ESCOLA NAVAL

talant de bien faire

Nuno Miguel Bicas Luís

Implementação do Cyber Range da Escola Naval: Uma Prova de Conceito

Dissertação para obtenção do Grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Alfeite
2023

ESCOLA NAVAL

talantde bienfaire

Nuno Miguel Bicas Luís

Implementação do Cyber Range da Escola Naval: Uma Prova de Conceito

Dissertação para obtenção do Grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Orientação de: Rui Miguel Soares Silva
Coorientação de: Vítor Sousa Lobo

O Aluno Mestrando,

Assinado por: **Nuno Miguel Bicas Luís**
Num. de Identificação: 15762378
Data: 2023.08.28 14:18:16 +0100

O Orientador,

Assinado por: **RUI MIGUEL SOARES SILVA**
Num. de Identificação: 09578584
Data: 2023.08.28 10:28:20 +0100

"The importance of epistemic security and cybersecurity is now comparable to that of national security."

(Roger Spitz)

Agradecimentos

A dissertação de mestrado marca o final do primeiro capítulo da formação de um Oficial de Marinha, terminando assim a formação base que o prepara para toda uma carreira de desafios. Gostaria assim de agradecer a todos os que contribuíram ao longo destes cinco anos para a minha formação, como pessoa e como militar, e que me prepararam para os desafios que se avizinham.

Em primeiro lugar gostaria de deixar os meus mais profundos agradecimentos ao Sr. Professor Doutor Rui Silva, pois sem ele esta dissertação não teria sido possível. Foi incansável ao longo deste ano, proporcionando me oportunidades de aprendizagem, como a frequência do Modulo de Introdução aos Testes de Penetração, da especialização em Ciberdefesa, do EMGFA, partilhando também a sua experiência profissional e pessoal, o que enriqueceu bastante o meu conhecimento.

Gostaria também de agradecer ao Sr. Professor Doutor Vítor Lobo pela disponibilidade, pela disponibilização de material para a elaboração da dissertação e pelas trocas de ideias que tivemos.

À Câmara de Oficiais do NRP *D. Francisco de Almeida*, que sempre me motivou a partilhar os progressos da minha dissertação durante o período de estágio, levando a que aprofundasse o meu conhecimento na área da cibersegurança. Um agradecimento especial ao 1TEN Martins Sobral e ao 1TEN Gaspar de Chaves pelas incontáveis conversas relativas à cibersegurança e a esta dissertação, fazendo com que me mantivesse motivado, desbloqueando também algumas ideias e problemas que surgiram durante a elaboração da dissertação.

Aos meus amigos e companheiros que sempre me apoiaram e me motivaram a chegar mais longe e dar o melhor de mim, desde os meus amigos de infância até aos meus grandes amigos que ganhei durante o meu percurso na Escola Naval.

À minha namorada e à minha família que não só durante o período de elaboração desta dissertação, mas também durante o meu percurso na Escola Naval, foram o meu porto de abrigo e me deram todo apoio que precisei, e que sem eles não teria atingido o sucesso e o objetivo final, alcançado com o término desta dissertação.

A todos vós, o meu mais sincero obrigado. Um bem-haja a todos.

Resumo

A sociedade encontra-se a atravessar a chamada era digital, estando esta bastante dependente da utilização da *Internet*. A *Internet* tornou-se vital em diversas áreas essenciais como a saúde, a educação e o setor financeiro. A enorme adesão à utilização da *Internet*, quase total nas sociedades mais evoluídas, leva também a que esta sirva de meio para a execução de atividades criminosas. Como tal, é necessário formar especialistas em cibersegurança e ciberdefesa, fornecendo-lhes os recursos necessários à sua formação.

Nesta dissertação irá ser desenvolvida uma solução *open source* que servirá o propósito de um *cyber range*, utilizando os equipamentos disponibilizados pela Escola Naval. Serão ainda desenvolvidos diversos cenários para treino em cibersegurança.

Será também abordada a visão do governo português relativamente ao ciberespaço, relacionando as suas diretivas com a edificação de novas estruturas e de novos organismos responsáveis pela cibersegurança e pela ciberdefesa em Portugal.

A solução construída constitui uma prova de conceito sobre o planeamento, a implementação e a administração de um *cyber range*, que dadas as limitações do equipamento disponibilizado, não foi possível de edificar. Esta é uma solução sim que permite a produção e recolha de dados relativamente ao tráfico de uma rede e à cibersegurança, assim como servir de meio de treino em segurança ofensiva.

Palavras-chave: cyber range; cibersegurança; ciberdefesa; Forças Armadas Portuguesas;

Abstract

Society is going through what is known as the digital era, and it is very dependent on the use of the Internet. The Internet has become vital in several essential areas such as health, education, and the financial sector. The huge adoption of Internet use, which is almost total in the most developed societies, has also led to it being used to carry out criminal activities. As such, it is necessary to train specialists in cybersecurity and cyberdefence, providing them with the necessary resources for their training.

This dissertation will develop an open-source solution that will serve the purpose of a cyber range, using the equipment provided by Escola Naval. Various scenarios will also be developed for cybersecurity training.

The Portuguese government's vision of cyberspace will also be addressed, relating its directives to the building of new structures and bodies responsible for cybersecurity and cyberdefence in Portugal.

The solution built is a proof of concept on the planning, implementation, and administration of a cyber range, which given the limitations of the equipment provided, it was not possible to build. This is a solution that enables the production and collection of data on network traffic and cybersecurity, as well as serving as a means of training in offensive security.

Keywords: cyber range; cybersecurity; cyberdefence; Portuguese Armed Forces

ÍNDICE

Índice de Gráficos

Índice de Figuras

Lista de Abreviaturas, Acrónimos e Símbolos

CEMGFA – Chefe do Estado-Maior-General das Forças Armadas

CLI – *Command Line Interface*

CNCS – Centro Nacional de Cibersegurança

CR – *Cyber Range*

CRaaS – *Cyber Range as a Service*

CSIRT – Centro Nacional de Cibersegurança

CSSC – Conselho Superior de Segurança no Ciberespaço

DDoS – *Distributed Denial of Service*

DNS – *Domain Name System*

DoS – *Denial of Service*

ENCD – Estratégia Nacional de Ciberdefesa

ENSC – Estratégia Nacional de Segurança no Ciberespaçp

GUI – *Graphic User Interface*

HDD – *Hard Disk Drive*

HTTP – *Hypertext Transfer Protocol*

IC3 – *Internet Crime Complaint Center*

IETF – *Internet Engineering Task Force*

IP – *Internet Protocol*

KVM – *Kernel-based Virtual Machine*

LAN – *Local Area Network*

MAC – *Medium Access Control*

MAN – *Metropolitan Area Network*

MitM – *Men-in-the-Middle*

NATO – *North Atlantic Treaty Organization*

OSI – *Open Systems Interconnection*

OSINT – *Open Source Intelligence*

OVA – *Open Virtual Appliance*

RAM – *Random-Access Memory*

SECGEN – *Security Scenarios Generator*

SMS – *Short Message Service*

SO – Sistema Operativo

SRI - Segurança das Redes e da Informação

SVED – *Scanning, vulnerabilities, exploits and detection*

TCP – *Transmission Control Protocol*

VE – *Virtual Environment*

VoIP – *Voice over IP*

VPN – *Virtual Private Network*

WAN – *Wide Area Network*

Introdução

A utilização da *Internet* sofreu um crescimento exponencial desde os seus primórdios, tendo a sua origem na década de 1980, derivada de um projeto que decorreu nos Estados Unidos da América na década de 1960. Deste então esta veio a tornar-se cada vez mais importante e presente no quotidiano da população mundial. Segundo a *Internet World Stats*, o gráfico 1 demonstra o crescimento da utilização da *Internet* desde 1995 até 2022,

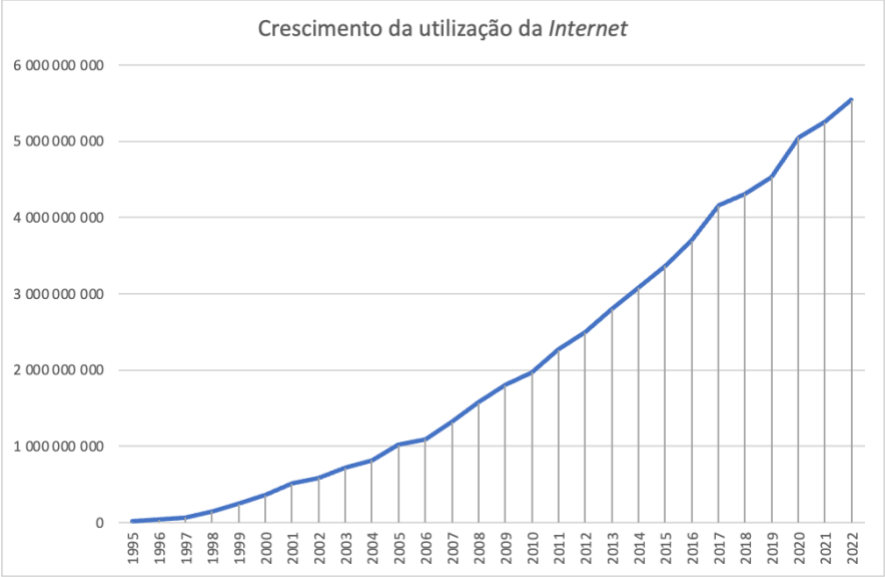

Gráfico 1 - Crescimento da utilização da Internet

A *Internet* veio possibilitar, devido à sua enorme utilização, a conexão entre sistemas e pessoas por todo o mundo, tornando possível realizar uma enorme quantidade de operações do dia-a-dia de forma remota. A *Internet* revolucionou diversas áreas tais como o mercado de trabalho, os métodos de aprendizagem, com as diversas academias *on-line* e até mesmo nas ditas universidades tradicionais, permitindo métodos como o ensino à distância e o *e-learning*. Revolucionou ainda áreas de extrema importância como o setor bancário, da saúde e da tecnologia.

Como seria de esperar, com toda a utilização deste valioso recurso e com toda a importância que ele representa, especialmente nas sociedades mais evoluídas como a que fazemos parte, abre-se uma janela de oportunidade para as práticas criminosas. A utilização da *Internet* acarreta atualmente diversos perigos, os quais serão abordados mais adiante.

O número de ciberataques e a sua complexidade têm evoluído ao longo dos anos, e em sociedades com uma grande dependência da *Internet*, estes têm particular relevância. A avassaladora quantidade de recursos muitas vezes essenciais no dia-a-dia que estão dependentes da mesma leva a que, combinada com a escassez de profissionais qualificados na área da cibersegurança, existam falhas de segurança, as chamadas vulnerabilidades, que podem ser exploradas pelos atacantes. Estes ataques têm frequentemente motivos financeiros ou de roubo de informação, visando tanto indivíduos como organizações. O Gráfico 2 apresenta o prejuízo financeiro causado pelos ciberataques entre 2001 e 2022, segundo o *Internet Crime Complaint Center* (IC3) do FBI, que demonstra o efeito, a nível financeiro, que estes ataques têm causado.

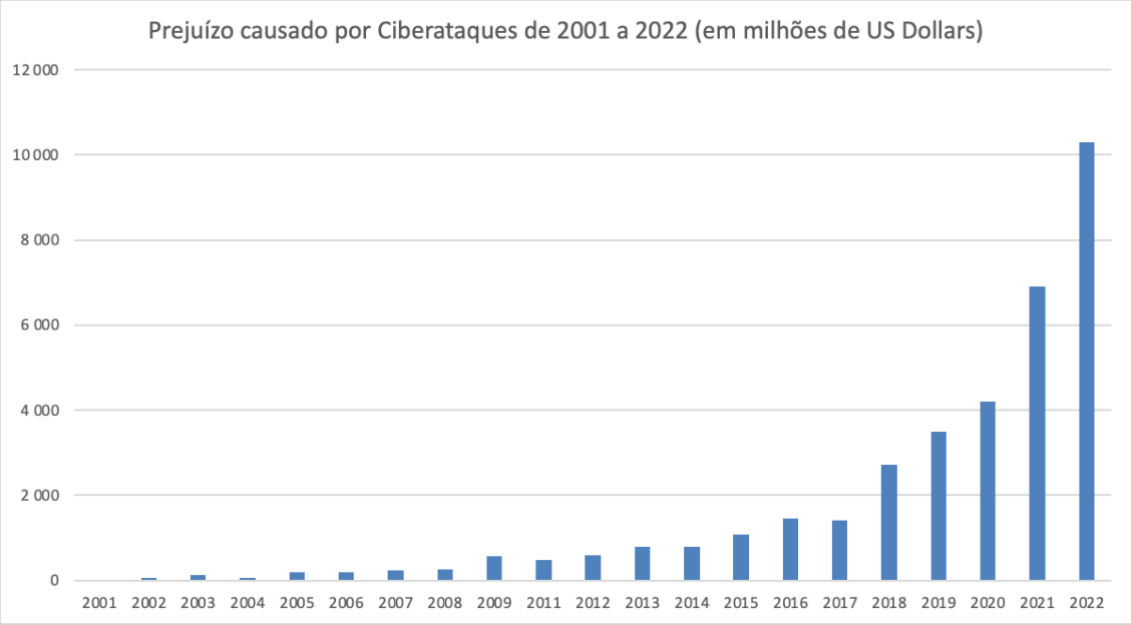

Gráfico 2 - Prejuízo causado por Ciberataques de 2001 a 2022 (em milhões de US Dollars)

A sociedade encontra-se, cada vez mais, na chamada era digital, pelo que se torna vital a proteção contra os agentes maliciosos. Cada vez mais os ciberataques deixam de ser meros incidentes isolados, passando a ser mais persistentes e em constante evolução e desenvolvimento. A utilização de equipamento e software de cibersegurança topo de gama tem-se revelado insuficiente pelo que se torna necessária a compreensão das táticas utilizadas pelos agentes maliciosos para perpetrarem estes ataques.

