



IPG Politécnico
da Guarda
Escola Superior
de Tecnologia e Gestão

RELATÓRIO DE ESTÁGIO

Curso Técnico Superior Profissional
em Cibersegurança

Miguel Francisco Antelo Coelho

julho | 2020





IPG

Politécnico
| da Guarda

Polytechnic
of Guarda

RELATÓRIO DE PROJETO

Curso Técnico Superior Profissional de Cibersegurança

Miguel Francisco Antelo Coelho

Julho | 2020



IPG

Politécnico
|da|Guarda

Polytechnic
of Guarda

Instituto Politécnico da Guarda

Escola Superior de Tecnologia e Gestão
Relatório De Projeto

Miguel Francisco Antelo Coelho

**Relatório Para a Obtenção do Grau Técnico
Superior Profissional em Cibersegurança**

Orientador: Engenheiro Pedro Pinto

2018/2020

Ficha de identificação

Discente: Miguel Francisco Antelo Coelho

Nº de matrícula: 1701388

Estabelecimento de ensino: Instituto Politécnico da Guarda

Escola: Escola Superior de Tecnologia e Gestão – Instituto Politécnico da Guarda

Curso: Técnico Superior Profissional de Cibersegurança

Docente orientador: Pedro Pinto / Fernando Melo Rodrigues

Entidade de acolhimento: GEF Guarda Ida.

E-mail: miguel.migas.coelho@gmail.com

Ano Letivo: 2019/2020

Morada: Av. Dr. Francisco Sá Carneiro, 50 – 6300-559

Telefone: +351 271 222 100

Fax: +351 271 222 690

E-mail: ipg@ipg.pt

Duração do estágio: 80 horas Complementadas pelo projeto

Data de início de estágio: 02-03-2020

Data de fim de estágio: 13-03-2020

Agradecimentos

Começo por agradecer ao meu Diretor de Curso, Professor Fernando Melo Rodrigues pela disponibilidade sempre demonstrada, auxiliando-me constantemente nas questões do projeto e ideias abordadas, na realização deste projeto, que em todos os momentos contribuiu com grande empenho, sabedoria fundamentada e dedicação.

Queria também, agradecer ao meu orientador de estágio, Pedro Pinto, por todo o apoio que me deu nesta etapa do meu percurso académico.

Agradeço também à Escola Superior de Tecnologia e Gestão no Instituto Politécnico da Guarda, pela atenção dispensada no decorrer do meu percurso nesta instituição.

Quero agradecer também à GEFGuarda pela forma como me aceitaram no estágio curricular e estarem sempre dispostos a ajudar, explicar e esclarecer qualquer dúvida existente.

Um obrigado aos meus pais por me apoiarem neste meu percurso, por todos os sacrifícios que fizeram para que eu pudesse concluir e por acreditarem em mim e nas minhas capacidades.

Por último, e não menos importante, ao resto da minha família e amigos que sempre desejam o melhor para mim e que foram inextinguíveis no seu apoio nesta etapa da minha vida.

Glossário

Ataque drive-by- É um ataque que se refere ao download não intencional de código malicioso para o computador ou dispositivo móvel.

Backdoor- É um vírus que nega o procedimento de autenticação normal para aceder a um sistema. Normalmente é colocado depois de um ataque, para o hacker poder voltar mais facilmente.

Cracking- É caracterizado como o ato de entrar num sistema sem permissões ou de formas ilegais

Hackear- É o processo de piratear algum sistema, invadindo um sistema. Entrar num sistema sem permissão é o que um hacker malicioso faz.

Hijacking- É um sequestro de dados informáticos.

Host- É um computador mestre que fornece informações, protocolos etc. a outros que lá se liguem.

Injection- Injeção de código malicioso / programas em outro sistema.

Keylogging- É a ação de gravar/registar as teclas pressionadas num teclado, normalmente de maneira ilegal.

Pentester- É alguém que faz testes de intrusão / teste de penetração.

Pivoting- É referido como um método que um atacante usa um sistema comprometido para atacar outros sistemas na mesma rede, assim não precisando de ter mais privilégios, pois já está na rede.

Poisoning- É quando alguém com más intenções infecta a máquina da vítima alterando o arquivo hosts do Windows, que é responsável pelo redirecionamento de endereços IP.

Rootkit- É uma série de programas que ficam num computador (depois de um ataque), projetado para permitir o acesso privilegiado a um computador.

Scripts- É um programa escrito para um sistema de tempo de execução especial que automatiza a execução de tarefas

Sniffing- Analisador de pacotes, um programa que pode interceptar e registar tráfego que passa sobre uma rede digital ou parte de uma rede.

Trojans- É um malware que engana os utilizadores sobre a sua verdadeira intenção.

Worms- É um vírus que se replica com o objetivo de se espalhar por outros computadores, geralmente usa uma rede de computadores para se espalhar, ou mesmo por unidades USB.

Resumo

O estágio tem uma duração de 750 horas, mas devido à pandemia que se encontra ainda ativa, o estágio teve de ser interrompido para nossa segurança, tendo feito assim 80 horas na GEF Guarda lda. Não tendo sido retomado em tempo útil pelo que se complementou o estágio com um projeto de pesquisa bibliográfica.

Nesta empresa, realizei múltiplas tarefas que me foram pedidas sob a orientação do responsável senhor João, e do técnico Daniel na manutenção a computadores, instalação de firewall e nas assistências técnicas em empresas clientes.

Com a suspensão do estágio foi proposto a realização de um Projeto para a conclusão do curso. Assim o relatório está dividido em duas partes: a primeira com a descrição do trabalho/tarefas realizadas na empresa; e uma segunda à análise e desenvolvimento de uma solução na área de estudos, selecionou-se o tema Ethical Hacking, um assunto abordado na unidade curricular de Técnicas de Hacking do professor Pedro Pinto.

Palavras-chave

Ethical Hacker; Hacking; Cibersegurança; Vulnerabilidades.

