IPG Politécnico da Guarda
Escola Superior de Tecnologia e Gestão

RELATÓRIO DE ESTÁGIO

Curso Técnico Superior Profissional
em Cibersegurança

Rui Pedro Lameira Condesso

outubro | 2020

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Relatório de Estágio

Rui Pedro Lameira Condesso

Relatório Para Obtenção do Grau Técnico Superior Profissional Em Cibersegurança

Data 28/10/2020

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Relatório De Estágio

Rui Pedro Lameira Condesso

Relatório Para a Obtenção do Grau Técnico Superior Profissional Em Cibersegurança

Orientador: Engenheiro Pedro Pinto - Administrador de sistema no IPG

Orientador Engenheiro Ricardo Santos - Diretor do Serviço de Sistemas e Tecnologias da Informação e Comunicações ULS

Supervisor: Engenheiro Ricardo Santos - Diretor do Serviço de Sistemas e Tecnologias da Informação e Comunicações ULS

Data 28/10/2020

Ficha de Identificação

Aluno:

Nome: Rui Pedro Lameira Condesso

Número: 171429

Curso: TeSP de Cibersegurança

Contacto: ruicondesso98@gmail.com

Estabelecimento de ensino:

Instituição: Instituto 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

Empresa Acolhedora:

Empresa: ULS-Guarda

Localidade: Guarda

Morada: Av. Rainha Dona Amélia 19, 6300-035 Guarda

Contacto: 271 200 200 ; **E-mail:** secretariado.ca@ulsguarda.min-saude.pt

Orientador:

Pedro Pinto - Administrador de sistema no IPG

Supervisor

Ricardo Santos - Diretor do Serviço de Sistemas e Tecnologias da Informação e Comunicações ULS

Duração do Estágio Curricular:

750 Horas

Período de Estágio Curricular:

26 de fevereiro 10 de julho

Agradecimentos

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

Em primeiro lugar, quero agradecer à minha família e aos meus amigos, que sempre me motivaram, apoiaram e me transmitiram forças para me focar no trabalho e no meu no futuro, e nunca me deixaram desistir quando aparecia um obstáculo no caminho.

Agradeço ao Instituto Politécnico da Guarda e aos seus professores pelo que me transmitiram durante todo o curso, em especial, ao meu orientador de estágio, professor Pedro Pinto, 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 último 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.

Plano de Estágio

O meu estágio começou pela apresentação da equipa constituída no departamento de informática da 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, elaborado pelo Eng. Ricardo Santos, tendo em consideração as necessidades da instituição realizou o meu plano de estágio em que consistiram os seguintes pontos fundamentais:

- Desenvolvimento de páginas em HTM.
- Criação e manutenção de VM (Virtual Machine) para realização de testes e execução de um ataque didático aos utilizadores da instituição;
- Apoio técnico aos utilizadores da instituição da ULS Guarda em caso de alguma avaria;
- Manutenção de Hardware.

Resumo

No âmbito de finalizar o Curso Técnico Superior (TESP) em Cibersegurança (TC), do 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 dia 26 de fevereiro de 2020 e terminou dia 10 de julho de 2020, e teve lugar na ULS-Guarda.
Durante o tempo decorrido na ULS-Guarda, tive a oportunidade de colocar em prática a matéria adquirida nas aulas e expor as minhas ideias. Todos os conhecimentos adquiridos durante o TeSP e durante o projeto que desenvolvi durante o estágio, serviram para alargar o meu conhecimento nas áreas da Cibersegurança.

Uma das tarefas que realizei, na ULS-Guarda foi desenvolver de um ataque didático com o fim alertar os colaboradores, para as fragilidades da internet, e para informar de algumas normas de segurança. A empresa contou também com a minha colaboração na execução de vários documentos sobre Políticas de Segurança da Informação

Em suma o estágio contribui para que os conhecimentos adquiridos durantes dois anos fossem colocados a prova, num contexto de vida real, conseguindo também evoluir muitos deles.