É no sentido deste último ponto que se pretende, no âmbito desta dissertação, o desenvolvimento de um *cyber range*, uma ferramenta poderosa e essencial para o treino e recolha de dados relativos aos ciberataques, onde se podem testar vários sistemas e táticas, tanto de forma ofensiva como defensiva, o que se prevê que seja da maior utilidade para as Forças Armadas Portuguesas.

Esta dissertação tem como objetivo o estudo do processo de construção e emprego de um *cyber range*, na Escola Naval, assim como a criação de cenários de teste que poderão ser utilizados futuramente.

A presente dissertação apresenta a seguinte estrutura:

- Introdução: A introdução apresenta uma visão geral sobre a utilização da *Internet* e os ciberataques provenientes desta mesma utilização, apresentando alguns dados estatísticos, assim como o objetivo da mesma.
- Capítulo 2: Neste capítulo apresenta-se uma revisão de literatura, contendo diversos conceitos presentes nesta dissertação, assim como subcapítulos dedicados exclusivamente aos ciberataques, aos *cyberranges* e aos hipervisores.
- Capítulo 3: É apresentada a orgânica institucional a nível nacional, assim como a natureza e a missão da ciberdefesa, aos olhos do Governo Português.

- Capítulo 4: Apresenta a construção da solução, visando o equipamento e a arquitetura da solução. Será ainda objeto de estudo a criação de cenários e o modelo de utilização da solução.
- Capítulo 5: São apresentados tanto o software utilizado na solução como os cenários de teste, assim como a sua implementação e os testes realizados.
- Conclusões e Trabalhos Futuros: Na conclusão são apresentadas as ilações baseadas nos resultados obtidos e também hipóteses de trabalhos futuros a serem desenvolvidos com recurso à solução criada.

1. Revisão de Literatura

A revisão da literatura foi crucial para a elaboração desta dissertação, dado que o seu tema é completamente diferente das matérias lecionadas durante o Mestrado Integrado em Ciências Militares Navais - Ramo de Marinha. Ao longo deste capítulo, serão explicados os temas fundamentais e as áreas de investigação e aprendizagem, bem como serão definidos alguns conceitos presentes nesta dissertação.

1.1. Conceitos

1.1.1. Redes: O que são e como são constituídas?

No contexto da informática e das telecomunicações, uma rede refere-se a um conjunto de dispositivos interligados, como computadores, servidores, *routers*, *switches* e outros componentes de *hardware*, que estão ligados entre si para facilitar a comunicação e a partilha de recursos (Kurose & Ross, 2017).

De acordo com Tanenbaum e Wetherall (2011), as redes podem ser classificadas em vários tipos com base na sua escala, cobertura geográfica e objetivo. Alguns dos tipos mais comuns de redes são:

Rede Local: Uma LAN (*Local Area Network*) é uma rede que abrange uma área relativamente pequena, como uma casa, um escritório ou um navio. São normalmente privadas e ligam dispositivos muito próximos, permitindo taxas de transferência de dados rápidas e uma partilha de recursos eficiente. Quando as LANs são utilizadas por empresas, são designadas por Redes Empresariais. As LANs sem fios são outro tipo de LANs e são muito populares atualmente, porque não é necessário instalar cabos para ligar os dispositivos à rede.

Rede de Área Metropolitana: Uma MAN (*Metropolitan Area Network*) cobre uma cidade. Um bom exemplo deste tipo de rede são as redes de televisão por cabo que existem em muitas cidades.

Rede de área alargada: Uma WAN (*Wide Area Network*) abrange uma área geográfica maior, como vários escritórios ou cidades. Utiliza ligações de comunicação públicas ou privadas, como linhas alugadas ou a Internet, para ligar dispositivos a longas distâncias.

Internet: A *Internet* é uma rede global que conecta milhões de dispositivos globalmente e permite a troca de informações e serviços entre diferentes redes e baseia-se no conjunto de protocolos TCP/IP.

Existem vários componentes que constituem uma rede, e cada um deles tem um papel importante para que a comunicação aconteça. Alguns dos principais componentes são (Meyers, 2018):

- Dispositivos ou nós: São os dispositivos que estão ligados à rede, como computadores, impressoras, *switches*, *routers*, servidores e todo o tipo de dispositivos que é possível ligar a uma rede. Todos estes dispositivos são identificados na rede pelo seu endereço IP e pelo seu endereço MAC. O endereço IP e o endereço MAC são únicos para cada dispositivo, sendo o endereço IP relacionado com a própria rede e o endereço MAC relacionado com o dispositivo.

- Ligações e conexões: Referem-se às ligações físicas e lógicas entre os dispositivos. Essas ligações podem ser com fios, através de cabos de cobre de pares entrelaçados ou cabos de fibra ótica. As ligações também podem ser sem fios, utilizando ligações Wi-Fi ou móveis.

- Infraestrutura de rede: Para além de serem considerados um nó, dispositivos como *switches*, *routers* ou pontos de acesso são cruciais e

permitem a conetividade da rede. Têm a função de direcionar o tráfego e garantir que os dados chegam ao destino pretendido.

- Protocolos: As redes utilizam protocolos para definir regras e normas de comunicação. Os protocolos garantem que os dispositivos podem compreender e trocar dados de forma consistente e fiável. A *Internet Engineering Task Force* (IETF) é responsável pelo desenvolvimento e manutenção de muitos dos protocolos da Internet.

Existem outras funcionalidades importantes que podem ser utilizadas nas redes, como as *Virtual Private Networks* (VPN) ou as *firewalls*, que aumentam a segurança e a privacidade da rede, que são valiosas e de extrema importância nos dias de hoje.

1.1.2. Príncipios de uma rede

O modelos *Open Systems Interconnection* (OSI) e *Transmission Control Protocol/Internet Protocol* (TCP/IP) são dois modelos concetuais diferentes utilizados para compreender e descrever a forma como diferentes protocolos e tecnologias de rede funcionam em conjunto para permitir a comunicação entre dispositivos numa rede.

a) Modelo OSI

A Organização Internacional de Normalização, ISO, definiu uma arquitetura comum na qual os computadores podem ser ligados. Esta arquitetura, o modelo OSI, define uma rede em sete camadas (Peterson & Davie, 2012). As sete camadas são:

1. Camada física: A camada física é responsável pela transmissão e receção de *raw data bits*. É responsável pela conversão de *bits* em sinais elétricos ou óticos e vice-versa.

2. *Data Link Layer*: Estabelece ligações lógicas entre dispositivos e trata da deteção e correção de erros, tornando a transferência de dados fiável.

3. Camada de rede: A camada de rede fornece encaminhamento lógico ponto-a-ponto de dados entre várias redes. Determina o caminho otimizado para a transmissão de dados e trata do controlo dos congestionamentos.

4. Camada de transporte: A função básica da camada de transporte é receber dados das camadas superiores e dividi-los em unidades mais pequenas, chamadas de segmentos, e garantir que todos os segmentos chegam corretamente ao destino.

5. Camada de sessão: A camada de sessão é responsável por permitir que os utilizadores de máquinas diferentes estabeleçam sessões entre si. As sessões são importantes porque são responsáveis pelo controlo do diálogo, pela gestão dos *tokens* e pela sincronização.

6. Camada de apresentação: A camada de apresentação é diferente das outras. Não é responsável pela transmissão dos dados, mas sim pela sua semântica e sintaxe. Torna os dados legíveis para computadores com diferentes estruturas de dados.

7. Camada de aplicação: A camada de aplicação interage diretamente com as aplicações do utilizador final. Fornece serviços e protocolos de rede que permitem que as aplicações comuniquem entre si através da rede.

b) Modelo TCP/IP

O modelo de referência TCP/IP foi descrito pela primeira vez por Cerf e Kahn (1974) e posteriormente aperfeiçoado, tornando-se um padrão na comunidade da Internet, por Braden, em 1989. Este modelo nasceu da preocupação do Departamento de Defesa dos EUA (DoD) de que a União Soviética atacasse o país e que a sua rede não pudesse suportar a perda de hardware sem que as ligações fossem interrompidas. O DoD queria que as ligações permanecessem activas mesmo que algumas das máquinas ou linhas de transmissão não estivessem a funcionar (Tanenbaum & Wetherall, 2011).

O modelo TCP/IP é composto por quatro camadas, em vez de sete como no modelo OSI. As quatro camadas estão interligadas e são semelhantes ao modelo OSI e são:

1. Camada de ligação: O objetivo da camada de ligação, também referida como camada de interface de rede (Kozierok, 2005), é "comunicar na sua rede diretamente ligada". Contém os protocolos necessários para que os dispositivos comuniquem dentro da mesma rede.

2. Camada de Internet: A camada Internet corresponde à camada de rede no modelo OSI. O principal objetivo desta camada é o endereçamento lógico de dispositivos, usando o Protocolo de Internet (IP), o empacotamento, a manipulação e a entrega de dados e o roteamento (Kozierok, 2005). O IP é um protocolo *best-effort*, pelo que não garante que as unidades de dados do protocolo, comummente designadas por Pacotes, cheguem ao seu destino, ou que cheguem em ordem ou em boas condições. Como tal, são as camadas superiores as responsáveis pela fiabilidade da entrega.

3. Camada de transporte: A camada de transporte fornece serviços de comunicação ponto-a-ponto, utilizando dois protocolos: *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP) (Braden, 1989).

4. Camada de aplicação: A camada de aplicação é a camada superior do modelo TCP/IP e é equivalente às camadas de sessão, apresentação e aplicação no modelo OSI. Nesta camada, existem protocolos que fornecem serviços diretamente ao utilizador e protocolos de suporte que fornecem funções comuns do sistema (Braden, 1989).

1.2. Ciberataques

Atualmente, devido à sua elevada prevalência, os ciberataques tornaram-se uma ameaça crítica e real para as civilizações modernas, que dependem de ativos informáticos. A maioria dos funcionários dos governos e das organizações depende de plataformas digitais e de computadores para fazer o seu trabalho. O ordinário perfil de qualquer colaborador é considerado vulnerável perante possíveis ataques, sendo considerado um risco para a sua entidade empregadora.

Os actores maliciosos exploram as fragilidades dos colaboradores para acederem aos dados ou serviços da organização ou mesmo para perturbarem o serviço que é prestado, tornando-o inacessível a quem quer ou precisa de aceder (White, Conklin, Cothren, Williams, & Davis, 2021).

Uma forma comum de o fazer é através de um ataque de negação de serviço, normalmente conhecido como DoS (*Denial of Service*). No ataque DoS, o atacante impede que utilizadores autorizados acedam a um sistema ou rede de computadores ou acedam a informações, colocando o sistema offline. Isso também pode ser feito enviando um grande número de solicitações, fazendo com que a máquina não

consiga responder a nenhuma outra solicitação (White, Conklin, Cothren, Williams, & Davis, 2021). Este tipo de ataque sobrecarrega os recursos do sistema de modo que este não possa responder ao pedido de serviço (Biju, Gopal, & Prakash, 2019).

Múltiplas máquinas de ataque podem melhorar este tipo de ataque e torná-lo ainda mais poderoso. São os chamados ataques distribuídos de negação de serviço, ou *Distributed Denial of Service Attacks* (DDoS).

As organizações e os governos também são susceptíveis a outros tipos de ataques, especialmente devido à falta de sensibilização dos seus funcionários para a cibersegurança. Isto leva os funcionários a cometerem quebras de segurança, as quais os atacantes podem explorar facilmente. Uma forma muito comum de o fazer é através da engenharia social.

Este capítulo aborda os diferentes tipos de ataques, dá alguns exemplos e fornece uma descrição do método de ataque.

1.2.1. Engenharia Social

Quando os atacantes utilizam pessoas como alvos durante os seus ataques, denomina-se Engenharia Social. É normalmente uma fase do ataque, durante as etapas iniciais, mas que é utilizada para iniciar os ciclos de ataque. Envolve manipulação e, muitas vezes, a falta de consciência do perigo por parte das vítimas.

