IPG Politécnico da Guarda
Escola Superior de Tecnologia e Gestão

RELATÓRIO DE ESTÁGIO

Curso Técnico Superior Profissional
em Cibersegurança

Hugo Germano Azevedo Pinheiro

outubro | 2020

RELATÓRIO DE PROJETO

HUGO GERMANO AZEVEDO PINHEIRO

CURSO TÉCNICO SUPERIOR PROFISSIONAL DE CIBERSEGURANÇA

2018/2020

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Relatório De Projeto

Hugo Germano Azevedo Pinheiro

Relatório Para a Obtenção do Grau Técnico Superior Profissional Em Cibersegurança

Orientador: Engenheiro Pedro Pinto

2018/2020

Ficha de Identificação

Aluno: Hugo Germano Azevedo Pinheiro

Nº de matrícula: 1701915

Curso: Técnico Superior Profissional de Cibersegurança

Email: hugopinheiroslb@gmail.com

Estabelecimento de Ensino: Instituto Politecnico da Guarda

Escola: Escola Superior de Tecnologia e Gestão

Entidade promotora de Estágio: Gesp – Gabinete de Estágios e Saídas Profissionais

Entidade Empregadora: Gefguarda - Serviços, Gestão, Informatica E Telecomunicações, Lda

Hórario de Trabalho: 09:00 às 12:00

14:00 às 18:00

Supervisor na Empresa:

Duração de Estágio: 80horas complementadas pelo Projeto

Inicio de Estágio:

Conclusão de Estágio:

Professor Orientador: Engenheiro Pedro Pinto/ Profº Fernando Melo

Agradecimentos

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

Começo por agradecer ao meu Diretor de Curso, Professor Fernando Melo Rodrigues, pela sua disponibilidade sempre demonstrada, contribuindo constantemente nas questoes e ideias do projeto e na realização do mesmo.

Queria tambem agradecer ao meu orientador de estágio, o Professor Pedro Pinto, por todo o apoio que me deu nesta etapa do curso.

Agradeço tambem a GEFGuarfa, Lda pela forma que me aceitaram no estágio e sempre estarem dispostos a ajudar, a explicar como fazer apesar de ter sido um trajeto curto.

Aproveito a oportunidade para agradecer a força transmitida pelos grandes amigos que criei ao longo do curso.

Por último, quero agradecer aos meus pais e minha irma por todos os sacrificios e viagens que tiveram de fazer e por acreditarem nas minhas capacidades.

Glossário

IPG	Instituto Politecnico da Guarda
TeSP	Curso Tecnico Superior Profissional
CPU	Central Process Unit
TI	Tecnico de Informatica
AUR	Arch user Repository
CLI	Command Line Interface
GUI	Graphical user Interface
IP	Internet protocol
SET	Social Engineering Toolkit
JTR	John the Ripper
Wi-Fi	Wireless

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 Projeto Final.

Inicialmente tive um estágio curricular que constituiu um dos primeiros contactos 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 estágio e onde iria ser o nosso local de trabalho, contudo devido á pandemia a empresa cancelou nosso estágio pois era um local pequeno e estavamos com muito contacto com o publico e como nao havia garantias de segurança, tivemos o estágio cancelado. A solução que nos foi apresentada foi o desenvolvimento de um projeto sobre uma area do nosso curso. O tema que me calhou foi o Kali Linux, que é a ferramenta mais poderosa e completa no ambito da cibersegurança.

Palavras-Chave

Cibersegurança; Kali Linux; Pandemia; Estágio; Hacker

Índice

Indice de Figuras

Introdução

Segurança de rede, cada vez é mais importante pois a vida das pessoas corre na internet. Nada é seguro, nos é que temos de tomar todas as medidas de prevenção e segurança.

Na area de cibersegurança, quase tudo funciona a volta de uma ferramenta. A essa ferramenta da-se o nome de Kali Linux. Kali linux é uma ferramenta perigosa e poderosa. Depende de cada utilizador se usa essa ferramenta Perigosa para o Bem ou para o Mal. Para o mal chamamos de hacker, e para o bem Cybersecurity.

Neste projeto irei falar dessa magnifica distribuição e irei explicar as melhores ferramentas e o que cada uma faz.

Figura 1 - CYBERSECURITY

Capítulo 1 – Caracterização da Cidade; Instituição; Estágio;

1.1. Caracterização da Cidade

Figura 2- Cidade da Guarda

A Guarda é uma cidade portuguesa, com 1056 metros de altitude máxima, o que torna a cidade mais alta de Portugal. Com 26565 habitantes no seu perímetro urbano, capital do distrito da Guarda, situada na região estatística do Centro e sub-região das Beiras e Serra da Estrela. É Sede de um município com 712,1 km² de área e 42 541 habitantes (censos de 2011), subdividido desde a reorganização administrativa de 2012/2013 em 43 freguesias.

Toda a região é marcada pelo granito, pelo clima contrastado de montanha e pelo seu ar puro e frio que permite a cura e manufatura de fumeiro e queijaria de altíssima qualidade. É também a partir desta região que vertem as linhas de água subsidiarias das maiores bacias hidrográficas que abastecem as três maiores cidades de Portugal.