Índice

Ficha de identificação.....	iii
Agradecimentos	iv
Glossário	v
Resumo	vi
Palavras-chave	vi
Índice Figuras	viii
Introdução.....	9
Capítulo 1 Caracterização da Instituição	10
1.1 Caracterização da empresa	11
1.2 Caracterização das tarefas realizadas.....	12
Capítulo 2 Enquadramento teórico	13
2.1 Cibersegurança.....	14
2.1.1 As atividades principais do curso Cibersegurança	15
2.1.2 Conhecimentos precisos.....	15
2.1.3 Aptidões	16
2.1.4 Atitudes	16
Capítulo 3 Projeto	17
3.1 Ethical Hacking	18
3.1.1 Tipos de hacking	19
3.1.2 Conhecimentos relevantes para um Hacker Ético	21
3.2 Importância do hacking ético	22
3.3 Hacking/Hackear é ilegal?	22
3.4 Ferramentas para verificação de vulnerabilidades.....	23
3.5 Etapas para um teste de intrusão / Pentest	27
3.6 Regras de um Hacker Ético	28
3.7 Tipos de problemas mais comuns	29
3.8 Certificados de um hacker ético	30
Reflexão Final	32
Referências Bibliográficas	33

Índice Figuras

Figura 1 Lógotipo GEF Guarda, Lda	11
Figura 2 NAS QNAP software.....	12
Figura 3 Evolução de crimes informáticos	14
Figura 4 Painel de Controlo do OpenVAS	23
Figura 5 Painel de controlo do Wireshark	24
Figura 6 Painel de controlo do Nessus	25
Figura 7 Painel de controlo do Comodo	26
Figura 8 Nikto a ser usado no KaliLinux.....	27
Figura 9 Esquema de certificação VAPT (https://www.eccouncil.org/ethical-hacking/)	30

Introdução

Na GEF Guarda, empresa onde estagiei por 2 semanas deu para aprender mais um pouco de como é o mundo do trabalho. Na primeira semana estive a aprender melhor como trabalhava a empresa, quais eram as maneiras de trabalhar e resolver os problemas. Muitos dos problemas que tínhamos era de clientes que chegavam à loja com um computador estragado (ecrã a funcionar mal, grande aquecimento do computador, ventoinhas a fazer barulho etc.) e reparávamos estes problemas.

Juntamente com o técnico Daniel que era o responsável por esta secção arranjávamos os computadores e também fazíamos serviço de nos deslocarmos a empresas clientes para fazer algumas instalações (instalar uma câmara de conferências numa sala de reuniões de uma das empresas, com o processo todo de cablagem e instalação do software da câmara e realizar testes).

Nos dias que tínhamos “menos” trabalho eu e o meu colega de estágio ficávamos na loja, a fazer algumas arrumações, e colocar os produtos da loja no seu site (fazíamos a gestão do site da empresa).

A realização do estágio curricular é muito importante para que se possam aplicar todos os conhecimentos adquiridos teoricamente ao longo destes dois anos, sendo este o primeiro contacto com o mundo do trabalho.

O curso de Cibersegurança proporciona uma aquisição de competências e conhecimentos para trabalhar na área do cibercrime, informática, programação.

Capítulo 1 Caracterização da Instituição

1.1 Caracterização da empresa

Escolhi estagiar na empresa GEF Guarda (conforme o logotipo abaixo) por ser uma empresa com variados serviços. São estes:

- Instalação de redes: Instalação de redes locais, atuando desde o projeto de cablagem e instalações, até a montagem e instalação de racks, tomadas, switch e routers;
- Consultoria: A empresa propõe este serviço quando um cliente necessita de uma opinião profissional, no apoio às tecnologias de informação;
- Software de Gestão: A empresa fornece soluções de gestão baseadas no software PHC. Este software por ser modular, permite adequar a implementação de soluções de gestão integradas direcionadas especificamente para cumprir o objetivo de cada empresa, operacionalizando os seus processos e regras de negócio de acordo com as necessidades dos vários intervenientes;
- Assistência Técnica: Oferecem suporte corporativo em informática para pequenas, médias e grandes empresas. Também na vertente de suporte remoto, para que a empresa possa prestar a assistência técnica via internet;
- Serviços de Recuperação de Dados: A empresa tem parceria com um laboratório de recuperação de dados, garantindo mesmo que as hipóteses de recuperar dados e ficheiros apagados de um disco rígido em caso de avaria;
- *Backup* na nuvem: A empresa também oferece serviço de cópia de segurança, para o caso de ser necessário migrar um servidor para a *cloud*;

Além de fornecer serviços também vende ao público produtos tais como Servidores, Computadores, Portáteis, Monitores, Impressoras, Software aplicativo, Projetores, Software de segurança e Smartwatches, entre muitos outros.



Figura 1 Logotipo GEF Guarda, Lda

1.2 Caracterização das tarefas realizadas

A maior parte das tarefas que realizávamos era quando chegavam clientes com algum problema no computador, e tínhamos de o reparar. A maior parte dos casos era sobreaquecimento do computador, por isso depois na oficina desmontávamos o computador, tirávamos o processador (CPU) e colocávamos pasta térmica, limpávamos o interior e montávamos tudo de volta. De seguida ligávamos e fazíamos os nossos testes, tais como abrir browsers e vídeos para ver se o computador aquecia e/ou ficava lento.

O mesmo acontecia em empresas clientes, ligavam para a loja e reportavam que tinham algum problema, ou que precisavam algum produto (monitores, computadores etc.) e então deslocávamo-nos lá e íamos reparar na hora, ou fazer a instalação do que fosse preciso na hora. Para casos mais fáceis, ligávamo-nos por controlo remoto e fazíamos sem ter de sair da loja da GEF.

Num destes serviços externos tivemos de fazer a instalação de uma câmara de conferências numa sala de reuniões de uma empresa cliente. Fizemos o processo todo desde a passagem de cabos, à instalação do software da câmara, testes à câmara e posicionamento da mesma.

Num dos dias tivemos de configurar um software para uma empresa cliente. O software chama-se QNAP NAS. É um sistema de armazenamento com vários discos rígidos (apenas colocamos 2 discos de 1Terabyte de armazenamento nela), que está constantemente online. Tem um sistema operacional próprio chamado QTS. Tem uma vasta gama de aplicações, incluindo um gestor de arquivos, um gestor de *backups*, gestor de *downloads*, permissões de acesso e segurança (firewall própria), centro de multimédia entre outros, como mostra a imagem 2. Este software foi explicado pelo técnico Daniel da empresa, que já tinha trabalho anteriormente com o mesmo.



Figura 2 NAS QNAP software

Capítulo 2

Enquadramento teórico

2.1 Cibersegurança

Cibersegurança é a prática que protege computadores, servidores, dispositivos móveis, redes e dados contra ataques maliciosos. É também chamada de segurança da tecnologia da informação. Atualmente a Cibersegurança está presente em diversos segmentos, tais como governamentais, pequenas e grandes empresas, entre outros.

Devido ao crescente número de crimes informáticos e consequentes perdas que as organizações enfrentam, é fundamental que haja a garantia que os dados e informações manipulados por sistemas informáticos corporativos não sejam vulneráveis.

