Relatório de Estágio

Bernardo José Lopes Dias

Curso Técnico Superior Profissional em Cibersegurança

ago | 2022

GUARDA
POLI
TÉCNICO

POLI TÉCNICO GUARDA

Escola Superior de Tecnologia e Gestão

RELATORIO DE ESTÁGIO

ESTÁGIO CURRICULAR
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL
EM CIBERSEGURANÇA

Bernardo Jose Lopes Dias
Agosto 2022

POLI TÉCNICO GUARDA

Escola Superior de Tecnologia e Gestão

RELATORIO DE ESTÁGIO

ESTÁGIO
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL EM CIBERSEGURANÇA

Professor(a) Orientador(a): Fernando Melo Rodrigues

Supervisor(a): Ricardo Santos

Bernardo Jose Lopes Dias

Agosto / 2022

Agradecimentos

Com a finalização deste relatório de estágio curricular, desde já agradeço aos meus professores, incansáveis ao longo destes dois anos, deram várias noções e métodos para a realização das tarefas em ambiente de trabalho.

Em primeiro lugar, agradeço ao meu orientador na entidade, Engenheiro Ricardo Santos pela sua disponibilidade e ensinamentos profissionais.

Em segundo, queria também agradecer aos Engenheiros Luís Domingos, Joel Osório que estiveram sempre predispostos a ajudar quer a nível técnico, como pessoal com o objetivo de me prepararem para o mundo profissional.

Em terceiro quero dar um agradecimento à restante equipa do Centro de informática da Unidade Local de Saúde da Guarda.

Ficha de Identificação

Aluno

Nome: Bernardo José Lopes Dias

Número: 1703414

Curso: Cibersegurança

Estabelecimento de Ensino

Politécnico da Guarda

Escola Superior de Tecnologia e Gestão (ESTG)

Entidade Acolhedora do Estágio

Nome: Centro de Informática da ULSG

Morada: Av. Rainha Dona Amélia 19, 6300-749 Guarda

Contacto 271 200 200

Supervisor de Estágio

Nome: Ricardo Santos

Email: Ricardo.Santos@ulsguarda.min-saude.pt

Função: Diretor do Centro de Informática

Docente Orientador de Estágio

Nome: Fernando Melo Rodrigues

Email: fmr@ipg.pt

Função: Professor Adjunto e Coordenador do Tesp Cibersegurança

Resumo

O presente estágio curricular foi realizado no âmbito da Unidade Curricular de Estágio pertencente ao Curso Técnico Superior Profissional de Cibersegurança, lecionado na Escola Superior de Tecnologia e Gestão (ESTG), pertencente ao Instituto Politécnico da Guarda (IPG), e teve como objetivos colocar em prática todos os conhecimentos adquiridos ao longo do percurso académico. Já no Centro de informática do Hospital Sousa Martins, pudemos aprender no que consiste o mundo do mercado de trabalho e adquirir novas competências para a vida profissional. O estágio teve uma duração de cinco meses, correspondendo a um semestre do ano letivo onde, durante esse período participei no desenvolvimento de atividades relacionadas com apoio ao colaborador, configuração de Swicth, realização de vários inventários, remodelação da infraestrutura de serviços da Unidade Local de Saúde da Guarda, prestação de apoios de informática e realização quatro documentos informativos.

Palavras-chave: técnico, cibersegurança, apoio ao colaborador, redes, conhecimentos, informações, documentos.

Índice

Índice de Figuras

Glossário de Abreviaturas

IPG	Instituto Politécnico da Guarda
BD	Base de Dados
CERT	Computer Emergency Response Team
ARP	Address Resolutio Protocol
PJ	Polícia. Judiciaria
CNCS	Centro Nacional de Cibersegurança
CSIRT	Computer Incident Response Teams
ESTG	Escola Superior de Tecnologia e Gestão
FIRST	Forum of Incident Response and Security Teams
IP	Internet Protocol
WPS	Wi-Fi Protected Setup
WPA	Wi-Fi Protected Acess
RNCSIRT	Rede Nacional de CSIRT
OSINT	Open Source Intelligence
SIEM	Security Information and Event Management
UCA	Unidade Clínica de Ambulatório
SOC	Security Operations Center
UE	União Europeia
ULS	Unidade Local de Saúde

1 Introdução

Este relatório baseia-se na descrição do meu estágio curricular, que decorreu durante

cinco meses e teve lugar no Centro de informática da Unidade Local de Saúde da Guarda.

Será feita uma descrição da instituição onde realizei o estágio, com todas as particularidades que merecem ser referidas.

Serão também expostas todas as tarefas realizadas, tal como as dificuldades a elas inerentes. Nesta secção estará presente uma descrição pormenorizada do tipo de trabalho realizado, juntamente com um apoio teórico, que me ajudou a refletir sobre os aspetos mais importantes da informática e cibersegurança, esses que são de extrema importância e utilidade na execução do trabalho de um técnico de cibersegurança.

Concluindo, este relatório é um exercício de reflexão e análise de cinco meses de trabalho nas áreas de cibersegurança, redes e informática, que se revelaram um desafio, mas que terminaram com uma sensação de dever cumprido.

1.1 Apresentação do Estágio

Este estágio curricular, que é parte integrante do curso Superior técnico em Cibersegurança do Instituto Politécnico da Guarda (IPG), teve a duração de cinco meses e tomou lugar no Centro de Informática da Unidade Local de Saúde da Guarda (ULSG). Iniciou-se no dia 7 de março de 2022 e acabou no dia 4 de agosto de 2022, sendo em regime tempo inteiro, das 9 às 17.30 horas, perfazendo assim sete horas diárias.

Os meus orientadores foram o Professor Fernando Melo Rodrigues, que era a responsável pelas minhas atividades curriculares no IPG, os Engenheiros Ricardo Santos e o Engenheiro Joel Osório e Engenheiro Luís Domingos, que eram as pessoas responsáveis pelo meu trabalho no Centro de informática, sendo eles que me atribuíam os trabalhos e que me orientavam.

