IPG Politécnico da Guarda
Escola Superior de Tecnologia e Gestão

RELATÓRIO DE ESTÁGIO

Curso Técnico Superior Profissional
em Cibersegurança

Rodrigo Alexandre Pires Martins

outubro | 2020

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Relatório De Estágio

Rodrigo Alexandre Pires Martins

Relatório para a obtenção do diploma Técnico Superior Profissional em Cibersegurança

Escola Superior de Tecnologia e Gestão

Instituto Politécnico da Guarda

Relatório de Estágio

Rodrigo Alexandre Pires Martins

Relatório para a obtenção do Grau Técnico Superior Profissional

Em Cibersegurança

Orientador: Professor Fernando Melo Rodrigues

Supervisor: Engenheiro Ricardo Santos – ULS Guarda

Ficha de Identificação

Aluno:

Nome: Rodrigo Alexandre Pires Martins

Número: 1701465

Curso: Tesp de Cibersegurança

Contacto: 927598463; Email rodasapm@hotmail.com

Estabelecimento de ensino:

Instituição: Instituo Politécnico da Guarda

Escola de Ensino: Escola Superior de Tecnologia e Gestão

Localidade: Guarda

Morada: Avenida Dr. Francisco Sá Carneiro, nº50, 6300-559

Contacto: 271 220 120; E-mail: estg-geral@ipg.pt; Website: www.estg.ipg.pt

Orientador:

Fernando Melo Rodrigues

Supervisor:

Ricardo Santos

Duração do Estágio Curricular:

750 Horas

Agradecimentos

Concluído o estagio curricular gostaria de agradecer a todas as pessoas diretamente e indiretamente quem me ajudaram e apoiaram nesta longa e importante fase da minha vida.

Gostaria de agradecer a minha família, que sempre me motivou, e deu forças em todas as fases mais importantes e criticas da minha vida sendo esta uma delas.

Agradeço ao Instituto Politécnico da Guarda e aos seus professores pelo que me transmitiram neste curso, em especial, ao meu orientador de estagio, professor Fernando Rodrigues Melo, por ter aceite este cargo, e claro por todo o apoio e disponibilidade prestado ao longo deste curso, e a todos os outros docentes pela aprendizagem.

Por ultimo quero agradecer a entidade da ULS Guarda por todo o carinho que me receberam e pelo conforto que nos deram nesta época pandémica, especialmente ao Engenheiro Ricardo Santos.

Resumo

No âmbito de finalizar o Curso de Técnico Superior Profissional em Cibersegurança no Instituto Politécnico da Guarda (IPG), foi desenvolvido o presente relatório sobre o estágio curricular do ano letivo 2019/2020. O período de estágio teve início no dia 26/02/2020 e terminou

O estágio curricular constitui um dos primeiros contactos, do aluno com o mundo laboral sendo muito importante para o aluno obter novos conhecimentos sobre o mundo do trabalho. A instituição acolhedora deu as condições necessárias para o desenvolvimento e prática das aptidões adquiridas ao longo do plano curricular e novos fundamentos.

Primeiramente realizaram-se as apresentações, definimos o plano de estagio e onde seria o meu local de trabalho.
O plano elaborado teve consideração as necessidades da instituição, sabendo que maior parte dos utilizadores da ULS não sabem proteger-se de possíveis ataques foi sugerido a realização de um ataque didático para advertir e ensinar algumas normas e técnicas que devem ter em consideração.

Plano De Estágio

O meu estágio começou pela apresentação da equipa constituída no departamento de informática da unidade local de saúde (Uls) e ao meu supervisor Eng. Ricardo Santos, este que definiu o meu plano de estágio e indicou-me o meu local de trabalho, sendo supervisionado e avaliado.

O plano de estágio, tendo em consideração as necessidades da instituição, consistiram os seguintes pontos fundamentais:

- Programação em HTML e C;
- Criação e manutenção de VM para realização de testes e execução de um ataque didático aos utilizadores da instituição;

- Apoio aos utilizadores da instituição da ULS Guarda;
- Manutenção de Hardware e assistência a incidentes na instituição.

A Tabela 1 representa o conhecimento a adquirir para concluir os objetivos propostos:

Plano de Estágio	Competências adquiridas
Programação em HTML e C / Criação e manutenção de VM para ataque didático	- Aprender como instalar, utilizar e alterar scripts em VM - Aprender como alterar páginas web em HTML
Apoio aos utilizadores / Manutenção de Hardware e assistência de incidentes	- Aprender a interagir com os utilizadores e resolver incidentes da rede na ULS - Instalação de novos equipamentos e configuração dos mesmos para novos locais de trabalho na instituição

Índice

Acrónimos:

TeSP	Curso Tecnico Superior Profissional
TC	Cibersegurança
IPG	Instituto Politécnico da Guarda
HTML	HyperText Markup Language
C	Linguagem de programação
ULS	Unidade Local de Saúde
APP	*Aplicação*
BD	Base de Dados
JRE	*Java Runtime Environment*
SO	Sistema Operativo
URL	*Uniform Resource Locator*
VM	*Virtual Machine (Maquina virtual)*
COVID-19	coronavírus (SARS-COV-2*)*
DGS	*Direção Geral de Saúde*

Capítulo 1

Introdução

Segurança de redes de dados começa com autenticação do utilizador, geralmente com um email e password. Já que isto requer apenas um detalhe para autenticar o utilizador, a senha isto é chamado de autenticação de um fator.

Sabendo isto, a segurança de rede nesta instituição é muito importante, pois pode ser facilmente feito um ataque de *phishing* para o roubo de credenciais de utilizadores menos informados sobre políticas e normas de seguranças a ter.

Foi proposto a realização de um projeto para ensinar e educar os utilizadores da rede ULS Guarda e restantes Centros de Saúde pertencentes ao concelho da Guarda. Em termos lecionados durante os semestres letivos, usamos uma *Virtual Machine* criada para testes e realização do ataque a instituição.

1.1 Contexto e motivação

A motivação para concluir esta etapa veio do apoio moral que tive das pessoas mais chegadas, mas principalmente na medida em que constitui um elemento essencial e necessário para a conclusão do curso para que assim possa continuar os estudos na Licenciatura de Engenharia Informática, na vontade de ter uma vida próspera e economicamente estável.