1.1.1. A cidade dos 5 F´s

A explicação mais conhecida e consensual do significado do epíteto de «cidade dos 5 F's» diz que estes significam **F**orte, **F**arta, **F**ria, **F**iel e **F**ormosa. A explicação destes *efes* tão adaptados posteriormente a outras cidades é simples:

1. **Forte**: a torre do castelo, as muralhas e a posição geográfica demonstram a sua força;
2. **Farta**: devido à riqueza do vale do Mondego;
3. **Fria**: a proximidade à Serra da Estrela e o facto de estar situada a uma grande altitude explicam este F;
4. **Fiel**: porque Álvaro Gil Cabral – Alcaide-Mor do Castelo da Guarda e trisavô de Pedro Álvares Cabral – recusou entregar as chaves da cidade ao Rei de Castela durante a crise de 1383-85. Teve ainda fôlego para combater na batalha de Aljubarrota e tomar assento nas Cortes de 1385 onde elegeu o Mestre de Avis (D. João I) como Rei;
5. **Formosa**: pela sua natural beleza.

1.2. Caracterização da Instituição

O **Instituto Politécnico da Guarda** é uma instituição de ensino superior politécnico pública portugesa, com sede na cidade da Guarda, onde se localizam quatro das suas cinco escolas, e uma escola na cidade de Seia.

O Instituto é constituído pelas seguintes escolas:

- Escola Superior de Educação, Comunicação e Desporto da Guarda
- Escola Superior de Saúde da Guarda
- Escola Superior de Tecnologia e Gestão da Guarda
- Escola Superior de Turismo e Hotelaria
- Escola de Enfermagem da Guarda

Figura 3- Instituto Politécnico da Guarda

1.2.1. História

O projecto de implementar o ensino superior na Guarda, remonta à década de 70. Contudo só em 1979 foi criada a primeira escola politécnica, a Escola Superior de Educação, posteriormente integrada no Instituto Politécnico.

Criado em 1980, pelo Decreto-Lei n.º 303/80, de 16 de Agosto, o IPG caracteriza-se por ser uma "pessoa colectiva de direito público, dotada de autonomia estatutária, pedagógica, científica, cultural, administrativa, financeira, patrimonial e disciplinar" (art. 3.º dos estatutos do IPG). O IPG foi um dos primeiros estabelecimentos de ensino superior a ver aprovados os seus estatutos, homologados pelo despacho normativo n.º 765/94, publicados em Diário da República (DR n.º 273, I Série-B) de 25 de Novembro.

1.2.2. Simbologia

As iniciais IPG aparecem na parte superior e na torre inferior. Apoiando todo o símbolo, está inserida a frase «Scientia lucet omnibus», o que traduz que a ciência ilumina o homem, acção que neste caso concreto é viabilizada através do IPG. Como figura central. o símbolo do IPG integra uma águia, simbolizando as alturas - a Guarda é a cidade de Portugal erguida na altitude mais elevada — e a sabedoria, destacando-se ainda na parte central uma porta da Sé Catedral da Guarda, monumento que constitui o principal ex-líbris da cidade, reflectindo igualmente as tradições históricas, culturais e de ensino desta zona do Pais.

Figura 4- Simbolo

1.3. Estágio

1.3.1. Empresa

A entidade de acolhimento do meu estágio é a GEF Guarda, LDA, que é uma empresa sediada na Guarda e está no mercado desde 1991. È uma empresa prestadora de serviços e fornecedora de soluções globais na área dos sistemas de informação. Os principais serviços é o software PHC.

Figura 5- GEF GUARDA

1.3.2. Tarefas Desenvolvidas no Estágio

No decorrer do estágio ocorreu uma pandemia, COVID19, o que nos obrigou a cessar o estágio para não nos colocarmos-nos em risco, porem ao longo das duas semanas efetuadas consegui aprender conhecimentos da minha area.

As tarefas ao longo das duas semanas eram sempre similares, pois a nossa principal tarefa que realizavamos era reparação de computadores, no entanto faziamos muitas outras coisas. Na reparação de computadores, acontecia quando um cliente chegava com um problema no computador e nos tinhamos de reparar. A grande parte dos casos era sobreaquecimento do computador e era uma reparação rapida pois era desmontar o computador, fazer umas limpezas no interior, em alguns casos colocavamos pasta termica, e depois era só realizar uns breves testes para testar o computador.

As outras tarefas que realizavamos foi a atualização do site e das diversas redes sociais pois era algo que estava bastante desatualizado e é sempre bom estar atualizado de forma a cativar mais clientes, o que hoje em dia as redes sociais sao um fator muito importante.

Uma das tarefas que mais gostei foi a criação de um servidor próprio para uma empresa, dado que aqui já envolvia a minha área. Utilizamos uma QNAP NAS que é um sistema de armazenamento com varios discos rigidos e tem um sistema operacional proprio. Depois incluimos uma Sophos que era para fazer a segurança do servidor, e foi essa parte que mais gostei, pois envolveu redes e cibersegurança.