Segundo os dados da mesma empresa, Kaspersky, Portugal registou mais de 150 mil ataques informáticos só durante o período de confinamento (março e abril 2020). A seguinte imagem foi retirada do jornal económico. <https://jornaleconomico.sapo.pt/noticias/portugal-registou-mais-de-150-mil-ataques-informaticos-em-abril-594287>

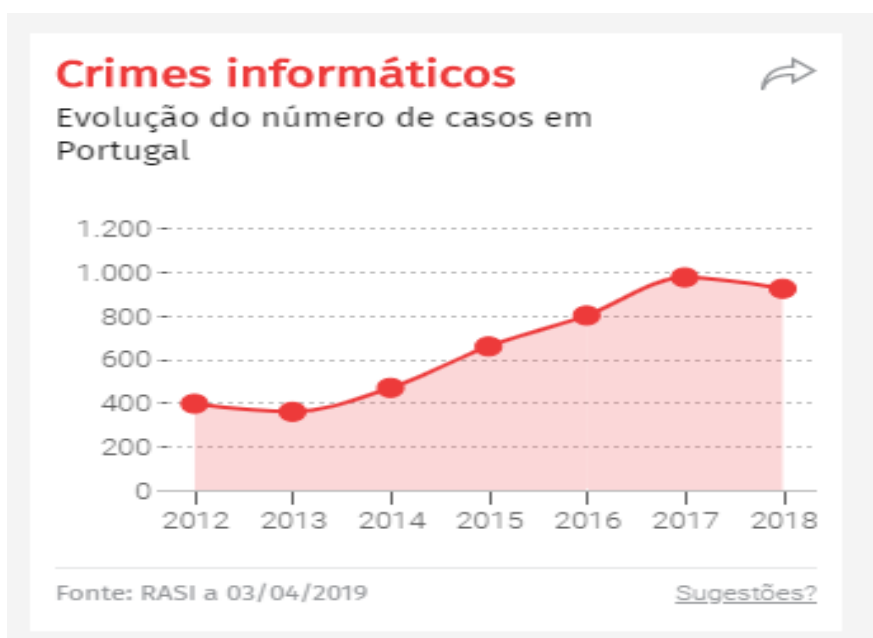


Figura 3 Evolução de crimes informáticos

A seguir transcreve-se os tópicos que constam em Diário da República, 2.ª série — N.º 55 de 19 de março de 2018 sobre a criação do curso de Cibersegurança

2.1.1 As atividades principais do curso Cibersegurança

1. Planear, instalar e configurar sistemas e equipamentos informáticos, e redes estruturadas.
2. Gerir redes de comunicação, sistemas, serviços e servidores, de forma segura, eficiente e fiável, com o objetivo de otimizar o funcionamento dos mesmos.
3. 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.
4. Desenvolver aplicações informáticas seguindo um processo de desenvolvimento de software e as boas práticas e tendo em conta os vários atributos de segurança.
5. Planear e projetar sistemas de bases de dados de acordo com os requisitos.
6. Testar e validar a segurança de sistemas e aplicações informáticas.
7. Testar diversas técnicas de análise de segurança, de modo a assegurar a identificação e mitigação das ameaças à Cibersegurança.

2.1.2 Conhecimentos precisos

1. Conhecimentos abrangentes de Sistemas Operativos.
2. Conhecimentos especializados de criptografia de dados.
3. Conhecimentos fundamentais factos, princípios e conceitos de arquitetura de sistemas computacionais (hardware e software).
4. Conhecimentos especializados de ferramentas de segurança.
5. Conhecimentos especializados de procedimentos e técnicas de Cibersegurança e Ciberdefesa.
6. Conhecimentos especializados de desenvolvimento de software seguro com acesso a bases de dados.
7. Conhecimentos fundamentais de escrita e manutenção de documentação técnica.
8. Conhecimentos especializados de mecanismos e técnicas de resolução de problemas.

2.1.3 Aptidões

1. Utilizar ferramentas e técnicas adequadas ao planeamento, instalação, manutenção e gestão de redes e sistemas.
2. Identificar e utilizar as várias tecnologias de infraestruturas de rede.
3. Interpretar indicadores e comportamentos de sistema que permitam a identificação de ameaças à segurança da informação e à segurança de redes e sistemas.
4. Instalar e configurar sistemas operativos.
5. Utilizar ferramentas destinadas a gerir as vulnerabilidades existentes e a garantir a Cibersegurança e ciberdefesa das redes e sistemas.
6. Propor soluções criativas no âmbito do projeto de desenvolvimento de software.
7. Interpretar requisitos de necessidades mais ou menos estruturados de forma a propor soluções de bases de dados adequadas.
8. Selecionar e propor políticas de segurança adequadas.
9. Programar aplicações seguras.

2.1.4 Atitudes

1. Demonstrar capacidade de iniciativa e responsabilidade.
2. Demonstrar autonomia na resolução de problemas técnicos.
3. Demonstrar disponibilidade, cortesia e respeito pelos outros no relacionamento com interlocutores diferenciados.
4. Demonstrar flexibilidade adaptando-se a diferentes situações e contextos profissionais.
5. Demonstrar capacidade de liderança.
6. Demonstrar autonomia na tomada de decisão.

Capítulo 3 Projeto

3.1 Ethical Hacking

Normalmente o termo “Hacker” é associado ao indivíduo que se dedica a analisar e/ou burlar os limites de segurança de dispositivos, sistemas e redes de computadores. *Hacker* normalmente é utilizado para caracterizar o sujeito com atitude maliciosa, cuja motivação leva ao comprometimento da proteção de dados/informações.

Adaptado de: <https://canaltech.com.br/hacker/O-que-e-um-Hacker/>

Ethical Hacking (Pirata informático ético) é um conceito que traduz o ato de *hackear*. As atividades de um hacker ético envolvem testes de penetração/intrusão.

Um Ethical Hacker é um profissional de tecnologia da informação que trabalha na área de Segurança da Informação, com a função de encontrar vulnerabilidades de segurança que um hacker malicioso poderia potencialmente explorar. Este profissional precisa desenvolver aptidões em técnicas de penetração de sistemas, redes de computadores e dispositivos computacionais em geral.

É também de relevar que um hacker ético deve ter conhecimentos iguais ou superiores a um hacker com intenções maliciosas. Mas, ao invés de usar este conhecimento para obter vantagem própria, utiliza a mesma para investigar, analisar e reportar vulnerabilidades para a empresa para a qual está a prestar serviços, evitando assim ataques e problemas de segurança.

Adaptado de <https://www.portalgsti.com.br/profissoes-de-ti/hacker-etico/>.

"A filosofia por trás do Hacker Ético é tentar capturar o ladrão, pensando como um ladrão" – in: “Grupo anonymous”

Hackers éticos estão também associados à expressão *Pentester*.

Adaptado de: <https://blog.eccouncil.org/what-is-penetration-testing-how-does-it-differ-from-ethical-hacking/>

3.1.1 Tipos de hacking

Quase todos os sistemas, processos, websites, dispositivos etc., podem ser hackeados. Para um hacker ético entender como um ataque pode acontecer e qual seria o seu dano precisa comportar-se e pensar como um hacker malicioso e conhecer as ferramentas e técnicas que provavelmente usará.