Alguns métodos de engenharia social muito utilizados são o *Phishing*, o *Spear Phishing*, o *Smishing* e o *Vishing*.

a) *Phishing*

O phishing é um tipo de engenharia social em que o atacante tenta obter informações sensíveis dos utilizadores fazendo-se passar por uma entidade de confiança num correio eletrónico ou em mensagens instantâneas enviadas a um grande grupo de utilizadores, muitas vezes escolhidos aleatoriamente (White, Conklin, Cothren, Williams, & Davis, 2021). O principal objetivo do atacante é

recolher o maior número possível de nomes de utilizador, palavras-passe, números de cartões de crédito e outras informações para as poder utilizar ou vender mais tarde. São utilizados frequentemente clones de *websites* de confiança para que, quando as vítimas clicam no *link* enviado no correio eletrónico, este pareça mais fiável e as faça acreditar na "falsa autenticidade", fornecendo as informações ao atacante.

b) *Spear Phishing*

Quando um ataque de *phishing* é direcionado para uma pessoa ou grupo específico, é designado de *Spear Phishing*. O rácio de ataques bem-sucedidos aumenta em comparação com os ataques de *phishing* porque as mensagens enviadas são mais plausíveis devido a serem enviadas para uma pessoa ou grupo específico em vez de um grande número de utilizadores aleatórios.

c) Smishing

O smishing é um ataque que utiliza o *Short Message Service* (SMS) nos telemóveis das vítimas. É como um ataque de *phishing*, mas enviado por SMS. Pode servir vários vetores de ataque. A mensagem contém uma hiperligação na qual a vítima é orientada a aceder. Esta ligação pode levar a uma página onde a vítima fornece as suas informações ao atacante, ou descarrega malware para o dispositivo que permite ao atacante obter acesso remoto ao dispositivo através de uma *Remote Shell* (White, Conklin, Cothren, Williams, & Davis, 2021).

d) Vishing

O vishing é uma variação do phishing que utiliza a tecnologia de comunicação por voz para obter as informações que o atacante procura, aproveitando-se da confiança que as pessoas têm na rede telefónica. Os atacantes simulam chamadas de entidades legítimas utilizando a tecnologia Voice Over IP (VoIP) (White, Conklin, Cothren, Williams, & Davis, 2021). Um exemplo deste tipo de ataque é uma chamada

em que o atacante finge ser funcionário de um banco para tentar obter as credenciais da conta bancária da vítima ou o número do seu cartão de crédito.

1.2.2. Ataques de Password

O nome de utilizador e a palavra-passe são uma das formas de autenticação mais utilizadas e, se não forem configurados corretamente, a combinação pode ser atacada de várias formas. Os ataques às palavras-passe baseiam-se na falta de conhecimento da vítima e no facto de não seguir bons procedimentos na configuração das palavras-passe. Alguns ataques que tiram partido deste facto são ataques como *spraying*, ataques de dicionário e ataques de força bruta.

a) Spraying

O password spraying é um ataque que testa um número limitado de palavras-passe frequentemente utilizadas e aplica-as a um grande número de contas (White, Conklin, Cothren, Williams, & Davis, 2021). Este método é vantajoso quando o objetivo é obter acesso à organização ou à rede, sendo que é considerado irrelevante em que conta o atacante obtém acesso.

b) Ataques de Dicionário

Os ataques de dicionário são amplamente utilizados e são efectuados através de um programa de quebra de palavras-passe, como o *John the Ripper* ou o *Hydra*, que utilizam uma lista de palavras e uma lista de utilizadores, ou apenas um único utilizador, e tenta fazer corresponder as palavras-passe da lista de palavras ao *hash* da palavra-passe do utilizador.

As listas de palavras funcionam melhor e obtêm melhores resultados quando são dirigidas a um grupo específico de utilizadores, quando o atacante conhece os seus interesses e outras informações sobre os alvos, ou quando há uma fuga de palavras-passe. Existem também *wordlists* conhecidas, como a *Rock You Wordlist*, em

que são combinadas várias fugas de palavras-passe e palavras-passe adivinhadas, bem como as palavras-passe mais utilizadas.

Há uma quantidade significativa de pessoas que utilizam os seus nomes, as suas datas de nascimento e os nomes dos seus animais de estimação nas suas palavras-passe, o que pode ser facilmente decifrado pelos cibercriminosos. Com o crescimento exponencial das redes sociais e o facto de as pessoas publicarem tudo sobre as suas vidas e informações pessoais na maioria dos casos, os atores maliciosos têm a oportunidade de procurar OSINT (*Open Source Intelligence*) e construir autonomamente uma lista de palavras com todas estas informações que estão abertamente disponíveis à distância de um clique. Existem ferramentas como o Maltego, que é um poderoso *software* de recolha de informações que pode procurar ainda mais profundamente a vida das vítimas.

c) Ataques de Força Bruta

Um ataque de força bruta é utilizado quando não existe correspondência para a palavra-passe nas listas de palavras-passe e é efectuado por programas que tentam todas as combinações possíveis (White, Conklin, Cothren, Williams, & Davis, 2021).

É por isso que é importante ter uma política eficaz e rigorosa sobre a configuração das palavras-passe, utilizando caracteres alfanuméricos e símbolos, bem como desactivando nomes conhecidos e palavras-passe que se assemelhem ao nome de utilizador. O comprimento da palavra-passe também é importante porque quanto maior for, mais difícilmente será descoberta.

1.2.3. *Man-in-the-middle Attack*

Um ataque man-in-the-middle (MitM) ocorre quando um ator malicioso intercepta a comunicação entre um cliente e um servidor. O cibercriminoso faz-se

passar pelo cliente e pelo servidor ao mesmo tempo para ter acesso a toda a informação que está a ser partilhada entre ambos. Estes ataques podem ser efectuados através de sequestro de sessão e de IP *Spoofing.*

1.2.4. Client-side Attacks.

Os ataques *client-side*, como o nome sugere, são efetuados a partir do computador da vítima. Estes ataques podem ser realizados através de vários métodos e são utilizados contra máquinas que tenham sido bem configuradas e que não tenham uma vulnerabilidade que o agente da ameaça possa explorar remotamente. As bases deste tipo de ataque assentam na engenharia social, de modo que o hacker consiga colocar o software malicioso, ou malware, na máquina da vítima e fazer com que esta execute o malware.

O *malware* é frequentemente incluído num ficheiro executável, com um *payload* que gera uma sessão para a máquina do atacante, com uma *remote shell*, e está disfarçado de *software* fiável de empresas muito conhecidas. O atacante pode enviar uma ligação à vítima para descarregar o ficheiro através de correio eletrónico, fingindo ser, por exemplo, uma empresa de antivírus, para descarregar a versão mais recente do seu software e, quando a vítima executa o ficheiro de instalação, este gera automaticamente a *reverse shell*. Em seguida, o atacante, utilizando por exemplo a *MSFconsole* da Metasploit, poderá gerar uma *reverse Shell e* tentar aumentar os privilégios para *root* ou administrador e, em seguida, instala uma *backdoor* na máquina da vítima, de modo que, sempre que a vítima inicie a sua sessão, seja gerada uma *reverse shell* para a máquina do atacante.

Este tipo de *malware* é criado utilizando o *MSFvenom por exemplo*, uma ferramenta do *Metasploit Framework* que surgiu para substituir o *MSFencode* e o *MSFpayload*, e que permite ao utilizador gerar um *payload*, colocá-lo dentro do software legítimo e depois codificar a sequência de bits do *payload* de forma a torná-lo indetetável para o antivírus. Os *encoders* que apresentam os melhores resultados

são o *Shikata Ga Nai*, para arquitecturas de 32 bits, e o *Zutto Dekiru* e *o Xor Context* para arquitecturas de 64 bits.

Alguns dos tipos mais comuns de *malware* são os *Trojans, Worms, Spyware, Ransomware, Keyloggers e Rootkits.*

a) Trojans

Os cavalos de Troia, ou *trojans*, são softwares que aparentam ser legítimos, como já mencionado anteriormente, como uma instalação de *software*, mas possuem outras funcionalidades ocultas. É um programa autónomo que tem de ser copiado e instalado por um utilizador autorizado, sendo feito uso de engenharia social na vítima por parte do atacante. (White, Conklin, Cothren, Williams, & Davis, 2021).

b) Worms

Os *worms* são pedaços de código que tentam penetrar numa rede ou num sistema informático. Quando isso acontece, o *worm* faz uma cópia de si próprio no sistema penetrado (White, Conklin, Cothren, Williams, & Davis, 2021). Atualmente, os *worms* são muito utilizados em ataques de *ransomware*, uma vez que se propagam de sistema para sistema sem a intervenção do atacante.

c) Ransomware

O *ransomware* é uma forma de *malware* que normalmente encripta ficheiros num sistema, tornando-os ilegíveis e inacessíveis ao utilizador (White, Conklin, Cothren, Williams, & Davis, 2021). Normalmente, este tipo de ataque é realizado com o fim de pedir um resgate pelos ficheiros. Os atacantes exigem então o pagamento para devolver as chaves de encriptação para desencriptar os ficheiros. A única forma de reparar este tipo de danos é reconstruir o sistema, o que pode ser moroso e, por vezes, impossível.

d) Spyware

O *spyware* é um *software* destinado a recolher informações sobre o utilizador, registando toda a atividade da máquina. Destina-se a espiar o utilizador sem o conhecimento da vítima (White, Conklin, Cothren, Williams, & Davis, 2021). O *spyware* monitoriza todo o sistema, mostrando ao atacante como as vítimas utilizam outro software e pode até gravar as teclas premidas, funcionando como um *keylogger*.

e) Keyloggers

Os *keyloggers* são um tipo de *software* que regista as teclas premidas no computador da vítima. Os atacantes podem então descobrir as credenciais do utilizador para iniciar sessão em várias plataformas, garantindo um acesso fácil à informação.

Os *keyloggers* só são considerados *malware* se a sua utilização for desconhecida do utilizador e se não estiver sob o seu controlo (White, Conklin, Cothren, Williams, & Davis, 2021).

f) Rootkits

Os *rootkits* são um tipo de *malware* que funciona como uma ferramenta administrativa do sistema operativo e são concebidos para modificar o seu funcionamento. Os *rootkits* apresentam as mesmas funcionalidades que o sistema operativo (SO). Permitem que os atacantes utilizem uma parte de um computador sem que o utilizador ou outras aplicações o detetem (White, Conklin, Cothren, Williams, & Davis, 2021).

1.3. Hypervisores

As tecnologias de virtualização têm desempenhado um papel significativo nos últimos anos, e o número de soluções de software nesta área tem vindo a crescer rapidamente. Uma das razões para a adoção e implementação de tecnologias avançadas neste domínio é a necessidade de acompanhar a crescente quantidade de dados trocados e a consequente necessidade de aumentar a capacidade dos centros de dados através da virtualização de servidores.

As principais vantagens da virtualização incluem a capacidade de funcionar independentemente do hardware, o isolamento de ambientes, ambientes de utilizador seguros e maior escalabilidade. Além disso, várias novas funcionalidades são otimizadas para diferentes casos de utilização. Como resultado, este tipo de solução tornou-se muito atrativo e competitivo, levando ao desenvolvimento de novas soluções nas duas principais categorias de tecnologias de virtualização: virtualização baseada em contentores e virtualização baseada em hipervisor (Morabito, Kjällman, & Komu, 2015).

1.3.1. Bare Metal vs Hipervisor Alojado

Um hipervisor é um tipo de software de virtualização que permite a criação de máquinas virtuais, separando o software de um computador do seu hardware. Os hipervisores atuam como um tradutor de pedidos entre recursos físicos e virtuais (VMware, 2023).

Um hipervisor que é instalado diretamente no *hardware* é designado por hipervisor *bare metal* ou hipervisor de tipo 1. Estes são instalados no mesmo nível que o BIOS da *motherboard*. Uma vez que está instalado no *hardware*, tira o máximo partido dos recursos do sistema.

Os hipervisores do tipo 1 suportam a migração de máquinas virtuais, sendo possível movê-las para outros servidores ou computadores dentro da rede sem necessidade de parar outras máquinas virtuais nos servidores (Walleit, 2022).

Um hipervisor que é instalado no SO é designado por hipervisor alojado ou hipervisor de tipo 2. Partilha recursos com o SO, afetando o desempenho das máquinas virtuais, mas funciona da mesma forma que o hipervisor de tipo 1, virtualizando recursos para criar máquinas virtuais (Walleit, 2022).

1.4. Cyber Ranges

O crescente aumento do cibercrime assim como a sua diversidade de táticas inovadoras e emergentes têm causado prejuízos à escala global e como tal, as organizações têm cada vez mais a necessidade de se proteger, numa sociedade cada vez mais imersa na era digital e dependente das tecnologias de comunicação.