1.2 Caraterização sumária da instituição

O local onde a atividade foi desenvolvida foi no Centro de informática nas instalações do Hospital Sousa Martins. O ambiente de trabalho foi sempre bastante agradável, facto que facilita a integração e à execução do trabalho. O gabinete era dividido com mais dez pessoas: Eng. Ricardo Santos, Eng. Luís Domingos, Eng. Telma Estrela, Eng. Dario, Eng. Sandra, Eng. Carlos Azevedo, Eng. Joel Osório, Técnico António Xavier, Técnico António Firmino, Técnico Miguel Aguiar, Técnica Mariana Antunes e por último o Pedro, Tiago, Andreia Santos, Bruno Correia sendo que estes eram colegas estagiários que estavam a desempenhar tarefas semelhantes às minhas.

No que diz respeito às condições para o desempenho das tarefas do estágio, foi-me atribuída ligação à Internet com restrições, só me podia conectar a rede "ULSUtentes" visionando a segurança do centro de informática.

Ainda em relação ao local de trabalho, há acrescentar que me proporcionou todas as condições necessárias para a execução do meu trabalho.

O único aspeto menos satisfatório no meu estágio foi o deficiente relacionamento com outros colaboradores do Hospital Sousa Martins, pois alguns dos colaboradores comprometiam alguns dos trabalhos realizados devido a falta de paciência perante a informática, ou, por não compreenderem algumas falhas informáticas.

Para além da inquestionável mais-valia curricular que este estágio representou, este serviu também para me aguçar o interesse nas temáticas da Cibersegurança e redes.

1.3 Objetivos

O estágio Curricular no Centro de informática da Unidade Local de saúde da Guarda teve como objetivos principais o apoio ao colaborador, redes, cibersegurança e o desenvolvimento profissional.

i. Pesquisa de informação relacionada com o domínio, e-mails e dados fornecidos;
ii. Montagem e configuração de uma rede *LAN e VLAN* completa com todos os equipamentos habitualmente usados para um bom funcionamento e segurança da mesma, na sala dos estagiários com o intuito de realização de testes;
iii. Aprendizagem e compreensão de eventuais imprevistos/problemas que surjam no desenvolvimento da mesma e pesquisa de soluções;
iv. Realização de testes de segurança a pontos de acesso, firewall e routers;
v. Configuração e demonstração de uma *fake wi-fi*;
vi. Elaboração de documentos informativos relacionados com as pesquisas, ataques e conclusões feitas e um plano de resposta a incidentes;
vii. Realização de análise forense a equipamentos da instituição.

1.4 Estrutura do Documento

O presente relatório está organizado em oito capítulos, que descrevem, as várias etapas/objetivos do estágio.

O primeiro capítulo é destinado a Introdução aborda uma breve descrição da instituição e os objetivos do estágio curricular.

O segundo é destinado a organização da estrutura do Centro de Informática, uma descrição das salas de trabalhos e Data Center.

O terceiro capítulo é destinado a descrição de algumas ferramentas mais utilizadas ao longo do estágio no Centro de informática.

O quarto capítulo são descritas as várias tarefas no decorrer do estágio no Centro de informática como apoio ao colaborador, realização de vários inventários, mudanças de serviços devido a obras na infraestrutura do hospital.

O quinto capítulo é destinado a descrição de outras atividades elaboradas pelos estagiários ao longo do estágio curricular.

O sexto capítulo fala sobre consultoria dada a funcionários do Centro de Informática no ramo da cibersegurança nomeadamente sobre implementação de EndPoints e outras "dicas" dentro do ramo.

O sétimo capítulo aborda a elaboração de quatro documentos de caráter informativo relacionados com cibersegurança, "Osint", "Documento de Defesa", "Respostas a Incidentes" e por último falamos sobre os cuidados a ter em emails de vários colaboradores da Unidade Local de Saúde da Guarda.

O último capítulo é destinado às conclusões gerais do desenvolvimento do estágio e uma reflexão.

2 Organização

2.1 Equipa técnica/Sala dos Estagiários

Foi apresentado o local onde seria a nossa segunda "casa" o nosso local de trabalho onde funcionários da ULS e o Centro de informática pedem ajuda ou propõem desafios.
São atribuídos computadores geridos pelos estagiários, a sala estava dividida por duas equipas de estagiários.

A primeira equipa constituída por alunos do IPG que contava com três estagiários, A Andreia Santos, O Bernardo Dias e o Bruno Correia.

A segunda equipa era constituída por dois estagiários pela parte da Escola Profissional da Guarda/Ensiguarda, sendo eles, O Tiago e o Pedro.

Figura 1 - Vista parcial da sala de estagiários.

2.2 Data Center

O serviço da ULS é suportado por uma sala de sistemas Data Center. Este é composto por bastidores, servidores, sistema de backups, sistema de refrigeração, Firewalls, sistema de segurança física. Como se pode ver nas figuras 2 e 3.

Figura 2 - Interior do Data Center.

Figura 3 - Porta do Data Center.

3 Ferramentas Utilizadas

Foram utilizadas diversas tecnologias de hardware, que são brevemente descritas em seguida.

3.1 Cable Tester

Ferramenta usada para medição, que visa garantir especificações técnicas e desempenho de uma rede de computadores.

Foi utilizado para verificar o estado das tomadas RJ-45, se estavam ou não funcionar e em outros cabos RJ45.

3.2 Draw IO:

É um software que permite desenhar diagramas para criação de diferentes soluções e topologias

Este software foi utilizado para desenvolver vários projetos ao longo do estágio onde teríamos de explicar a "rede" e seria mais simplificado se desenhássemos o esquema da rede como modelo logico.

3.3 Putty:

É um emulador, console serial e aplicativo de transferência de dados de rede. O software suporta vários protocolos de redes como: SCP, SSH, Telnet e porta serial.

Este software foi utilizado para configurar os Swicth da Cisco Catalyst 2960 e da Avaya 4548GT.