Capítulo 2 - Enquadramento teórico

2.1. Cibersegurança

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra-ataques maliciosos. O termo tem uma grande variedade de contextos, e por isso pode ser dividido em algumas categorias comuns:

- *Segurança de rede* é a prática de proteger uma rede de computadores contra intrusos, sejam eles invasores direcionados ou malware oportunista.
- *Segurança de programas* foca em manter o software e os dispositivos livres de ameaças. Um programa comprometido pode fornecer acesso aos dados que pretende proteger. O sucesso da segurança começa na fase de projeto, bem antes de um programa ou dispositivo ser implantado.
- *Segurança de informações* protege a integridade e a privacidade dos dados, tanto no armazenamento como em trânsito.
- *Segurança operacional* inclui os processos e decisões para tratamento e proteção dos arquivos com dados. As permissões que os usuários têm ao acessar uma rede e os procedimentos que determinam como e onde os dados podem ser armazenados ou compartilhados se enquadram nesta categoria.
- *Recuperação de desastres e continuidade dos negócios* definem como uma organização responde a um incidente de cibersegurança ou qualquer outro evento que cause a perda de operações ou dados. As políticas de recuperação de desastres ditam como a organização restaura suas operações e informações para retornar à mesma capacidade operacional de antes do evento. A continuidade dos negócios é o plano ao qual a organização recorre ao tentar operar sem determinados recursos.
- *Educação do usuário final* aborda o fator de cibersegurança mais imprevisível: as pessoas. Qualquer pessoa pode introduzir acidentalmente um vírus em um sistema seguro se deixar de seguir as práticas recomendadas de segurança. Ensinar os usuários a excluir anexos suspeitos de e-mail, não conectar unidades USB não identificadas e várias outras lições importantes é vital para a segurança de qualquer organização.

2.2. Objetivo e atividades principais do curso Cibersegurança

2.2.1.Objetivo

O objetivo do curso de Cibersegurança é implementar, analisar e gerir redes de comunicação e equipamentos, e planear, projetar e desenvolver software, salvaguardando os requisitos de segurança e de acordo com as necessidades das organizações

2.2.2 As Atividades Principais

As atividades principais so curso são:

- Planear, instalar e configurar sistemas e equipamentos informáticos, e redes estruturadas
- Gerir redes de comunicação, sistemas, serviços e servidores, de forma segura, eficiente e fiável, com o objetivo de otimizar o funcionamento dos mesmos
- Projetar ambientes de trabalho seguro para redes empresariais, nomeadamente, através da definição e aplicação de políticas de segurança, estratégias coerentes de cópia de segurança de dados, confidencialidade, integridade e disponibilidade
- Desenvolver aplicações informáticas seguindo um processo de desenvolvimento de software e as boas práticas e tendo em conta os vários atributos de segurança
- Planear e projetar sistemas de bases de dados de acordo com os requisitos
- Testar e validar a segurança de sistemas e aplicações informáticas
- Testar diversas técnicas de análise de segurança, de modo a assegurar a identificação e mitigação das ameaças à cibersegurança

Capítulo 3 – Projeto

3.1. Kali Linux

Figura 6 - Kali Linux

Entre as diversas distribuições Linux existentes no mundo, o Kali Linux é uma das mais avançadas. Ele foi desenvolvido para fins específicos, como testes de intrusão e auditoria de segurança, e conta com uma gama de ferramentas para hackers (éticos).

Esta é uma distribuição Linux out-of-box, baseada em Debian, que possui um conjunto de ferramentas ideais para realizar auditorias de segurança, computação forense, testes aos níveis de segurança, testes de penetração, hacking, entre outros.

A distribuição, antes conhecida como BackTrack, foi criada, desenvolvida e lançada pela equipe do Offensive Security em 2006, tendo rapidamente se popularizado entre os profissionais de segurança em TI. Além da mudança de nome, outras alterações foram feitas no sistema.

Um grande diferencial do Kali Linux é o seu repertório de ferramentas nativas para executar testes diversos — são mais de 300. Isso sem contar que o sistema é gratuito, estável, confiável e pode ser complementado por uma vasta quantidade de aplicações desenvolvidas por terceiros.

Figura 7 - Kali Linux: Ambiente trabalho

3.2.Distribuições Alternativas ao Kali Linux

3.2.1. BackBox Linux

Figura 8- BackBox Linux

O Backbox Linux é uma distribuição baseada no Ubuntu. Utiliza por padrão o ambiente gráfico Xfce bem amigável, o que é ótimo para quem está começando no mundo Linux. Pode ser uma alternativa para aqueles que são familiarizados com o Ubuntu, já que a forma de instalação é bem-parecida. Também possui ferramentas além da parte de cibersegurança, como ferramentas de escritório (LibreOffice) e cliente de e-mail (Thunderbird).

3.2.2. BlackArch Linux

O BlackArch é uma distribuição baseada em Arch Linux, portanto é compatível com o AUR e PKGUILDs. O seu ponto forte é a sua rapidez. Em questão de segundos é possível ter uma ótima distribuição pronta para uso com diversas ferramentas de análise de segurança. Utiliza por padrão o ambiente gráfico Fluxbox. É interessante destacar que as ferramentas estão agrupadas por áreas de interesse.