1.2 Objetivos

Com a realização deste estágio pretende-se aplicar diariamente os conhecimentos adquiridos durante o ano curricular, e criar, bem como fortalecer, novos conhecimentos. Esta experiência não só contribuiu para o meu crescimento como futuro profissional, mas também me ajudou a superar inseguranças, tornando-me mais confiante e preparado para o futuro.

1.3 Estrutura do Relatório

Este relatório encontra-se estruturado em sete capítulos com os seguintes objetivos:

Capítulo 1: Contextualização do estágio e objetivos do mesmo.

Capítulo 2: Apresenta a instituição da ULS da Guarda e as suas instalações.

Capítulo 3: Atividades Desenvolvidas no Estágio.

Capítulo 4: Tarefas semanais

Capítulo 5: Descreve as Tecnologias Usadas e os seus conceitos.

Capítulo 6: Descreve como foi realizado o ataque didático.

Capítulo 7: Conclusão

Capítulo 2

Entidade de acolhimento

Neste capítulo será apresentada a entidade de acolhimento do estágio que é a Unidade local de saúde da Guarda.

2.1 Unidade local de Saúde da Guarda

Associada à vida do Sanatório e da própria cidade foi criado o Hospital Sousa Martins, primeiro como sanatório para a cura da tuberculose pulmonar da Europa, inaugurado em 18 de maio de 1907. Mais recentemente, foi integre como Unidade Local de Saúde na Guarda.

Figura 1 - Logotipo da ULS Guarda

2.2 Missão

Missão A ULS Guarda, EPE tem como missão proporcionar serviços públicos de saúde que permitam a maior abrangência de cuidados à população da sua área de influência e a todos os cidadãos em geral, num projeto partilhado e global que vise a obtenção de Qualidade, Acessibilidade, Eficácia e Eficiência, contribuindo também para o futuro sustentável do SNS. Desenvolve ensino e investigação de alta responsabilidade, por integrar a Faculdade de Ciências da Saúde da Universidade da Beira Interior e colaborar com as Escolas Superiores de Enfermagem e Escolas Superiores de Tecnologias da Saúde e diferentes estabelecimentos de ensino secundário, superior e universitário.

Fonte http://www.ulsguarda.min-saude.pt/servicos/saudepublica/visao-missao-e-valores/

2.3 Princípios

No desenvolvimento da sua atividade, a ULS Guarda, e os seus colaboradores regem-se pelos seguintes princípios:

- Legalidade, Igualdade, Proporcionalidade, Colaboração e Boa fé;
- Humanismo no relacionamento com os utentes e colegas de trabalho;
- Respeito pela dignidade humana;
- Qualidade nas prestações, com níveis de serviço e de resultados elevados;
- Competência e da responsabilidade.

Fonte http://www.ulsguarda.min-saude.pt/servicos/saudepublica/visao-missao-e-valores/

2.4 Valores

Os Valores que orientam o comportamento e a atuação a ULS Guarda, são:

• Atitude centrada no doente e na promoção da saúde pública e da comunidade, respeitando os valores do cidadão e da família;

• Cultura de excelência técnica, científica e do conhecimento, como um valor a prosseguir continuamente;

• Cultura interna de multidisciplinaridade e de bom relacionamento no trabalho;

• Responsabilidade Social, contribuindo para a otimização na utilização dos recursos e da capacidade instalada.

Fonte http://www.ulsguarda.min-saude.pt/servicos/saudepublica/visao-missao-e-valores/

2.5 Serviço de Sistemas de Informação e Comunicação

O serviço de sistemas de informação e comunicação da ULS mais conhecido por informática, situa-se no andar abaixo da maternidade perto do antigo sanatório.

O centro de informática tem um papel fundamental no Hospital e nos restantes do distrito pois é lá que tudo é gerido, monitorizado e efetuadas as manutenções e reparações.

2.6 Análise SWOT

A Análise SWOT é uma ferramenta de gestão muito utilizada pelas empresas para o diagnóstico estratégico, por isso a ULSG adotou esta ferramenta como um meio para analisar a sua posição estratégica no ambiente da saúde do distrito e no contexto da Beira Interior e Região Centro.

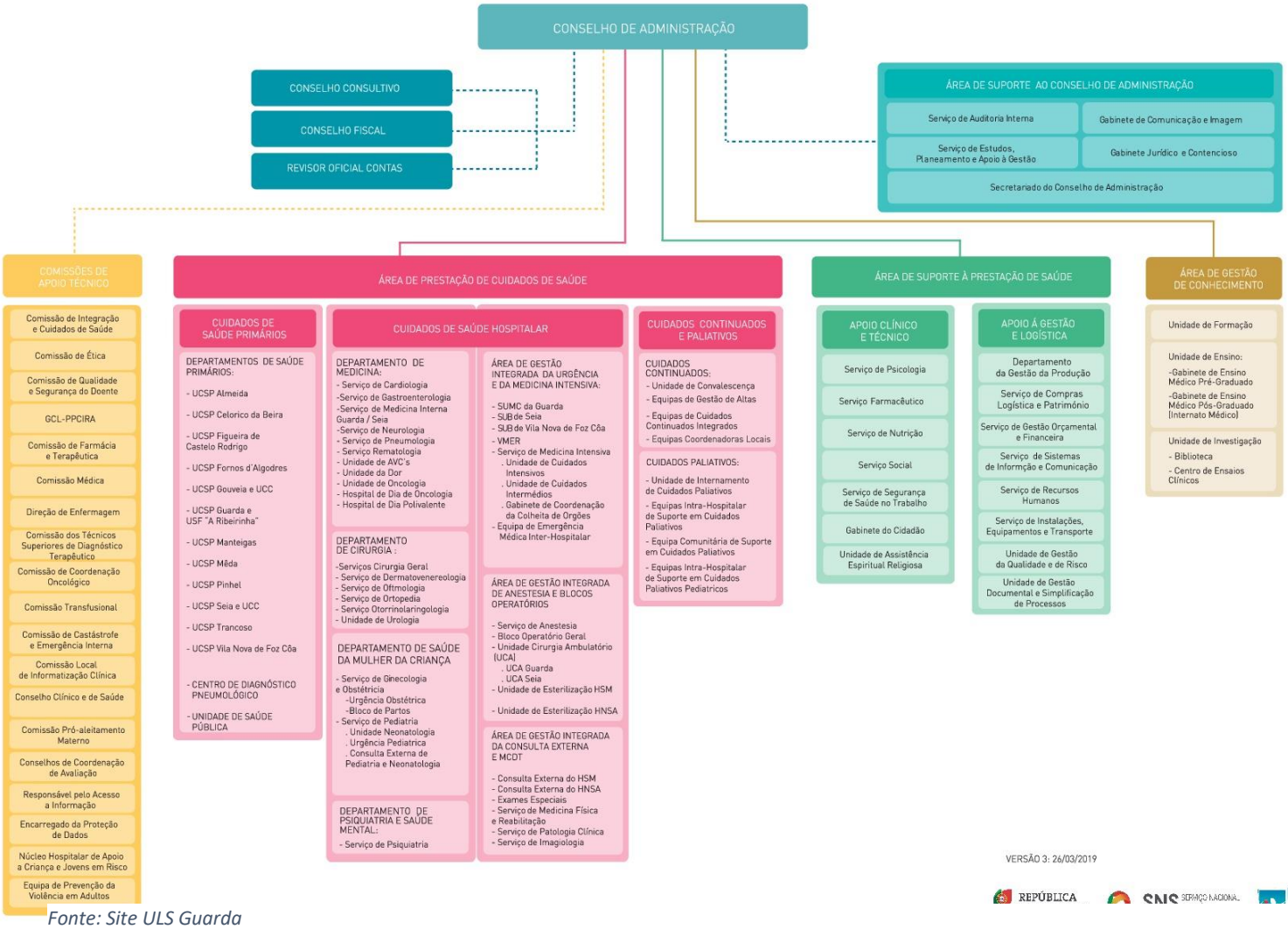
Tabela 2- Análise SWOT *(Fonte: Site Uls Guarda 1)*