4 Descrição Geral das Tarefas Elaboradas Durante o Estágio

Durante o estágio realizaram-se várias tarefas: No início do estágio as minhas funções consistiram em fazer entregas de material informático e de prestar apoio ao colaborador, analisar o funcionamento, melhores deslocações dentro do Hospital Sousa Martins e regras do Centro de informática. Posteriormente, com o desenvolvimento do estágio, foram-nos atribuídos desafios mais relacionados com a área de cibersegurança e de gestão de redes com um pouco de receio, pela responsabilidade que estas tarefas exigiam.

Designadamente, foram realizadas as seguintes tarefas: Substituição de hardware em computadores de vários serviços do Hospital; Diagnósticos de problemas dos computadores e da rede informática; Manutenção de impressoras; Instalação dos Sistemas Operativos, Assistências e apoio aos colaboradores; Elaboração de vários inventários e de documentos informativos relacionados com cibersegurança.

4.1 Apoio ao Colaborador “HelpDesk”

No decorrer do estágio geralmente apareciam todos os dias computadores para se efetuarem reparações e substituição de peças, ou periféricos, maioritariamente a troca de discos internos e de cabos. Para a manutenção de qualquer dos computadores era sempre feita uma ficha de entrada “ticket” para se verificar os problemas que os computadores tinham e as tarefas que podemos fazer ou não realizar.

Durante o decorrer do estágio realizei a substituição de cerca de 100 discos, ou seja, este tipo de apoio ao colaborador era o mais monótono e diário do estágio.

No final dos computadores estarem limpos iam para o centro de informática, eram feitos testes para ver se os mesmos apresentavam algum defeito. Depois de se efetuarem os testes era prosseguida a instalação do sistema operativo, geralmente o Windows 10 e por fim o computador seria levado de volta para o serviço como podemos ver no exemplo seguinte e na figura 5.

O processo de apoio divide-se em vários passos para a realização das tarefas:

Passo 1: Falar com os colaboradores do serviço sobre o problema.

Passo 2: Saber IP dos PC e/ou impressoras normais e zebras (se for zebra ligada por USB é preciso saber a porta USB).

Passo 3: Desinfetar tudo o que vem dos serviços.

Passo 4: Limpar o PC com um compressor de ar.

Passo 4: Mudar HD para SSD se for o caso e/ou mudar toner das impressoras.

Passo 5; levar aos funcionários do Centro de informática os devidos equipamentos que necessitam de privilégios, já que os estagiários não podiam ter por questões de segurança;

Passo 6; Entrega dos PC / Impressoras.

Passo 7: Testar programas, redes, páginas de teste das impressoras e zebras.

4.1.1 Exemplo:

O Centro de informática recebeu um "Ticket" oriundo do serviço de Cardiologia relativamente a um computador. O pedido dizia que o computador estava "lento". O Eng. Joel então pediu aos estagiários que falassem com o serviço e averiguassem o que se estava a passar com o computador em questão.

Em seguida chegou-se ao serviço e perguntou-se ao colaborador que efetuou o "Ticket" e perguntamos qual seria o problema para que este desse uma informação inicial do problema para se poder dar uma solução ao problema proposto o mais rápido possível.

Registou-se que o problema seria de facto o computador ter instalado um sistema operativo antigo. Resolveu-se recolher o computador do serviço da Cardiologia com o objetivo realizar uma assistência no Centro de informática por isso registam-se os IP do computador e da impressora.

Em seguida já no Centro de informática limpam-se os equipamentos com o recurso de um compressor.

Posteriormente deu-se os IP que registamos aos funcionários do Centro de Informática e troca-se o disco interno HD de 500Gb por um disco interno SSD de 240GB.

Por fim, levou-se de volta o computador para o serviço e efetuaram-se testes as aplicações que esse serviço utiliza diariamente.

Figura 5 - Limpeza e mudar o HD para SSD.

4.2 Manutenção e Instalação de impressoras

Durante o estágio foram efetuadas várias manutenções e configurações de impressoras em vários serviços, na maior parte das vezes eram impressoras normais, no entanto, em outras situações eram "zebras" maioritariamente a substituição de rolos de etiquetas, mas caso fosse necessário levávamos a impressora/zebra para se verificar o problema, ou se necessário mudar.

Posteriormente retornávamos ao serviço e instalávamos a impressora, efetuam-se os testes, neste caso ver se imprimia, fotocopiava e se digitalizava.

Em outros casos, só seria necessário a troca de toner de impressoras como no exemplo seguinte e na figura 6.

4.2.1 Exemplo:

O Centro de informática recebeu um "Ticket" oriundo do serviço de Recursos Humanos relativamente a uma impressora. O pedido dizia que a impressora não tinha "tinta legível". O Eng. Joel pediu aos estagiários que se deslocassem ao serviço dos Recursos Humanos localizado na sede, assim que chegássemos devíamos falar com o colaborador desse serviço e averiguar o que se estava a passar com a impressora.

Chegou-se ao serviço e perguntamos a um colaborador qual era a impressora que tinha o problema para que este desse uma informação inicial.

Registou-se que a anomalia seria que a impressora imprimia sem cor praticamente nenhuma por isso trocamos o toner da impressora, fizemos testes tais como: IP, imprimir uma folha de teste e quando estivesse tudo operacional então levávamos o toner antigo para o centro de informática e registamos o ID do toner para que este ficasse registado no sistema de entrada e saída de peças do Centro de Informática.

Trocou-se o toner e posteriormente fizeram-se testes para verificar se estaria a imprimir sem problemas.

Figura 6 - Troca de Toner de uma impressora.

4.3 Apoio ao Colaborador Redes

No decorrer do estágio geralmente apareciam todos os dias problemas com cabos de rede para se efetuarem a substituição de cabos, ou tomadas de rede, maioritariamente a troca de cabos RJ45 Cat6. Para a substituição de qualquer das tomadas era sempre feita uma ficha de entrada "Ticket" para se verificar os problemas que as tomadas tinham e as tarefas que podemos fazer ou não realizar.

Caso apenas fosse necessária a troca de cabos não era feita uma ficha de registo de entrada ou saída de peças do Centro de Informática.