Acrónimos

TeSP	Curso Técnico Superior Profissional
IPG	Instituto Politécnico da Guarda
HTML	HyperText Markup Language
ULS	Unidade Local de Saúde
VM	Virtual Machine
COVID-19	Coronavírus Disease 2019
DGS	Direção Geral de Saúde
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
FTP	File Transfer Protocol
API	Interface de Programação de Aplicações

Índice

Índice de Figuras

Capítulo 1

Introdução

A origem da Internet trouxe vários benefícios para a Humanidade, mas ao mesmo tempo trouxe muitas "desvantagens", como a criação de novos crimes, ou a evolução dos crimes tradicionais com o uso da internet.

Depois do surgimento desses crimes vieram as preocupações com a segurança das redes informáticas, proveniente do grande número de utilizadores e da sua falta de segurança.

Com o rápido crescimento e dependência das Tecnologias de Informação e Comunicação, no quotidiano, dos diversos sectores económicos e governamentais, qualquer pessoa proporciona um ataque informático a estas entidades que, por consequência, colocam em causa a segurança de uma nação. Visto isso todas as empresas tiveram de delinear medidas e estratégias de segurança.

Sendo elas

- Criptografar informação sensível;
- Fazer backup regulares;
- Seguir boas práticas no que diz respeito à criação e gestão de passwords, as passwords devem deter letras maiúsculas, minúsculas, caracteres especiais e números;
- Não fornecer dados pessoais em qualquer situação;
- Não abrir correio eletrónico cujo a origem é desconhecida.

1.1 Contexto e Motivação

O presente relatório, corresponde ao estágio curricular ocorrido no 2º semestre, do 2º ano do Curso Técnico Superior Profissional em Cibersegurança no Instituto Politécnico da Guarda. Curso Técnico Superior Profissional (TeSP): formação de ensino superior politécnica, que confere uma qualificação de nível 5 do Quadro Nacional de qualificações nos anos letivos 2018/2019 e 2019/2020.

Trata-se de uma formação académica em contexto de trabalho, que se realizou entre os dias 26 de fevereiro de 2020 a 10 de julho de 2020, e que a sua cotação total é de 30ECTS. Com lugar na ULS - Unidade de Saúde Local da Guarda.

1.2 Objetivos

Com a realização deste estágio pretende-se aplicar diariamente os meus saberes, adquiridos durante todo o curso, bem como fortalecer, e adquirir novos conhecimentos. Esta experiência não só contrui para o meu crescimento como para o meu futuro profissional, mas também me ajudou a superar receios e inseguranças, tornando-me mais confiante e preparado para o futuro. O estágio curricular foi acompanhado, ao longo de cinco meses por um supervisor e orientador da empresa, e ainda, por um professor do Instituto Politécnico da Guarda.

Capítulo 2

Entidade de Acolhimento

Neste capítulo, irá ser apresentado um resumo, de forma breve, de modo a que o leitor saiba mais sobre a ULS - Unidade de Saúde Local da Guarda

2.1 ULS - Unidade de Saúde Local da Guarda

A Instituição onde o estágio foi realizado tem a denominação de Unidade Local de Saúde da Guarda, (ULS), sendo uma pessoa coletiva de direito público, de natureza empresarial dotada de autonomias administrativa, financeira e patrimonial, nos termos do Decreto-Lei nº 558/99, de 17 de dezembro.

A ULS da Guarda tem sede no Parque da Saúde da Guarda, Avenida Rainha D. Amélia 6300- 858 Guarda.

A ULS da Guarda tem por objeto principal a prestação de cuidados de saúde primários, diferenciados e continuados à população, designadamente aos beneficiários do Serviço Nacional de Saúde, aos beneficiários dos subsistemas de saúde, ou entidades externas que com ele contratualizem a prestação de cuidados de saúde e a todos os cidadãos na área de influência por ela abrangida.

Inserem-se ainda no seu objeto o desenvolvimento da investigação, formação, ensino e atividades de saúde pública, bem como o desenvolvimento dos meios necessários ao exercício das competências da autoridade de saúde, na área geográfica por ela abrangida.

Capítulo 3

Ataque Didático

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.

3.1 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,…

O ataque consistiu em, enviarmos um email 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 direcionou-os 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.