PONTOS FORTES	A ULSG como elemento integrador. Motivação e formação dos recursos Humanos; Formação articulada com IPG, UBI. Urgência Geral 24h por dia; Bom rácio médio de família/utente.
Pontos Fracos	Muito tempo de espera para intervenções
Ameaças	Crise económico/financeira. Desertificação do Interior do País. População muito envelhecida. Elevada taxa de desemprego. Emigração.
Oportunidades	Melhorar a articulação entre os recursos; melhorar a rentabilização de Recursos entre as várias unidades de saúde;

2.7 Estrutura da organização

O Organograma é um gráfico que representa a estrutura formal de uma organização. Os organogramas mostram como estão dispostas unidades funcionais, a hierarquia e as relações de comunicação existentes entre estes. Num organograma, os órgãos são dispostos nos níveis que representam a hierarquia existente entre eles. Num organograma vertical, quanto mais alto estiver o órgão, maior é a sua autoridade e a abrangência da atividade. O organograma da ULS Guarda, que é apresentado na figura 2, mostra como está estruturada a instituição.

Fig.2 Organograma da ULS Guarda



Fonte: Site ULS Guarda

A organização interna de cada uma destas áreas é suportada por uma estrutura que pode incluir: departamentos, serviços e unidades funcionais, sendo cada uma delas dirigida por um responsável próprio, de acordo com o princípio da hierarquia e unidade de comando.

Capítulo 3

Atividades Desenvolvidas no Estágio

3. Introdução

Neste capítulo pretende-se fazer uma descrição das atividades que foram realizadas durante o período de estágio.

Durante o estágio, realizei todas as tarefas propostas pelo supervisor. Realizaram-se tarefas com hardware e software, a nível software trabalhei na rede da ULS, exercendo manutenção a bastidores e switch's através de um computador. Exerci trabalho a nível de formatação e arranjo de computadores danificados. Até ao final do estágio tentei sempre respeitar e socializar com os profissionais que trabalham neste local, assim criando um bom ambiente e ao mesmo tempo mostrar empenho da minha parte.

O meu plano de atividades que se segue foi definido pela ULS Guarda, mais concretamente pelo diretor do Serviço de Sistemas de Informação e Comunicação pelo Eng.º Ricardo Santos:

1. As apresentações foram feitas pela Eng.º Ricardo Santos com o objetivo de dar a conhecer: a instituição, os objetivos e os sistemas como também os equipamentos.
2. No serviço de Sistemas de Informação e Comunicação deram-me conhecimento das necessidades que tinham acerca da segurança e dos utilizadores mal informados sobre normas e cuidados a ter.

De seguida descrevem-se as atividades que foram realizadas durante o período de estágio.

3.1 Resolução de Incidentes

Maioritariamente dos dias de estágio era chamado para a resolução de um ou mais incidentes, isto é, quando alguma máquina falhava eram chamados os técnicos para a restauração da mesma sem que afetasse o serviço em que estivesse a ser utilizada. Primeiramente ia sempre acompanhado por um técnico com experiência, passado umas semanas ia eu mais a o resto da equipa de estagiários para a resolução do incidente.

3.1.1 Como gerir os incidentes

A finalidade é manter este processo ativo para que fosse possível a reposição rápida do serviço. Assim, a entidade é capaz de manter os níveis de disponibilidade dos seus serviços e reduzir os prejuízos decorrentes em períodos de inatividade. A gestão dos incidentes era realizada da seguinte maneira através dos seguintes métodos:

1. Identificação do incidente:

O primeiro passo é reconhecer o incidente. Os incidentes na maior parte das vezes são diagnosticados pelo sistema de informática, ou até mesmo em algumas situações pelos utilizadores do sistema a informar o problema.

2. Categorização do Incidente:

   O incidente tinha de ser categorizado depois de chegar ao local, isto é, tentava-se resolver o incidente no local, caso não fosse possível era necessário tomar outras medidas e avaliar o incidente de forma correta para que não fosse afetado um serviço que poderia agravar ainda mais o incidente.

3. Priorização do incidente:

   Caso existisse mais do que um incidente identificado sem que não houvesse mais técnicos escalados, era necessário priorizar a resolução dos incidentes

4. Verificação

   Apos a resolução do incidente, eram feitos testes para garantir se o problema foi solucionado corretamente e se não havia qualquer outro problema antes de acabar.

3.2 Criação e manutenção de postos de trabalho

Foi necessário a criação de novos postos de trabalho ou local para utentes da ULS, como aconteceu nesta época pandémica, foi necessário a criação de novas salas isoladoras, ligação de internet, e VOIP como também novas salas para serem realizados os testes ao COVID-19, com máquinas a disposição.