1. Hacking de aplicações na web

Tal como o nome diz, é o facto de *hackear* uma aplicação que esteja na web. Alguns dos métodos usados são SQL injection, RCE (execução de código remoto), Hijacking/poisoning de sessão (O atacante ganha acesso de uma comunicação do site), Cross-site scripting (O atacante injeta scripts nas páginas web que depois são executados no sistema da vítima).

2. Hacking de sistemas

Este é o ataque em que o hacker ganha acesso individual a um computador numa rede. Um hacker ético aprende a fazer isto para detetar, prevenir e contrariar este ataque. Alguns dos métodos usados são *cracking* de passwords(uma ferramenta conhecida é o *Aircrack-ng*); escalção de privilégios (é feito para obter acesso elevado a recursos que normalmente são protegidos); instalação de spyware (software que permite ao atacante monitorar vários dados de um utilizador) e *keylogging* (o atacante tem acesso a tudo o que é escrito num computador), por exemplo usando uma ferramenta chamada: *Spyrix* que pode ser instalada num computador sem se aperceber, e regista tudo o que é escrito.

3. Hacking de servidores web

Tudo o que acontece na web está a correr em tempo real num servidor. Então os tipos de hacking que se pode fazer normalmente são roubos de informação credenciais do servidor; ataques DoS (uma sobrecarga no servidor que indisponibiliza o mesmo) por exemplo uma ferramenta conhecida é o *LOIC*(*Low Orbit ION Cannon*), é uma ferramenta

escrita em C# que envia pedidos HTTP, TCP e UDP para um servidor; *SYN flood* (muito parecido com DoS mas para a camada de transporte, e indiretamente para a camada de aplicação do modelo OSI) pode ser feito com uma ferramenta do sistema Kali Linux chamada HPING3, scan de portas (discriminado no ponto 3.5); ataques *sniffing* (intercepção de dados capturando o tráfego de rede) por exemplo pode ser feito com a ferramenta Wireshark, que tanto pode ser usada para evitar estes ataques como para os fazer.

4. Hacking redes sem fios (Wi-Fi)

Estes são ataques também realizados muitas vezes, por as redes sem fios serem omnipresentes. Alguns dos métodos de ataques destas redes são *Sniffing* (interceptar os pacotes da rede, e com isso descodificar estes); ataque *Man-in-the-middle* (os dados trocados entre duas partes, são interceptados, registados e alterados pelo atacante sem que as vítimas se apercebam) Este ataque pode ser feito usando várias ferramentas do Kali Linux como *arp spoof* para redirecionar o tráfego da rede para o endereço FTP do atacante e *dsniff* para fazer *sniffing* nessa rede.

5. Engenharia Social

O método/tipo de *hacking* mais usado atualmente segundo dados do CNCS (Centro Nacional de Cibersegurança Portugal <https://www.cncs.gov.pt/engenharia-social/>)

A engenharia social refere-se à manipulação de pessoas para a execução de ações, ou divulgar informações confidenciais de forma inadvertida.

A engenharia social é um método que pode ser usado para outro tipo de crimes e não só informáticos. Mas no meio digital a engenharia social pode ser feita através de e-mails, mensagens, perfis falsos nas redes sociais ou até mesmo por uma chamada telefónica. O hacker ao entrar em contato com a vítima, tenta ganhar confiança da mesma e pergunta por informações que normalmente se pensam não ser importantes, tais como emails, data de nascimento.

Segundo a empresa *Compugraf*, a Engenharia Social explora vulnerabilidades emocionais numa vítima, e usa estas como isca para assuntos atuais, promoções ou até mesmo falsas premiações, o que leva a vítima a dizer as informações que não devia, ou carregar em algum link que não devia. Adaptado de: <https://www.compugraf.com.br/quais-sentimentos-sao-explorados-na-engenharia-social/>

3.1.2 Conhecimentos relevantes para um Hacker Ético

Um hacker deve ter um conhecimento profundo das seguintes áreas.

- **Redes de Computadores:** Saber topologias de rede (Como organizar cada dispositivo numa rede), Modelo OSI (Padrão para protocolos de comunicação de uma rede local), Protocolos (conhecer os protocolos de rede mais utilizados TCP,IP,UDP,ARP,DHCP,FTP etc. Saber como fazer 2 dispositivos comunicarem na mesma rede, que protocolos usar).
- **Programação:** Escrever programas de raiz (Saber como criar um script para automatizar algum processo que fosse demorar tempo), Conhecer várias linguagens (HTML por exemplo se o alvo for uma página na internet, Python por exemplo se o hacker precisar de desenvolver alguma aplicação, ou mesmo alterar alguma aplicação existente para uso próprio, C & C++ , Java etc.) Cada linguagem tem o seu uso/alvo
- **Segurança da Informação:** Saber proteger cada sistema (Antivirus diferentes, diferentes maneiras de navegar na internet de forma segura), saber proteger redes (Identificar os recursos mais importantes numa rede e ver quem tem acesso a cada coisa, contribuir para um uso seguro nessa rede, saber avaliar vulnerabilidades nessa rede).
- **Sistemas Operacionais (Linux, Windows, Android, iOS):** Saber trabalhar com diferentes sistemas operativos é importante para conhecer as vulnerabilidades em cada um, como as contornar. Linux normalmente é o mais importante para saber programar nesse sistema, criar aplicações próprias que ajudem numa investigação.

E também depois mais especificamente:

- **Segurança em Redes:** Saber como proteger uma redes sem fio, redes locais.
- **Pentester (Testes de intrusão):** Saber diferentes técnicas de invasão com diferentes ferramentas, testes de intrusão em redes sem fio e as diferentes maneiras de o fazer. Adaptado de: <https://blog.corujadeti.com.br/o-que-e-ser-um-pentester/>
- **Criptografia:** É importante saber criptografia porque todos os dados que passam por um *hacker* tem de ser criptografados, para evitar que dados sigilosos sejam expostos. E vice-versa, por exemplo algo que esteja criptografado o hacker tem de perceber o que esses dados contêm. Adaptado de: <https://www.strongsecurity.com.br/blog/criptografia-de-dados-importancia-para-seguranca-da-empresa/>

- IDS e IPS (sistemas de detecção de intrusão e sistemas de prevenção de intrusão):
No caso do IDS é importante saber como consultar através de regras preestabelecidas o gestor de pacotes para efetuar análises. E perceber como a junção destes 2 sistemas podem ajudar a detetar uma intrusão e ao mesmo tempo prevenir essa vulnerabilidade.
Adaptado de: <https://blog.starti.com.br/ids-ips/>

3.2 Importância do hacking ético

Ataques contantes aos sistemas informáticos, roubo de informações confidenciais, disseminação de *worms*, *trojans* e vírus conhecidos são algumas evidências de que cada vez há mais necessidade de implementar práticas eficazes na área da segurança de sistemas e da informação, e com isso ter um profissional de segurança ou um hacker ético a trabalhar nas empresas.