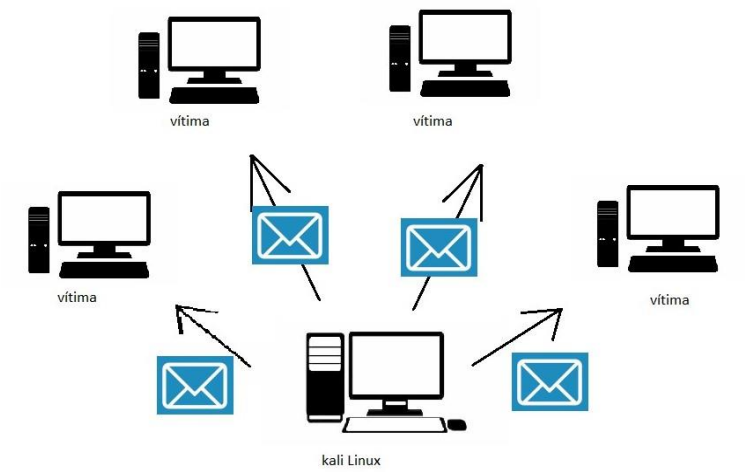

Figura 1- Esquema do ataque

3.2 Plataforma de testes

Os testes foram realizados na virtualbox é uma das plataformas gratuitas mais populares no campo da virtualização. Permitindo criar máquinas virtuais de uma forma muito simples. Com esta ferramenta é possível virtualizar sistemas como o Windows, Linux e até mesmo macOS.

Em termos de funcionalidades, destaque para a possibilidade de realizar snapshots, partilhar pastas entre o sistema virtual e o nativo.

3.3 Resultados

Logo após o envio dos primeiros emails, 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 guardar 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

Capítulo 4

Tecnologias Utilizadas

Neste capítulo são descritas as ferramentas e o software utilizados para concluir os objetivos do estágio

4.1 Servidor Apache

O servidor Apache é o servidor Web mais usado no mundo, flexibilidade, documentação e uma grande comunidade são alguns dos pontos fortes que tornaram o Apache diferente de seus concorrentes.

É um servidor de código aberto, compatível com os protocolos HTTP, HTTPS, FTP, entre outros, as suas funcionalidades são mantidas através de uma estrutura de módulos, permitindo os utilizadores escreverem os seus próprios módulos usando software de API.

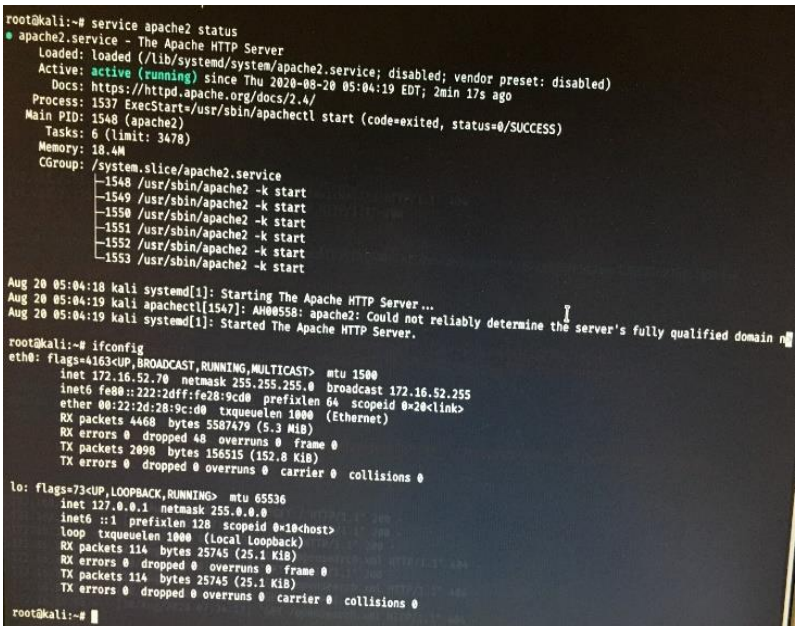

Figura 2-Servidor Apache

4.2 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.