Cada vez mais a utilização de software de proteção, como é o caso dos antivírus, por si só, se torna incapaz de proporcionar uma boa capacidade de defesa. Se antigamente se considerava o utilizador dos sistemas como apenas uma ligação vulnerável, atualmente o paradigma da cibersegurança é bem diferente. O utilizador é, hoje em dia, considerado mais uma camada de defesa, mas para que isso aconteça de forma eficiente, é necessário treinar o utilizador para que ele consiga prever as cyber-ameaças e gerir os ataques à infraestrutura (Vozikis, et al., 2020), passando a garantir assim um maior conhecimento situacional, reforçando a segurança da organização.

É precisamente neste ponto em que os *cyber ranges* (CR) se tornam fulcrais para as organizações.

1.4.1. O que é um *cyber range*?

Um *cyber range*, na sua conceção, é um sistema que providencia protótipos de várias complexidades de situações de cibersegurança, como é o caso dos ciberataques e da ciberguerra. Estes têm o propósito de treino ao nível da cibersegurança, de servir como um ambiente de pesquisa e investigação e também

ao nível do ensino, onde se pode ensinar acerca da gestão de incidentes assim como a resposta aos mesmos.

Um CR ideal é um sistema que, simultaneamente (Urias, Stout, Van Leeuwn, & Lin, 2018):

- Fornece *feedback* instantâneo através de uma simulação fiável,
- Fornece configurações virtuais onde várias equipas possam executar o seu treino,
- Fornece um ambiente de investigação onde várias equipas podem testar as suas estratégias,
- Fornece métricas de avaliação baseadas no desempenho.

Os CRs têm a capacidade de providenciar arenas para uma simulação dinâmica, acesso aos participantes, infraestrutura e cenários técnicos para serem conduzidos exercícios de cibersegurança, sendo estes cruciais para o treino e para testar a resiliência dos membros da organização (Pandey & Ahmad, 2022).

Os cyber ranges podem ser acedidos na forma de um serviço, sendo estes chamados de *Cyber Range as a Service,* CRaaS. Existem empresas que são proprietárias destes CRs e fazem toda a sua administração, fornecendo vários modelos, com as mais diversas funcionalidades e capacidades, consoante a necessidade do cliente. Estes CRs são inteiramente desenvolvidos na *cloud* e são acedidos remotamente pelo cliente (Formento & Cerini, 2022).

Os CRs se forem alojados dentro de um espaço físico da organização são denominados de CRs locais (Pandey & Ahmad, 2022). Comparando com os serviços de CR baseados na *cloud*, estes são bastante mais dispendiosos, pois compreendem todo o *hardware* e *software* necessários à construção do mesmo, um espaço físico onde é realizada a instalação, assim como salas próprias para executar *briefings* e *debriefings*, sendo assim adequados para satisfazer as necessidades de segurança da organização, obtendo esta um controlo reforçado dos exercícios e da implantação dos recursos desejados.

1.4.2. Tipos de cyber ranges

Os CRs podem ter diferentes tipos baseados no *hardware* e no *software* que utilizam e se utilizam tecnologias de virtualização ou não. Os tipos de CRs que existem são os físicos, os virtuais e os híbridos (Pandey & Ahmad, 2022).

CRs físicos são caracterizados por criarem um protótipo de uma rede ou infraestrutura com recurso a equipamento por forma a imitar uma rede já existente ou testar novas ideias.

Quando se utilizam tecnologias de virtualização para simular toda a infraestrutura, os CR são então virtuais. Todos os componentes desta infraestrutura são emulados com recurso a máquinas virtuais que utilizam a tecnologia *Software Virtual Network* na sua essência, o que permite a caracterização da estrutura da rede com um elevado grau de fiabilidade (Wihl & Varshney, 2012)

Se é um sistema que utiliza tanto infraestruturas físicas como tecnologias de virtualização, é considerado um CR híbrido, sendo também apelidado de *cyber-physical range*. Neste tipo de CR ambos os elementos físicos e virtuais são implementados e utilizados mediante a necessidade do utilizador (Pandey & Ahmad, 2022).

Um exemplo da utilização de um sistema desta tipologia é a utilização de um sistema virtual Windows ou Linux com uma ligação física a um dispositivo de videovigilância.

Os CRs híbridos são também utilizados pelos sistemas de abastecimento de água e pelas centrais de produção de energia elétrica.

1.4.3. Casos de utilização dos *cyber ranges*

Os CRs são ferramentas eficazes para as organizações para o treino dos seus membros, para executar testes de cibersegurança, analisar componentes com falhas e também as falhas no sistema, assim como cultivar a ética de trabalho em equipa.

As organizações ao nível empresarial têm nos CRs ferramentas bastante importantes, os quais utilizam para testar as capacidades de um novo software, testar produtos e ainda testar uma reorganização a nível organizacional.

Estas organizações utilizam ainda os CRs para preparar as suas equipas de cibersegurança para diversos cenários assim como para desenvolverem as suas capacidades pessoais.

Os CRs são também bastante utilizados academicamente, onde professores os utilizam como um suporte para a aprendizagem na sala de aula e onde os estudantes podem utilizar os CRs para gerarem e recolherem dados, adquirir "*cyber-skills*" e trabalhar em equipa para responder a ciberataques.

1.4.4. Soluções Existentes

Inúmeros são os casos de utilização dos CRs e como tal, existem já variadas soluções criadas, em Portugal e no mundo, dada a importância da cibersegurança e também da ciberdefesa na sociedade.

Empresas como a EDP criaram, em 2016, um CR com a finalidade de sensibilizar o maior número de colaboradores da EDP para os perigos do ciberespaço e também disponibilizar ferramentas e informações para prevenir possíveis ataques.

Este é constituído por um laboratório de segurança, uma arena para exercícios de cibersegurança e uma academia de formação.

Em 2017, o Exército Português recorreu à plataforma de treino FEE(P) Cyber Range, da Indra, que serviu de apoio ao exercício Ciber Perseu 2017, o que permitiu simular ambientes operacionais reais para formação e treino de profissionais, assim como experimentar, testar e validar novos conceitos, tecnologias, técnicas e táticas de cibersegurança e ciberdefesa.

O Centro de Ciberdefesa do Estado-Maior General das Forças Armadas é também detentor de um CR topo de gama, com uma capacidade mínima de alocar 300 máquinas virtuais em simultâneo, permitindo 30 utilizadores com 10 máquinas cada um ou 60 utilizadores com 5 máquinas cada um, o que permite uma grande capacidade de formação e de investigação.

A NATO possuí também um CR, em Tallin, Estónia, desenvolvido pela CR14, uma empresa criada pelo Ministério da Defesa Estónio, onde são conduzidos e desenvolvidos os maiores exercícios de ciberdefesa da NATO.

A NATO partilha este CR com a CR14 desde a Cimeira da NATO no País de Gales, em 2014.

2. Cibersegurança e Ciberdefesa em Portugal

2.1. Orgânica Institucional

Ao nível nacional têm sido desenvolvidos inúmeros esforços em relação à cibersegurança e no combate ao cibercrime. Estes esforços vêm no sentido de acompanhar as diretivas da União Europeia, as diretivas relativas à Segurança das Redes e da Informação (SRI). Estas diretivas constituíram a primeira medida legislativa ao nível da União Europeia, tendo como objetivo reforçar a cooperação entre os Estados-Membros, estabelecendo também as obrigações de segurança a cumprir pelos operadores de serviços essenciais nos setores dos transportes, da energia, da saúde e das finanças, sendo considerados setores críticos.

A Lei nº46/2018, de 13 de agosto, estabelece a estrutura de segurança no ciberespaço em Portugal sendo esta constituída pelo Conselho Superior de Segurança no Ciberespaço (CSSC), órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço e pelo Centro Nacional de Cibersegurança (CNCS) enquanto Autoridade Nacional de Cibersegurança, estando este na alçada do Gabinete Nacional de Segurança. Esta estrutura fica completa com a Equipa de Resposta a Incidentes de Segurança Informática, a CERT.PT.

Existe ainda a Rede Nacional CSIRT (Computer Security Incident Response Team) que tem como objetivos criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança e criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão, promovendo assim uma cultura de segurança em Portugal. Esta rede tem membros de grandes empresas das telecomunicações como é o caso da Altice e da Vodafone, mas também do setor financeiro como o Banco de Portugal e a Caixa Geral de Depósitos. Tem ainda vários membros académicos de diferentes universidades e institutos, empresas ligadas à tecnologia e à cibersegurança e conta ainda com a presença do Sport Lisboa e Benfica.

Na estrutura institucional de combate ao cibercrime são destacados o Gabinete de Cibercrime do Ministério Público e ainda Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária. Sendo o Centro Nacional de Cibersegurança a Autoridade Nacional de Cibersegurança, este coopera com as duas entidades de combate ao cibercrime por forma a combater a criminalidade informática e no ciberespaço.

2.2. Ciberdefesa em Portugal

De acordo com o Conceito Estratégico de Defesa Nacional, a cibersegurança é considerada uma prioridade nacional, sendo recomendada a construção de uma capacidade de ciberdefesa ao nível das Forças Armadas. De acordo com a Lei das Bases da Organização das Forças Armadas, o órgão de ciberdefesa assegura o comando das operações militares no e através do ciberespaço. Para dar cumprimento à Lei Orgânica do Estado-Maior-General das Forças Armadas, aprovada pelo Decreto-Lei n.º 19/2022, de 24 de janeiro, foi criado o Comando de Operações de Ciberdefesa, ao qual compete planear, dirigir, coordenar, controlar e executar operações no e através do ciberespaço. Até à publicação do decreto regulamentar do EMGFA sobre o Comando de Operações de Ciberdefesa, prevê-se que se mantenha em funcionamento o Centro de Ciberdefesa, que depende do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA).

Foi também criada, através do Despacho nº 15/MDN/2020, de 6 de fevereiro, a Comissão de Monitorização da Ciberdefesa, que é composta por entidades da defesa nacional com competência em matéria de ciberdefesa. O seu objetivo é acompanhar e assegurar a articulação dos assuntos relacionados com a ciberdefesa para manter o Governo informado.

Na Estratégia Nacional de Segurança do Ciberespaço (ENSC), o ciberespaço é definido como sendo "o ambiente complexo de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

De acordo com a ENSC, a ciberdefesa é definida como a "atividade que visa assegurar a Defesa Nacional no, ou através do, ciberespaço". Para tal, é necessário que o país se adapte, desde o nível concetual até ao nível estratégico, para ter uma maior resiliência operacional, gerando assim uma nova capacidade. Esta estratégia exige uma perspetiva colaborativa, entre os vários intervenientes responsáveis pela mesma, definindo que a segurança do ciberespaço é "uma responsabilidade partilhada", quer se trate de intervenientes públicos ou privados.

A Lei de Programação Militar, aprovada pela Lei Orgânica n.º 2/2019, de 17 de junho, prevê a atribuição de verbas para o desenvolvimento de capacidades de ciberdefesa, o que constitui um importante reforço por parte do Governo.

A Estratégia Nacional de Ciberdefesa (ENCD) estabelece uma visão segundo a qual se pretende promover o desenvolvimento de capacidades nacionais de ciberdefesa, articuladas entre as Forças Armadas e as estruturas civis de defesa nacional.

2.2.1. Natureza e missão da ciberdefesa

O desenvolvimento da capacidade nacional de ciberdefesa exige a construção de uma capacidade militar conjunta que depende do CEMGFA e que tem componentes estratégicas e operacionais, garantindo a máxima interoperabilidade.

Para além dos tradicionais domínios de operações militares, mar, ar e terra, e mais recentemente o espaço, o ciberespaço é também reconhecido como um domínio de operações militares. Assim, é também um elemento integrante do processo de planeamento estratégico e operacional das Forças Armadas.

De acordo com a Resolução do Conselho de Ministros nº106/2022, de 2 de novembro, a missão da ciberdefesa é "assegurar a defesa nacional no ou através do ciberespaço, consubstanciada na capacidade de garantir o direito soberano de

Portugal aceder e utilizar o ciberespaço, de forma livre, segura e em pé de igualdade com os demais Estados da comunidade internacional, contribuindo para a promoção do desenvolvimento, do progresso e dos legítimos interesses nacionais e contribuindo para a segurança cooperativa do ciberespaço no âmbito das entidades internacionais que Portugal integra". Para cumprir esta missão, torna-se necessária a conjugação de ações defensivas e ofensivas, tendo em conta o enquadramento legal e político.

A capacidade de assegurar permanentemente um perímetro dinâmico de proteção das redes e sistemas de informação, considerados críticos para a defesa nacional, deve ser garantida através de ações defensivas.