3.3 Hacking/Hackear é ilegal?

Segundo o artigo 6º da lei nº 109/2009 de 15 de setembro quem não está autorizado pelo proprietário de um sistema a aceder a este é punido com pena de prisão. No entanto uma parte dos hackers que trabalham em empresas e que utilizam o seu conhecimento para melhorar e proteger os softwares estão a trabalhar de forma legal. Os tipos de atividades ligadas ao *Hacking* que são ilegais são aquelas onde se configura eventos como roubo de serviços, fraudes e o acesso ilegítimo a um sistema sem permissão.

O hacker ilegal é conhecido como o *Black Hat*. É o oposto de um hacker ético e não respeita os códigos de ética da comunidade em que se insere. É este que usa o conhecimento de hacking para o seu próprio benefício, e com isto faz chantagens e roubos de informações sensíveis.

Depois existe também os *Grey Hat* que são os tipos de hacker que invadem sistemas apenas por “diversão”. No entanto não divulgam dados sensíveis ou confidenciais. Muitas vezes atuam apenas para terem algum lucro, ou seja, exploram as vulnerabilidades do sistema de uma determinada empresa, e caso encontrem alguma, oferecem-se para resolver a troco de dinheiro, ou por vezes resolvem comunicando com a empresa sem receber nada de volta.

Adaptado de: <https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/>

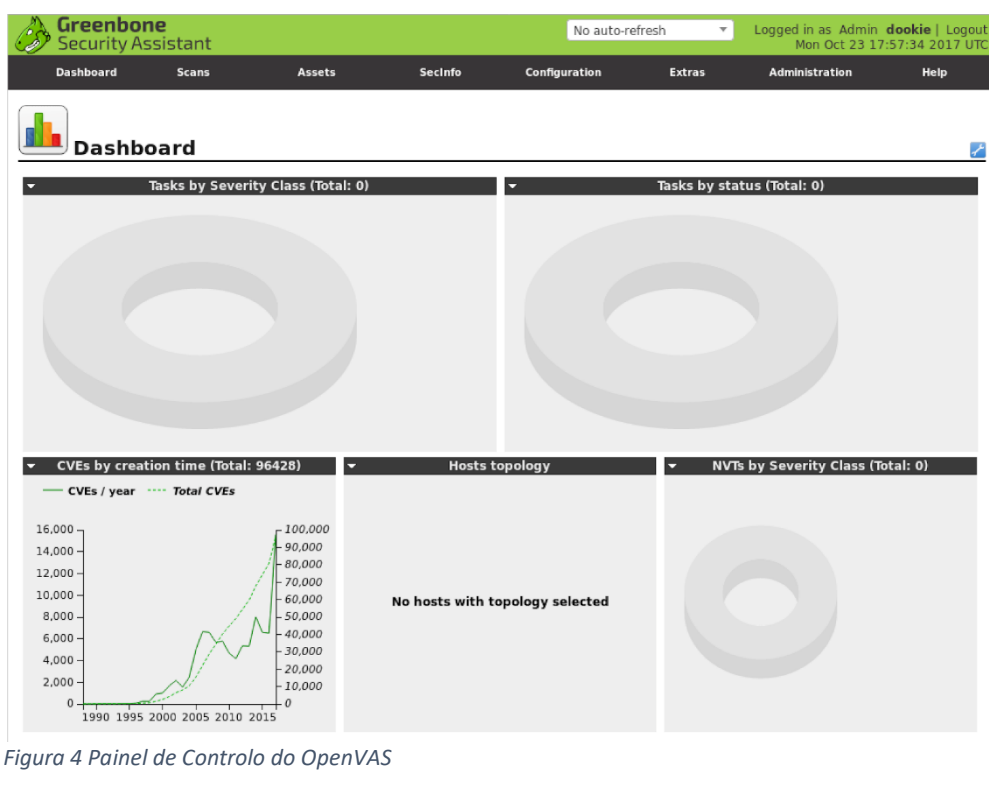
3.4 Ferramentas para verificação de vulnerabilidades

Segundo vários autores/empresas de Cibersegurança tais como: *Kaspersky*, empresa de segurança informática; Jeff Barr que desenvolveu e administra no momento a *AWS* (Serviços *Web* da Amazon); Runa Sandvik uma das criadoras da ferramenta *TOR* (ferramenta utilizada para aceder à *deep web*) estas são as melhores ferramentas para testes e verificação de vulnerabilidades de 2019. Estas ferramentas ajudam a detetar vulnerabilidades de segurança nas aplicações, sistemas operativos, hardware e sistemas de rede.

Adaptado de <https://blog.marketingenvy.com/top-21-cybersecurity-experts-you-need-to-follow-in-2020>

1. OpenVAS

É uma ferramenta de análise de vulnerabilidades que permite ao hacker ético verificar servidores e dispositivos de rede. Esta ferramenta verifica qualquer endereço IP (daquela rede), serviços abertos, portas, configurações incorretas e aplicações existentes. Depois de ser feito a análise esta ferramenta envia um email com um ficheiro a dizer todas as vulnerabilidades encontradas. (Figura 4)



2. Wireshark

Provavelmente a ferramenta mais conhecida pelos técnicos da área de redes de segurança, o wireshark é seguramente o melhor analisador de protocolos de rede. Várias agências governamentais, empresas, serviços de saúde o utilizam por ser fácil e intuitivo. Quando é detetado uma ameaça ao que estamos a analisar a ferramenta coloca essa função offline, para que seja melhor analisado, ou seja o wireshark captura o tráfico analisado, e guarda para depois ser verificado quando estiver offline.

O wireshark tem um navegador de pacotes padrão de três painéis, filtros de exibição, análise de VoIP (Voz sobre IP), suporte de decriptografia para protocolos como Kerberos, WEP, SSL/TLS etc. Também é uma ferramenta que pode ser usada em vários sistemas operativos diferentes tais como Linux, macOS e Windows. (Figura 5)

