CIBERSEGURANÇA

Universidade de Aveiro

Rúben Gomes, Tiago Garcia

VERSÃO 1

CIBERSEGURANÇA

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

Rúben Gomes, Tiago Garcia
113435 rlcg@ua.pt, 114184 tiago.rgarcia@ua.pt

10 de dezembro de 2022

Resumo

Neste trabalho é abordado o tema de cibersegurança, tema este que, com desenvolver gradual das tecnologias, torna-se cada vez mais importante. Vulnerabilidades surgem a cada dia, e há cada vez mais ataques cibernéticos. Com este projeto procuramos tocar nos pontos mais importantes do mundo digital.

Este trabalho está dividido em 2 grandes capítulos, a Cibersegurança no geral e as Vulnerabilidades.

O capítulo da Cibersegurança no geral fala de uma ideia geral da cibersegurança, a sua importância, os tipos de ameaças existentes, como ataques, botnets, malware, entre muitos outros. O grande objetivo deste capítulo é introduzir ao leitor o conceito de cibersegurança, o que é, para que é importante bem como os diversos perigos a que o usuário comum está exposto nos dias que correm.

O capítulo das Vulnerabilidades fala, como o nome indica, de vulnerabilidades em sistemas. Entre os métodos de análise, definições de termos usados em cibersegurança, e programas utilizados para o combate às mesmas, procura-se demonstrar ao leitor o quão vasto é o mundo online, e que o mundo todo está constantemente exposto a vários tipos de vulnerabilidades. Embora acabem por existir soluções, cada um deve ter sempre o seu cuidado a usar uma máquina. É também importante reforçar a ideia que o software usado em análises é permutável, ou seja, ao usá-lo mutuamente, obtém-se melhores resultados(desde que não tenham os mesmos propósitos!).

Com isto, os autores consideram que este relatório é ideal para qualquer leitor que deseja saber algo mais sobre o mundo digital.

Conteúdo

Lista de Tabelas

Lista de Figuras

Introdução

Com o passar dos anos, as tecnologias que temos ao nosso dispor tem evoluído de uma forma rápida e sem fim, como, por exemplo, o *hardware* de um computador. Mas, com constantes evoluções, também vem uma necessidade de responsabilidade, pois com quanto mais recursos existirem, maior será o impacto de danos a indivíduos ou entidades.

Com este relatório, irá ser abordado um tópico bastante sensível na atualidade, a Cibersegurança, bem como as diversas vulnerabilidades associadas de formas de nos protegermos contra as mesmas.

Capítulo 1

Cibersegurança no geral

1.1 Conceito

Quando os sistemas e ambientes digitais foram criados não existia quase nenhuma interação entre dispositivos e a pouca que existia era efetuada por cabo. Porém, quando a internet foi criada, a interação entra dispositivos digitais aumentou e com isso, tal como acontece com interações humanas, vieram diversos perigos e ameaças aos utilizadores. Da mesma forma que existem crimes no mundo físico também existem crimes digitais e da mesma forma que existem soluções e entidades responsáveis pela prevenção e combate a crimes físicos, também os mesmos existem para o mundo digital, proporcionando cibersegurança aos utilizadores da internet e ambientes digitais.

1.2 Tipos de ameaças

1.2.1 Ameaças cibernéticas

Conjunto de malware e software com capacidade de afetar o funcionamento normal de equipamentos digitais. Muitas vezes usadas para ciberterrorismo e causar danos graves com o intuito de lucrar ou impossibilitar o trabalho usual de uma entidade.

Botnets

Botnets são robos digitais que conseguem infetar dispositivos, tal como um vírus e a partir daí permitir que utilizadores remotos tenham acesso à máquina onde se encontram alojados. Estas máquinas são muitas vezes usadas para fazer tarefas ilícitas e ilegais por parte do utilizador remoto sem que este seja exposto por não ser a máquina do mesmo a realizar as ações.

Estes botnets podem contaminar computadores, dispositivos móveis, *routers* e dispositivos Internet of Things (IOT).