3.2.3. Parrot Security OS

O Parrot Security OS é uma distribuição baseada em Debian. Possui uma interface um pouco mais amigável, utilizando o ambiente gráfico Mate. Pode ser uma boa alternativa para quem está começando na área de cibersegurança. Além disso, o Parrot Security OS se destaca por ter ferramentas de programação e desenvolvimento Web na sua instalação padrão.

Figura 9- Parrot Security OS

3.2.4. Fedora Security Lab

A distribuição Fedora possui algumas "variantes" chamadas de Fedora Labs. O Fedora Labs cria imagens do próprio Fedora com várias ferramentas agregadas ao perfil desejado. Um desses perfis é o Security Labs: Uma distribuição Fedora com várias ferramentas instaladas voltadas para cibersegurança, como por exemplo aplicativos de testes de penetração, testes de força bruta e análise de tráfego de rede. Utiliza por padrão o ambiente gráfico Xfce.

Independente das ferramentas presentes no Fedora Security Lab, acredito que se pode considerar uma alternativa ao Kali Linux devido a questão do modelo de pacotes que cada distribuição utiliza. O Kali Linux é baseado no Debian, portanto utiliza pacotes tipo deb, já o Fedora Security Lab é baseado no Fedora, que utiliza pacotes tipo rpm.

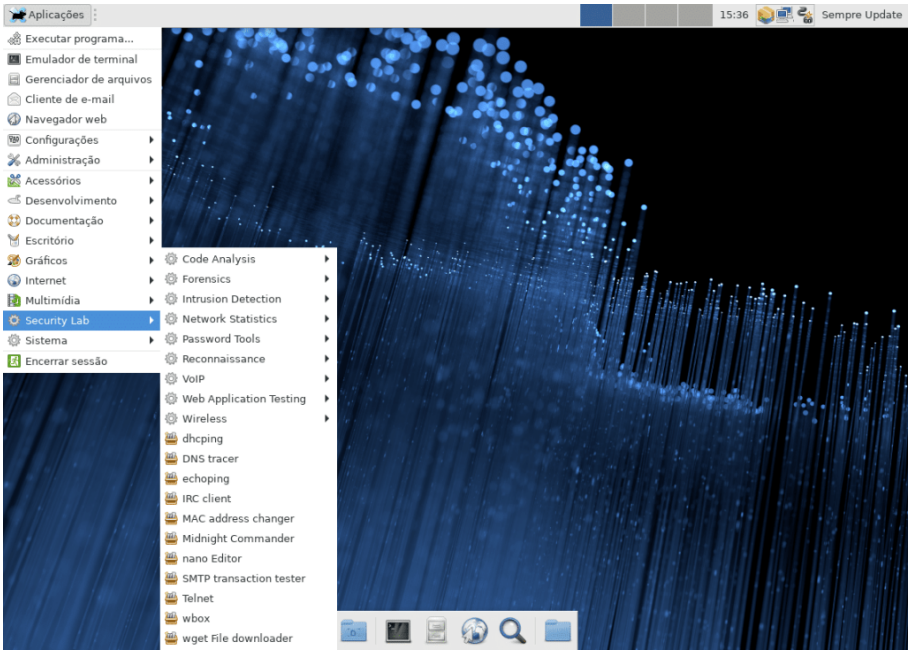

Figura 10 - fedora Security Lab

3.2.5. Pentoo

O Pentoo Linux é uma distribuição baseada no gentoo Linux, portanto é compatível com o Portage (gerenciador de pacotes padrão do Gentoo Linux) e pacotes ebuild. Utiliza por padrão o ambiente gráfico Xfce. É interessante destacar que ele mantém as características do CLI ao invés do GUI. Em outras palavras, o sistema inicializa primeiramente na linha de comando e a interface gráfica precisa ser inicializada manualmente.

Figura 11 - Pentoo

3.3. Kali Linux ao Pormenor

3.3.1. Organização do Kali Linux

O kali linux está organizado conforme o tipo de cada aplicação, de forma a melhorar a experiência do utilizador. No total existem 13 grupos de aplicações, onde algumas aplicações se podem repetir em diferentes grupos, pois as vezes as aplicações tem diversas utilidades. Alem dos 13 grupos de aplicações, ainda tem o Firefox ESR, um gestor de ficheiros, um terminal, um editor de texto, entre outras aplicações de utilizade do dia a dia. Na imagem 11, podemos ver os diversos grupos existentes.