Em casos raros seria necessário reiniciar, ou noutros casos, trocar o cabo dos pontos de acesso devido a problemas de rede em que os colaboradores não se conseguiam conectar a rede sem fio "*Wi-Fi*" como na figura 7.

Em outros casos, seria necessária a troca de tomadas de rede e posteriormente testávamos as tomadas, com o auxílio de uma ferramenta de testes, ligávamos um cabo a ferramenta e conectávamos com a outra parte da ferramenta em outro cabo, este, já no bastidor desse serviço como no exemplo seguinte e na figura 8.

O processo de apoio divide-se em vários passos para a realização das tarefas propostas ao longo do estágio.

Passo 1: Falar com os colaboradores do serviço sobre o problema.

Passo 2: Saber IP dos PC e/ou impressoras normais e zebras

Passo 3: Desinfetar tudo o que vem dos serviços.

Passo 4; Configurações feitas por funcionários com privilégios.

Passo 5: Testar programas, redes/cablagem, páginas de teste das impressoras e zebras.

4.3.1 Exemplo:

O Centro de informática recebeu um "Ticket" do serviço da Ortopedia, o problema seriam várias falhas no aceso ao Wi-Fi no serviço mencionado anteriormente. O Eng. Luís pediu aos estagiários que falassem com o serviço e averiguassem o que se estava a passar com o ponto de acesso.

Em seguida levamos um cabo RJ45 Cat6 e Cat5e e as ferramentas de testes de rede depois de recolher as ferramentas necessárias chegamos ao serviço e perguntou-se a um colaborador qual era o problema para que este colaborador nos pudesse transmitir informação do problema visando dar uma resposta o mais rápido possível para prejudicar o menos possível o serviço.

Substituiu-se o cabo RJ45 que conectava o ponto de acesso e o problema de rede wireless foi resolvido.

Figura 7 - Ponto de acesso com conectividade

4.3.2 Exemplo:

O Centro de informática recebeu um “Ticket” do serviço da Oncologia, o problema era que vários computadores não tinham ligação á internet.

O Eng. Luís pediu aos estagiários que falassem com o serviço e averiguassem o que se estava a passar com o computador ou com o cabo de rede e caso necessário nos deslocássemos ao bastidor mais próximo.

Em seguida levamos um cabo RJ45 Cat6 e Cat5e e a ferramenta de testes de rede em seguida chegamos ao serviço e perguntou-se ao colaborador que mandou o “Ticket” qual era o problema para que este desse uma informação inicial do problema para se poder dar uma resposta o mais rápido possível.

Após receber as informações do colaborador, fizemos testes, tentamos substituir o cabo RJ45 que estava ligado ao computador e não resolveu o problema.

Com isso em mente, decidimos ir ao bastidor fazer testes na rede, mas o problema também não seria no bastidor. Em seguida verificámos que o problema seria então da própria tomada de rede que estaria danificada, portanto em seguida fizeram-se testes às tomadas do serviço.

Registou-se que a anomalia seria da tomada, então trocámos a tomada de rede e consequentemente cravamos o cabo seguindo a norma B como podemos verificar na figura 8.

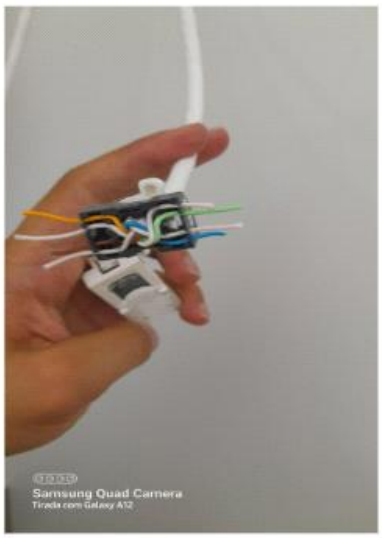


Figura 8 - Troca de tomada de Rede.

Figura 9 - Teste a um cabo de Rede.

4.4 Alterações na Rede da ULS

O Centro de informática recebeu uma "ordem" da administração para se realizarem mudanças de serviços devido a elaboração de obras no edifício 5 na parte antiga da estrutura do hospital.

Esta tarefa consiste maioritariamente na identificação e verificação atempadamente das tomadas de rede e caso seja necessária substituição de tomadas de rede, cabos de rede para os serviços que necessitam de realizar mudanças no serviço.

Passo 1: Contar o número de tomadas de rede para qual os serviços se iriam deslocar.
Passo 2: Verificação da conectividade das tomadas com o bastidor.
Passo 3: Ligar para a informática para remotamente configurar os equipamentos.
Passo 4: Testar as configurações.

Como o serviço da UCA "Unidade Clínica de Ambulatório" dentro de duas semanas iria mudar de instalações devido a obras no edifício velho da Unidade Local de Saúde da Guarda e seria remodelado para o edifício novo do Hospital.

Assim foi testada a conectividade e contar a quantidade de portas registadas na sala vaga para onde se iria mudar o serviço.

Figura 10 - Testagem da conectividade de portas.

5 Outras Atividades

5.1 Manutenção de UPS

No decorrer do estágio foi realizada uma manutenção de UPS por parte de uma empresa exterior para a realização e manutenção de todos os bastidores da Unidade Local de Saúde da Guarda então o Eng. Luís pediu aos estagiários que indicassem os locais dos bastidores e acompanhassem essa equipa de técnicos e teríamos como funções: Abrir os bastidores e garantir a sua segurança nesse trabalho.

Neste trabalho fizemos perguntas aos técnicos e eles ensinaram a ver que os níveis das UPS. Registaram que os níveis de duas UPS estavam a 7/8% e consequentemente só conseguiriam suportar os gastos energéticos dos bastidores uns minutos, ou seja, caso a energia sofresse uma falha de energia os equipamentos já com as UPS só conseguiriam aguentar aproximadamente nove minutos até que a energia fosse reposta, ou caso, se estivéssemos perante um problema elétrico os responsáveis pela eletricidade teriam cerca de oito minutos para resolver o problema.