Da mesma maneira que um vírus tenta infetar o corpo humano através de falhas no sistema imunitário, também estes bots tentam infetar os dispositivos através de falhas de segurança. É possível detetar que o dispositivo se encontra infetado a partir da deteção de comportamentos anormais por parte da máquina, por exemplo quando esta trabalha de forma mais lenta do que o normal ou quando durante a utilização aparecem mensagens de erro aleatórias.

Tipos de botnets

Dentro dos botnets existem dois tipos: Cliente Servidor e Peer-to-Peer

- Cliente servidor → Este é o modelo dos botnets mais antigos em que os dispositivos infetados (clientes) recebem intruções de um outro dispositivo que os controla (servidor)
- Peer-to-peer → Este modelo corrige algumas falhas que o modelo de cliente servidor tinha. Em vez de ser establecida apenas uma conexão entre dois dispositivos (cliente e servidor), neste modelo todos os dispositivos infetados estão conectados entre si, todos a ser controlados pelo mesmo dispositivo que dá as intruções a todos os outros. Isto permite que no caso de haver uma falha com um dos dispositivos infetados, a rede continue online e funcional.

Distributed denial-of-service (DDOS)

Estas ameaças são das mais comuns e mais utilizadas pela comunidade de atacantes. O objetivo destes ataques é levar o consumo de recursos do servidor/aplicação ao limite. Uma vez sem recursos disponiveis, o servidor acaba por ter falhas de funcionalidade ou pode chegar mesmo a ir abaixo e ficar offline.
A quantidade dste tipo de ataques têm vindo a aumentar substancialmente, segundo a Microsoft[1], a Azure Networking registou, em 2021, um aumento de 25% a mais de casos de DDOS em relação a 2020.

Functionamento de DDOS

Durante estes ataques, um conjunto de Botnets (1.2.1) ataca uma aplicação/servidor com o objetivo de desgastar e levar o consumo de recursos ao limite. Fazem isto procedendo ao uso exagerado de solicitações Hypertext Transfer Protocol (HTTP). Uma vez que os atacantes usam estes bots, conseguem também acesso à base de dados, podendo conseguir roubar informação sensivel e, uma

[1] Fonte: `https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack`

vez que os recursos do servidor já estão no limite, os proprietários e responsáveis pela segurança do servidor têm dificuldade na defesa do seu sistema. Estes ataques podem demorar diversos intervalos de tempo, desde minutos até mesmo dias.

Tipos de ataques DDOS

Existem três tipos de ataques DDOS:

- Ataque volumétrico → estes ataques baseam-se na sobrecarga do servidor com tráfego, sendo o tipo de ataque mais comum.
- Ataque de protocolo → estes ataques atacam certas camadas de protocolos de segurança eliminando limites de tráfego o que permite uma mais fácil sobrecarga dos recursos.
- Ataque a camadas de recursos → estes ataques são usados principalmente em redes de servidores pois permitem o bloqueio na troca de informação entre os diversos hospedeiros.

Durante um ataque DDOS podem ser usados apenas um ou mais destes tipos, muitas vezes começa como um dos tipos para debilitar os sistemas de segurança para que depois possam ser usados ataques de exaustão do sistema.

1.2.2 Guerras cibernéticas

Por vezes estas ameaças e armas cibernéticas são usadas para criar guerras. Estas são muito prejudiciais para as vítimas da guerra mas benificial para o atacante pois este consegue muitas vezes vencer a guerra sem qualquer custo para si mas leva a sérios danos à vítimas, explorando falhas de segurança nos seus sistemas.

As vítimas são muitas vezes países ou empresas e não entidades pequenas, sendo atacados não apenas dados das entidades mas também os próprios sistemas, levando ao corrompimento de parte do functionamento da entidade.

Estas guerras são também usadas no roubo de informação desde dados simples até mesmo dados bancários ou na espionagem de dados militares ou diplomáticos. Outro uso dado a estas guerras é a corrupção e a manipulação de dados para benificio de uma certa entidade como acontece em algumas disputas de poder.