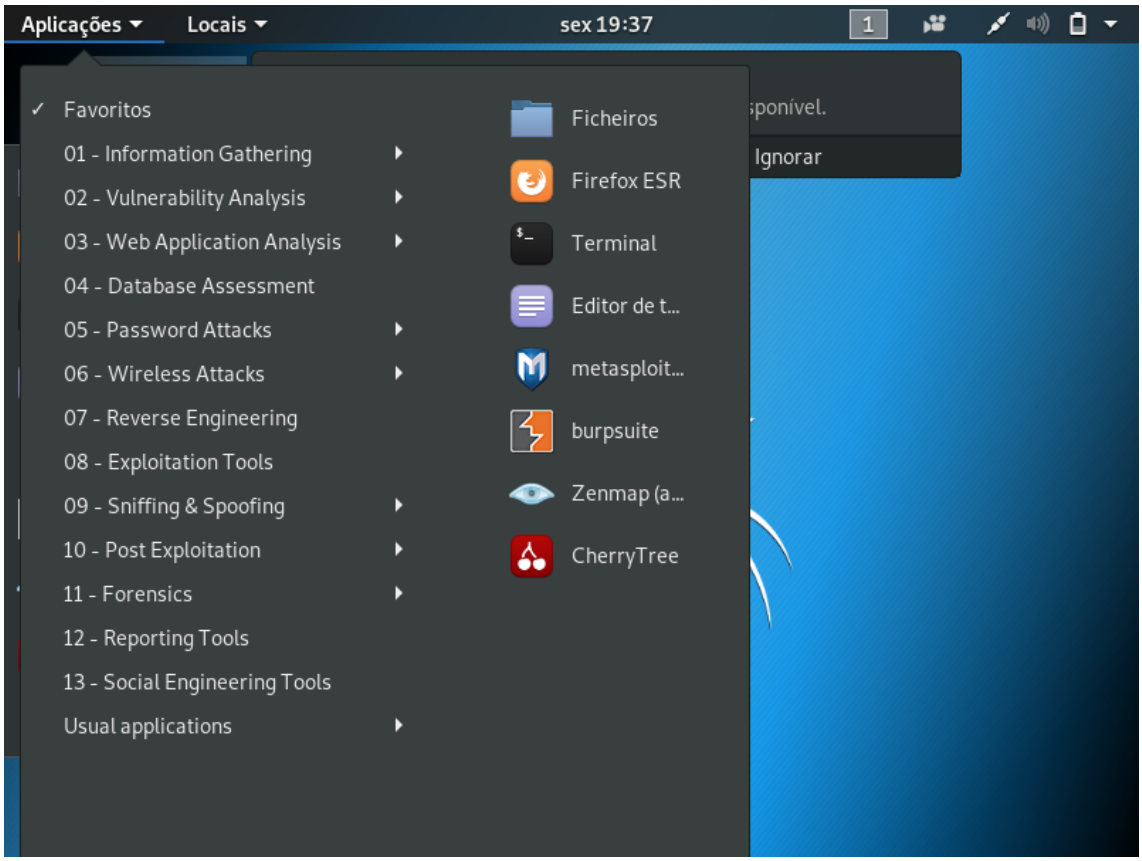

Figura 12 - Ferramentas Kali Linux

3.4. Ferramentas do Kali Linux

Neste tópico irei falar das melhores e talvez as mais conhecidas aplicações do Kali Linux. Irei explicar com algum detalhe o que cada aplicação faz e que outra aplicação parecida existe.

3.4.1. NMAP

Figura 13- NMAP

Sem dúvida alguma, o Nmap é uma das principais ferramentas do Kali Linux pois é a uma das ferramentas mais utilizadas pelos profissionais da area de cibersegurança e é usada normalmente para detecção de redes, analises e auditorias de segurança. Em resumo o nmap é considerado essencial para levantar detalhes de informação especifica de qualquer máquina, como por exemplo:

- Descobrir endereços IP numa Rede
- Saber quais portos TCP abertos de uma máquina
- Saber se um porto específico está aberto
- Saber o sistema operativo de uma determinada máquina
- Inventário de todas as máquinas de uma determinada rede

O nmap está inserido nos grupos Information Gathering e no Vulnerability Analysis

A ferramenta mais parecida ao NMAP é o ZenMap que é uma interface grafica do cliente para o Nmap Security Scanner, o que facilita o uso do Nmap para os iniciantes.

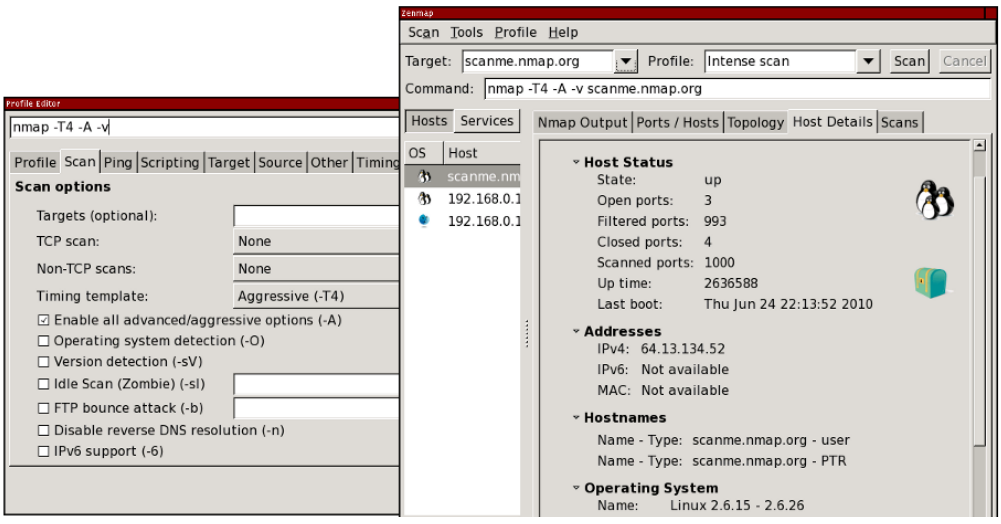

Figura 14- ZenMap Interface

3.4.2. Social Engineering Toolkit

Social Engineering, mais conhecida por Engenharia Social, mas também conhecido como SET, foi desenvolvido para auxiliar em testes de penetração contra elementos humanos, levando em consideração que as pessoas costumam ser o elo mais frágil na invasão. Eles são normalmente muito letais em seus ataques, obtendo quase 100% de sucesso com suas vítimas, onde a maioria não percebe a ação.