No Pavilhão Novo, na área de internamento e Bloco Operatório - Piso 1, ficarão afetos a doentes suspeitos ou confirmados de infeção por coronavírus. Manter-se-ão as restantes unidades e serviços que funcionam nos restantes pisos. Nos denominados Pavilhões 1 e 5, serão internados todos os outros doentes com necessidade, das diversas especialidades. Houve necessidade de deslocar serviços, por isso, o Serviço de Ortopedia passou a ocupar as instalações do serviço de Cardiologia; o Serviço de Cardiologia passou a partilhar o piso de Medicina Interna; o Serviço de Cirurgia passou a ocupar as instalações do Serviço de Ginecologia; o Serviço de Ginecologia passou a partilhar um espaço no Serviço de Obstetrícia; e o Serviço de Pneumologia passou a ocupar as instalações onde se encontra o internamento de Psiquiatria.

Capítulo 4

Tarefas Semanais

Neste Capítulo, vai ser descrito os passos de semana a semana, até ao término do estágio curricular.

1. Integração na instituição;
2. Aprender e pesquisar sobre formas como criar um ataque didático;
3. Criação de uma VM para realização de testes;
4. Realização de testes na VM dentro da rede da ULS;

5. Começo de estágio em regime (teletrabalho);
6. Criação de páginas HTML para uso no ataque didático;
7. Melhoramentos a nível de design no ataque;
8. Ensinar normas e cuidados a ter aos utilizadores da ULS via página HTML;
9. Alteração em HTML de páginas office365 para a realização do ataque;
10. Realização de documentos internos para o SSTIC na ULS;
11. Criar e apresentar um documento de apresentação do ataque a várias instituições;
12. Escolha de emails de variados serviços da ULS para a realização do ataque;
13. Realização do ataque didático;
14. Monitorizar o ataque e a taxa de sucesso
15. Realização do relatório de estágio;

4.1 Fevereiro

No mês de fevereiro foram apenas realizadas as apresentações devidas e conhecimento da instituição realizando poucas tarefas para o enquadramento dos estagiários, para realização de futuras tarefas.

4.2 Março

No mês de março realizou-se o plano de estágio e foi proposto a realização de um ataque didático à instituição como também a criação de salas e postos de trabalho isolados para um possível futuro pandémico que estava por vir. Sob ordens da DGS foi proposto à instituição a criação de salas para realização de testes e salas isoladoras para portadores do Vírus COVID-19.

A partir do dia 10 de março de 2020 os estágios presenciais ficaram suspensos na ULS, e começamos um regime de “teletrabalho” para continuidade do estágio e das tarefas

pretendidas para a instituição. Trabalhando no ataque como pesquisar sobre o que iriamos realizar e também realização de várias tarefas pretendidas pelo supervisor.

4.3 Abril

Continuidade em regime de teletrabalho comecei com a realização de portfolios sobre Políticas de Segurança da Informação para regulamentar a atuação nos seguintes casos:

- Gestão passwords;
- Gestão de alterações a programas;
- Audit logs;
- Gestão de incidentes;
- Gestão de backups;
- Segurança de redes;
- Disaster Recovery Planning.
- Gestão passwords;

Para a realização destes documentos era necessário enquadrar a instituição de forma a que fosse possível consultarem qualquer um destes documentos.

Para que isso fosse possível foi necessário falar com o Eng Luis Domingues, completamente integrado e com experiência suficiente na instituição.

4.4 Maio

Continuidade em regime de teletrabalho, no mês de Maio demos continuidade ao ataque distribuindo tarefas, fiquei de realizar um site em HTML que seria a pagina a aparecer depois da pagina Office365 falsa em que teria de exprimir logo ao inicio medo à vitima do ataque e outra parte que ensinasse a vitima a não voltar a cair em ataques de *phishing* colocando alguns tipos de politicas e normas a ter na internet como podemos ver na figura 3.

Continuei também com a realização dos portfolios sobre as Políticas de segurança, a capa de um dos portfolios na figura 4.

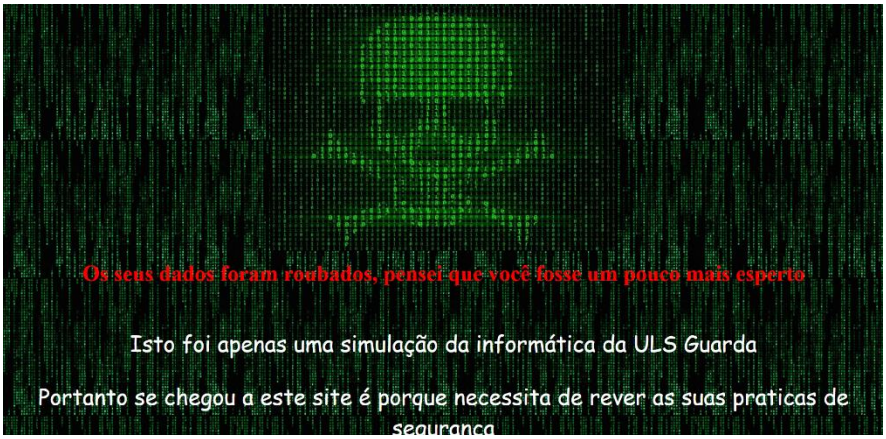


Figura 3

Figura 4

4.5 Junho

No mês de Junho finalizou-se o ataque, criamos uma imagem em uma VM com o SO Linux Khali com as ferramentas atualizadas, e colocamos numa maquina que nos foi disponibilizada pela equipa de informática do hospital.

Usamos as páginas HTML criadas em regime de teletrabalho, para as vítimas colocarem os seus dados e outra com as políticas e normas de segurança (Fig. 5).

