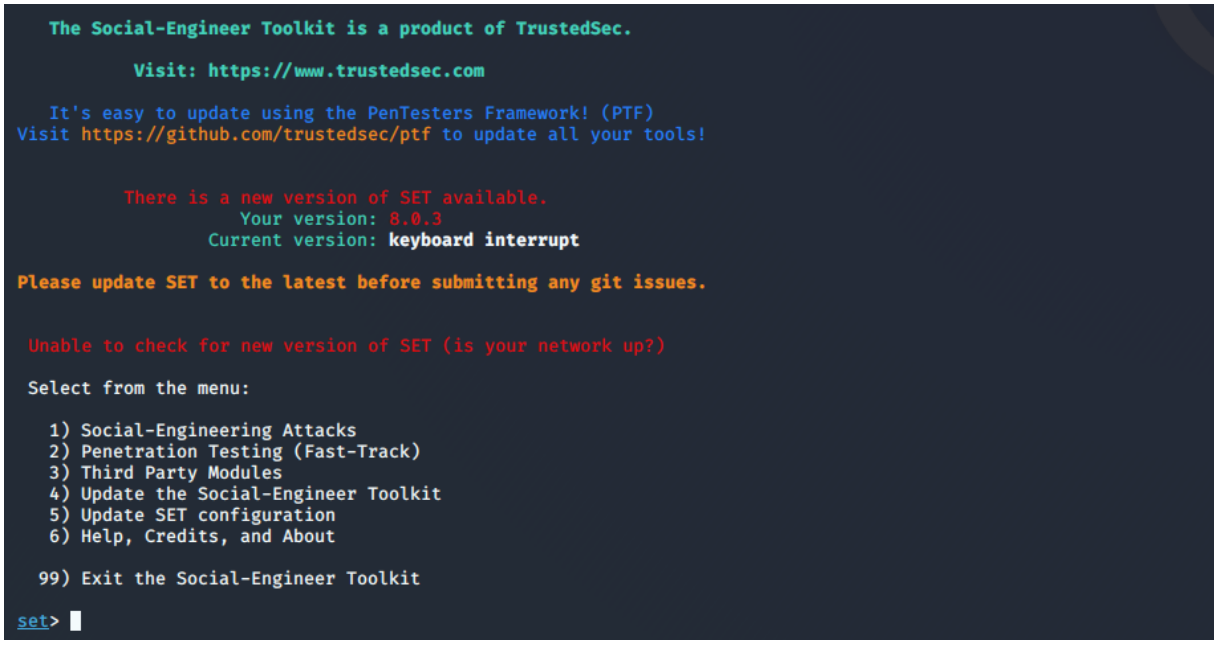

Figura 39. Imagem ilustrativa primeiro menu setoolkit

Selecionei a segunda (2ª) opção (Website Attack Vectors), como pode ser vista na Figura 40**, digitando 2.**