Exixtem duas formas de guerras: ARC e ERC .

ARC

Estas guerras são responsáveis pela destruição e degradação de redes e da informação com a qual estas trabalham. Podem ser usados DDOS para provocar sobrecarga no servidor fazendo pedidos de informação de quantidade superior à que o servidor aguenta ou podem-se criar bloqueios nos servidores para impedir o acesso aos mesmos por parte dos utilizadores.

ERC

Estas guerras são as responsáveis pelo espionamento de entidades e por vezes provocar danos colaterais na rede durante o processo.

1.2.3 Internet banking

Tal como o nome sugere estas ameaças procuram tirar proveito de falhas em sistemas bancários quer bancos financeiros quer bancos de dados. Com a exploração de vulnerabilidades nestes bancos, o atacante consegue um grande acesso à informação dos utilizadores, usando essa informação para proveito próprio posteriormente.

Muitos dos sistemas usam uma Application Programming Interface (API) que permite a utilização do sistema por parte de aplicações externas. Por exemplo, o PayPal tem uma API que permite que outras aplicações o usem como método de pagamento. No entanto, estas API são também bastante sujeitas a ataques DDOS (1.2.1), entre outros. Outro problema com a sua encriptação é o baixo nível da complexidade das chaves de autenticação usadas (muitas vezes são pins numéricos com poucos digitos).

1.2.4 Mobile Malware

Este género de malware pode ter a capacidade de roubar a informação do dispositivo, inutilizar aplicações. Estas ameaças podem facilmente se espalhar através do Bluetooth.

Mobile malwares mais usados

- Banking → Captura dados de logins do usuário
- Ransomware → Bloqueia ficheiros locais
- Spyware → Controla a atividade do utilizador
- Adware → Constantes publicidades
- MMS → Usa mensagens para explorar falhas nas bibliotecas do andriod

Com estes malwares, o usuário corre o risco de ter dinheiro, informação pessoal/profissional/empresarial roubadas, podendo ser posteriormente vendidas no mercado negro da internet.

1.3 Programação aplicada à Cibersegurança

Como é óbvio, para a automatização quer seja para os sistemas de ataque ou para os sistemas de defesa é usada bastante programação e como isto não são sistemas dísponivels a todos os utilizadores, cada hacker cria a sua aplicação à sua maneira para atingir os seus objetivos.

1.3.1 Linguagens mais usadas em hacking

1. Python
2. C
3. PHP
4. C++

1.3.2 Sistemas operativos usados em hacking

Todos os hackers optam pelo uso de uma distribuição de linux e embora a maior parte delas funcionem, o Kali Linux é o mais usado, entramos em mais detalhes mais à frente em 2.2.2.

Capítulo 2

Vulnerabilidades

2.1 Análise de vulnerabilidades

A análise de vulnerabilidades no papel da Cibersegurança é muito importante. Sem ela, não existiria nenhuma melhoria no ramo de combate às ameaças cibernéticas, pois sem desenvolvimento, não haveria métodos de nos proteger dos diversos tipos de ataque que se conhece.

Este tópico é dividido em vários ramos, como a **Digital Forensics**, a **Incident Response**, entre outros.

2.1.1 Digital Forensics

A Digital Forensics é, como o nome indica, a forense digital, e é a obtenção e análise de dados de uma forma pura, sem quais quer tipos de distorção e sem tendências para qualquer lado, de modo a reconstruír o que se passou no passado com o sistema.

Tem como objetivo examinar dados de sistemas, ativdidade de utilizadores do sistema, programas em execução, entre outras métricas que possam ajudar a determinar se está a decorrer um ataque e quem está por detrás do ataque.

Deve-se ter sempre em conta a preservação dos dados. Se o caso a ser estudado for levado a tribunal e se descobrir que os dados foram, de qualquer forma, manipulados, é o suficiente para a prova de esses mesmos dados ser completamente anulada, e até mesmo levar o caso contra quem apresentou essa prova.