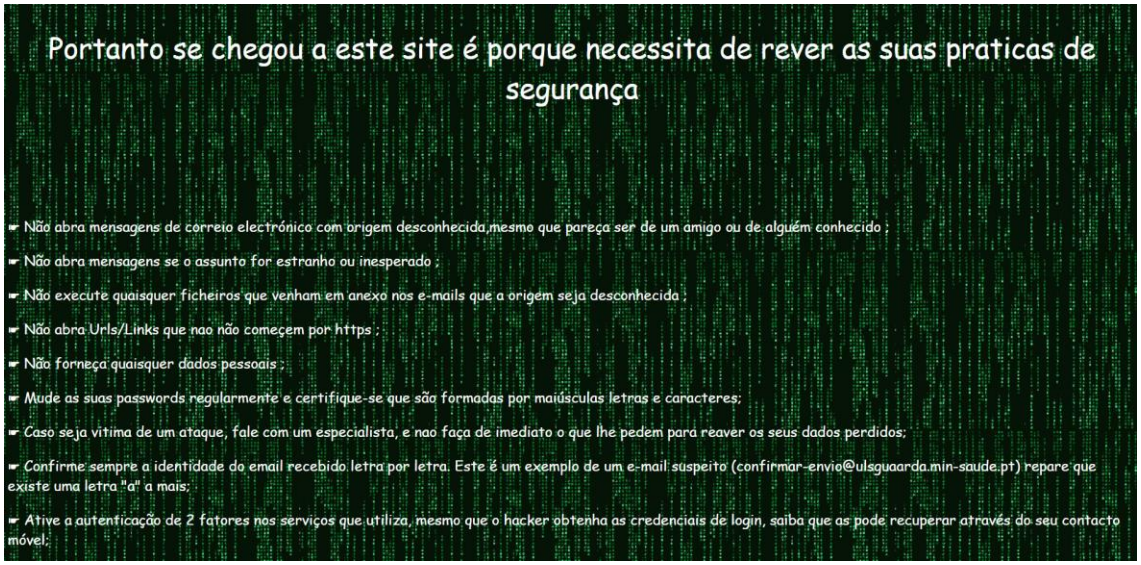


Figura 5

Posto isso, com tudo pronto, foi necessário a realização de um relatório com tudo o que íamos fazer documentado para várias instituições para que as entidades necessárias tivessem conhecimento. Apresentado o relatório conseguimos a aprovação para a realização do ataque didático.

Começamos a fazer a seleção dos emails das vítimas, escolhidas por nos e pela equipa de informática, usando os métodos que os atacantes costumam fazer.

4.6 Julho

No último mês de estágio curricular, realizamos o ataque didático, e monitorizamos enquanto decorria. Aproveitando o tempo para começar a realizar o relatório.

No último dia, deixamos o posto de trabalho arrumado como o encontramos e fizemos as despedidas, fazendo uma reunião sobre o empenho e serviço prestado durante o estágio.

Capítulo 5

Tecnologias Usadas e os seus conceitos

Introdução

Este capítulo apresenta os conceitos e termos mais importantes para obter uma compreensão sobre as ferramentas que foram usadas ao longo do estágio. São tambem apresentados alguns conceitos de tecnologias usadas.

5.1 Servidor

E um computador que pertence a uma rede, com a função de fornecer serviços a outros computadores, designados de clientes. Também serve para armazenar ficheiros digitais, que os utilizadores podem aceder sobre os dados acerca de um paciente por exemplo.

5.2 Sistema Operativo

E um programa ou um conjunto destes, cuja função e a gestão de recursos do sistema (por exemplo, qual o programa que recebe a atenção do processador). Também fornece uma interface para que o utilizador possa manipular o computador. O mais usado foi o Linux.

5.4 Linux

Linux*:* e um sistema operacional baseado no UNIX que foi criado em 1991 por Linus. Os utilizadores podem modificar e criar variações de código-fonte, conhecidas como distribuições, para computadores e outros dispositivos.

5.5 Software

E uma sequência de instruções, que ir a ser interpretada por um computador, para executar uma tarefa específica. Num computador o Software, e a sua parte lógica, com a função de comandar o seu hardware (parte física, como o disco, CPU, dispositivos de entrada e saída...)

5.6 Website

E uma coleção de páginas, que estão interligadas e publicamente acessíveis, em que compartilham um único nome de domínio (por exemplo, facebook.com).

5.7 Browser

Programa que permite a navegação na Internet, ou seja, aceder a websites e aos recursos neles disponibilizados.

5.8 Base de dados

E um conjunto de dados devidamente organizado, que permite o armazenamento de dados, que podem ser acedidos para serem manipulados ou eliminados. São normalmente utilizados por empresas, para armazenar, gerir e retirar informações.

5.9 Testes de sistema

O objetivo e executar o sistema no ponto de vista de um utilizador, para verificar, se existe alguma falha nas funcionalidades em relação aos objetivos originais. Os testes são executados em condições similares aquelas que o utilizador utilizar a no seu quotidiano de manipulação do sistema.

5.10 VirtualBox

O *VirtalBox* e um software de virtualização, que permite criar ambientes para instalação de sistemas operativos distintos. Ele permite a instalação e utilização de um ou mais sistemas operativos dentro de outro, assim como seus respetivos softwares, como por exemplo, dois ou mais computadores independentes, mas compartilhando fisicamente o mesmo hardware. Ele suporta a criação e a gestão de máquinas virtuais executando versões e derivações de vários´ sistemas operativos.

Foi com o auxílio da ferramenta VirtualBox que foi possível a criação de uma máquina virtual para a realização de testes (Fig. 6). Foi feita também uma imagem do sistema operativo que a máquina virtual tinha para a instalação em um servidor.