Reportamos a situação ao Eng. Ricardo Santos e posteriormente este problema critico foi resolvido ao substituir as UPS mais antigas por outras UPS mais recentes para corresponder as necessidades energéticas dos bastidores e garantir que se acontecesse algum problema energético os equipamentos no interior dos bastidores conseguiriam aguentar mais tempo e garantir assim o bom funcionamento da unidade Local de Saúde da Guarda.

5.2 Inventários

No decorrer do estágio foram realizados vários tipos de inventários nestes seguintes exemplos foi pedido aos estagiários que realizassem equipas para realizar vários tipos de inventariação.

No primeiro inventário, foi pedida uma contagem de todos os discos internos contidos em caixas que tinham chegado ao Centro de Informática. As caixas continham discos internos SSD como podemos ver no exemplo da figura 11 mais concretamente eram 100 discos internos com capacidade de 240GB.

Figura 11 - Caixa com cem unidades de SSD.

No segundo exemplo de inventário, foi pedido uma contagem de todos os pontos de acesso da Unidade Local de Saúde da Guarda e se caso faltasse algum ponto de acesso como podemos ver na figura 12 ou se víssemos que tinham problemas de rede, ou se, caso os colaboradores manifestassem queixas em relação ao acesso Wi-Fi que ligássemos ao Centro de informática visto que existiram alguns telefonemas de colaboradores por não se conseguirem conectar a rede Wi-Fi.

Figura 12 - Pontos de acesso Conectados.

No segundo exemplo de inventário, foi pedido para nos deslocarmos a todos os locais de funcionamento da Unidade Local de Saúde da Guarda devido as necessidades que o Centro de informática precisava de realizar atualizações aos Sistemas Operativos Windows7 e o levantamento de os computadores em serviços que ainda tinham como disco interno HD e se tivessem seria necessário mais tarde mudar para discos internos SSD. Este trabalho foi realizado por uma equipa de dois elementos com o objetivo de fazer uma contagem a todos os Sistemas Operativos e monitores para trocar de toda a ULS.

Hospital Parte Nova	
Sala/Gabinete	**Monitores**
Receção	1
	1
Colheitas	1
	1
Secretariado Con. Ext. Medicina	1
Gabinete Trab. Codificadores - Arquivo	1
	1
Tratamento de imagem	1
Sala Relatórios (acompanhado de 2 verticais)	1
RX convencional	1
Enf. Imagiologia	1
	1
Gabinete Enf. Supervisor - Peq. Cirurgia	1
Laboratório do Sono	3
Internamento Covid	4
TOTAL de monitores da parte nova do hospital	20

Tabela 1 - Contagem parte nova.

Segurança	1
Nutrição	1
Urgencia Obstetricia	1
Cuidados Paliativos- Secretariado	1
Cardiologia - Secretariado	1
Cardio. Internamento - enf chefe	1
Cardio. Internamento - Sec AVC	1
Consulta Ext Pediatria - Secretariado	2
UPG - Enf Chefe	1
UPG - Admissão Urgencia Pediatrica	1
Segurança - Bar	1
UCA - Secretariado	2
UCA - Gab 3	1
UCA Bloco Operatorio	3
Gab Utente/Cliente	2
Med B - Sala dos Médicos	1
Med B - Sala Enf	1
Med B - Sala Tecnicos	1
Secretariado Dor e Oncologia	1
Oncologia	2
Oncologia - Sala Enf Chefe	1
Med A - Sala Enf	2
Med A - Sala dos Medicos	1
Med A - Sala de Reabilitação	1
Farmácia	2
Farmácia - Open Space	1
Farmácia - Secretariado	2
Farmácia - Gab. Responsavel	1
Oficinas	6
TOTAL de monitores da parte velha do hospital	60
Quantidade total de ambas as partes	80

Armazém hoteleiro	1
Rouparia	1
Fisioterapia	2
Terapia da Fala	1
EGA	1
Serviço Social	2
Serviço Social Atendimento	2
Gestao Hotelaria	1
Expediente	1
Motoristas	2
Pediatria- Sala de Reuniões	1
Pediatria- Sala de Trabalho	1
Obstetricia- Secretaria Unidade	1
Segurança	1
Nutrição	1
Urgencia Obstetricia	1
Cuidados Paliativos- Secretariado	1
Cardiologia - Secretariado	1
Cardio. Internamento - enf chefe	1
Cardio. Internamento - Sec AVC	1
Consulta Ext Pediatria - Secretariado	2
UPG - Enf Chefe	1
UPG - Admissão Urgencia Pediatrica	1
Segurança - Bar	1
UCA - Secretariado	2
UCA - Gab 3	1
UCA Bloco Operatorio	3
Gab Utente/Cliente	2
Med B - Sala dos Médicos	1
Med B - Sala Enf	1
Med B - Sala Tecnicos	1
Secretariado Dor e Oncologia	1
Oncologia	2
Oncologia - Sala Enf Chefe	1
Med A - Sala Enf	2

Tabela 2 - Contagem parte velha.

5.3 Montagem de um bastidor

Foi elaborado um pedido ao Diretor do Centro de informática o Eng. Ricardo Santos, se podíamos configurar algumas configurações básicas em Swicth o pedido foi imediatamente aceite e o Eng. Luís Domingos posteriormente emprestou-nos dois Switch sendo eles: Cisco Cataclyt 2960 e Avaya Norten 4548GT e por último um cabo de consola para tentarmos configurar os dois swicth.

No processo da montagem do bastidor foram utilizados três cabos RJ45 Cat6, Swicth, UPS e o bastidor.

Após a entrega limpámos o bastidor com o recurso de um compressor de ar e de seguida testámos os cabos de energia e de rede. Em seguida passamos à montagem dos swicth no bastidor como podemos ver na figura 13.

A terceira etapa era a configuração dos Swicth, ficamos encarregues da manutenção e limpeza do bastidor e por último garantir a segurança.

Figura 13 - Bastidor estagiários.