Digital Forensic Investigation (DFI)

Com a DFI, entra-se na parte judicial das investigações. É uma investigação mais especializada, pois devem-se usar métodos e técnicas que permitam a que as evidências apresentadas possam ser admissíveis num tribunal.

O grande objetivo é chegar à causa raíz do problema/evento e garantir com clareza que as evidências não foram manipuladas de forma alguma, não levantando quaisquer questões ou dúvidas.

Deve ser realizado um DFI, por exemplo:

- Resposta a um incidente
- Investigações criminais
- Corrigir falhas de segurança

2.1.2 Métodos de Análise

Existem dois tipos conhecidos de métodos de análise de evidências, o **Método Tradicional** e **Método Vivo**

Método Tradicional(Post mortem)

O método tradicional consiste na análise de evidências com o ststema desligado, acedendo ao disco numm modo inalterável(read-only), e examinar, por exemplo:

- Logs do sistema
- E-mails
- Ficheiros
- Metadados

Método Vivo (Live forensic)

O método vivo resulta da análise da máquina, com a mesma ligada. Pode ser usado como prova uma screenshot da máquina. No caso de ser necessário examinar um disco, pode vir a demorar algum tempo, especialmente se for de grande capacidade de armazenamento.

2.1.3 Incident Response

Incident Response(resposta ao incidente) é o procedimento que um sujeito ou, nomeadamente uma empresa toma para que se prepare, detete, contenha e recupere de uma eventual perda de dados.

Esta é bastante importante em empresas para minimizar os danos eventuais de uma invasão de dados, ou seja, não haver perda de dados e, até mesmo, impedir que a mesma aconteça.

Existem vários tipos de equipas específicas para cada tipo de invasão, como Computer Incident Response Teams (CIRTs), Computer Emergency Response Teams (CERTs), entre outras.

Threat Intelligence

A Threat Intelligence baseia-se na obtenção e análise de informações que ajudem a identificar possíveis ataques. Esta vem com o benefício de ter uma segurança proativa, ou seja, evitar qualquer tipo de ameaças a uma empresa.

O esquema seguinte demonstra o que constitui uma Kill Chain:

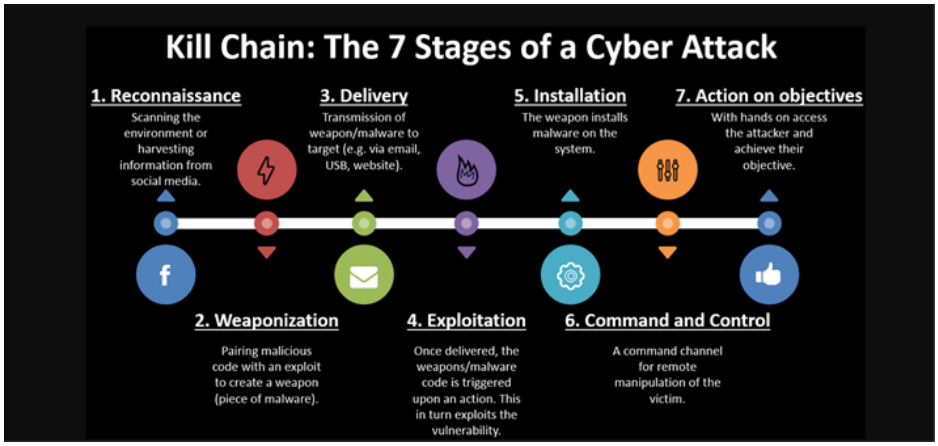

Figura 2.1: As 7 fases de um ataque cibernético
[1]

Também é importante mencionar as inúmeras organizações que ajudam e facilitam o combate aos ataques cibernéticos, sendo a mais destacada a MITRE ATT&CK.

A MITRE ATT&CK é uma organização focada na obtenção de informações de ciberataques apenas por observação do que acontece no mundo digital. É conhecida por ter uma vasta base de dados de ataques com informações de quase todos os ataques que aconteceram.