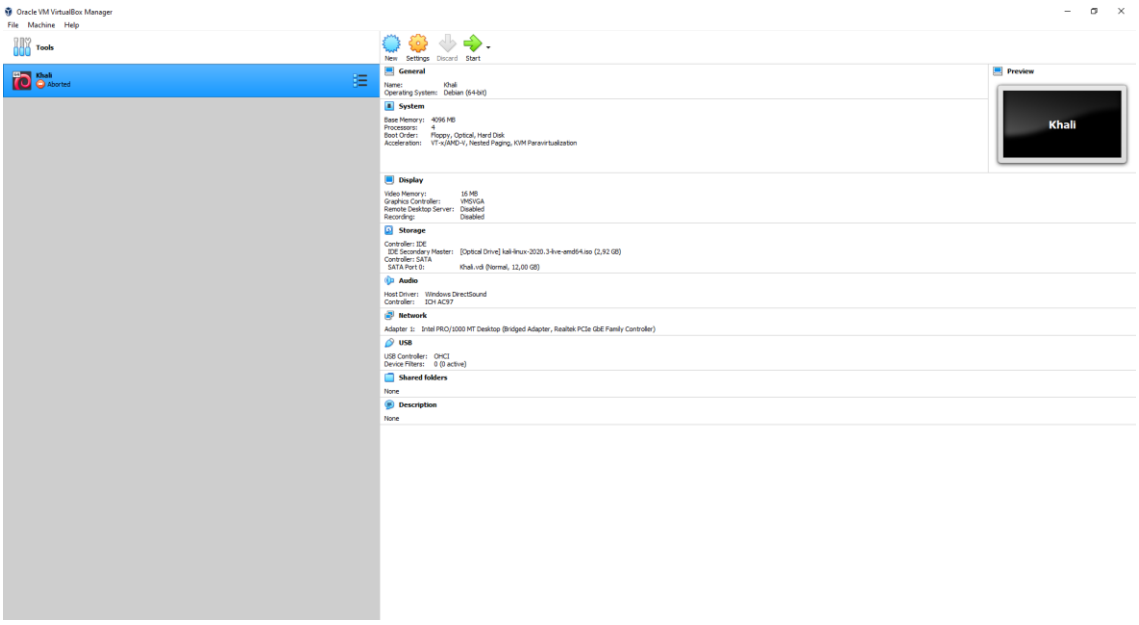


Figura 6

5.11 Servidor Apache

O Apache é um servidor de código aberto que suporta cerca de 46% de todos os sites hospedados na internet, permitindo que os donos de sites mostrem e mantenham os seus conteúdos na internet. A sua primeira versão, foi lançada em 1995, há mais de 20 anos. Quando alguém visita um site, esse visitante entra num domínio na barra de pesquisa por um navegador.

Disponibiliza todos os recursos que podem ser acessados pelo internauta. Envio de e-mails, mensagens, compras online e diversas outras funções podem ser executadas graças a servidores como o Apache. O que vale destacar no Apache é que, apesar de tudo, ele é distribuído sob a licença GNU, ou seja, é gratuito e pode ser estudado e modificado através de seu código fonte por qualquer pessoa (Arranque serviço apache na Ilustração 6)

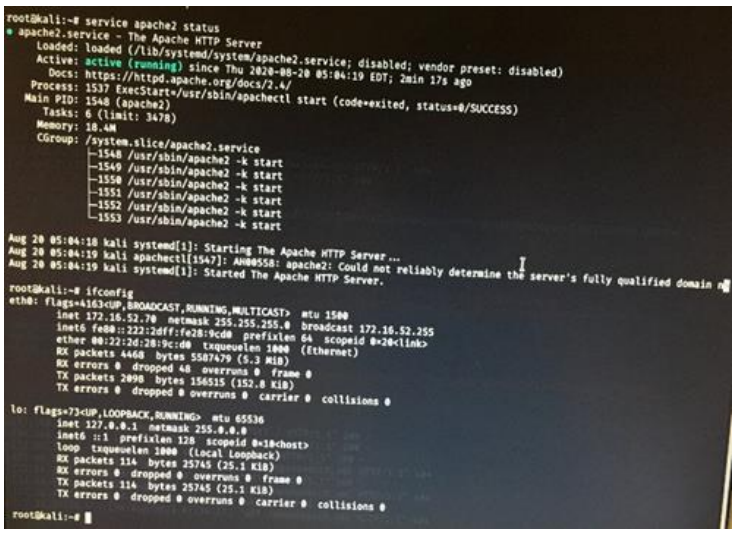


Ilustração 6

5.11 Notepad++

Notepad++ é um programa para editar código fonte em qualquer linguagem de programação. É um editor de código que oferece várias ajudas, como ressaltado de cores, possibilidade de editar vários documentos de uma só vez, menus contextuais, auto-completar código, etc. É um presente para os programadores, já que além de tudo é gratuito (Fig. 7).