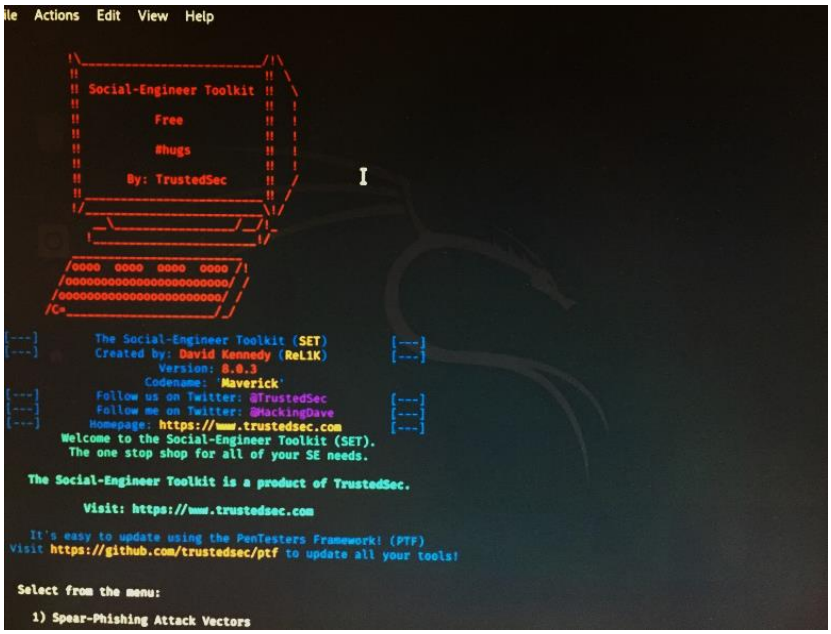

Figura 3-Demonstração da ferramenta Setollkit

Capítulo 5

Tarefas Semanais

Neste Capítulo, vão ser descritas as tarefas de cada semana, até ao término do estágio curricular.

1. Integração na instituição;
2. Deliberação e pesquisa sobre a melhor ferramenta para a realização do ataque;
3. Conceção e realização de testes numa VM;
4. Preparação do ataque dentro da rede ULS;
5. Inicio de estágio em regime teletrabalho;
6. Deliberação do trabalho que iria ser feito durante o teletrabalho;
7. Aprimoramento e realização dos últimos testes do ataque;
8. Coleta de normas e cuidados a ter na internet;
9. Realização de documentos sobre gestão de incidentes;
10. Realização de documentos sobre gestão de *backups*;
11. Realização de documentos sobre segurança de redes;
12. Realização de documentos sobre *disaster recovery planning*;
13. Escolha aleatórias de emails e realização do ataque didático;
14. Monitorizar o ataque e a taxa de sucesso
15. Realização do relatório de estágio;

5 .1 fevereiro

5.1 1º Semana - Integração na Empresa

Durante a primeira semana de fevereiro tive o prazer de conhecer o meu orientador de estágio e toda a equipa do Serviço de Sistemas e Tecnologias da Informação e Comunicações, foi me também apresentado a sala onde o meu estágio iria decorrer, o servidor, e todos os bastidores espalhados pela entidade acolhedora.

Durante esta primeira semana também realizei apoio técnico a alguns colaboradores, como mudança de monitores, substituição de cabos de Ethernet, …

5.2 março

5.2.1 2º Semana - Deliberação e pesquisa sobre a melhor ferramenta para a realização do ataque

Na segunda semana foi me apresentado um desafio, que consistia na realização de um ataque didático de *phishing* à instituição, para alertar os colaboradores para os riscos da Internet. O ataque consistia no envio de um email que chamasse a atenção dos colaboradores para clicarem no link que os levaria a uma pagina onde eles iriam inserir novamente as suas credencias, e assim iriam ser enviados para uma página, na qual iriam ser avisados que tinha sido alvo de um ataque didático e tinham de rever as normas de segurança

O clone da página foi feito através da ferramenta *setoolkit*, que é uma ferramenta pré-instalada no *kali Linux*, e a sua utilização era bastante intuitiva visto que já tinha trabalhado com ela durante o semestre letivo.