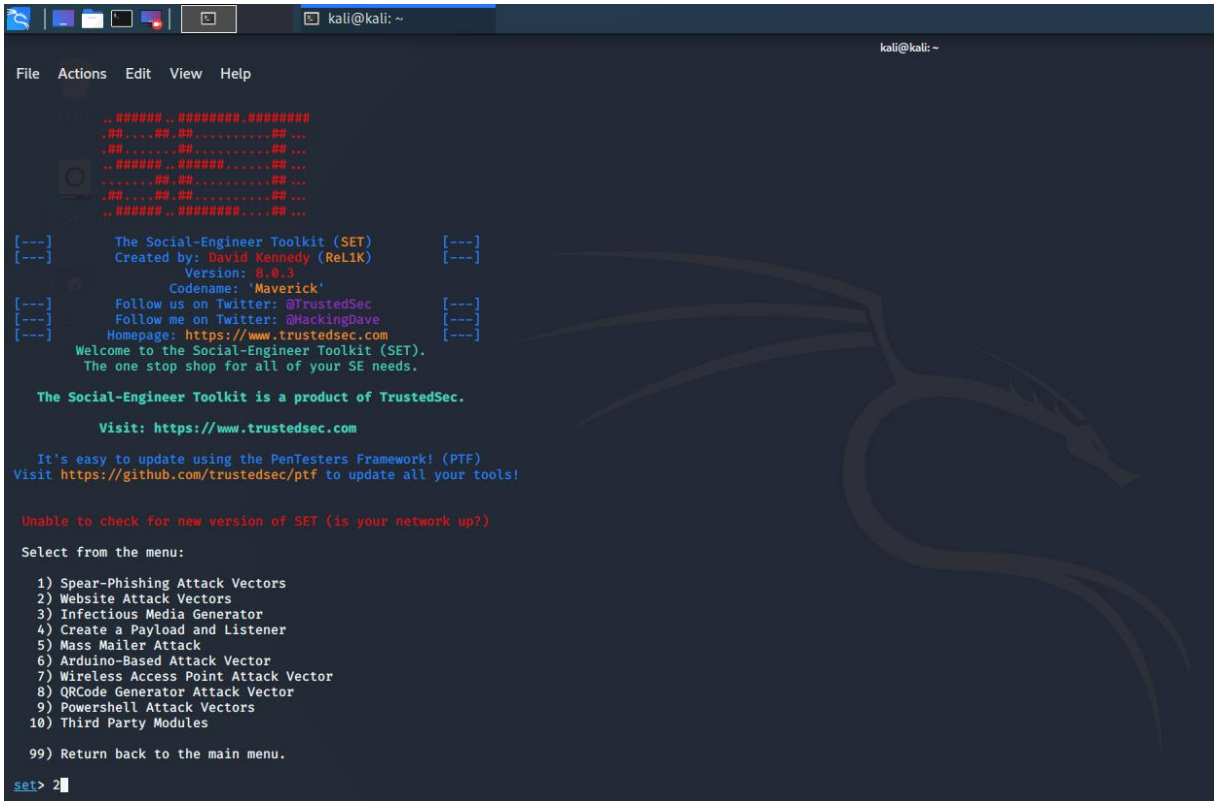

Figura 40. Imagem ilustrativa segundo menu setoolkit

Selecionei a terceira (3ª) opção (Credential Harvester Attack Method), como pode ser vista na Figura 41**,digitando 3.**

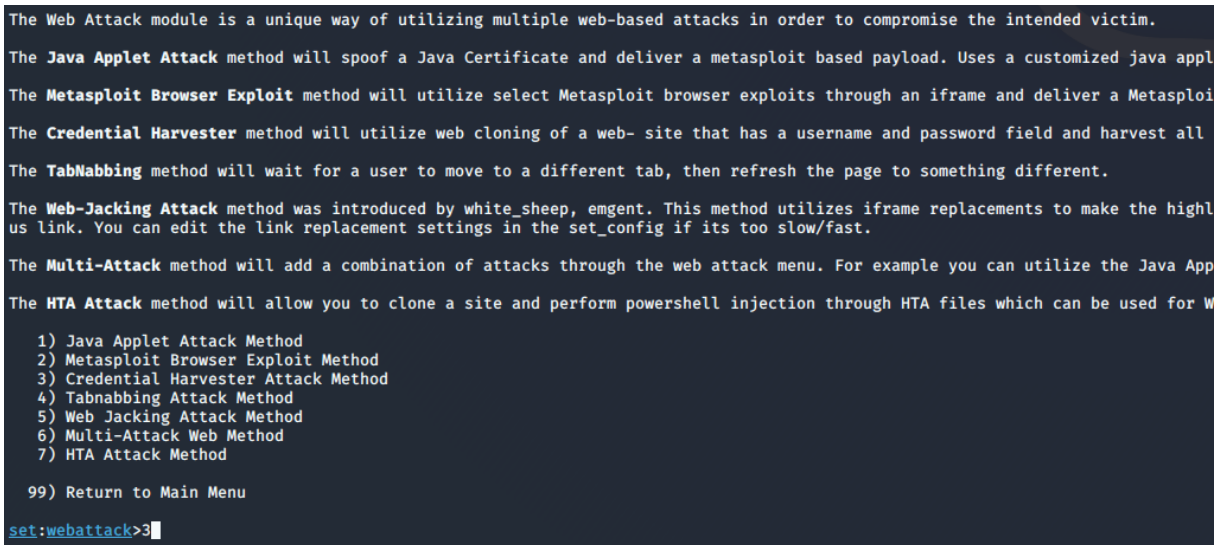

Figura 41. Imagem ilustrativa terceiro menu setoolkit

Selecionei a segunda (3ª) opção (Custom Import), como pode ser vista na Figura 42**,digitando 3.**