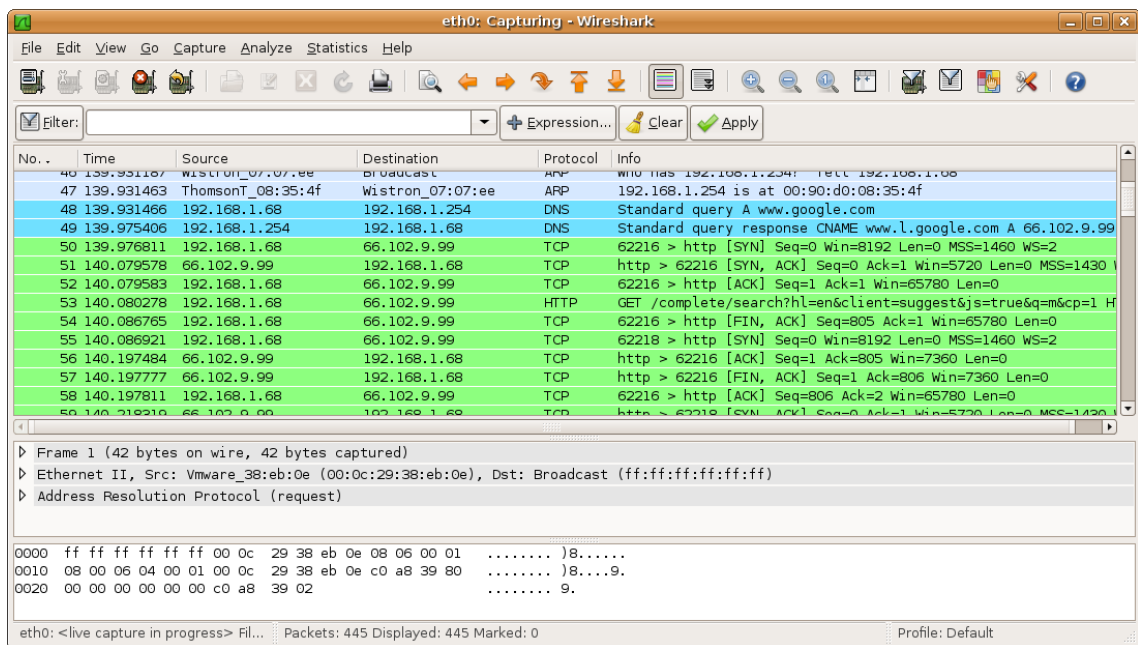


Figura 5 Painel de controlo do Wireshark

3. Nessus

É uma ferramenta que faz correções, problemas de software, remoção de malware, adware e configurações incorretas numa ampla variedade de sistemas operativos e aplicações.

O Nessus cria um procedimento de segurança proativa, identificando as vulnerabilidades, corrigindo falhas de execução de código de um dispositivo de rede, infraestrutura virtual ou em nuvem.

Esta ferramenta é de fácil instalação, mas é necessário algum conhecimento avançado em redes de computadores para configurar tudo. (Figura 6)

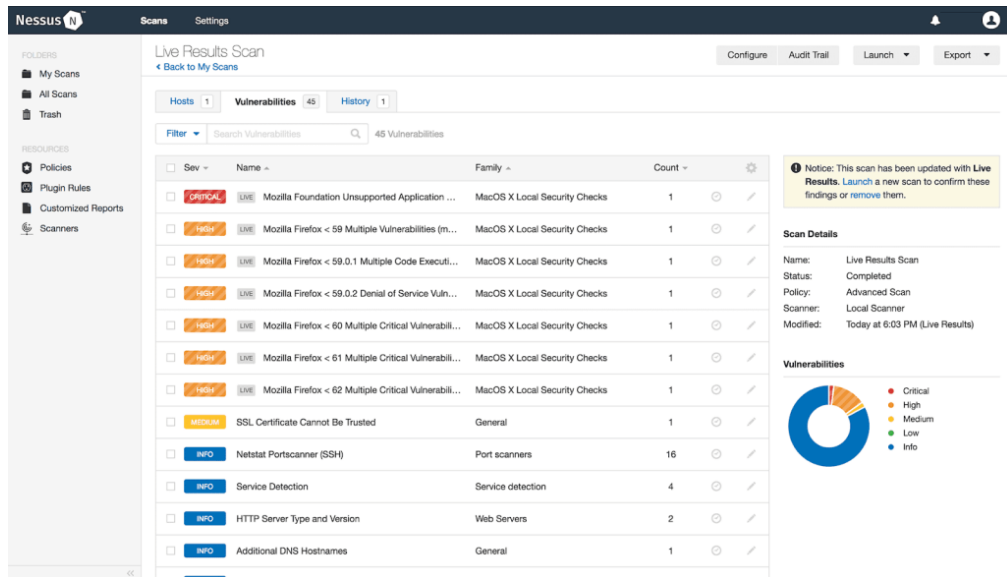
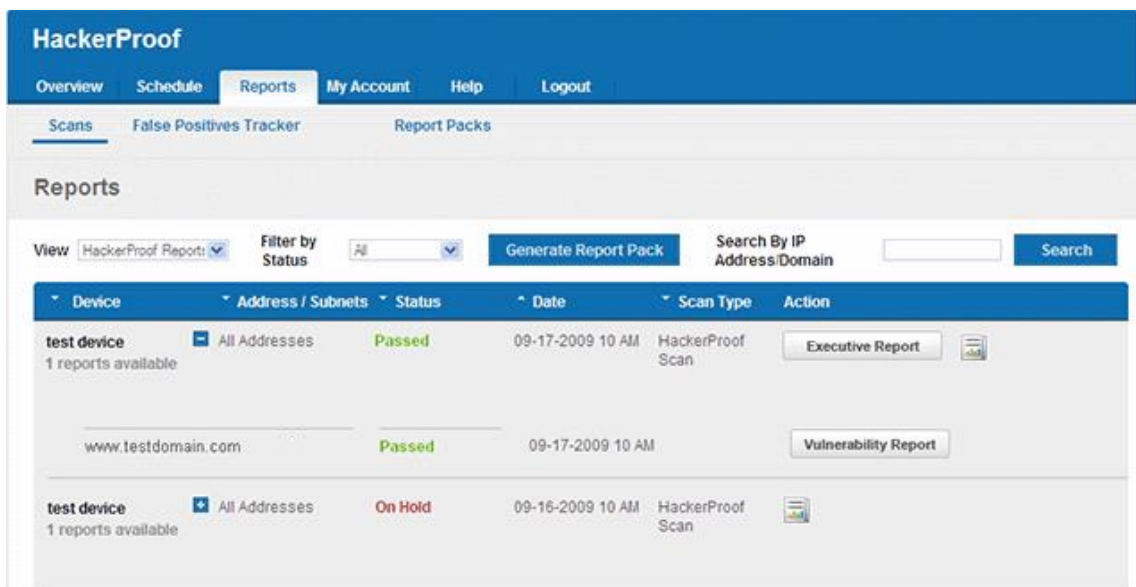


Figura 6 Painel de controlo do Nessus

4. Comodo HackerProof

É um dos líderes também em scanner de vulnerabilidades, pois tem recursos que permitem verificar vulnerabilidades diariamente. Tem opções de scanner PCI (barramento para ligar periféricos numa motherboard por exemplo), prevenção de ataques drive-by e tecnologia de inspeção de sites (erros de código e falhas de segurança no mesmo).