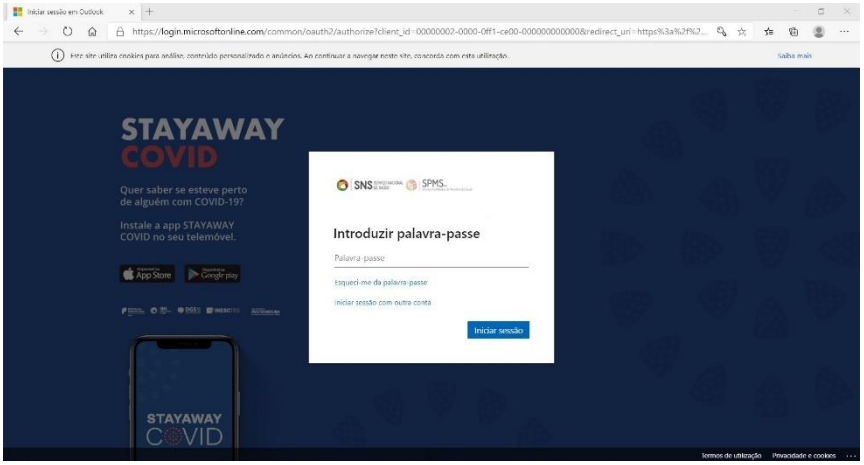

Figura 4-Página clonado

5.2.2 3º Semana - Conceção e realização de testes numa VM;

Depois de deliberar qual as ferramentas que iria para a realização do ataque, nesta semana comecei por fazer uma imagem do sistema operativo kali Linux na virtual box e realizei ataque o ataque numa rede externa a rede da ULS para ver se o ataque funcionava, ou se precisava de alguma detalhe mais.

5.2.3 4º Semana - Preparação do ataque dentro da rede ULS;

Para preparar o ataque dentro da rede ULS foi me dado uma máquina ligada a rede interna na qual instalei um sistema operativo kali Linux, e segui todos os passos que tinha feito na VM

5.2.4 5º Semana e 6 º Semana - Preparação do ataque dentro da rede ULS e Deliberação do trabalho que iria ser feito durante o teletrabalho;

A partir da 5º semana os estágios presenciais da ULS foram suspensos sob ordem da DGS devido ao Vírus COVID-19, visto que a entidade era um lugar de risco para os estagiários, pois iria ser um dos cinco hospitais nacionais referência de "segunda linha" para a contenção da infeção pelo COVID-19.

5.3 abril / maio

5.3.1 7º a 12º Semana – Realização de documentos e recolha de informação em teletrabalho

Assim que o teletrabalho começou, o meu estágio mudou completamente, passou de ser um estagio totalmente prático onde todos os dias lidávamos com problemas diferentes, deixando-me assim pronto para o mundo de trabalho, passando a ser um estagio onde tinha de recolher informação sobre vários tópicos e adaptar para o contexto da empresa para assim realizar vários portfolios, alguns dos temas eram:

- Gestão passwords;
- Gestão de alterações a programas;

- Audit logs;
- Gestão de incidentes;
- Gestão de backups;
- Segurança de redes;
- Disaster Recovery Planning.

A realização destes documentos foi sempre enquadrar com a instituição de forma a que fosse possível consultarem qualquer um destes documentos, mais tarde assim se necessário.

Para que isso fosse possível foi necessário falar com um docente completamente integrado e com experiência suficiente na instituição por isso fui falar com o eng. Luís Domingos para a realização dos mesmos.

5.4 junho/julho

5.4.1 13º a 14º semana Escolha aleatórias de emails e realização do ataque didático, Realização e monitorizar o ataque

Após o número de novos casos de COVID-19 diminuir e a DGS autorizar, os estágios voltaram ao normal, fazendo com que eu voltasse a estagiar na ULS e que conseguisse acabar o ataque didático.

O primeiro passo a ser feito foi apurar uma amostra aleatória de alguns mails do ULS, assim com os emails selecionados só faltava deliberar o assunto do email e o corpo da mensagem.

Depois dos emails enviados a máquina foi entregue aos serviços informáticos, pois os dados que se iriam obter seriam dados sensíveis.