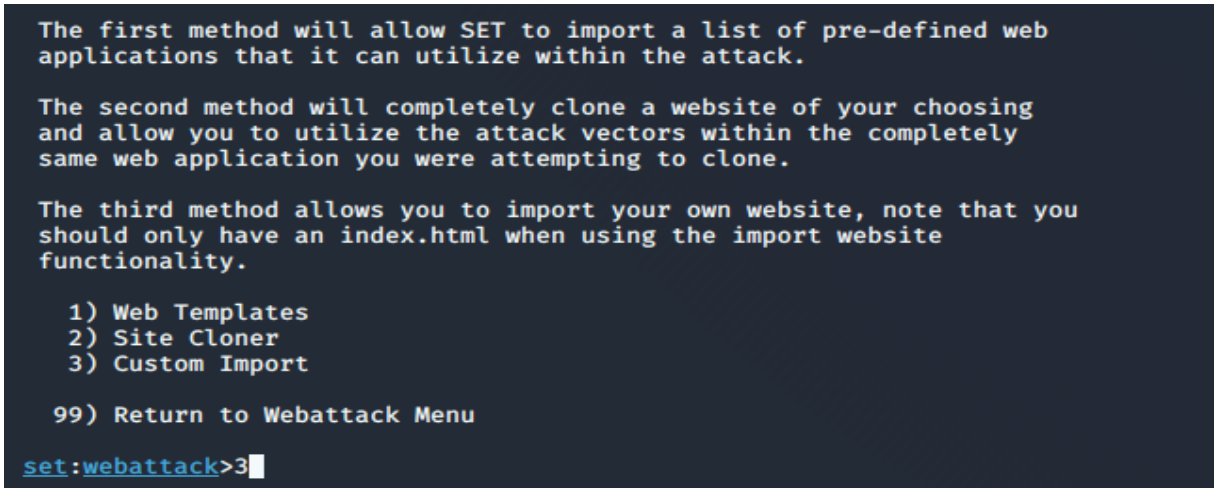

Figura 42. Imagem ilustrativa quarto menu setoolkit

Cliquei na tecla "Enter" do teclado, no passo representado na Figura 43**, dessa forma o software vai automaticamente utilizar o ip da máquina que vai lançar o ataque.**

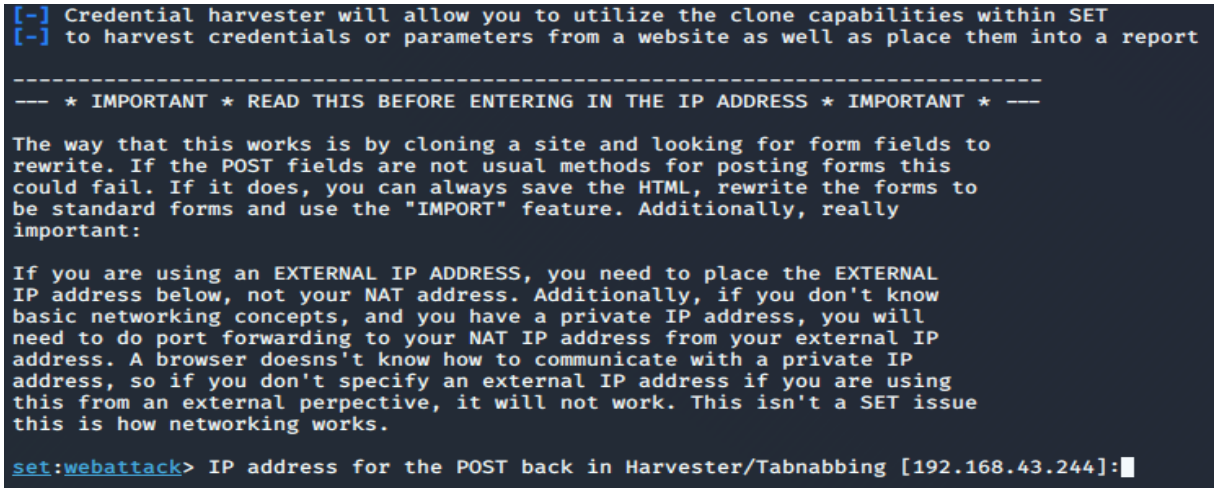

Figura 43. Imagem ilustrativa endereço ip setoolkit

Digitei o diretório para a primeira página (index.html) que é:

/var/www/html/

E escolhi a primeira (1º) opção (Copy just the index.html) como pode ser vista na Figura 44**,digitando 1.**