É usado muito para sites de compras, pois *Comodo* é um selo de certificação de segurança online, e então um cliente ver que um site tem o selo da *Comodo* gera mais confiança entre cliente-vendedor. (Figura 7)



The screenshot displays the HackerProof web interface. At the top, there is a navigation bar with tabs for Overview, Schedule, Reports (selected), My Account, Help, and Logout. Below this, there are sub-tabs for Scans, False Positives Tracker, and Report Packs. The main content area is titled 'Reports' and includes a filter section with a 'View' dropdown set to 'HackerProof Reports', a 'Filter by Status' dropdown set to 'All', a 'Generate Report Pack' button, and a search box for IP Address/Domain with a 'Search' button. The main part of the interface is a table with the following data:

Device	Address / Subnets	Status	Date	Scan Type	Action
test device 1 reports available	All Addresses	Passed	09-17-2009 10 AM	HackerProof Scan	Executive Report
	www.testdomain.com	Passed	09-17-2009 10 AM		Vulnerability Report
test device 1 reports available	All Addresses	On Hold	09-16-2009 10 AM	HackerProof Scan	

Figura 7 Painel de controlo do Comodo

5. Nikto

Outra grande ferramenta, usada no Kali Linux que ajuda a analisar as funções de um servidor, tal como a sua versão, realizar teste nos servidores da Web para identificar ameaças e presença de malware e verificar diferentes protocolos como HTTPS e HTTP. Também é capaz de verificar várias portas de um servidor rápido (comparado com outras ferramentas). Também de salientar que está inserido na comunidade Nexpose, que é uma das maiores e mais conhecidas comunidades de Cibersegurança no mundo. (Figura 8).

```
NIKTO - WEB SCANNER
Note: This is the short help output. Use -H for full help text.
root@kali:~# nikto -h 192.168.1.104
Nikto v2.1.5
-----
+ Target IP:      192.168.1.104
+ Target Hostname: 192.168.1.104
+ Target Port:    80
+ Start Time:    2014-03-16 13:12:38 (GMT0)
-----
+ Server: Apache/2.2.14 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 294236, size:
177, mtime: 0x4a4e4a1080a00
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.22). Apache
1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found
```

Figura 8 Nikto a ser usado no KaliLinux

3.5 Etapas para um teste de intrusão / Pentest

Para um hacker ético começar a analisar, ou fazer os testes de intrusão para descobrir as vulnerabilidades tem de seguir uma certa ordem, estas descrevem-se de seguida.

1. Coletar informações gerais

Potenciais vulnerabilidades, como funciona o sistema que vai fazer a intrusão, DNS's, emails, redes da intranet.

Com estas informações um hacker ético por exemplo já consegue saber se a empresa utiliza VPN (Rede privada virtual) e endereços de servidores DNS (Sistema de nomes de domínio)

2. Mapear informações específicas de rede

Depois de ter informações dos endereços DNS já é possível descobrir a topologia de rede, IP e a quantidade de computadores na rede interna, assim como a configuração e características de servidores e sistemas operacionais de cada máquina.

3. Enumeração de Serviços

Com as informações obtidas anteriormente e devidamente mapeadas o hacker ético já consegue investigar os serviços que estão a ser executados numa determinada porta, utilizando um programa que monitore as conexões.

4. Procurar vulnerabilidades

Cada serviço/porta é examinado para que seja revelada alguma vulnerabilidade que possa ser explorada. São feitas várias tentativas de intrusão de métodos diferentes para ver a resposta do sistema.

5. Exploração destas vulnerabilidades

O hacker ético aqui invade o software/serviço com as vulnerabilidades encontradas, para explorar a quantidade e a severidade do dano que pode ser feito, ou informações confidenciais que possam ser recolhidas.

6. Implementação de Backdoors e Rootkits

O hacker deixa instalado um programa que facilita o retorno ao software/serviço com esta vulnerabilidade. Pode ser um *Backdoor* que deixa uma porta disponível de acesso ou um *Rootkit* que é um programa que se mantém no núcleo do sistema operacional, muito difícil de localizar.

3.6 Regras de um Hacker Ético

Um hacker ético para ser chamado de hacker ético e não ser confundido com um hacker malicioso tem de seguir certos protocolos ou regras, que são:

1. Trabalhar legalmente:

Para poder usar as ferramentas de análise / intrusão e procurar vulnerabilidades tem de ter uma aprovação da entidade que será analisada.

2. Aprovação da direção da entidade:

Dependente da autorização concedida, seleciona as ferramentas mais adequadas. Estas acessibilidades irão definir os métodos de trabalho que tem de tomar.

3. Encontrar vulnerabilidades e reportá-las:

Quando o hacker encontrar as vulnerabilidades, este tem de ir sugerindo soluções para a sua correção.

4. Guiar-se pelo motivo ético:

Quando o trabalho é terminado o hacker tem de concordar com as políticas de privacidade da empresa, não divulgando os ficheiros que teve acesso temporariamente.

3.7 Tipos de problemas mais comuns

Existem vários problemas e vulnerabilidades encontradas todos os dias em vários dispositivos, de seguida apresento as mais conhecidas segundo dados de empresas de cibersegurança.

1. Perdas nas autenticações:

Faz com que o atacante consiga ultrapassar o processo de autenticação numa aplicação web, executando ataques por tentativa e erro de credenciais até descobrir (ataques de força bruta).

2. Configurações incorretas de segurança:

Estas configurações incorretas fazem a empresa pensar que está bem protegida devido a sistemas de segurança adquiridos, mas que por vezes estão mal configurados. Cabe ao hacker ético ajudar a encontrar estas más configurações e repará-las contra hackers maliciosos.

3. Ataques de injeção:

É um tipo de ataque que permite aos invasores injetar programas/código malicioso nos sistemas e com isso infetar grandes sistemas. O hacker ético para poder ajudar também faz ataques de injeção, para depois fazer o reverso, e descobrir onde no código está uma falha e reparar.

4. Exposição de dados sensíveis:

São ataques muito importantes para serem corrigidos rapidamente, pois com estas exposições números de contactos, passwords, credenciais de cartões de crédito, dados de saúde são expostos para os hackers maliciosos, e posteriormente postos ou vendidos online. Depois de fazer um teste de intrusão os hackers éticos listam as vulnerabilidades encontradas e as informações.

3.8 Certificados de um hacker ético

Existem atualmente vários cursos/certificados de ethical hacking, o mais conhecido é o VAPT (Hacker Ético Certificado), que é um curso que engloba vários tipos de certificações independentes, tal como mostra a figura 9. Conforme se vê vai se evoluindo até chegar ao LPT (Master em testes de penetração).