5.4 Switch

Utilizou-se o software Putty para a configuração básica destes dois Switch.
Primeiramente no Swicth da Cisco Catalyst 2960 usamos o terminal para configurar o IP 192.168.0.0, atribuímos o nome "SWestagiariosIPG", foi atribuída uma palavra-passe encriptada, nome de portas, VLAN tais como: 1, Security, Data, Estagiários, teste e por último configuramos a hora correta.
Este Swicth do cisco foi mais fácil de efetuar as configurações devido a termos adquirido conhecimento de configurações em Swicth da Cisco abordadas nas aulas de redes.

Já no Swicth Avaya 4548GT usamos o modo gráfico para configurar o IP, 192.168.0.0, atribuímos o nome de "swestagiarios", foi atribuída uma palavra-passe encriptada, nome de portas, VLAN tais como: 1, Estagiarios, Security, Data e Teste.
Neste swicth encontramos uma maior dificuldade em conseguir algumas informações sobre as configurações concluímos assim em utilizar o modo gráfico para efetuar as configurações.

5.4.1 Configurações:

1) Mudar nome (hostname).
2) Atribui-se um IP ao Switch.
3) Palavras-Passe de acesso ao switch.
4) Encriptação das palavras-passe.
5) Criamos Vlans, atribui-se nomes as portas.

5.4.2 Cisco Catalyst 2960

Figura 14 - Cisco Catalyst 2960.

5.4.3 Algumas Especificações:

- *Flash memory - 64 MB*
- *DRAM - 128 MB*
- *Maximum active VLANs – 255*
- *VLAN IDs available – 4000*
- *IEEE 802.1D Spanning Tree Protocol*
- *IEEE 802.1p CoS Prioritization*
  IEEE 802.1Q VLAN
- *IEEE 802.1s*
- *IEEE 802.1w*
- *IEEE 802.1X*
- *IEEE 802.1ab (LLDP)*
- *IEEE 802.3ad*
- *IEEE 802.3af and IEEE 802.3at*
- *IEEE 802.3ah (100BASE-X single/multimode fiber only)*
- *IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports*
- *RFC 768 - UDP*
- *RFC 783 - TFTP*
- *RFC 791 - IP*
- *RFC 792 - ICMP*
- *RFC 793 - TCP*
- *RFC 826 - ARP*
- *RFC 854 - Telnet*
- *RFC 951 - Bootstrap Protocol (BOOTP)*
- *RFC 959 - FTP*
- *RFC 1112 - IP Multicast and IGMP*
- *RFC 1157 - SNMP v1*
- *RFC 1166 - IP Addresses*
- *RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery*
- *RFC 1305 - NTP*
- *RFC 1492 - TACACS+*

- *RFC 1493 - Bridge MIB*
- *RFC 1542 - BOOTP extensions*
- *RFC 1643 - Ethernet Interface MIB*
- *RFC 1757 – RMON*

5.4.4 Avaya 4548GT

Figura 15 - AVAYA 4548GT.

5.4.5 Algumas Especificações:

- *100BASE-FX ports: 24 MTRJ ports per 4526FX Switch*
- *10/100BASE-TX Ethernet ports: 24/48 per 4500TSwitch*
- *10/100/1000BASE-T Ethernet ports: 24/48 per 4500GT Switch*

- *SFP support: T, SX, LX, XD & ZX CWDM, BX, 100FX & T1 (selectedModelsonly)*
- *XFP support: SR, LRM, LR, ZR*
- *Total Stacking capacity: up to 320Gbps*
- *Switch packet throughput: 6.6 -138Mpps*
- *Switch capacity: 48.8 -184Gbps*
- *Concurrent VLANs: 256*
- *MAC Addresses: 8,000*
- *Jumbo Frame Support on all Gigabit & 10 Gigabit Ethernet ports*

- *IEEE 802.1Q VLANs*
- *IEEE 802.1p Traffic Class Expediting*
- *IEEE 802.1D MAC Bridges (Spanning Tree Protocol)*
- *IEEE 802.1w Rapid Reconfiguration of Spanning Tree*

- *IEEE 802.3 10BASE-T Ethernet*
- *IEEE 802.3u 100BASE-TX Fast Ethernet*
- *IEEE 802.3u 100BASE-FX Fast Ethernet*

- *IEEE 802.3ae 10Gb/s Ethernet*
- *RFC 768 User Datagram Protocol (UDP)*
- *RFC 783 Trivial File Protocol (TFTP)*
- *RFC 791 / 950 Internet Protocol (IP)*
- *RFC 792 Internet Control Message Protocol (ICMP)*
- *RFC 793 Transmission ControlProtocol (TCP)*
- *RFC 826 Address Resolution Protocol (ARP)*
- *RFC 854 Telnet Server and Client*
- *RFC 2865 Remote Authentication Dial In User Service (RADIUS)*

- *Operating temperature: 0 to 50 degrees C*
- *Storage temperature: -25 to 55 degrees C*

- *IEC 60950 International CB certification*
- *•EN 60950 European certification*
- *•UL60950 US certification*
- *•CSA22.2, #60950 Canadian certification*

6 Consultoria de Cibersegurança

Como o sistema operativo mais utilizado nos serviços do Hospital atualmente era o Windows 10, dei algumas recomendações tais como:

6.1 CIS Critical Security Controls

O Center for Internet Security (CIS) é uma organização que tem como objetivo apoiar a comunidade mundial, responsável pelos CIS Controls que são práticas recomendadas mundialmente reconhecidas para proteger sistemas e dados de empresas.

No ponto de vista defensivo é sempre mais difícil para quem é responsável pela defesa de uma organização então podemos utilizar o recurso da "*CIS Critical Controls*", esta recomendação tem três níveis de segurança que uma empresa poderá seguir consoante as necessidades de cada organização.

o g1 de cor verde é o nível básico, o g2 de cor laranja intermedio, o g3 de cor azul é o mais completo. São as recomendações básicas que devem ter, mas 100% seguro nunca podemos estar.

No total são 18 controlos e cada um tem os seus níveis recomendados para a defesa de uma organização.

Figura 16 -CIS Critical Security Controls.