A capacidade de executar operações de natureza ofensiva cabe exclusivamente, nos termos da legislação em vigor, às Forças Armadas. Estas operações materializam-se, de acordo com a Resolução do Conselho de Ministros nº106/2022, de 2 de novembro, em operações reativas, preventivas e outras deliberadas, que visam "neutralizar, manipular, negar, perturbar, degradar ou destruir a capacidade de uma entidade aceder livremente ao ciberespaço". A atividade ofensiva, em resposta à ação de entidades, será regulada por normas próprias, sob a forma de regras de empenhamento, autorizadas pelo poder político, de acordo com a legislação em vigor.

2.2.2. Princípio de atuação da ciberdefesa

De acordo com a Resolução do Conselho de Ministros nº106/2022, de 2 de novembro, a ciberdefesa deve reger-se pelos princípios da proteção e sustentação, da proporcionalidade e credibilidade e da parceria e cooperação.

Ao nível da proteção e da sustentação, a ciberdefesa, através da sua capacidade defensiva, deve ser capaz de "detetar e antecipar ciberataques, impedir ou atrasar a sua progressão" e contribuir para a recuperação dos sistemas

comprometidos. Deve contribuir com avisos e recomendações para evitar vulnerabilidades e corrigir rapidamente as que forem detetadas.

Assim, para garantir a defesa, e para que esta seja contínua e ininterrupta, esta capacidade terá de ser sustentável, estando disponível todos os dias, 24 horas por dia. Para isso, será necessário incorporar nos seus recursos humanos o conhecimento técnico necessário para a tarefa. Pretende-se ainda que a ciberdefesa seja capaz de "assegurar a necessária resiliência contra ataques sofisticados, de saturação e prolongados no tempo".

De acordo com os princípios da proporcionalidade e da credibilidade, as operações militares de ciberdefesa devem respeitar os quadros legais em vigor, tendo como objetivo a dissuasão no ciberespaço. Deverá existir a "flexibilidade operacional necessária para ajustar proporcionalmente a resposta a cada tipo de situação", tendo em conta o direito nacional e internacional.

A utilização de capacidades ofensivas deve ser proporcional e só deve ser feita se necessário, em conformidade com o direito humanitário internacional.

De acordo com os princípios de parceria e cooperação, a segurança do ciberespaço "deve ser abordada de uma forma inclusiva, ampla e integradora, promovendo a indispensável cooperação entre instituições civis e militares".

A ciberdefesa faz parte do conjunto de capacidades do Estado português definidas na ENSC, utilizando mecanismos de cooperação e troca de informações. Será o ponto único de contacto para todas as entidades militares das alianças e coligações a que o país pertence.

Para fazer face a situações de crise ou de estados de exceção, é imperativo "reforçar os sistemas de partilha de informação e de classificação de incidentes existentes", promovendo a interoperabilidade técnica e funcional entre o Centro de Ciberdefesa, o Centro Nacional de Cibersegurança, a Polícia Judiciária e o Sistema de Informações.

No que diz respeito ao reconhecimento das ameaças e à sua partilha, o princípio a seguir é o da necessidade de partilha, independentemente dos parceiros serem nacionais ou estrangeiros.

2.2.3. Objetivos estratégicos

A liberdade de ação do País no ciberespaço deve ser assegurada, através da ciberdefesa, pela capacidade de conduzir operações militares. De acordo com a Resolução do Conselho de Ministros nº106/2022, de 2 de novembro, os objetivos estratégicos são os seguintes:

a) Consolidar as capacidades de ciberdefesa;
b) Maximizar a resiliência e a coesão da ação nacional;
c) Promover a investigação, o desenvolvimento e a inovação;
d) Garantir recursos qualificados.

2.2.4. Eixos de desenvolvimento da ciberdefesa

A Resolução do Conselho de Ministros nº106/2022, de 2 de novembro, define seis eixos orientadores para a elaboração de um plano de ação a desenvolver pela Defesa Nacional, destinado a reforçar a capacidade de ciberdefesa.

O primeiro eixo é designado por "Utilização do ciberespaço como domínio de operações". Define que a capacidade militar das Forças Armadas Portuguesas deve ter, como parte integrante, a capacidade autónoma de conduzir operações no, ou através do ciberespaço. Desta forma, o ciberespaço é um elemento integrante do processo de planeamento estratégico e operacional, tendo em conta a sua potencial influência nas missões nos restantes domínios de operações.

O segundo eixo - Reforço das capacidades nacionais de ciberdefesa - tem como objetivo desenvolver as capacidades de ciberdefesa e assegurar a defesa nacional no e através do ciberespaço. Para concretizar esta visão, a Resolução do

Conselho de Ministros n.º 106/2022, de 2 de novembro, descreve três grandes linhas de ação:

a) "Aumentar o conhecimento e o número de operacionais de ciberdefesa para uma dimensão suficiente, de modo a garantir a missão e os princípios definidos para esta capacidade".

b) "Assegurar permanentemente uma infraestrutura tecnologicamente avançada - sofisticada, robusta e resiliente - que permita um potencial diferenciador para operar com vantagem no ciberespaço".

c) "Garantir a independência tecnológica na maior medida possível, através de uma combinação criteriosa de sistemas abertos e comerciais e do aumento das capacidades nacionais, fomentando o desenvolvimento de parcerias com o tecido económico e académico nacional".

Tendo em conta estas linhas de ação e tendo em conta que a ciberdefesa exige conhecimentos altamente especializados, o recrutamento, a seleção e a formação dos recursos humanos devem ser extremamente importantes e prioritários.

O terceiro eixo - Criação da Escola de Ciberdefesa - assegura o constante aumento e adaptação das qualificações necessárias, de modo que os recursos humanos estejam aptos a desenvolver operações multi-domínio, com vantagem sobre os agentes hostis. A construção da Escola de Ciberdefesa pretende ser a entidade formadora conjunta, no âmbito das Forças Armadas, em colaboração com entidades de referência nacionais e internacionais, como o Instituto Politécnico de Beja.

Este deverá também tornar-se um centro de referência a nível internacional, estando aberto à cooperação no âmbito de alianças, com vista à participação de Portugal no Centro de Excelência Cooperativo de Ciberdefesa da NATO.

O quarto eixo - Reforçar a cooperação nacional e internacional - afirma que, a nível estratégico, a cooperação nacional e internacional é da maior importância para os objetivos da ciberdefesa. Esta cooperação assegura a ligação entre o desenvolvimento das capacidades nacionais e a participação na defesa europeia.

O quinto eixo - Promover a investigação, o desenvolvimento e a inovação no ciberespaço, incentivando o desenvolvimento de soluções de dupla utilização - promove o desenvolvimento de melhores ferramentas e capacidades para combater as tecnologias emergentes e disruptivas que os agentes de ameaças possam utilizar.

A sensibilização para os perigos do ciberespaço, bem como para as boas práticas, é da maior importância, contribuindo para uma maior segurança no ciberespaço.

O sexto e último eixo - Garantir as capacidades necessárias de ciberdefesa em contextos de estado de exceção - define que, em situações de estado de sítio e de estado de emergência, a utilização da ciberdefesa será feita de acordo com a legislação em vigor. A ciberdefesa terá também a capacidade de "coordenação e gestão centralizada das ações no ciberespaço". A ciberdefesa deve ser apoiada por um Estado-Maior e um serviço de informações específicos, responsáveis pela compilação e atualização de um quadro de situação das ameaças promovidas pelos Estados ou de fenómenos como o terrorismo, a insurreição e a intolerância radical.

3. Solução Proposta

Durante o processo de construção de um CR, existem variados aspetos sobre os quais é necessária haver uma consideração e discussão, entre os quais o propósito de construir um CR, qual a sua arquitetura, qual o custo associado e qual a abordagem a ter na construção do mesmo (Pandey & Ahmad, 2022).

3.1. Equipamento

Aquando do processo de decisão acerca dos componentes a utilizar no CR, existem alguns fatores a ter em consideração, consoante o tipo de CR e a sua finalidade, sendo estes (Pandey & Ahmad, 2022):

- Poder de computação: Os CR devem ter máquinas, idealmente servidores, que disponham de um elevado poder de computação, por forma a suportarem várias máquinas virtuais a correrem ao mesmo tempo. Neste caso, quanto maior o número de núcleos dos processadores e a memória RAM, mais máquinas virtuais conseguem correr em simultâneo e cada máquina com mais recursos alocados a ela mesma, o que contribui para uma experiência mais fluída na execução dos cenários.

- Armazenamento: Os CR devem ter uma boa capacidade de armazenamento, na medida que permite que seja possível armazenar diversas máquinas virtuais com as mais variadas configurações, por forma a conseguir correr diversos cenários. Quando o objetivo da utilização do CR é a geração de dados e bases de dados, o armazenamento tem aqui também um papel fulcral.

- Rede: Os CR devem ser capazes de suportar conexões com baixa latência e com uma elevada largura de banda, assim como importantes protocolos de comunicações. As especificações dos próprios

equipamentos de rede, como *switches, routers* e *firewalls*, e serviços como VPN e DNS, devem ser considerados (Priyadarshini, 2018).

- Backup: A existência de um *backup* no CR é essencial pois permite salvaguardar a integridade da estrutura e dos dados em caso de falha.

3.1.1. Equipamento utilizado na solução

O equipamento utilizado para a construção da solução a que esta dissertação se refere não foi alvo do processo de seleção e deliberação mencionado anteriormente como sendo um ponto essencial para a construção de um cyber range.

Foi proposto proceder à construção de CR com recurso a equipamento existente na Escola Naval, e como tal, o equipamento utilizado para a construção da solução foi:

- 4 *desktop* DELL OptiPlex 5070
- 1 *desktop* HP PRO ONE 600
- 1 *Switch* Cisco 2960

O equipamento utilizado foi, anteriormente, parte de um laboratório de cibersegurança existente na Escola Naval, porém, são equipamentos que contam com apenas 4 cores e 4GB de memória RAM no caso do *desktop* HP, e 8 cores com 8GB de RAM no caso dos *desktops* DELL.

Relativamente ao armazenamento das máquinas, estas possuem discos HDD, enquanto que se possuíssem discos SDD, estes seriam muito mais rápidos e eficientes, tornando toda a experiencia de utilização mais fluída, aumentando também a fiabilidade do sistema.

3.1.2. Limitações do equipamento

Os *cyber ranges* são sistemas complexos que exigem bastantes recursos. Estes utilizam sistemas de virtualização, que servem os mais variados propósitos e, como

tal, é necessário que tenham um elevado poder de computação, tanto maior quanto for a dimensão da estrutura e do trabalho desenvolvido nos mesmos.

Uma das principais limitações, se não a principal limitação, destes equipamentos prende-se exatamente neste ponto. Os equipamentos disponibilizados pela Escola Naval são equipamentos obsoletos, com pouca capacidade de processamento e computação, não possuindo a capacidade de suportar *software* de virtualização de forma efetiva.

3.2. Arquitetura

A conceção de uma arquitetura de rede é um processo que exige conhecimentos não só a nível de redes, compreendendo todos os aspetos das redes, incluindo *subnetting*, que é uma parte essencial da configuração da rede, mas também é extremamente importante saber qual é o objetivo final da rede.

O objetivo desta rede é criar um ambiente fechado, uma *sandbox* e uma *testbed,* que permita a realização de testes e recolha de dados de forma segura, podendo ser operada por um único utilizador. Esta rede poderá assim, no futuro, servir de base e de recurso para o desenvolvimento de novas investigações no domínio da recolha de dados relacionados com a cibersegurança ou com as próprias redes, tendo uma grande capacidade de geração de dados nestas áreas.

Para criar esta solução, foi utilizado o Cisco Packet Tracer. O Cisco Packet Tracer é um simulador de rede da Cisco que permite a criação de uma visão lógica da rede, o que constitui uma ajuda muito valiosa na configuração da rede.

A solução construída, com base no hardware disponível, é uma rede com cinco máquinas ligadas a um switch, sendo que em cada máquina foi instalado um hipervisor tipo 1, para melhor aproveitamento dos recursos das máquinas.

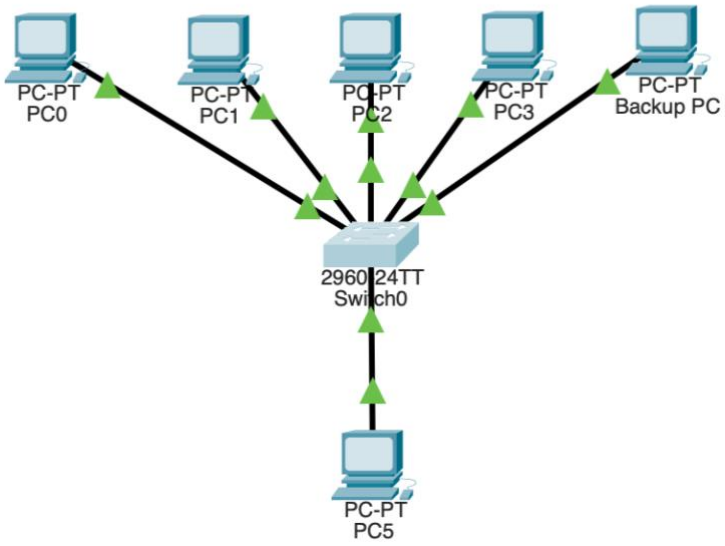

Figura 1 - Esquema lógico da rede, no Cisco Packet Tracer

Na Figura 1 é possível observar o esquema lógico da solução, onde constam as cinco máquinas referidas anteriormente, ligadas a um *switch*, permitindo assim que estejam todas interligadas na mesma rede, sem ter acesso ao exterior, constituindo um ambiente fechado.