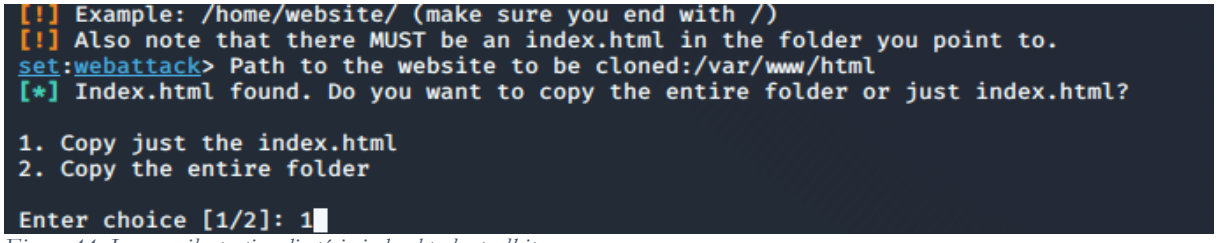

Figura 44. Imagem ilustrativa diretório index.html setoolkit

Digitei o endereço url da segunda página, como se pode verificar na Figura 45**, página essa que funciona através do Apache.**

O endereço é o ip da máquina, dois pontos, a porta 4444 porque foi a porta que configurei para o Apache e o nome da segunda (2ª) página:

192.168.43.244:4444/index2.html

Figura 45. Imagem ilustrativa endereço url do index2.html setoolkit

Assim que o ataque ficou pronto, fui a um encurtador de url (www.cutt.ly, s.d.), como se pode verificar na Figura 46 para parecer um link comum, em vez de aparecer o IP da máquina atacante.

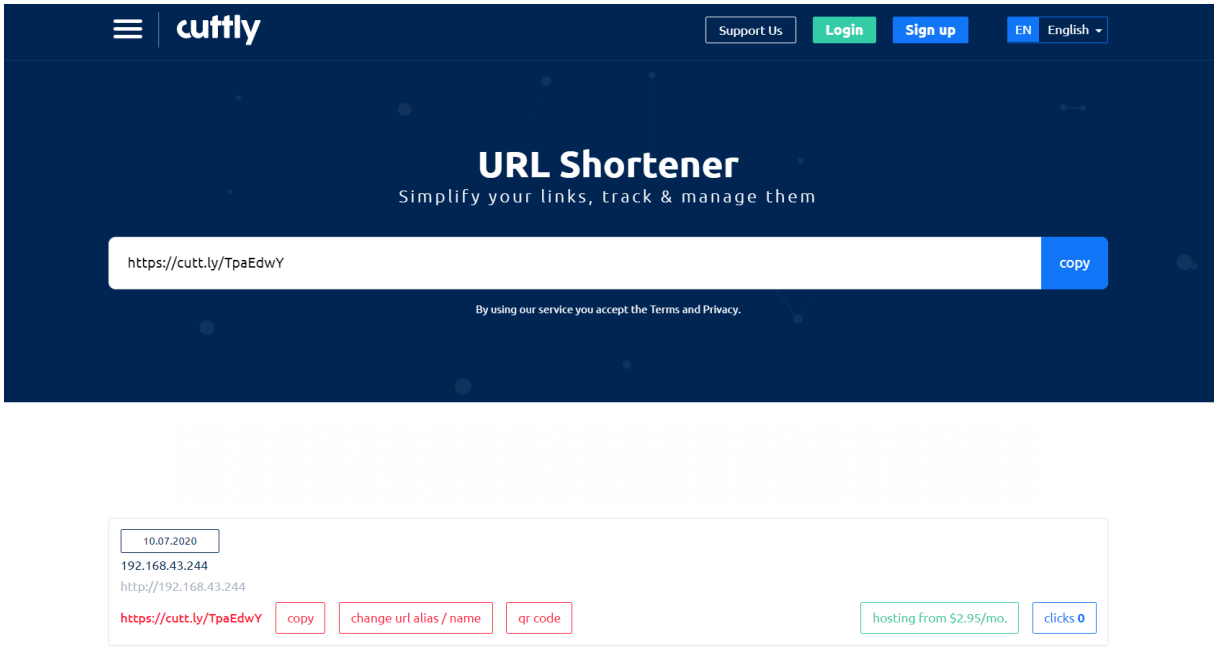

Figura 46. Imagem ilustrativa do encurtador do link

No e-mail foi utilizado esse link, mas em http em vez de https, para dessa maneira as credenciais não serem encriptadas.

O e-mail utilizado foi fornecido pela equipa de informática.