Figura 5-Email enviado

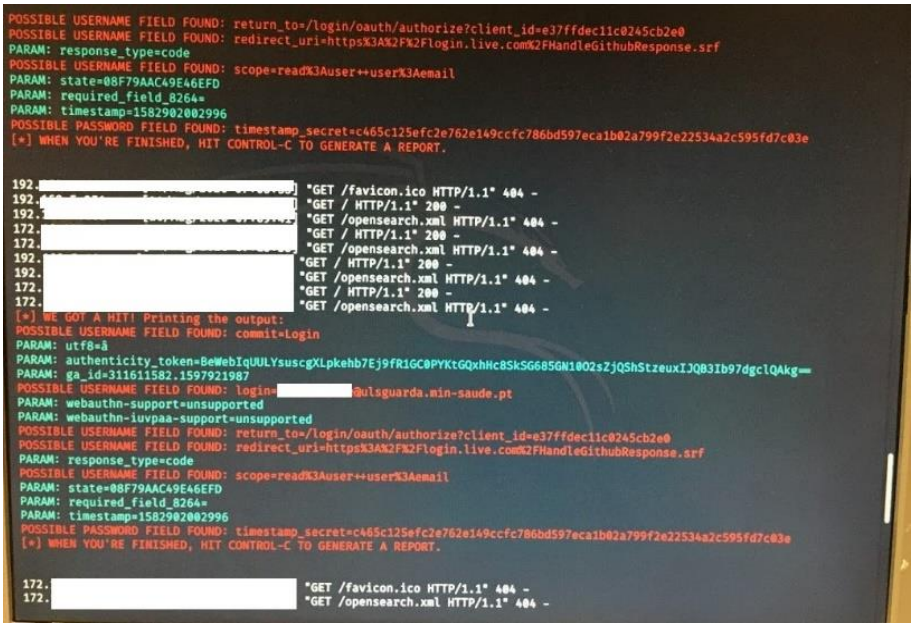

Figura 6-Ataque em curso

5.4.2 15º semana Realização do relatório de estágio;

Ao concluir, 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 6

Conclusão

Com o estágio curricular pude aprofundar o que já sabia da teoria, ter experiências em contexto de trabalho profissional e, ao mesmo tempo desenvolver novas capacidades nas áreas de segurança de redes, criação de páginas HTML. Pode também evoluir os meus conhecimentos nas áreas de:

- Gestão passwords;
- Gestão de incidentes;
- Gestão de backups;
- Segurança de redes;
- Disaster Recovery Planning.
- Gestão de passwords;

O que contribui para a minha evolução profissional e pessoal, mas também contribui para o futuro da empresa. Todos os conhecimentos teóricos que adquiri nas diversas unidades curriculares do plano de estudo do Curso de Cibersegurança foram fundamentais para a realização com susceção do meu estágio.

Bibliografia

ULS (10 julho de 2020). ULS About us. Obtido de Web Site da ULS: http://www.ulsguarda.min-saude.pt/

SNS (10 julho de 2020). SNS About us. Obtido de Web Site da SNS: https://www.sns.gov.pt/

IPG (10 julho de 2020). IPG About us. Obtido de Web Site da IPG: http://bdigital.ipg.pt/dspace/

Wikipédia (12 julho de 2020). Wikipédia About Neatbens us. Obtido de Web Site da Wikipédia: https://pt.wikipedia.org/wiki/NetBeans

Medium (12 julho de 2020). Medium About us. Obtido de Web Site da Medium: https://medium.com/search?q=setoolkit

Virtual box (12 julho de 2020). Virtual box About us. Obtido de Web Site da Virtual box: https://www.virtualbox.org/

Wikipédia (12 julho de 2020). Wikipédia Notepad About us. Obtido de Web Site da Wikipédia: https://fr.wikipedia.org/wiki/Notepad%2B%2B

Wikipédia (15 julho de 2020). Wikipédia Falha (tecnologia) About us. Obtido de Web Site da Wikipédia https://pt.wikipedia.org/wiki/Falha_(tecnologia)

Wikipédia (15 julho de 2020). Wikipédia Site About us. Obtido de Web Site da Wikipédia https://pt.wikipedia.org/wiki/S%C3%ADtio_eletr%C3%B3nico

Wikipédia (15 julho de 2020). Wikipédia Browser About us. Obtido de Web Site da Wikipédia https://pt.wikipedia.org/wiki/Navegador_web

Wikipédia (15 julho de 2020). Wikipédia Base de Dados About us. Obtido de Web Site da Wikipédia https://pt.wikipedia.org/wiki/Banco_de_dados

Wikipédia (20 julho de 2020). Wikipédia Apache About us. Obtido de Web Site https://pt.wikipedia.org/wiki/Servidor_Apache