Das cinco máquinas, quatro foram alocadas para virtualização, ou seja, quatro das máquinas estão destinadas a correr os cenários propostos ou qualquer outro tipo de investigação que venha a ser desenvolvido. A quinta máquina foi designada como um servidor de *backup*, essencial neste tipo de soluções. A sexta máquina existente na Figura 1 representa uma máquina externa ao sistema, através da qual é feita a administração ou utilização do sistema.

Esta arquitetura permite que a solução seja escalável, ou seja, é possível adicionar tantas máquinas, quer para alojar *software* de virtualização, quer para utilização do sistema, quantas forem pretendidas, tendo sempre em consideração o material utilizado, havendo também a possibilidade de alterar o equipamento para equipamento mais recente e robusto sem prejudicar a integridade do sistema.

3.3. Cenários

O cenário define o ambiente de execução assim como a narrativa, que indica os passos a prosseguir durante um teste ou exercício. Este representa o cenário operacional de forma precisa, conduzindo a execução dos exercícios e do treino por forma a que os objetivos sejam cumpridos. Os cenários fornecem documentação, resumos, ordens de ação, por forma a apoiar os objetivos de treino e de teste.

Estes cenários são ainda classificados relativamente ao seu propósito, ao ambiente onde são executados, à narrativa, ao tipo de cenário e ao domínio (Yamin, Katt, & Gkioulos, 2019).

a) Propósito: O propósito explica quais são os objetivos do cenário, como por exemplo, a execução de um exercício de cibersegurança ou a validação de novas ferramentas e técnicas de cibersegurança.

b) Ambiente: O ambiente do cenário é a topologia onde o cenário é executado. Este é dependente dos objetivos do exercícios ou dos testes e pode ser um ambiente com uma infraestrutura técnica, *"computer based*", podendo ser física, virtual ou híbrida, ou um ambiente "*non computer based"* , que pode ser utilizado num exercício baseado na discussão e troca de ideais, ou uma *table-top*.

c) Narrativa: A narrativa de um cenário conta um ou múltiplos enredos, acerca da forma de como se vai desenrolar o exercício. Esta incluí o desenvolvimento de ações e eventos relevantes que constituem o cenário e a forma como estes estão interligados para gerar toda a narrativa do cenário.

d) Tipo: Os cenários podem ser classificados como estáticos ou dinâmicos. Os cenários são considerados estáticos se o ambiente for estático e não forem efetuadas alterações durante a execução do cenário. São considerados dinâmicos os cenários que incluem, apesar

do ambiente estático, componentes dinâmicas que efetuam alterações durante a execução do cenário.

e) Dominío: Existem vários domínios possíveis para o cenário, como por exemplo, *IoT*, rede, nuvem, etc.

Para permitir que no *cyber range* exista a oportunidade para executar exercícios práticos, torna-se necessária a criação de cenários, pois sem estes não é possível uma prática *hands-on*.

Durante a criação destes cenários, baseados em máquinas virtuais, devem ser criadas máquinas virtuais vulneráveis, quer contenham aplicações vulneráveis ou que o próprio sistema operativo seja vulnerável por si próprio, e também máquinas de ataque.

Após a criação das máquinas virtuais com configurações com vulnerabilidades é possível exportar as mesmas para um ficheiro no formato OVA (*Open Virtual Appliance*). Estas ficheiros são posteriormente disponibilizados aos alunos, que depois podem ser importados no sistema pelos mesmos, sem necessitar de proceder à configuração de uma nova máquina virtual.

3.4. Modelo de Utilização

Os modelos de utilização dos cyber ranges variam consoante o tipo de finalidade da tarefa a ser realizada, quer sejam testes para a recolha de dados, que sejam exercícios de cibersegurança. Os exercícios de cibersegurança nos cyber ranges regem-se, usualmente, em exercícios por equipas, que desempenham papeis diferentes no desenrolar dos mesmos. Estas equipas são:

- Equipa Vermelha: A equipa vermelha tem como objetivo a identificação de vulnerabilidades e falhas de segurança no sistema durante o teste ou exercício. Esta, após a identificação das vulnerabilidades deve, de acordo com o cenário, explorar essas mesmas vulnerabilidades, fornecendo assim uma avaliação de segurança ao sistema, sendo em tudo semelhante a um teste de penetração, também conhecidos por *PenTests*.

- Equipa Azul: A equipa azul tem como objetivo a defesa ativa contra ataques durante os exercícios de cibersegurança. Esta para além desta defesa contra ataques a decorrer, tem também o objetivo de identificar as vulnerabilidades no sistema e proceder à sua correção, antes de serem exploradas pela equipa vermelha.

- Equipa Branca: A equipa branca é responsável por determinar qual será o cenário a ser jogado, experimentando o mesmo, os seus objetivos e regras e os critérios de avaliação. Esta equipa atua como moderador do exercício, definindo regras de empenhamento entre a equipa vermelha e a equipa azul, injeta as vulnerabilidades no cenário, no caso de este ser dinâmico, e todas a alterações carecem de autorização por parte da mesma.

- Equipa Verde: A equipa verde é responsável pelo desenvolvimento, a monitorização e manutenção da infraestrutura utilizada no cenário.

- Equipas Autónomas: Em algumas situações, os papéis das equipas podem ser desempenhados por ferramentas autónomas. Ferramentas como a *Secgen, Security Scenarios Generator,* que gera cenários de forma autónoma, substituindo assim a equipa verde. Existem também ferramentas como a SVED (*Scanning, vulnerabilities, exploits and detection*) que automatiza a função da equipa vermelha.

Como referido anteriormente, a solução criada apresenta diversas limitações ao nível do *hardware*, dificultando, e por vezes tornando impossível a utilização normal que teria um *cyber range*. Como tal, esta foi pensada na perspetiva de ser utilizada apenas por um número reduzido de utilizadores, mais focada no papel desempenhado pela equipa vermelha, pretendendo que os alunos utilizem máquinas de ataque para explorar diversos cenários por forma a complementar a sua aprendizagem na área da segurança ofensiva, tendo os professores o papel da equipa verde, gerando cenários com as vulnerabilidades que se pretende que sejam exploradas pelos alunos.

Esta é, também, passível de ser utilizada por apenas uma pessoa, sendo ela uma ferramenta que permite a autonomia dos estudantes ou professores durante a condução do treino ou de investigações a decorrer.

Durante o decorrer dos exercícios de cibersegurança, todas as máquinas virtuais associadas aos cenários, tanto as de ataque como as máquinas com vulnerabilidades, estão já inseridas no *software* de virtualização, ou podem ser inseridas durante o mesmo.

4. Implementação e testes

4.1. Software

Durante a fase de planeamento para a construção da solução, foi decidido que seria necessário recorrer a software de virtualização por forma a maximizar as capacidades da solução e se possível, através de ferramentas *Open Source*. Dadas as limitações do *hardware* disponível para a construção da solução, a alternativa passava por encontrar um *software* de virtualização onde o consumo dos recursos das máquinas hospedeiras fosse reduzido e otimizado.

Como tal, a solução passava for utilizar um hipervisor de tipo 1, que é instalado diretamente no hardware da máquina, sendo assim poupados os recursos utilizados pelo sistema operativo nativo da máquina. Entre os hipervisores de tipo 1 disponíveis, era importante que o *software* escolhido tivesse um baixo consumo de recursos, e onde os recursos fossem otimizados para a criação de máquinas virtuais, que como descrito anteriormente, são a base de qualquer cenário de exercício de cibersegurança. Após a consideração de todos estes aspetos, e o facto de ser um *software Open Source*, o hipervisor escolhido foi o *Proxmox Virtual Environment*.

O Proxmox VE é uma plataforma de gestão de servidores, diretamente orientada para a virtualização, que atua como um hipervisor de tipo 1, estando instalado diretamente sobre o *hardware*, possuindo este várias valências úteis para a solução.

O Proxmox VE utiliza a tecnologia KVM, *Kernel-based Virtual Machine*, que permite uma virtualização completa e eficiente para Windows e Linux, que são precisamente os tipos de sistemas operativos mais utilizados nos exercícios de cibersegurança por serem dos mais utilizados a nível global.

Este *software* foi instalado em todas máquinas que, com recurso a uma das capacidades do mesmo, foram agregadas num *cluster*, o que permite a clonagem de

máquinas virtuais de uma máquina para outra. Este *software* é administrado através de uma *web-based GUI,* ou seja, uma interface gráfica que é acedida através do browser através do endereço IP de cada máquina.

É através desta interface gráfica que são importados tantos os ficheiros OVA das máquinas virtuais como também ficheiros ISO de sistemas operativos para a criação de máquinas virtuais. As máquinas virtuais podem ser criadas numa máquina diferente daquela onde está armazenado o ficheiro, sendo isto possível apenas se as máquinas se encontrarem agrupadas num *cluster*.

Para além da interface gráfica, está disponível ainda o acesso a uma CLI (*Command Line Interface*) onde é possível administrar cada máquina individualmente.

As máquinas de ataque utilizam sistemas operativos concebidos especificamente para esse propósito, para explorar vulnerabilidades de máquinas e sistemas, e são usadas por *PenTesters* por todo o mundo. Existem várias possibilidades de sistemas operativos para este propósito como o ParrotOS ou Backbox, mas o sistema operativo escolhido foi o Kali Linux por ser o de mais ampla utilização e com mais maturidade.

O Kali Linux é um sistema operativo *open source*, baseado em Debian, que foi desenvolvido especificamente para executar testes de penetração e análises forenses, pelo que as suas distribuições têm um grande número de ferramentas instaladas de origem que são utilizadas durante os exercícios de cibersegurança. Ferramentas como o Metasploit Framework, Nmap, John The Ripper, Hydra, sqlmap ou ainda Burp Suite são ferramentas que são de extrema utilidade durante a execução dos cenários, e o facto de serem pré-instaladas facilita bastante a fluidez dos exercícios, especialmente num sistema isolado, sem conexão à *Internet*, no qual não é possível fazer o *download* de novos programas.

Nas máquinas vítima o *software* utilizado varia consoante o cenário. Os sistemas operativos utilizados contemplam várias versões do Windows e várias distribuições Linux, como por exemplo, Ubuntu.

4.2. Cenários de Teste

O objetivo da escolha dos cenários para teste da solução tinha como objetivo selecionar uma diversidade de cenários que corressem em várias distribuições de sistemas operativos, procurando explorar algumas das vulnerabilidades mais conhecidas com recurso a técnicas bastante utilizadas. Os cenários testados foram:

A. Um dos cenários corre num sistema Windows XP, configurado sem *password* de acesso. Neste cenário, o sistema apresenta a vulnerabilidade identificada como MS08-067, que pode ser explorada com recurso ao *Metasploit Framework*, que permite a execução de código de forma remota, garantindo assim o acesso remoto à máquina vítima. O Windows XP, embora seja um sistema operativo obsoleto, permite a prática de uma grande variedade de técnicas de ataque, o que é muito vantajoso do ponto de vista pedagógico, permitindo preparar os alunos para alvos mais bem protegidos.

B. Outro cenário corre num sistema Windows 7 PRO, configurado com a vulnerabilidade WannaCry, identificada como MS17-010. Esta é também uma vulnerabilidade que permite a execução remota de código e teve um grande impacto em 2017, quando a sua exploração afetou empresas como a *FedEx*, o *Banco BBVA* e a *Portugal Telecom*, agora denominada de *Altice Portugal*.

C. Foi também utilizado um cenário que corre num sistema Ubuntu 13.10 onde pode ser explorado o *shellshock bug*. Este causa uma vulnerabilidade que pode ser explorada com recurso à execução de uma função malformada utilizando o programa *curl*, sendo esta função enviada através de um cabeçalho HTTP. Com esta vulnerabilidade é possível criar uma *reverse Shell* para a máquina atacante ou ainda

utilizar a máquina vítima para executar um *portscan* a outra máquina, mantendo assim a máquina atacante incógnita.

D. O sistema Windows XP utilizado no cenário A é também utilizado para explorar a técnica de *Buffer Overflow* que faz o sistema ser interrompido por violação de acesso. É ainda possível, com recurso a esta técnica, executar *Shell code*, gerando uma *reverse Shell*.

E. Para explorar técnicas de *SQL Injection*, foi utilizado um cenário com um sistema Ubuntu Server, no qual se pode explorar um sistema que está exposto a esta vulnerabilidade e no qual pode ser praticado com recurso à ferramenta *sqlmap* ou de forma manual. Esta vulnerabilidade permite descobrir informações relativas aos utilizadores, incluindo a *hash* da *password*, que estão presentes numa base de dados. Após obter a *hash*, é possível decifrar a *password* com recurso à ferramenta *John The Ripper*.