A Figura 47 mostra a mensagem de e-mail que será utilizada.

Figura 47. Imagem ilustrativa E-mail

No impedimento de mostrar o verdadeiro ataque, neste presente relatório, para não revelar as credenciais dos trabalhadores da ULSG, fiz uma pequena demostração do que seria o resultado do ataque, ao atacar-me a mim mesmo.

Cliquei no link, no *Login* falso preenchi "exemploemail@ulsguarda.min-saude.pt" no campo E-mail e no campo Palavra-passe preenchi "exemplopassword", vale lembrar que foi feita a alteração no código do index.html para que apenas os e-mails fossem capturados e não as palavras-passe.

Pode-se verificar na Figura 48 que o e-mail foi capturado e apenas o e-mail.

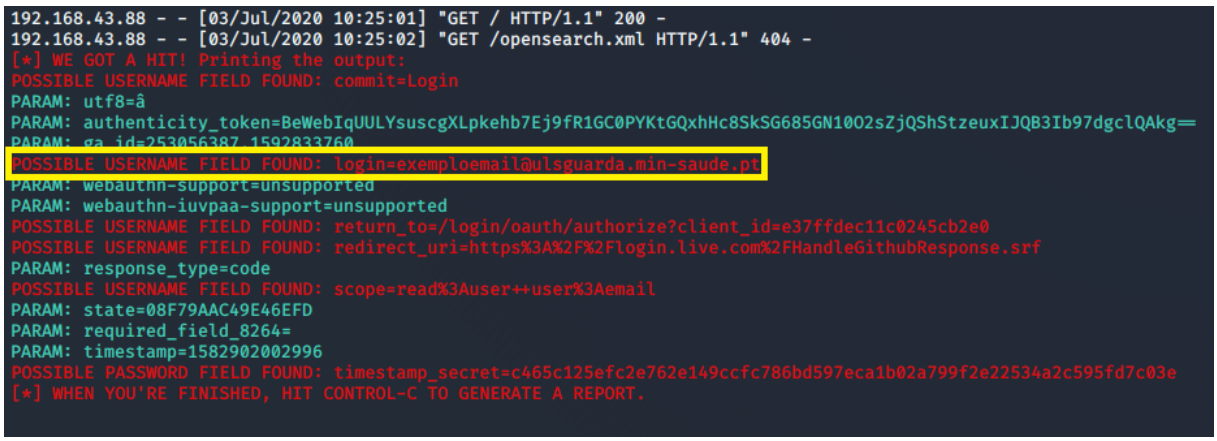

Figura 48. Imagem Ilustrativa Demonstração do ataque

3. Tema secundário de estágio

Como referido anteriormente, fiz também inúmeras tarefas.

Alguns exemplos do que fiz como estagiário:

A Figura 49 representa o Data Center da ULSG, onde tive uma breve explicação de como funciona a rede telefónica do hospital e respetivos centros de saúde associados ao hospital (treze (13) centros de saúde), Realizei algumas tarefas, como por exemplo, montagem de uma linha telefónica analógica de urgência na ULSG, para os quartos de isolamento destinados aos pacientes infetados de coronavírus (COVID-19). Foi feito o mapeamento e a ligação entre a central telefónica e os switches nos bastidores do Data Center com cabos RJ45, ligação nos bastidores/distribuidores de piso para as portas RJ11 dos quartos e por fim ligação dos telefones nos quartos de isolamento e execução de testes para verificar se estava tudo a funcionar com os números de telefone corretos.

Figura 49. Imagem ilustrativa do Data Center ULSG

A Figura 50 representa a correção de uma tomada de rede que deixou de funcionar no bloco operatório, através de um bastidor de piso.

Figura 50. Imagem ilustrativa Switchs

A Figura 51 representa o interior de um dos bastidores do Data Center.