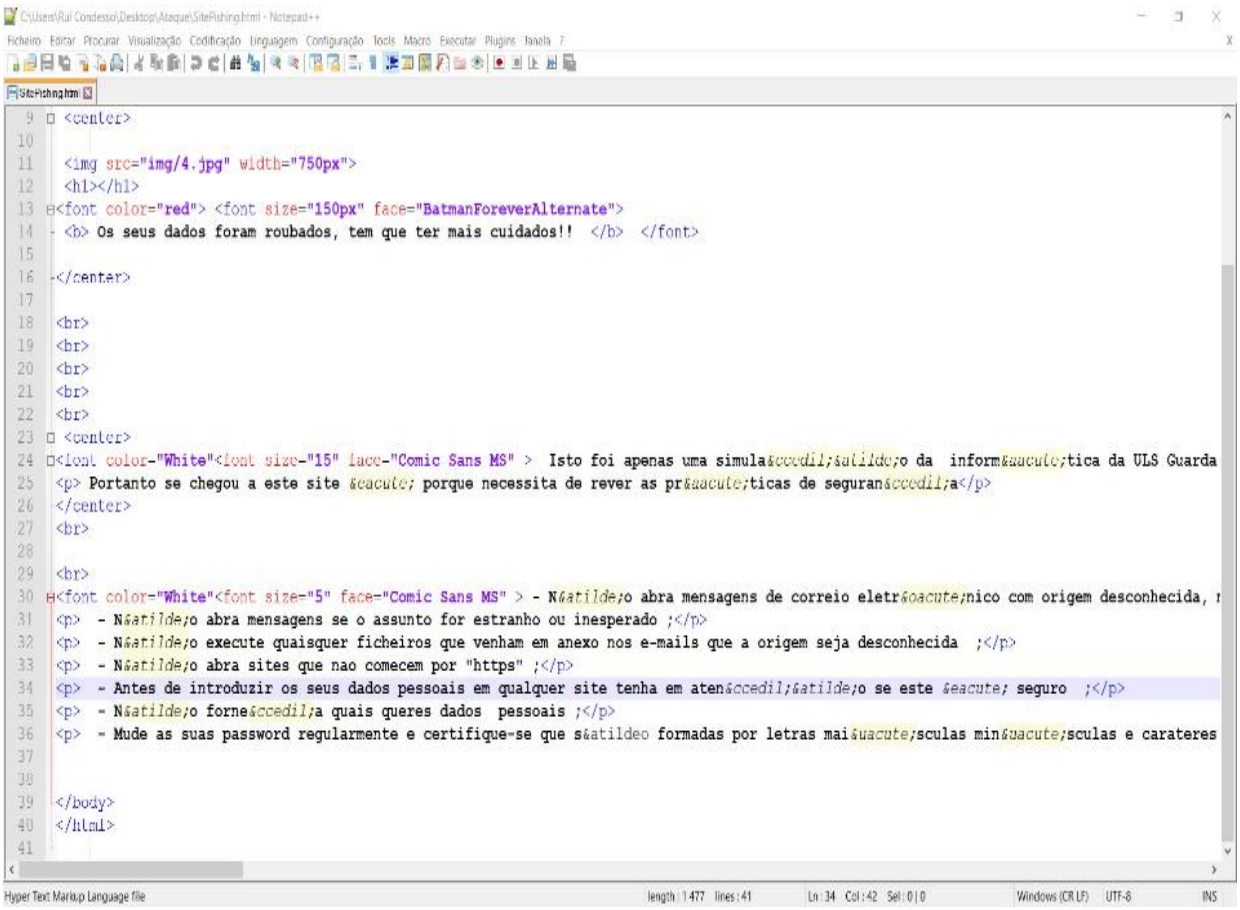


Figura 7

5.12 SetoolKit

O Social-Engineer Toolkit é uma ferramenta baseada em Python de código aberto voltada para testes de penetração em Engenharia Social. Tem mais de 2 milhões de downloads e visa alavancar ataques tecnológicos avançados em um ambiente do tipo engenharia social (Fig. 8).

Principais características:

- Pode ser executada em varias plataformas, como em Linux, unix, etc;
- Código aberto, ou seja, pode ser modificada como o utilizador pretender;
- Ajustes nos menus de configurações;
- Opções de ataques de phishing, ataques a sites, envio em massa, etc.

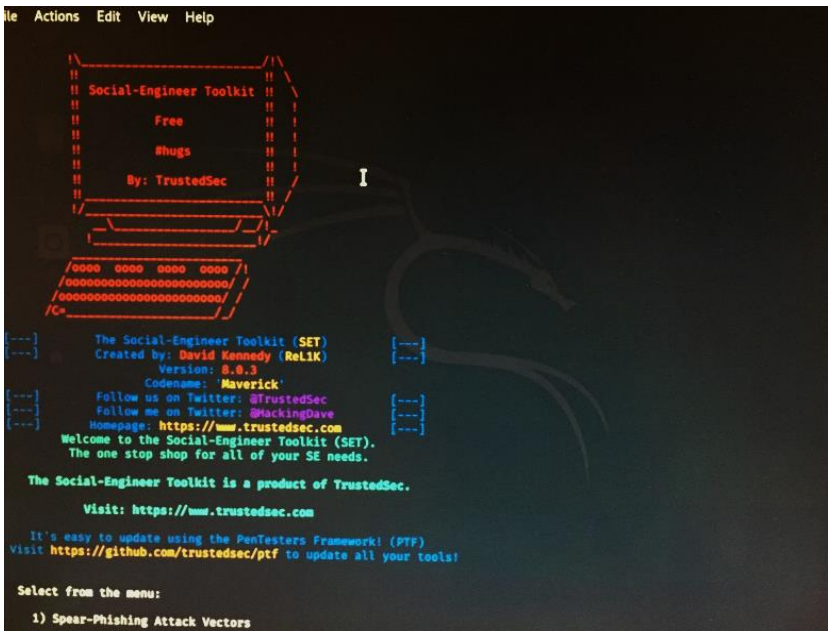


Figura 8

Capítulo 6

Ataque Didático

Este capítulo apresenta e explica o ataque didático realizado durante o estágio, esse ataque consistia para alem de alertar os colaboradores para as boas praticas no uso da internet, relembrar que a internet é um lugar sem lei e qualquer ação inconsciente pode ter sequelas graves.
O ataque inicialmente foi pensado, para ser realizado a todos os colaboradores, mas rápido nos recordamos, que muitos deles não iram ver o email num curto espaço de tempo.

O ataque tinha de ser algo rápido de executar e que os colaboradores não achassem algo fora do comum.

Depois de muito deliberar chegamos a ideia de realizar um ataque de phishing através do email a uma amostra de 200 colaboradores da ULS, para alertar os colaboradores para os riscos da internet, e relembrá-los que eles lidam com dados sensíveis e necessitam de uma atenção redobrada o ataque iria se realizar na rede interna da ULS.

6.1 Identificação do ataque

O ataque educativo de *phishing* ou engenharia social e tem como âmbito da educação das vítimas sem existir furto de qualquer dado pessoal. Preocupar e assustar a vítima vai ter de ser representado no ataque pois para parecer o mais real possível, e de seguida colocar medidas de prevenção para que a vítima perceba que pode ser real e pode acontecer a qualquer momento.

6.2 Descrição Genérica do ataque

Irá ser criada uma página web idêntica à original onde as vítimas terão de colocar as suas credenciais para aceder a conta Outlook365. Quando colocadas, irá para outra página web que irá alertar o utilizador de um possível roubo de dados, mas como é educativo irão aparecer algumas medidas de segurança para que não volte a acontecer ou então prevenir a vítima.

6.3 Descrição técnica do ataque

Iremos utilizar o Kali Linux para a criação do ataque de engenharia social, criamos as páginas web com o apache, de seguida clonamos e alteramos a página de login do office 365 onde os utilizadores terão de colocar os dados, de seguida com a ferramenta “setoolkit” fazemos o ataque de engenharia social/Phishing com o clone do site (Fig. 9). Faremos uma página web para advertir os utilizadores que podem ser facilmente enganados colocando umas normas básicas de segurança.

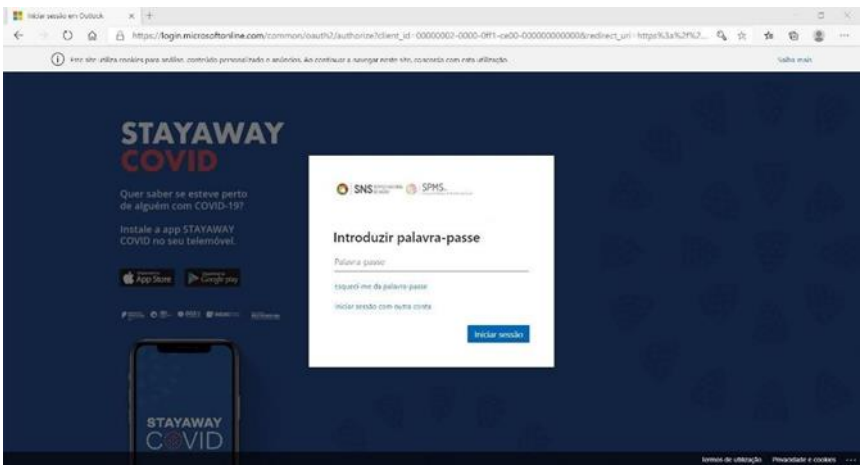


Figura 9

6.4 Identificação das partes envolvidas

A criação deste ataque educativo irá ser elaborado pela equipa do centro de informática da ULS Guarda e dos alunos de cibersegurança que estão em formação em contexto de trabalho do IPG.