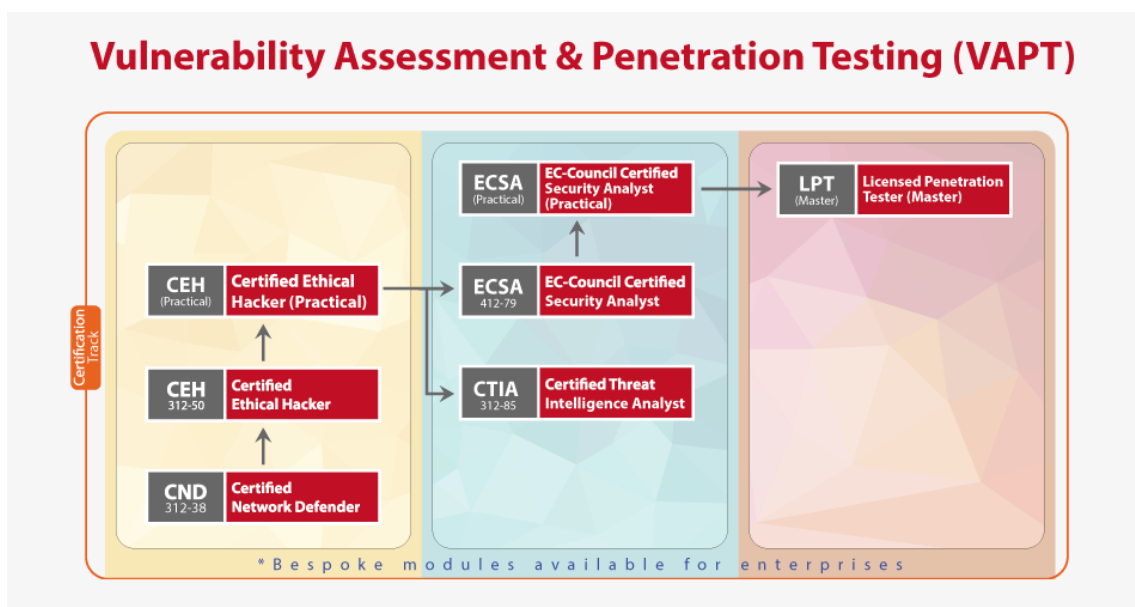


Figura 9 Esquema de certificação VAPT (<https://www.eccouncil.org/ethical-hacking/>)

No primeiro nível o curso inclui 3 certificações:

CND (Certified Network Defender):

Este foca-se na preparação de administradores de redes para que estes ganhem uma compreensão detalhada de defesa da rede. O suficiente para conseguir projetar ativamente uma rede segura numa empresa/organização. Este curso mostra a compreensão fundamental da verdadeira construção de transferência de dados, tecnologias de rede, tecnologias de software para se perceber como as redes operam.

CEH (Certified Ethical Hacker):

Esta certificação destina-se a obter um amplo conhecimento e prática real sobre as mais atuais ferramentas e técnicas de ataque e defesa, permitindo atuar profissionalmente diante de uma ameaça. O CEH e o CEH Practical são basicamente o mesmo, sendo um mais teórico e o outro com um treino completamente focado na parte prática.

De seguida já é considerado o nível avançado, que tem 3 certificações:

ECSA (EC- Council Certified):

Esta certificação apresenta um conjunto de metodologias abrangentes distinguíveis que cobrem os requisitos de *pen-testing* em níveis diferentes. Este curso é quase todo prático com laboratórios e exercícios que cobrem cenários do mundo real. É permitido aceder dinamicamente a um host de máquinas virtuais já pré configuradas com vulnerabilidades, explorações, ferramentas e scripts ligados a internet.

CTIA (Certified Threat Intelligence Analyst):

O objetivo desta certificação é permitir que as empresas tenham capacidades preditivas em vez de apenas medidas proactivas para além do mecanismo de defesa ativa, capacitar os futuros hackers éticos a desenvolver um programa profissional, sistemático e repetível de inteligência de ameaças na vida real.

De seguida o último nível deste curso, de nível Mestre:

LPT (Master) Licensed Penetration Tester:

Este como já dito anteriormente, é o último nível, a última certificação que existe para se tornar um verdadeiro hacker ético mestre. Neste exame é preciso demonstrar um domínio da implementação de técnicas e ferramentas avançadas, incluindo *pivoting* (explicado no glossário) de vários níveis, explorações de vulnerabilidades de Sistema Operativos, Exploração de túneis SSH, explorações de aplicações baseadas em host, escalonamento de privilégios, exploração de aplicações e servidores web, injeção SQL e manipulação de parâmetros. Basicamente todas as ferramentas e métodos de hacking são testados neste teste. Vale a pena dizer também que este teste prático tem uma duração de 18 horas, dividido em 3 exames de 6 horas cada um.

Reflexão Final

Num balanço geral e final do estágio curricular apesar de ter sido curto, sinto que consegui superar algumas dificuldades, pois, estive em contacto com problemas em algumas empresas que precisavam ser arrançados na hora, e então trabalhar sob pressão ensinou-me bastante.

Relativamente ao projeto, senti algumas dificuldades no início por não ser um tema assim tão fácil de abordar, mas sinto que as superei e obtive um bom resultado com as explicações que fiz.

Gostaria de terminar este projeto lembrando que o conhecido Steve Jobs (fundador da Apple) antes de criar e de se concentrar na criação de um novo hardware e software iniciou as suas pesquisas como se fosse um hacker, no entanto resultou na criação de uma enorme empresa conhecida por todos, e que trabalha pela sua segurança diariamente.

Referências Bibliográficas

<https://www.eccouncil.org/ethical-hacking/>

<https://www.portalgsti.com.br/ethical-hacking/cursos/>

<https://www.galileu.pt/curso/ceh-ethical-hacking-and-countermeasures/>

<https://computerworld.com.br/2019/03/16/5-melhores-cursos-de-hacking-etico-e-certificacoes/>

<https://blog.varonis.com.br/ids-vs-ips-qual-a-diferenca/>

<https://www.portalgsti.com.br/profissoes-de-ti/hacker-etico/>

<https://www.portalgsti.com.br/ethical-hacking/sobre/>

<https://devqa.io/hacking-web-applications-methodologies/>

<https://www.lynda.com/IT-Infrastructure-tutorials/Ethical-Hacking-System-Hacking/476620-2.html>

<https://ilabs.eccouncil.org/hacking-web-servers/>

<https://www.greycampus.com/opencampus/ethical-hacking/introduction>

<https://www.guru99.com/how-to-hack-wireless-networks.html>

<https://www.csoonline.com/article/2124681/what-is-social-engineering.html>

<https://gbhackers.com/best-vulnerability-scanner/>

<https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/network-recon/what-is-vulnerability-identification/>

<https://www.eccouncil.org/programs/certified-network-defender-cnd/>

<https://minutodaseguranca.blog.br/as-10-melhores-ferramentas-de-verificacao-de-vulnerabilidades-para-testes-de-penetracao-2019/>

<https://blog.eccouncil.org/what-is-ethical-hacking/>

<https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>