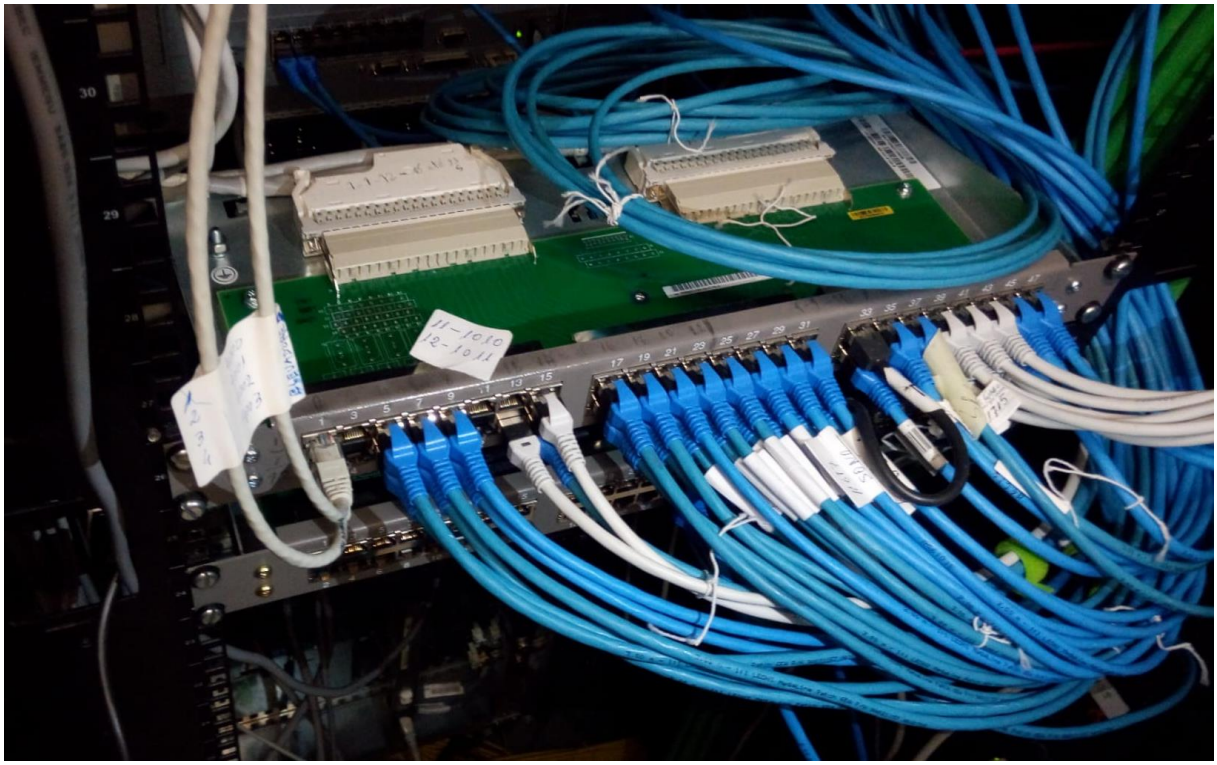

Figura 51. Imagem ilustrativa do Interior de um Bastidor

A Figura 52 representa a manutenção do hardware do computador utilizado para o projeto de ataque de engenharia social.