Além de identificar os problemas, também disponibiliza soluções para os mesmos, tudo isto sem qualquer custo tanto para uso pessoal como para uso empresarial. Isto obviamente reforça a ideia de colaboração, que é bastante importante no ramo da informática.

Ordem de Volatilidade

É muito importante ter em conta a ordem de volatilidade dos ficheiros criados por um sistema, pois devemos começar sempre pelos ficheiros que estão mais em contacto com o sistema em si(como ficheiros cache, RAM, etc.). A ordem por base no tempo em que estão disponíveis e acessíveis é, respetivamente:

1. Ficheiros cache
2. Memória(RAM)
3. Estado da rede
4. Processos ativos
5. Armazenamento
6. Backups / Cópias de Segurança
7. DVD's ou impressões

Esta ordem é importante pelo facto de ao examinar um sistema, é preciso ter precisão para encontrar a origem do problema, e na maioria dos casos essas evidências estão na memória gerada pelo sistema no instante em que ocorre o ataque, sendo esse o foco principal de um investigador.

2.2 Análise de evidências

A análise de evidências é muito importante para o desenvolvimento de métodos eficazes para combate a malwares, pois permite-nos examinar máquinas que foram afetadas por qualquer tipo de ameaça. Estas podem ser, por exemplo:

- Malware
- Spyware
- Trojans
- Ransomware

2.2.1 Vulnerabilidades e como combatê-las

Quando se fala em vulnerabilidades, refere-se a uma possível falha num sistema que, a partir da mesma, pode ser comprometido o sistema, o utilizador ou uma empresa. Deve ser encarada como algo de alta prioridade, e deve ser resolvida o quão antes possível, antes que ocorra algo inesperado. Por este motivo deve sempre existir a identificação, análise e retificação de vulnerabilidades.

Como forma de ajuda a combater vulnerabilidades, existem vários websites com as vulnerabilidades mais comuns, e todas as informações necessárias para poder saber a sua origem e como combatê-las.

Common Vulnerabilities and Exposures (CVE)

A CVE (website) e um projeto da MITRE, cujo intuito é identificar, definir e catalogar as várias vulnerabilidades que existem no mundo digital. Estas ameaças são sempre publicadas por parceiros da própria CVE, obtendo assim uma consistência nas descrições das vulnerabilidades, para quem desejar explorar múltiplas vulnerabilidades e não ter muitos conflitos com as explicações das mesmas.

Common Vulnerability Scoring System (CVSS)

A CVSS (website) é um sistema que atribui a cada vulnerabilidade um grau de gravidade. Este é classificado[1] do seguinte modo:

Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Tabela 2.1: CVSS Score
A tabela acima representa os graus de gravidade na classificação CVSS

Apenas são usados valores definitivos, que significa que não vai existir mudança de valores para uma vulnerabilidade. Daí surgir a importância de uma calculadora capaz de medir com precisão o grau de gravidade de uma vulnerabilidade. Se a mesma se agravar, é criado um novo catálogo com a nova ameaça.

[1] Fonte: `https://nvd.nist.gov/vuln-metrics/cvss`

Common Weakness and Enumeration (CWE)

A CWE (website) é outro projeto da MITRE, que lista todos os tipos de fraquezas de software e hardware comuns. Uma fraqueza é uma condição num software, hardware, firmware ou serviço que pode vir a introduzir uma vulnerabilidade a partir delas.

O grande objetivo da CWE é parar as vulnerabilidades na sua raíz, educando qualquer pessoa que trabalha no ramo da informática, de modo a evitar erros comuns e contribuir para um espaço mais seguro numa empresa.

Open Web Application Security Project (OWASP)

O OWASP (website) é uma fundação open-source com o intuito de melhorar a segurança de softwares no geral, ensinando pessoas pelo mundo todo para existir uma web mais segura.

Dentro desta fundação, foi criada um projeto bastante importante no mundo cibernético, o OWASP Top Ten [2]. Este projeto consiste em, no final de cada ano, organizar um top 10 das ameaças mais comuns nesse mesmo ano. É feito sempre uma comparação com anos anteriores para verificar as mudanças e melhorias que aconteceram. Ao ser realizada a comparação, consegue-se saber se houve melhorias face ao combate de vulnerabilidades anteriores, as novas vulnerabilidades introduzidas e uma breve explicação de cada uma delas.