4.3. Implementação

A implementação da solução dividiu-se em duas partes: a montagem do hardware e a instalação e configuração do software. A montagem do hardware, mais concretamente das máquinas e do switch, foi apoiada pelo Serviço de Informática da Escola Naval, sendo este responsável pela montagem e manutenção do mesmo.

A instalação do *software* fez-se com recurso a um *bootable USB Drive*, contendo o instalador para o Proxmox VE. Cada máquina foi configurada individualmente, atribuindo os endereços IP, por forma a criar uma rede local, sem ligação à *Internet*.

Como demonstra a Figura 2 - Interface web de gestão do Proxmox, o Proxmox VE oferece uma interface gráfica, *web-based*, onde é realizada toda a administração

do sistema, juntamente com a linha de comandos, que pode ser acedida diretamente na interface gráfica ou na máquina.

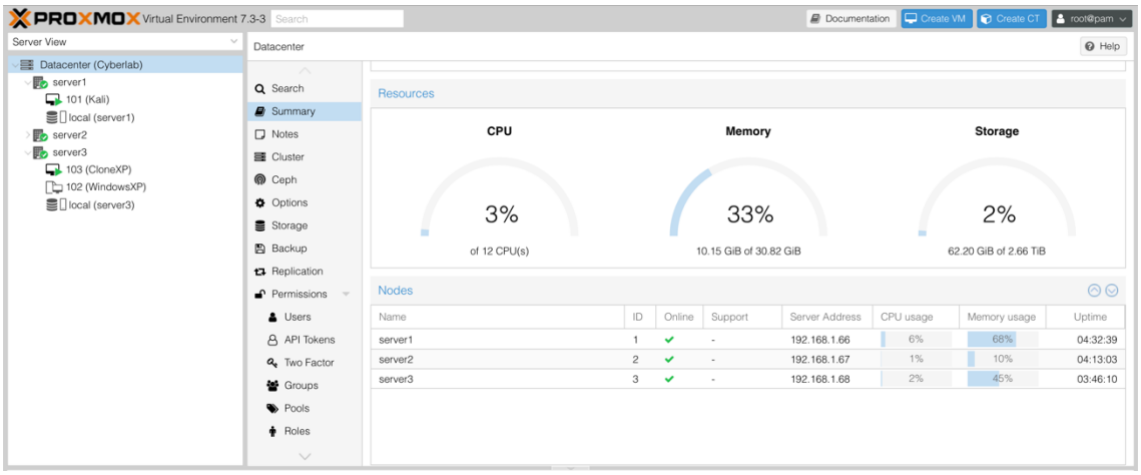

Figura 2 - Interface web de gestão do Proxmox

O primeiro passo na configuração do sistema, após este estar operacional, é garantir que o sistema consegue utilizar todo a memória do disco rígido. Esse processo é efetuado com três comandos, como demonstra a Figura 3.

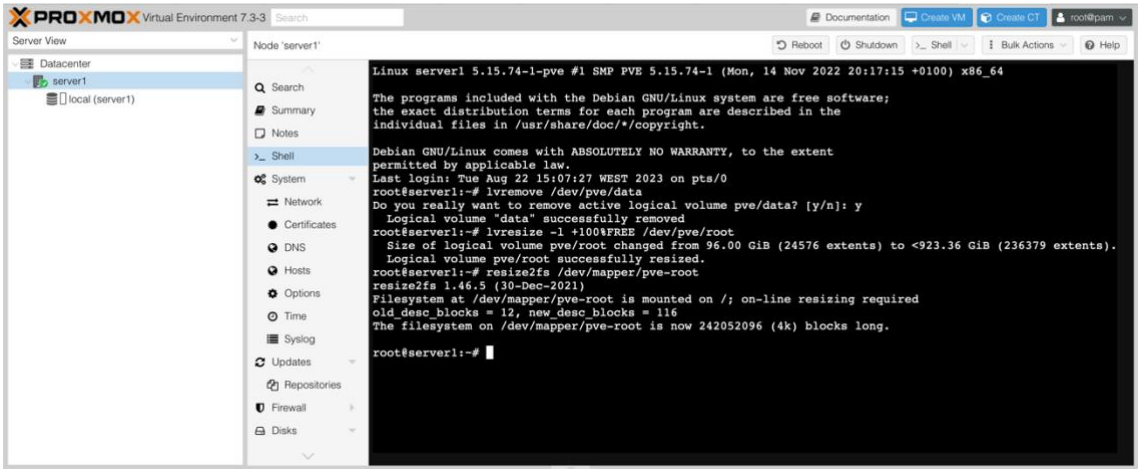

Figura 3 - Comandos para disponibilizar toda a memória

Posteriormente, é necessária a configuração de um *cluster*, ou seja, agregar todas as máquinas na rede por forma a conseguirem partilhar recursos e executar a migração de máquinas virtuais entre elas. A Figura 4 apresenta o *cluster* criado, denominado de *Cyberlab*, apresentando as máquinas a ele associadas.

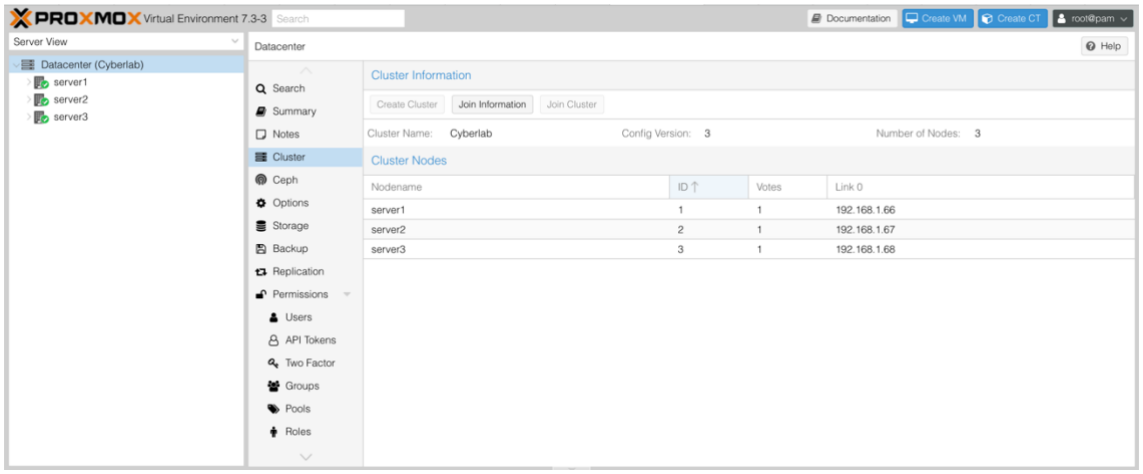

Figura 4 - Cluster criado no Proxmox

Após as configurações iniciais, é possível importar os ficheiros ISO dos sistemas operativos, procedendo depois à sua instalação. A Figura 5 demonstra a importação de um ficheiro ISO, neste caso referente ao Kali Linux.

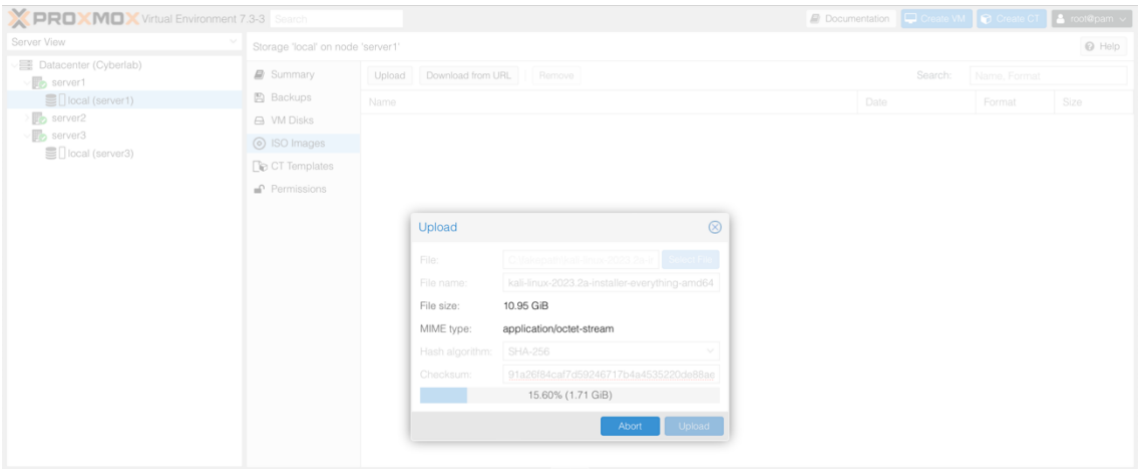

Figura 5 - Importação de ficheiro ISO no Proxmox

Após a importação dos ficheiros ISO pretendidos, pode então proceder-se à criação de máquinas virtuais, e à posterior instalação do sistema operativo na máquina virtual. A Figura 6 apresenta a interface para a criação de uma máquina virtual e a Figura 7 apresenta uma máquina virtual, a correr, disponível para utilização.

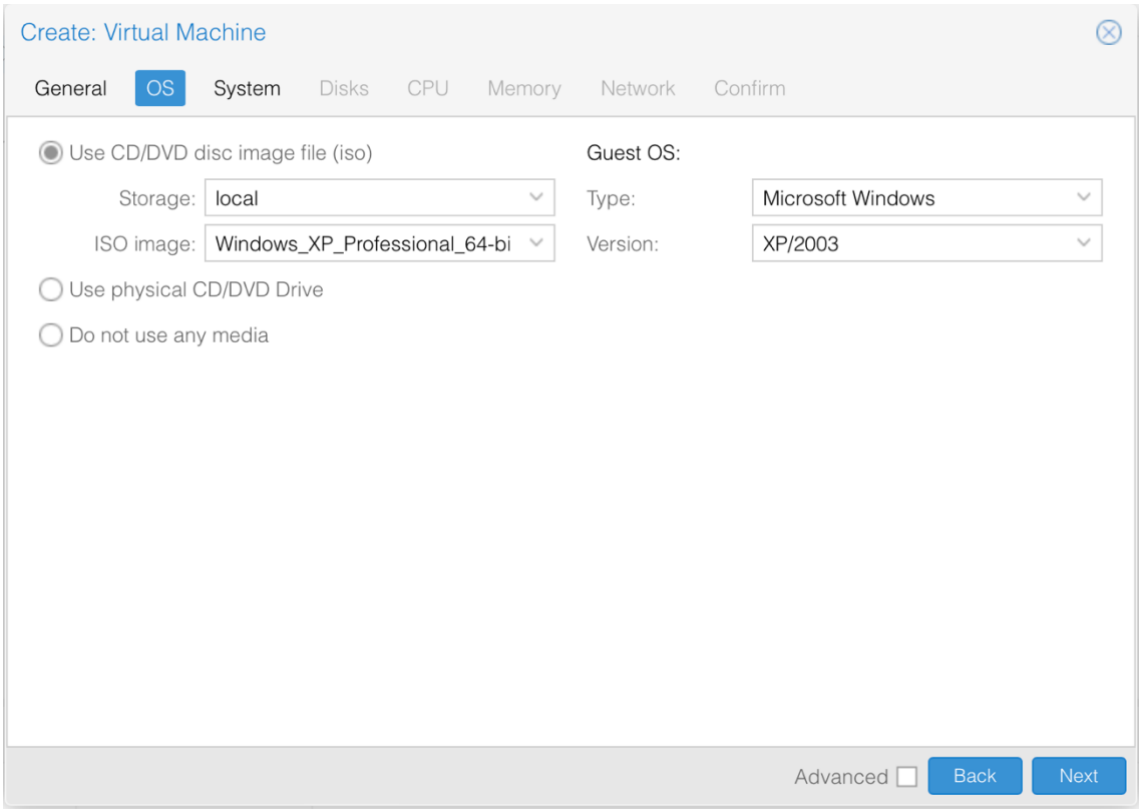

Figura 6 - Criação de máquinas virtuais no Proxmox

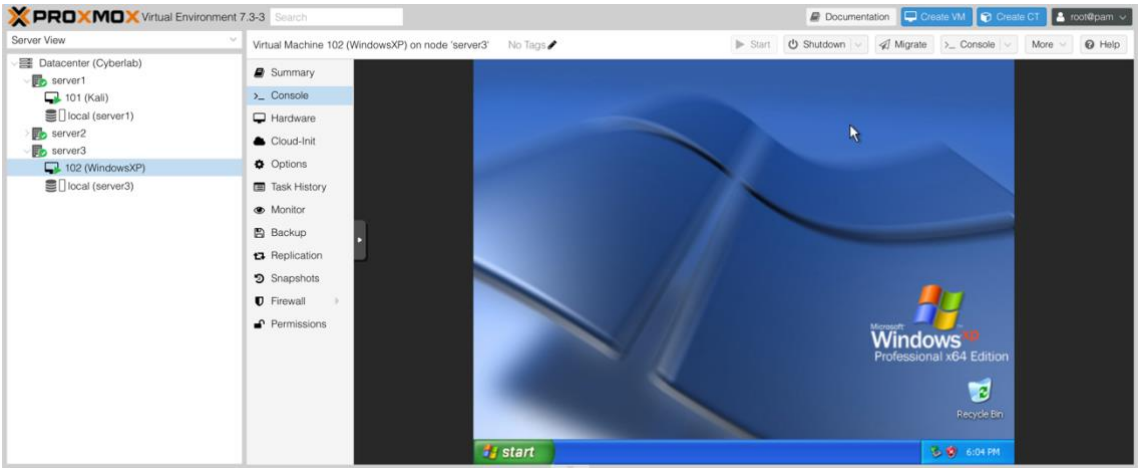

Figura 7 - Máquina virtual a correr um sistema Windows XP

Estas máquinas virtuais podem também ser migradas ou clonadas, conforme a necessidade do utilizador. As máquinas podem ser clonadas integralmente para a máquina de origem, ou para uma outra máquina do cluster. A Figura 8 demonstra a interface gráfica onde é feita a configuração para a clonagem de uma máquina virtual.