Nesta ferramenta tenho varis tipos de aplicações tais como:

- Ataques de engenharia Social, onde se pode fazer diversos ataques desde QRCode Acess Point a ataques de website
- Testes de penetração, onde contém ataques de SQL bruter até a Exploits personalizados

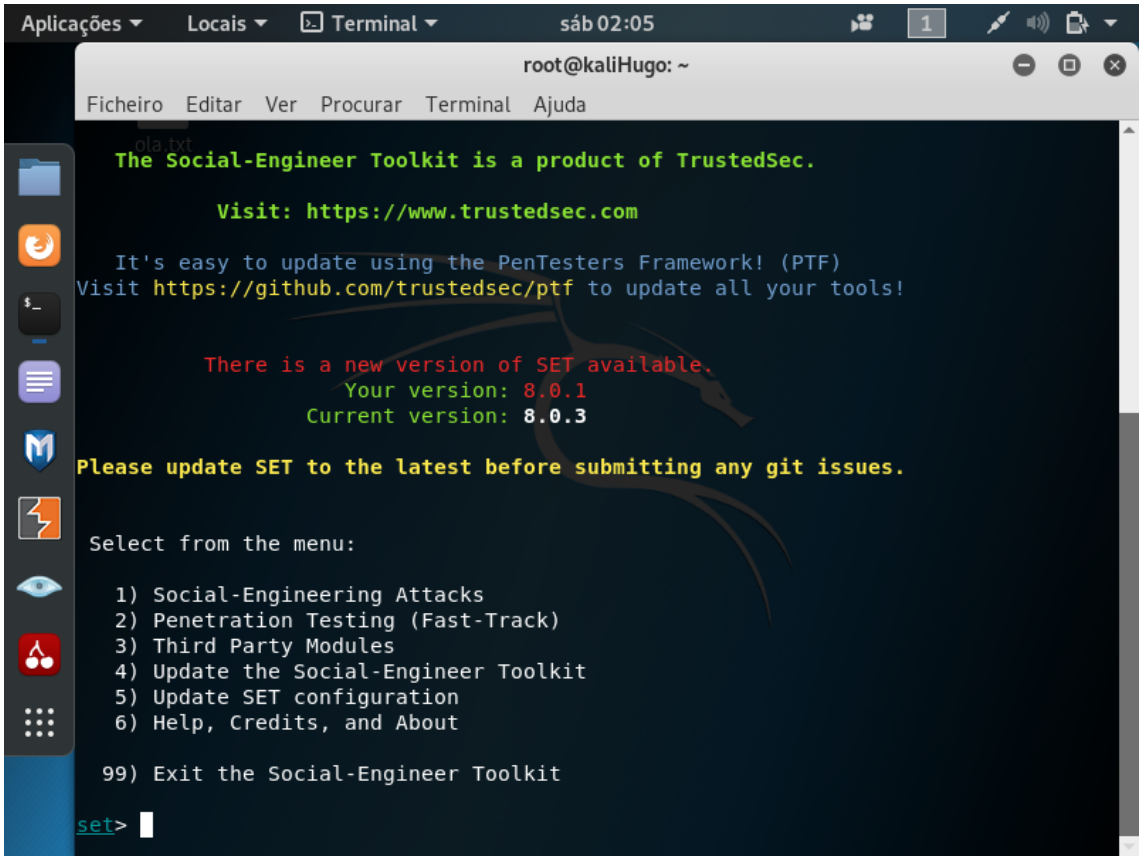

Figura 15 - SET - Index

3.4.3. WIRESHARK

Figura 16 - WireShark Logo

A ferramenta que agora vamos falar é o sniffer mais popular para redes informáticas, o Wireshark. O Wireshark é uma ferramenta de analise protocolar, que permite a captação, em tempo real, de pacotes de dados, e apresenta essa informação num formato legível para os utilizadores. O processo de captura de tráfego é realizado via placa de rede, funcionando esta num modo especial que é designado de modo promíscuo (possibilidade de capturar todos os pacotes, independentemente do endereço de destino).

Muitas pessoas não sabem, mas um sniffer é uma poderosa ferramenta de trabalho, porem para outros é aquela ferramenta capaz de capturar umas *passwords* na rede, alguns dados confidenciais.

Uma das vantagens do Wireshark é que permite analisar os pacotes recebidos e transmitidos por qualquer interface de rede, sendo possível aplicar vários tipos filtros.

Wireshark está inserido no grupo dos Sniffing & Spoofing, juntamente com outros Sniffers como por exemplo “Responder” ou “netsniff-ng” ou Traceroute.