6.2 Implementação de mais Endpoints Security

Segurança de *Endpoint* é a prática de proteger pontos de entrada de dispositivos de colaboradores da Unidade Local de Saúde

da Guarda, como computadores, dispositivos móveis, de serem explorados por os famosos "hackers". Os sistemas de segurança de *Endpoint* protegem esses *Endpoints* em uma rede. A segurança de *Endpoint* evoluiu de um software antivírus tradicional para fornecer proteção contra *Malware* e ameaças de dia zero em evolução.

Duas das soluções relacionadas com a implementação de IDS/IPS/NIDS/HIDS e SIEM sugeridas são as ferramentas "suricata" que é um NIDS "*Network Intrusion Detection System"* e a segunda ferramenta que pertence a categoria de *HIDS "Host Intrusion Detection System" é a "OSSEC".*

Outra solução é a utilização da ferramenta da Microsoft a "UAC" mais concretamente Controle de Conta de Utilizador. Mas o que faz?

O Controlo de Contas do Utilizador UAC ajuda a evitar que o *Malware* danifique um PC e ajuda as organizações a implantar uma área de trabalho mais "segura" e gerida com segurança. Com o UAC, aplicações e tarefas sempre são executados no contexto de segurança de uma conta de não administrador, a menos que um administrador deia autorização de acesso a nível de administrador ao sistema.

7 Elaboração de Documentos Informativos

Como já referido anteriormente, o tema central do estágio curricular que realizei no Centro de informática passa pela cibersegurança e a consequente sensibilização para os riscos que a entidade e colaboradores enfrentam. Tendo integrado durante cinco meses o Centro de informática, onde se insere a equipa de informática, percebi que mais do que comunicar o risco, o importante é sensibilizar e orientar para mitigar esses riscos.

O aumento e a maior criatividade dos ataques informáticos e a necessidade de adoção de medidas de cibersegurança para combater os ataques informáticos temos nos técnicos de cibersegurança um enorme desafio em sensibilizar os colaboradores do Hospital da Guarda ao ponto de adotarem diariamente comportamentos seguros com o objetivo de proteger a organização e os utentes, estes que podem ser severamente prejudicados caso aconteça um ataque aos sistemas informáticos estamos a falar de vidas em risco.

Na cibersegurança, este é um processo comum para se fazer a avaliação do risco e a mitigação do mesmo. A simulação de um ataque informático na organização, a elaboração de documentos informativos, realização de pesquisas de fontes abertas, utilização de ferramentas "*have i been pwned*" e *"inotsu*" para a verificação de emails expostos da organização. Se um "hacker" obtiver vários emails da organização, ou informações, pode dar início a vários tipos de ataques informáticos dos quais se predominam enviar um email fraudulento e enviado por correio eletrónico do colaborador da entidade.

Passo a dar um exemplo de como eu "Bernardo Dias" faria para tirar o melhor partido, se tivesse uma simples informação de um certo email, e obter uma informação de que x colaborador esteve a contratar um serviço de comunicações, ou, comprou um artigo online no dia X e este abordou o funcionário, ou, um amigo numa conversa de café sobre o preço e referiu o nome do amigo.
Tinha uma vantagem e mandaria um email fraudulento. ""Bom dia, Senhor, X, Https: zzzz.zzz sou o X falamos na semana passada!! Clica e vê o preço! Afinal não é como dizias no café X" com uma necessidade vem algum desespero e as pessoas acabam por baixar a guarda e
assim conseguiria acesso ao email e quem sabe a algo mais dentro da entidade.

Mesmo que a entidade tivesse um sistema de defesa por registo de MAC Address, ao termos acesso a certas informações conseguimos "escalar" patamares dentro de uma empresa… bastava saber o email do diretor do serviço desse colaborador e assim mandar outro email fraudulento "Boa Tarde Sr. Diretor X, "uma PNG" de um raio X contendo um

(*Backdoor* e um *rootkit*) é a analise de x utente veja e quanto possível responda visto que o utente tem prioridade máxima!" neste caso se o colaborador x é o diretor de x serviço e o computador tem o acesso privilegiado a informações, mesmo tendo um sistema por segurança Mac Address, podemos assim utilizar ferramentas como o "aerodump-NG" e um simples *Wireless Adapater* em modo monitor para "clonar" esse

Mac Address e assim negar acesso ao diretor e usar assim um computador dentro da entidade e
posteriormente poderíamos infetar outas máquinas desse serviço com N tipos de *Malwares, Trojans, Ransomwares*, ou, afins são imensas opções que um atacante tem””.

Com base neste tipo de ataques realizaram-se documentos visando a pesquisa por fontes abertas, documentos de defesa, documentos de respostas a incidentes e um documento de cuidados a ter em emails.

7.1 Osint

Foi fornecida uma lista de e-mails dos serviços de sistemas e tecnologias da informação e comunicações, recursos humanos, finanças, aprovisionamento e conselho administração para análise de dados possivelmente expostos na internet/Google/dark. Para a elaboração desta análise de dados foram utilizadas as ferramentas "*have i been pwned", "inotsu"* ferramentas para pesquisa de emails contidos em "*data leaks*", e adicionalmente foram usadas técnicas OSINT "*Open Source Intelligence"* e *Google Dorks*.

São todos os dados sensíveis, confidenciais, copiados, roubados e/ou transmitidos por um indivíduo/grupo não autorizado.

Respeitando a Lei n.º 58/2019, de 8 de agosto RGPD, os nomes de funcionários, dados pessoais e os nomes dos respetivos serviços, não serão identificados neste documento.

7.2 Documento de Defesa

Uma vez conhecidos os tipos de criptografias sem fio (WEP/WPA/WPA2) é relativamente mais fácil proteger as redes contra estes tipos de ataques.
Esta informação mostra os pontos fracos que podem ser usados por hackers para permitir o acesso através destas criptografias.

Usar a ferramenta Xarp contra-ataques do tipo MITM (Man in the midle).

Este tipo de ataque pertence aos ataques MITM. É uma forma de ataque em que os dados trocados entre duas partes são de alguma forma intercetados, registados e, possivelmente, alterados pelo atacante sem que as vítimas se apercebam.