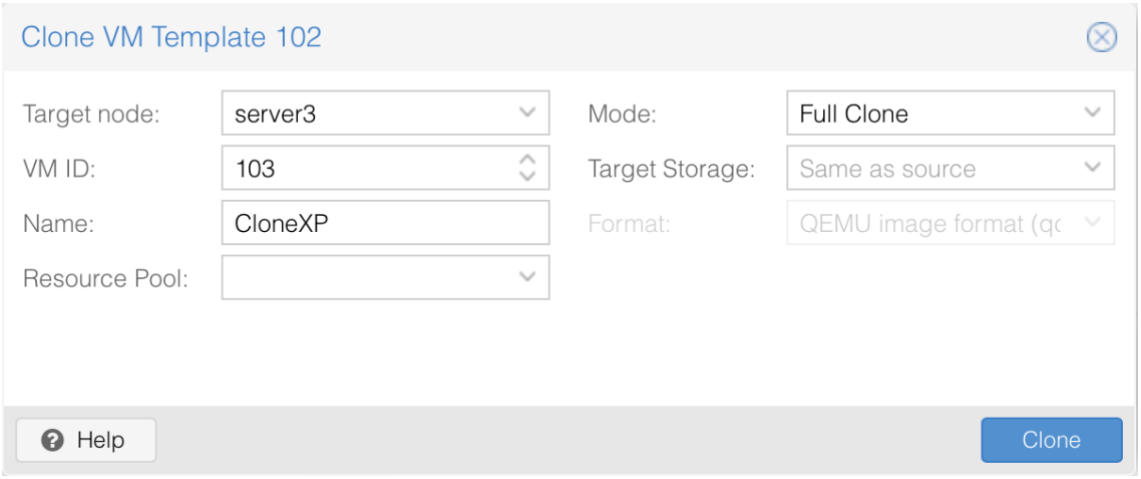

Figura 8 - Clonagem de máquina virtual no Proxmox

Durante o processo de configuração da solução, foi detetada uma anomalia, que consistia na impossibilidade das máquinas se conectarem umas às outras, havendo apenas a conexão dessas máquinas à máquina externa, utilizada para a configuração e administração do sistema. Esta anomalia impossibilita a agregação das máquinas no *cluster*, negando toda a operacionalidade do sistema.

Foram executadas diversas ações de *troubleshooting*, consistindo em diversos testes e reconfigurações do sistema por forma a descobrir ou resolver a anomalia. A solução desta anomalia passou pela substituição do *switch*, que possuía uma avaria. Após a substituição do equipamento, a anomalia ficou resolvida, sendo possível proceder a toda a configuração.

4.4. Testes

Após a implementação do sistema e garantir toda a sua operacionalidade, foi necessário verificar se cumpria o propósito para o qual foi desenvolvido. Foram realizados quatro testes diferentes, jogando os cenários de teste A, B, C e E, que foram anteriormente determinados.

O primeiro teste foi realizado recorrendo ao cenário A onde se procedeu à exploração de vulnerabilidades de um sistema Windows XP. Este cenário apresenta um grau de dificuldade reduzido, sendo um bom cenário para utilização durante o início da aprendizagem dos alunos. Relativamente ao teste, foi inicialmente realizado um *portscan* com recurso à ferramenta *Nmap,* que permitiu verificar quais as vulnerabilidades do sistema. Foi identificada a vulnerabilidade MS08-067.

Após a identificação da vulnerabilidade, procedeu-se à exploração da mesma com recurso à *Metasploit Framework*, a qual tinha um *exploit* para essa vulnerabilidade, sendo apenas necessário executar o mesmo. Após a execução do *exploit*, a máquina atacante garantiu, com sucesso, o acesso à máquina vítima. Foram executados vários testes tais como a criação e manipulação de ficheiros na máquina vítima, a captura de um *screenshot* do ecrã da mesma, a migração do processo onde o *payload* do *exploit* se encontrava.

No segundo teste foi jogado o cenário B, com um sistema Windows 7 PRO, configurada com a vulnerabilidade *WannaCry*. Procedeu-se então novamente a um *portscan* com o *Nmap,* identificando a vulnerabilidade com que a máquina foi configurada e deu-se início à exploração da mesma com recurso à *Metasploit*. Foi efetuada uma pesquisa dentro desta ferramenta pela vulnerabilidade encontrada, também conhecida por MS17-010, tendo como resultado uma lista de *exploits*, entre os quais, um *exploit* denominado de EternalBlue, que injeta um *payload* na máquina vítima, neste caso o *meterpreter*, gerando uma *reverse shell*. Após a exploração ter sido bem-sucedida, procedeu-se a um escalonamento dos privilégios, ou seja, o atacante passou agora a controlar a máquina vitima com privilégios de *root* ou administrador, permitindo descobrir a hash das passwords dos utilizadores da máquina e navegador por todos os ficheiros da vítima, tenho acesso completo à máquina.

O terceiro teste foi relativo ao cenário C, onde é utilizado um sistema ubuntu 13.10. Neste teste pretendia avaliar-se a capacidade de explorar a vulnerabilidade conhecida como *shellshock bug*. Para tal, foi necessária a criação de um ficheiro *Bash Shell Script* para testar se o servidor Ubuntu estaria vulnerável. Para testar, fez-se

recurso ao programa curl, por forma a enviar uma função malformada através de um cabeçalho HTTP, para o servidor. Após verificar que existia a vulnerabilidade, foi possível, através deste método, gerar uma *reverse Shell* para a máquina atacante e executar um ataque de Negação de Serviço, DoS.

No quarto teste, foi utilizado um sistema Ubuntu Server, sendo jogado o cenário D. Neste teste pretendia-se executar um ataque por SQL *Injection*. Este foi executado utilizando a ferramenta *sqlmap*, que é uma ferramenta que automatiza o processo de deteção da vulnerabilidade do sistema a um ataque deste género, procedendo depois à exploração desta mesma vulnerabilidade. Após esta exploração, foi obtido o acesso à base de dados contida no servidor, dando acesso aos nomes de utilizador e às *hash* das *passwords*. Por forma a decifrar as *passwords*, com recurso às *hash*. Foi utilizada a ferramenta *John The Ripper*, que juntamente com a lista de palavras *RockYou*, conseguiu decifrar com sucesso a *password* do administrador, dando assim o acesso total ao sistema por parte do atacante, podendo este ligar-se diretamente utilizando as credenciais e o protocolo SSH.

Conclusões e Trabalhos Futuros

Foi proposto como objetivo base desta dissertação a construção de um *cyber range* na Escola Naval, utilizando *hardware* existente de um antigo laboratório de cibersegurança.

Este projeto ganha relevância com a necessidade de formação na área da cibersegurança, onde a solução criada pode desempenhar um papel importante, permitindo aulas e formações extracurriculares a serem ministradas na Escola Naval. Outra valência da solução criada é o apoio no desenvolvimento e investigação, onde permite gerar dados para posterior análise.

Após a fase da revisão da literatura e tendo em consideração o *hardware* disponível para a construção do *cyber range*, foi reconhecida a impossibilidade de construção do *cyber range* na essência do seu termo. O material *harware* disponibilizado apresenta diversas limitações ao nível da capacidade de computação, com pouca capacidade de memória RAM e tendo processadores com um reduzido número de núcleos e de *threads*, sendo, portanto, material que se considera, obsoleto.

A solução implementada utiliza um sistema de gestão de servidores, o Proxmox VE, que é um sistema diretamente orientado para a virtualização, que atua como um hipervisor de tipo 1. Esta é uma solução *Open Source* que utiliza o *hardware* disponibilizado e serve como prova de conceito à construção de uma solução válida, embora com as limitações já referidas, sendo provada a capacidade de implementação de soluções desta tipologia com outras valências e capacidades, consoante a qualidade e capacidade do *hardware* disponibilizado para a construção da mesma, tendo sido adquiridos os conhecimentos de instalação e administração sistemas desta tipologia.

Relativamente a trabalhos futuros a serem desenvolvidos, esta solução fornece inúmeras possibilidades. Uma sugestão de um trabalho futuro seria a utilização do sistema implementado para gerar dados relativos à cibersegurança e aos ciberataques, que posteriormente servissem de base de dados para a construção de sistemas de apoio à decisão ou para apoio a dissertações futuras.

Outra possibilidade é o desenvolvimento de uma interface gráfica para os utilizadores da solução, onde seja possível atribuir credenciais de acesso específicas a cada um dos mesmos e que facilite o acesso ao sistema, e também uma interface gráfica orientada para a administração do sistema, que será utilizada pelos administradores do mesmo.

Bibliografia

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber Attacks and its Different Types. *International Research Journal of Engineering and Technology*, 4.

Braden, R. (Outubro de 1989). Requirements for Internet Hosts - Communication Layers. *Requirements for Internet Hosts - Communication Layers*.

Distributed Managment Task Force, i. (2010, 01 12). *dmtf.org.* Retrieved from https://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf

Formento, J., & Cerini, A. (12 de Dez de 2022). *What is a cyber range and how do you build one on AWS?* Obtido de AWS Security Blog: https://aws.amazon.com/blogs/security/what-is-cyber- range-how-do-you-build-one-aws

Kozierok, C. M. (2005). *The TCP/IP Guide.* (C. M. Kozierok, Ed.) Vermont, Estados Unidos da América.

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach.* New Jersey, Estados Unidos da América: Pearson.

Meyers, M. (2018). *CompTIA Network+ All-In-One Exam Guide.* McGraw-Hill Education.

Morabito, R., Kjällman, J., & Komu, M. (2015). Hypervisors vs. Lightweight Virtualization: a Performance Comparison Roberto. *2015 IEEE International Conference on Cloud Engineering Hypervisors*, (pp. 386-393).

Pandey, B., & Ahmad, S. (2022). *Introduction to the Cyber Ranges.* Boca Raton, Estados Unidos da América: Chapman & Hall.

Peterson, L. L., & Davie, B. S. (2012). *Computer Networks: A systems approach.* Burlington, Estados Unidos da América: Elsevier.

Priyadarshini, I. (2018). *Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey .* Newark, NJ: University of Delaware.

Stats, I. W. (s.d.). *Internet Growth Statistics*. Obtido em Março de 2023, de Internet World Stats: https://www.internetworldstats.com/emarketing.htm

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks.* Estados Unidos da América: Pearson.

Urias, V. E., Stout, W. M., Van Leeuwn, B., & Lin, H. (2018). Cyber range infrastructure limitations and needs of tomorrow: A position paper. *International Carnahan Conference on Security Technology (ICCST)* (pp. 1-5). Montreal: IEEE.

VMware. (2023, April 09). *What is a bare metal hypervisor?* Retrieved from VMware: https://www.vmware.com/content/vmware/vmware-published-sites/us/topics/glossary/content/bare-metal-hypervisor.html.html

Walleit, S. (2022, January 12). *What Is Bare Metal and How Is It Driving the Remote Work Industry?* Retrieved 2023 February, from Parallels: https://www.parallels.com/blogs/ras/what-is-bare-metal/

White, G., Conklin, W. A., Cothren, C., Williams, D., & Davis, R. L. (2021). *CompTIA Security+ Exam Guide Sixth Edition.* McGraw Hill.

Wihl, L., & Varshney, M. (2012). A virtual cyber range for cyber warfare analysis and training. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference.* National Training and Simulation Association.

Obtido de https://www.scalable-networks.com/sites/default/files/White-Paper– Virtual-Cyber-Range-IITSEC-2012.pdf
Yamin, M. M., Katt, B., & Gkioulos, V. (2019). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Elsevier*.