6.5 Conceitos sobre o ataque

O ataque realizou-se a partir de uma máquina com o sistema operativo Kali Linux, fornecida pela equipa de sistemas de informática da ULS, aí usou-se uma ferramenta chamada *setoolkit* que é utilizada na sua maioria das vezes para executar ataques de *phising,* que consistem em uma fraude on-line, através de mensagens de email falsas, spams, sites maliciosos, tentam revelar informações sigilosas, como números de conta bancárias e de cartões de crédito, login e password (Ilutração 10).

O ataque consistia em, enviarmos um email (Fig. 11) de uma conta, que nos foi fornecida pelos serviços de informático, para uma amostra de 200 colaboradores, no corpo do email iria constar um texto apelativo para os colaboradores clicarem num link, esse link direcionouos para a página de login do seu email, a qual já foi previamente clonada através do setoolkit, assim que eles colocassem as suas credenciais na página estas iram ser guardadas na máquina.

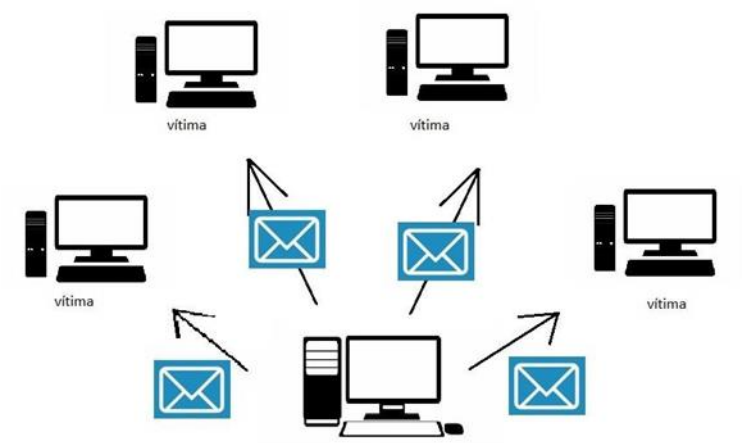


Ilustração 10

6.6 Resultados

Logo após o envio dos primeiros emails (corpo do email Fig. 11), começou logo a interação dos colaboradores com o email, houve alguns que inseriram as suas credenciais, outros apenas viram que o email era suspeito e contactaram os serviços de informática, para terem a certeza do que se tratava.

Passado alguns dias, a equipa de sistemas de informática da ULS decidiu desligar o ataque e a guardas as informações, que conseguiram angariar. Com base nos resultados a equipa de sistemas de informática da ULS, começou a pensar em forma para alertar os colaboradores para os riscos da internet.

Em suma o ataque teve um resultado positivo, embora seja assustador ter havido pessoas que diariamente lidam com dados sensíveis e caíram neste tipo de ataque.

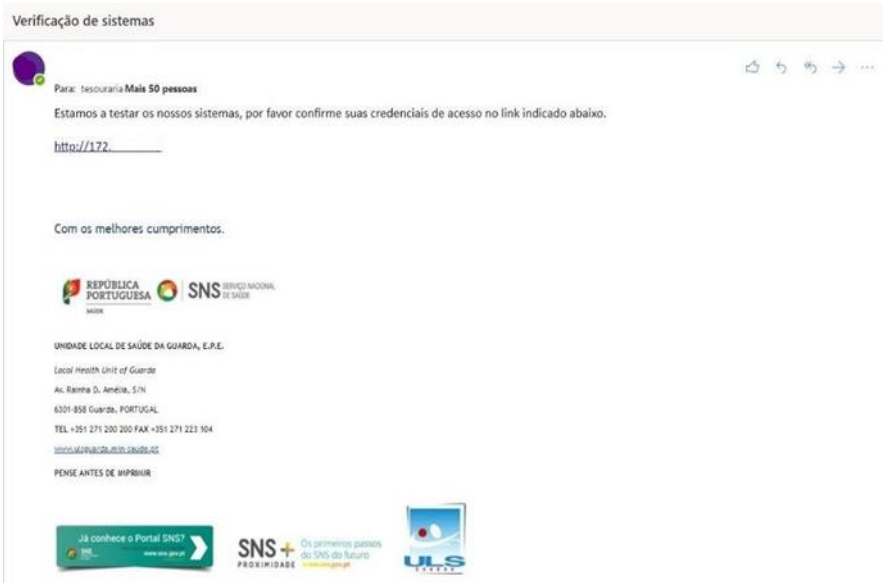


Figura 11

Capítulo 7

Conclusão

Com o estágio curricular pude aprofundar os conhecimentos adquiridos na componente, ter experiências em contexto de trabalho profissional e, ao mesmo tempo, desenvolver novas capacidades.

Acrescento que ainda aprendi muito e evolui na área de cibersegurança, em que consegui adquirir conhecimentos adicionais, nomeadamente sobre deteção de vulnerabilidades.

Todos os conhecimentos teóricos que adquiri nas diversas unidades curriculares do plano de´ estudo do Curso de Cibersegurança foram fundamentais para a realização, com sucesso, do ataque didático e da realização dos portfolios.

O projeto individual, alem de ter contribuído para a minha evolução profissional e pessoal, também ir a contribuir para projetos futuros da instituição. Foi graças a ajuda dos meu colegas de trabalho, e do meu supervisor, que consegui concluir os projetos a tempo.

O aspeto mais positivo deste estágio foi o facto de ter tido a oportunidade de trabalhar numa instituição tao importante para a saúde publica como também valorizada como deve ser nestes tempos pandémicos.

Com o ataque conseguimos perceber que bastantes utilizadores não sabem que as suas credenciais podem ser roubadas com apenas um ou dois cliques, derivado a taxa de sucesso que o ataque didático teve. O ataque realizado teve unicamente a intenção de fazer os utilizadores reverem as suas práticas no uso da rede numa página web fornecida depois da realização do ataque.

Concluído o estágio curricular, atingi os objetivos pretendidos e definidos no plano de estágio.