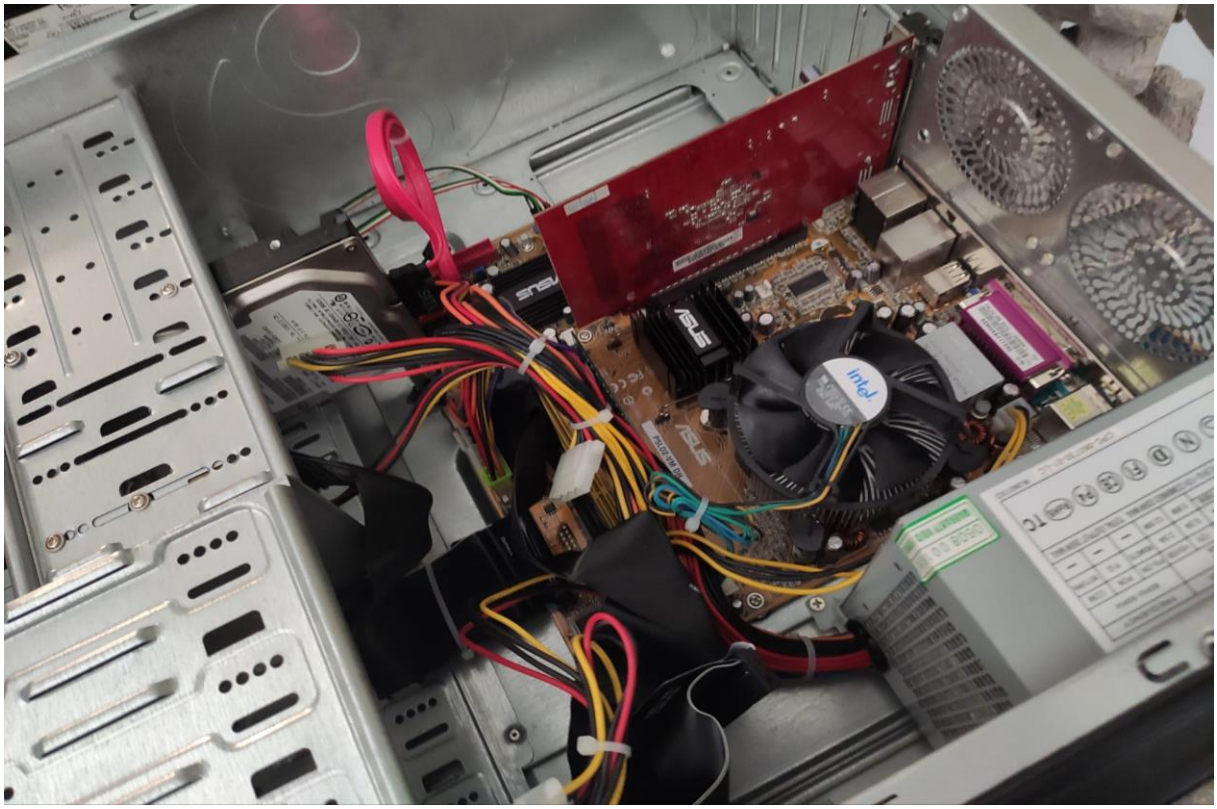

Figura 52. Imagem ilustrativa do interior do computador utilizado no ataque

A Figura 53 representa a substituição de cilindro de fotorrecetor da unidade de imagem para impressoras da marca LexMark.

Figura 53. Imagem Ilustrativa Unidade de Imagem

A Figura 54 representa uma manutenção geral preventiva de uma impressora da marca Xerox (Desmontagem da impressora, limpeza de peças, substituição de peças gastas e montagem).

Figura 54. Imagem ilustrativa Interior de Impressora Xerox

4. Conclusão

Ao longo do estágio, foi desenvolvido um projeto de ataque de engenharia social, na área do *phishing*, consistindo na criação de uma página de *login* falsa. Esta página teve de parecer fidedigna para conseguir obter as credenciais de acesso dos utilizadores da rede ULSG, sem que eles se apercebessem.

O projeto ainda não foi realizado, por falta de autorização, autorização essa que não chegou a tempo do término do estágio, no entanto foram realizados vários testes com alguns computadores da ULSG e tudo funcionou na perfeição. Assim que obtiver a autorização, irei disponibilizar um dia para ir à ULSG realizar o projeto real, sendo que o principal objetivo é alertar os utilizadores e ensinar-lhes algumas medidas de prevenção.

O estágio findou com todos os objetivos previstos alcançados, tanto nas tarefas diárias como no projeto realizado.

Ao longo do estágio, adquiri muito conhecimento de diversas áreas da informática, tendo sido um estágio extremamente enriquecedor. Adquiri bastante conhecimento em algumas áreas como, impressão, rede informática, eletrónica, manutenção, entre outras.

Este estágio foi uma mais valia ao longo destes meses, pois permitiu-me aplicar conhecimentos adquiridos ao longo do meu percurso académico. Aprendi ainda novas técnicas e conheci novos métodos de trabalho, que serão fundamentais para o mercado de trabalho e para o futuro.

Anexo

SEGURANÇA NA INFORMÁTICA

GUIA DE BOAS PRÁTICAS A SEREM USADAS NO MUNDO DIGITAL

Ter especial atenção ao navegar em sites:

Verificar se o protocolo é http ou https. O https o único seguro tendo as informações todas encriptadas (o browser normalmente avisa o utilizador, no canto superior esquerdo, dizendo que a ligação não é segura).
Nunca expor credenciais de acesso sem ter a certeza da veracidade do site.
Verificar se o endereço url é legítimo.
Nunca navegar em sites indevidos que possam infetar o computador ou telemóvel.
O uso de Ad-blocker no browser pode prevenir vírus no computador, pois alguns anúncios são de hackers a tentarem infetar o seu equipamento.

No e-mail:

Desconfiar sempre do remetente e verificar a veracidade do endereço de e-mail.
Nunca clicar em nenhum link do e-mail dentro da ULS, principalmente se for o seu e-mail pessoal e não de trabalho.
Ter especial atenção ao link recebido no e-mail e verificar a sua veracidade.