No seguinte esquema [2], está representada a comparação das vulnerabilidades do ano 2017, e do ano 2021:

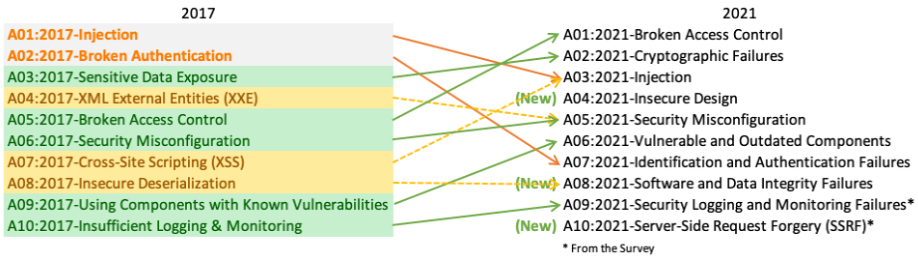

Figura 2.2: Comparação das ameaças mais comuns entre 2017 e 2021

2.2.2 Softwares usados para análises

Para poder examinar e tirar conclusões de anomalias nos sistemas, é necessário utilizar software dedicado para este tipo de problemas. Os softwares mais utilizados são o Autopsy, o OWASP-ZAP (referido na Seção 2.2.2), e o Docker.

Também é importante referir que para examinar discos e outras unidades de memória, é necessário usar uma máquina virtual Kali.

[2] Fonte: `https://owasp.org/www-project-top-ten/`

Kali

O Kali é um sistema operativo Linux de base Debian. É usada especificamente para análise de vulnerabilidades, invasão de redes, entre outros fins de forense. No site oficial existem várias opções de download do Kali. Uma das mais utilizadas para análise de máquinas é a Live Boot.

A Live Boot consiste num sistema operativo temporário e inalterável, ou seja, ao reiniciar ou desligar, volta às definições default. Como não se pode fazer alterações definitivas na máquina, ela tem de estar pré-definida com os programas necessários para qualquer tipo de análise. Por ser um sistema inalterável, tem a vantagem de ser possível mexer nas evidências sem correr o risco de alterar as mesmas, algo que invalidaria automaticamente as provas.

Por ser um sistema de base Linux, grande parte dos sistemas de ficheiros são acessíveis, algo que não é possível num sistema Windows.

Existe também a possibilidade de usar o Kali em máquina virtual, usando um disco virtual, que significa que guarda todas as alteracções como um computador faria. Este tipo de máquina é usada para explorar vulnerabilidades, por exemplo, em redes.

Estas ferramentas devem ser usadas explicitamente com o consentimento total da vítima, sendo estritamente proibido realizar um ataque não autorizado a qualquer empresa ou indivíduo. São apenas ferramentas para fundos de educação.

Autopsy

O Autopsy é uma aplicação open-source que é capaz de analisar quase todos os tipos de discos, e foi escrita em Java. Esta usa plugins feitos pela comunidade para uma experiência customizável para cada utilizador, permitindo assim uma livre escolha dependendo das necessidades de cada pessoa.

Esta aplicação é focada em vários campos, como, por exemplo:

- Pesquisas em Universidades/Academias
- Investigações em empresas
- Governo e Órgãos militares
- Investigações na polícia

A grande vantagem de usar o Autopsy ao invés de usar um sistema Kali por Live Boot, é que pode-se analisar unidades de disco diretamente a partir do sistema operativo principal, aumentando significamente a performance da análise, pois não se usa uma pen ou uma máquina virtual para usar o sistema operativo.

OWASP - Zed Attack Proxy (OWASP-ZAP)

A OWASP-ZAP é uma aplicação open-source desenvolvida pela OWASP, com o objetivo de explorar vulnerabilidades num website. O programa vem com inúmeras ferramentas de Penetration Testing, para detetar o máximo de vulnerabiliades possíveis.