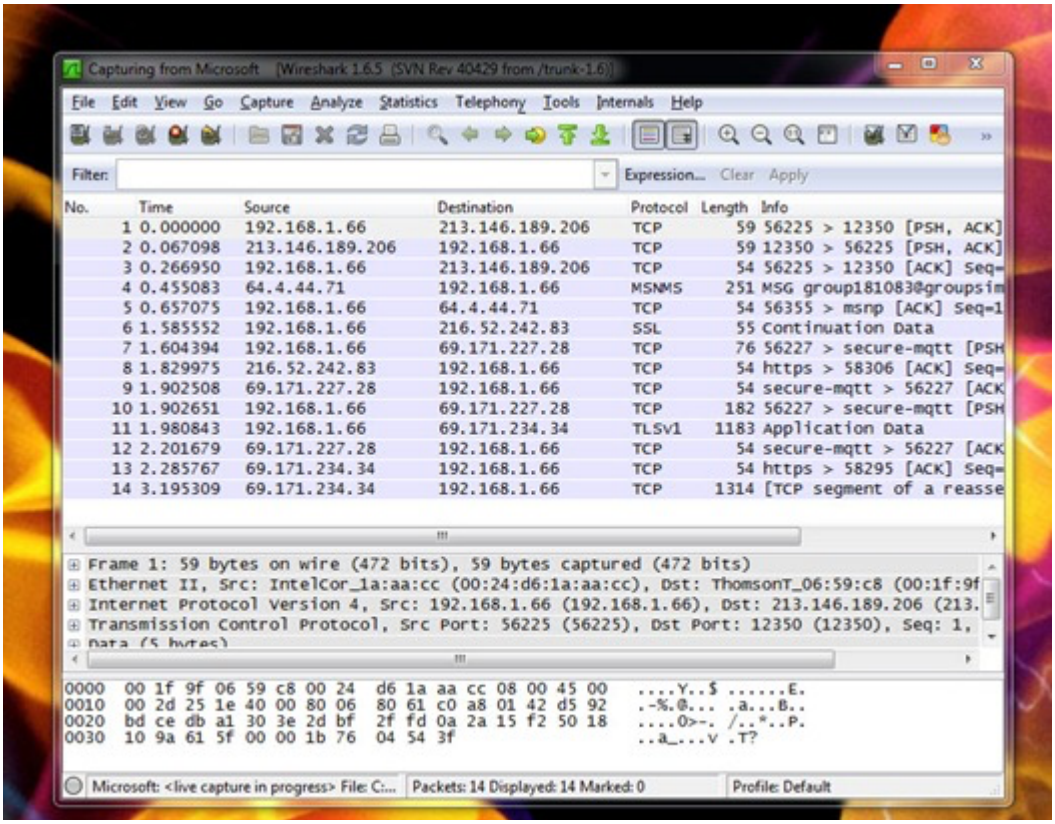

Figura 17 - WireShark - Index

3.4.4. THC Hydra e JOHN THE RIPPER

O THC Hydra é uma ferramenta gratuita e online, ou seja, trabalha em cima de ataques como password guessing, que consistem na captura de senhas a partir de tentativas de login, que executa rapidamente a quebra de senhas por meio de dicionário (lista de passwords) ou força bruta (brute force) para testar várias combinações de senha / login.

Figura 18 - THC Hydra - Logo

Um destaque do THC Hydra é o suporte a mais de 50 protocolos, como HTTP, FTP, Mail, SSH, Banco de Dados etc.

JOHN THE RIPPER, seja pelo nome criativo (até mesmo premiado) ou pelas suas funcionalidades, o JTR é uma das mais conhecidas ferramentas de password cracking (processo de recuperação ou violação de senhas, no ponto de vista da criptoanálise) e tem versões free e pro.

Figura 19 - John The Ripper - Logo

Assim como o THC Hydra, o JTR utiliza ataques de força bruta e dicionários, fazendo uma varredura pelos dados contidos no computador. Porém, a diferença é que o John atua contra os ataques offline.

As duas ferramentas está incluidas apenas no grupo de Password Attacks, juntamente com outras aplicaçoes menos conhecidas como por exemplo o Medusa, o HashCat, pois são todas muito parecidas pois usam a força bruta para conseguir. Umas tem as suas WordLists as outras precisam de ir buscar na net as WordLists.

3.4.5. APKTOOL e AIRCRACK-NG

Com a ferramenta APKTOOL, podemos trabalhar com engenharia reversa decodificando recursos em suas formas quase originais e reconstruindo-as aplicando algumas modificações. Tudo isso fazendo o debug de códigos smali.

As funcionalidades do Apktool como ferramenta para hackers éticos são um excelente meio de acrescentar novos recursos, funcionalidades e aprimoramentos de uma aplicação.

Figura 20 - APKTOOL

Contudo a ferramenta AIRCRACK-NG é totalmente diferente pois esta já opera apenas em redes Wi-Fi. O Aircrack-ng tem como especialidade a proteção e detecção de ameaças de redes Wi-Fi (Wireless), devido às ferramentas para WEP/WPA/WPA2 cracking configuração de falsos pontos de acesso, captura de pacotes, wireless password cracking, entre outros.

Figura 21 - AIRCRACK-NG

Uma ferramenta parecida ao AIRCRACK-NG é o Fern WIFI Cracker que é muito parecida só que esta ferramenta consegue realizar ataques de força bruta ou de dicionarios, de forma a descobrir a senha da Ethernet.