Nas contas:

Nunca use palavras-passe comuns, como datas de aniversário, o nome do seu animal de estimação, ou dos filhos.
Deve ter palavras-passe fortes, com letras maiúsculas, minúsculas, caracteres especiais, números e compridas.
Mude as suas palavras-passe com alguma regularidade.
Use palavras-passe diferentes para todas as contas, desse modo se alguma pessoa mal intencionada tiver acesso a uma das suas palavras-passe, não ficará com acesso em todas as suas contas.
Nunca divulgar as credenciais de acesso a outra pessoa por nenhum motivo.
Ative a autenticação multifator sempre que esse recurso estiver disponível nas suas contas.

Outras medidas de segurança:

Manter o software do computador e telemóvel sempre atualizado (a maioria das atualizações são correções de falhas encontradas e exploradas por hackers no software).
Nunca inserir nenhum dispositivo externo no computador da ULS (PenDrive, CD ou DVD, discos externos, etc) porque pode infetar o computador.
Quando ligado à rede wi-fi, deve sempre desconfiar das redes sem palavra-passe e conectarse sempre à rede da ULS, podem ser pessoas mal intencionadas a querer ficar com os seus dados.
Não instale nenhum software (programas, jogos, etc) sem autorização do serviço de informática.
Ao mandar caixas ou pacotes de encomendas que recebeu para o lixo, certifique-se de que não está nenhum dado seu escrito e risque-o, pois algum hacker mal intencionado pode tirar vantagem dos seus dados. Pode, por exemplo, enviar-lhe um e-mail a fazer-se passar por uma empresa e ao ter os seus dados, o e-mail parecer mais legítimo podendo ter dados tais como a sua morada e o seu número de telemóvel, fazendo passarem-se pela empresa onde fez a encomenda. Assim, o e-mail vai parecer mais credível e enganá-lo mais facilmente.
Em caso de dúvida, entre em contacto com o serviço de informática.

Bibliografia

Cezar, M. (31 de Janeiro de 2018). *change-apache-port-in-linux*. Obtido em 25 de Junho de 2020, de www.tecmint.com: www.tecmint.com/change-apache-port-in-linux/

Fruhlinger, J. (25 de Setembro de 2019). *what-is-social-engineering.html*. Obtido em 24 de Junho de 2020, de www.csoonline.com: www.csoonline.com/article/2124681/what-is-social-engineering.html

ghost. (23 de Julho de 2017). *trustedsec/social-engineer-toolkit/issues/441*. Obtido em 9 de Julho de 2020, de www.github.com: www.github.com/trustedsec/social-engineer-toolkit/issues/441

Kali. (s.d.). *about-us*. Obtido em 25 de Junho de 2020, de www.kali.org: www.kali.org/about-us/

Linuxize. (19 de Novembro de 2019). *how-to-use-nano-text-editor*. Obtido em 25 de Junho de 2020, de www.linuxize.com: www.linuxize.com/post/how-to-use-nano-text-editor/

neorampage. (28 de Abril de 2020). *social-engineer-toolkit/issues/721*. Obtido em 25 de Junho de 2020, de www.github.com/trustedsec: www.github.com/trustedsec/social-engineer-toolkit/issues/721

Notepad. (s.d.). *www.notepad-plus-plus.org*. Obtido em 26 de Junho de 2020, de www.notepad-plus-plus.org: https://notepad-plus-plus.org/

Santos, R. (29 de Março de 2019). *como-instalar-o-servidor-web-apache-7ac337075f43*. Obtido em 25 de Junho de 2020, de www.medium.com: www.medium.com/@ruben199925/como-instalar-o-servidor-web-apache-7ac337075f43

Social-engineer. (s.d.). *about*. Obtido em 24 de Junho de 2020, de www.social-engineer.org: www.social-engineer.org/about/

Terranovasecurity. (s.d.). *examples-of-social-engineering-attacks*. Obtido em 24 de Junho de 2020, de www.terranovasecurity.com: www.terranovasecurity.com/examples-of-social-engineering-attacks/

Trustedsec. (s.d.). *the-social-engineer-toolkit-set*. Obtido em 25 de Junho de 2020, de www.trustedsec.com: www.trustedsec.com/tools/the-social-engineer-toolkit-set

Virtualbox. (s.d.). *www.virtualbox.org*. Obtido em 25 de Junho de 2020, de www.virtualbox.org: www.virtualbox.org

www.cutt.ly. (s.d.). *www.cutt.ly*. Obtido de www.cutt.ly.