Esta aplicação tem como vantagens:

- Ser reutilizável, sendo capaz de guardar reports
- Bom para iniciantes
- É grátis

Por outro lado, não é a ferramenta mais prática de usar em empresas, pelo facto de ser open-source e não ter tanta privacidade como outras ferramentas pagas.

É recomendado pela OWASP o uso desta aplicação juntamente com o Docker, para a automatização das ferramentas existentes no programa.

Também é importante referir o projeto Juice Shop, que consiste numa aplicação escrita em JavaScript e que simula uma loja genérica de vários produtos, que contém uma série de vulnerabilidades.

É aconselhado usar a imagem deste projeto no Docker, para a exploração dos erros ser efetuada localmente e eficientemente. Estes erros têm vários graus de dificuldade de serem explorados, e à medida que se descobre os erros, eles vão sendo guardados num ficheiro log que contém o que já foi descoberto pelo untilizador.

Docker

O Docker é um programa usado para desenvolver, enviar e correr aplicações. Desta forma, pode-se criar vários containers para correr ou enviar qualquer tipo de aplicação num espaço isolado. Tem a vantagem de poder ter várias aplicações a correr localmente no mesmo sistema sem consumir muito hardware, que é um grande benefício na área da cibersegurança, pois é usado vários programas ao mesmo tempo.

Na seguinte imagem é apresentado um esquema [3] que mostra a lógica por detrás do Docker:

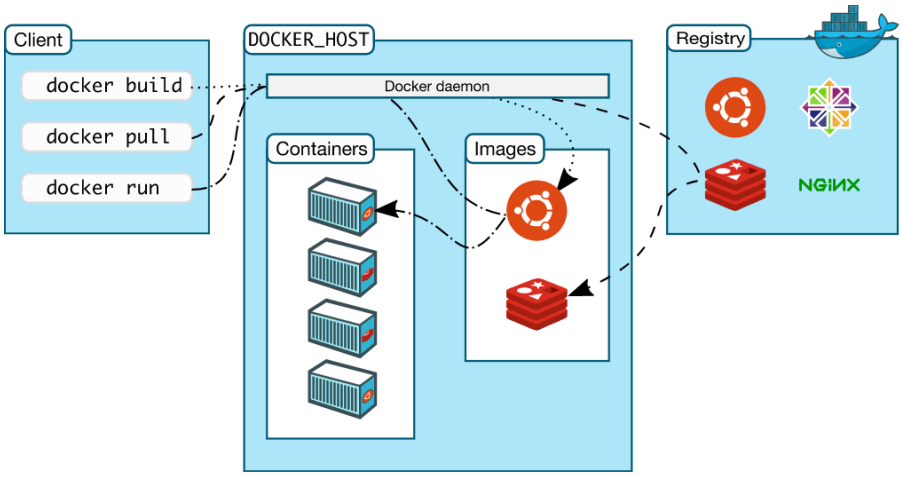

Figura 2.3: Esquema que representa o funcionamento do Docker

Os containers são feitos e funcionam em base de imagens, semelhante a um sistema operativo. Estas são normalmente imagens de outras imagens, apenas com algumas modificações feitas.

Uma imagem bastante conhecida neste campo é a imagem do Juice Shop, um projeto referido na Seção 2.2.2 Com o Docker e a imagem deste projeto, podemos criar um container que vai correr o site, localmente. A grande vantagem de correr ficheiros localmente é que pode-se fazer os testes sem qualquer problema, é possível fazer certos tipos de ataque que na Internet seriam considerados ilegais mas que são, sem dúvida alguma, cruciais para o bom funcionamento de um website.

Capítulo 3

Soluções de segurança

Para combater todas as ameaças cibernéticas (1.2) e combater possíveis falhas de segurança, é necessário encontrar soluções de defesa do sistema e dos servidores. Há diversas formas de melhorar a segurança e de testar o sistema contra as ameaças, mesmo sem o danificar.