A ferramenta Apktool está no grupo “ Reverse Engineering” enquanto o AIRCRACk-ng e o Fern Wifi Cracker está no grupo “ Wireless Attacks”.

3.4.6. METASPLOIT

Metasploit é um projeto de segurança de informação que divulga informações relacionadas a vulnerabilidades e busca facilitar testes de penetração e o desenvolvimento de Sistema de detecção de intrusos. O metasploit ajuda as equipas de segurança a fazer mais do que apenas verificar vulnerabilidades, gerenciar avaliações de segurança e melhorar a segurança. Ele capacita e arma as equipas de segurança de forma a estarem sempre um passo a frente dos invasores.

Figura 21 - Metasploit

O metasploit conta com um conjunto de ferramentas para hackers e frameworks que podem ser utilizados para fins diversos: é exatamente isso o que propõe oMetaSploit, seguindo à risca a filosofia de segurança ofensiva inserida no Kali Linux.

Praticamente todas as ferramentas que o usuário precisa para explorar vulnerabilidades — inclusive as que envolvem o tráfego de rede — são encontradas nesse incrível framework que é o Metasploit.

O metasploit está inserido no grupo “Exploitation Tools”.

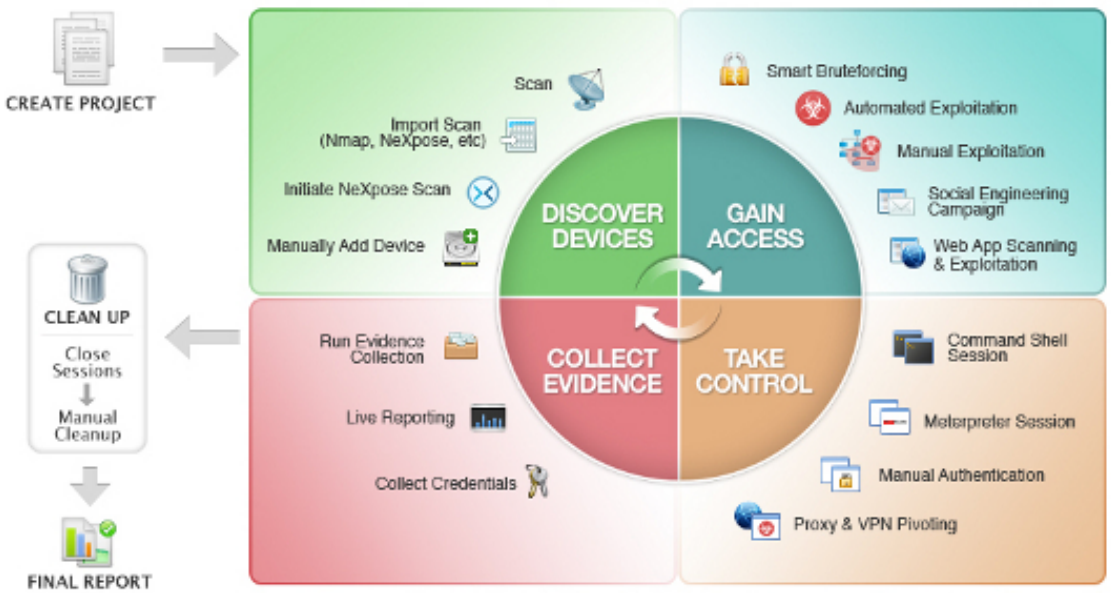

Figura 22 - Metasploit - Funcionalidades

Reflexão Final

Inicialmente, este relatorio de projeto seria algo totalmente diferente pois seria um relatório de estágio. Apesar de ser muito diferente do que estava a espera devido a pandemia, deu para entender algumas coisas nas duas semanas que estive a estagiar, pois consegui entender que meu foco será mesmo a area mais virada para software, desde programação a cibersegurança, em vez da area do hardware. Durante o curto período de estágio, eu sentia me mais a vontade na altura que era para fazer programaçao e ainda mais quando montamos um servidor onde ja ponha os meus conhecimentos de cibersegurança, em vez de que desmontar e arranjar computadores. Apesar de ser algo que goste, não me cativa muito pois é quase sempre a mesma coisa e eu gosto de inovar.

Acrescento ainda que durante o estágio, aprendi e evolui na area de cibersegurança, em que consegui adquirir conhecimentos extras, nomeadamente na proteção de um servidor com a SOPHO.

No decorrer deste projeto, consegui aprender e descobrir ferramentas muito importantes da minha area de que nao tinha conhecimento, o que é uma grande ajuda para o futuro. Neste projeto falo sobre a melhor Ferramenta para a area de cibersegurança que é o Kali Linux, pois tem tudo que é essencial, desde analises, a sniffings entre outra variedade de ferramentas.

Referencias Bibliograficas

https://sempreupdate.com.br/5-distribuicoes-alternativas-ao-kali-linux/

https://e-tinet.com/linux/27-ferramentas-hackers-kali-linux-parte-1/

https://pplware.sapo.pt/

https://pt.wikipedia.org/

https://www.kali.org/

https://securityonion.net/

https://www.metasploit.com/

https://nmap.org/book/zenmap.html

https://www.offensive-security.com/