3.1 Soluções para o usuário

Por mais que a cibersegurança tenha de ser assegurada pela entidade responsável pelo sistema em questão, a verdade é que o usuário comum deve ajudar no combate às ameaças e ataques cibernéticos. Pode começar pela instrução dos usuários para um melhor uso da internet e outras tecnologias web no intuito de não serem tão facilmente expostas. O não abrir links desconhecidos ou suspeitos, a não confiança em toda a informação disponível online (pois por vezes acaba por ser maliciosa), a não transferência de ficheiros e aplicações sem que o seu criador ou gerenciador seja confiável e o não uso de sistemas web piratas pois com eles podem vir uma data de problemas.

3.2 Soluções para empresas

As empresas de tecnologia têm um papel bastante importante no que toca à segurança tanto dos seus sistemas como dos usuários dos seus serviços. Para isto as empresas têm de implementar medidas para promover esta mesma segurança. Para isto, um dos primeiros passos pode ser o teste da sua segurança que passa por provocar um ataque aos seus próprios sistemas (usando Owasp-Zap para realizar Pen Testing 2.2.2) para poderem proceder à deteção das suas vulnerabilidades para posteriormente corrigirem os seus problemas e falhas de segurança. Outra medida que podem tomar é a monitorização a tempo inteira dos seus recursos e do tráfego dos seus serviços para garantir o bom funcionamento dos mesmos (principalmente para empresas grandes) bem como a resposta rápida por parte da empresa no evento de um ataque. Outro possível método, para

a proteção de dados dos usuários, é o uso de diferentes servidores para que a informação não roubada caso algum tenha problemas.

Capítulo 4

Conclusões

Com isto verifica-se a importância que a cibersegurança tem não só nos dias de hoje mas como no futuro uma vez que a internet, sistemas IOT e sistemas web vão estar cada vez mais presentes nas vidas do ser humano. Para as diversas ameaças 1.2 é necessário encontrar soluções de combate à altura. Para além disso, muitas empresas não se dão ao trabalho de corretamente corrigir os problemas de cibersegurança o que acaba por expor os seus usuários a riscos desnecessários. Com estas falhas das empresas, também os atacantes acabam por ter facilidade nos ciberataques o que lhes proporciona diversas vantagens, desde monetárias até mesmo vantagens diplomáticas (no caso de hacking entre organizações governamentais).

Com o capítulo sobre vulnerabilidades 2 é possível também ver diversos métodos de analisar os possíveis problemas da segurança de sistemas e posteriormente as formas mais eficazes de os corrigir e que softwares usar para este efeito.

Contribuições dos autores

Cada autor contribuiu igualmente para o produto final do trabalho, sendo justamente atribuído a nota de 50% a cada um.
O autor Rúben Gomes (RG) realizou o capítulo de Vulnerabilidades completo.
O autor Tiago Garcia (TG) realizou o capítulo de Cibersegurança no geral e Soluções de segurança.

Indicar a percentagem de contribuição de cada autor.

RG, TG : 50%, 50%

Acrónimos

API Application Programming Interface

CERTs Computer Emergency Response Teams

CIRTs Computer Incident Response Teams

CVE Common Vulnerabilities and Exposures

CVSS Common Vulnerability Scoring System

CWE Common Weakness and Enumeration

DDOS Distributed denial-of-service

DFI Digital Forensic Investigation

HTTP Hypertext Transfer Protocol

IOT Internet of Things

OWASP Open Web Application Security Project

OWASP-ZAP OWASP - Zed Attack Proxy

RG Rúben Gomes

TG Tiago Garcia

Bibliografia

[1] S. Karki, «Cyber Kill Chain — Offensive and Defensive Approach», *CryptoGen Nepal*, 2021.

[2] T. O. Foundation, *OWASP Top Ten*, [Edição mais recente], 2021. URL: `https://owasp.org/www-project-top-ten/`.

[3] T. D. Team, *Docker Overview*. URL: `https://docs.docker.com/get-started/overview/`.