Um sandbox, é um local onde qualquer ficheiro irá ser executado e posteriormente analisado.
Como é um ambiente isolado é possível realizar testes sem arriscar danos ao dispositivo ou à rede. No final também oferece um relatório sobre o ficheiro.
Com o relatório é possível obter informações úteis em termos de segurança informática, em relação ao comportamento do mesmo, podendo saber se tem a capacidade de abrir portas, ou modificar entradas de registo e atividades suspeitas, se possui Trojan.

Os ataques informáticos causam um enorme impacto negativo nas empresas, desde a perda de confiança e financeira, espionagem industrial, dados expostos e questões legais. Além dos conselhos apresentados no documento de sensibilização serão apresentados alguns pontos importantes com o objetivo de melhorar a segurança dos sites e aplicações das empresas.

Usar a ferramenta Xarp
Algumas características deste software:
- Deteção de falsificação ARP;
- Monitorização passiva;
- Validação ativa;
- Níveis de segurança predefinidos;
- Monitorização de rede;
- Alerta de e-mail.

Este software envia uma notificação a alertar o utilizador das alterações feitas no caso de uma eventual deteção de um "arp spoofing". Regista e informa os MAC e IP que foram consequentemente comprometidos.

1 - Programação segura;
2 - Revisões constantes às aplicações;
3 - Contratar um serviço de "Pentest" ou criar um posto;
4 - Aderir a plataformas de "Bug Hunt" ou "Bug bounty";

7.3 Resposta a Incidentes

Sempre que um incidente é detetado, devem ser prontamente registados todos os elementos disponíveis e a partir daí, todos os eventos com ele relacionado. A informação recolhida durante a investigação deve ser igualmente armazenada, registada e assinada pelo responsável pela investigação. A validade destas informações como provas usadas em tribunal ou no âmbito de processos disciplinares internos depende do correto dos procedimentos do tratamento dos mesmos.

Qualquer resposta a incidentes relacionados com Cibersegurança deve seguir a orientação "OODA LOOP", este que se predomina, observar, orientar, decidir e agir, seja qualquer tipo de ameaça a uma organização, ou, a um sistema informático.
Todos os incidentes seguindo a lei portuguesa deverão ser reportados pelas entidades às autoridades competentes, tais como, polícia judiciária (PJ), Centro Nacional de Cibersegurança (CNCS).

7.4 Cuidados a ter perante ataques

O Serviço de Sistemas e Tecnologias da Informação e Comunicações da Unidade Local de Saúde da Guarda apela à sensibilização de todos os utilizadores com o objetivo de proteger não só os seus dados pessoais assim como o nosso hospital e os centros de saúde.

8 Conclusões

Ao longo do estágio, foram desenvolvidos vários documentos relevantes para a Cibersegurança, consistindo em documentos de sensibilização, Ciberdefesa, respostas a incidentes informáticos.

Foram realizados vários trabalhos de apoio ao colaborador.

O estágio acabou com praticamente todos os objetivos finalizados, mas outros projetos eram necessários acessos privilegiados tais como acesso a uma base de dados e autorizações para testes de segurança dos quais não se conseguiu autorização antes do término do estágio.

Ao longo do estágio, foram adquiridos muitos conhecimentos nas áreas de Cibersegurança, Redes e Manutenção Informática, tendo sido um estágio muito produtivo em níveis pessoais como profissional.

Todos estes desenvolvimentos adquiridos deram outra perspetiva do mercado de trabalho e testaram os conhecimentos lecionados no curso de Cibersegurança.

Anexos

OSINT

Relatório dos e-mails fornecidos

Unidade de Saúde Pública da Guarda

Andreia Santos

Bernardo Dias

Bruno Correia

Guarda, 4 de maio de 2022

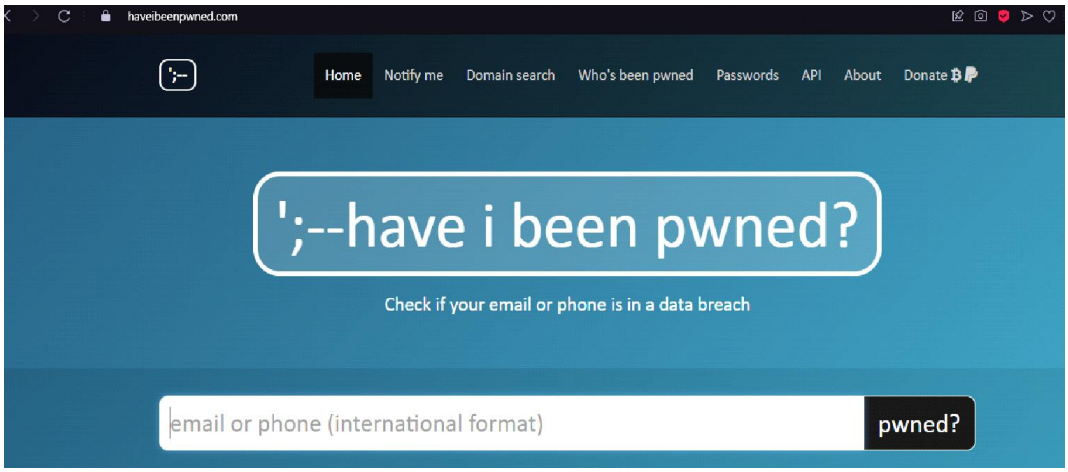
Resumo

Foi fornecida uma lista de e-mails dos serviços de sistemas e tecnologias da informação e comunicações, recursos humanos, finanças, aprovisionamento e conselho administração para análise de dados possivelmente expostos na internet/Google. Para a elaboração desta análise de dados foram utilizadas as ferramentas “have i been pwned”, “inotsu” ferramentas para pesquisa de emails contidos em “data leaks” em fontes abertas, e adicionalmente foram usadas técnicas OSINT (*Open Source Intelligence)* e *Google Dorks*.

Tecnologias utilizadas

Estas ferramentas foram utilizadas com a finalidade de pesquisar por informações/dados (e-mail e número de telemóvel) que estão expostos na internet.

- Have i been pwned



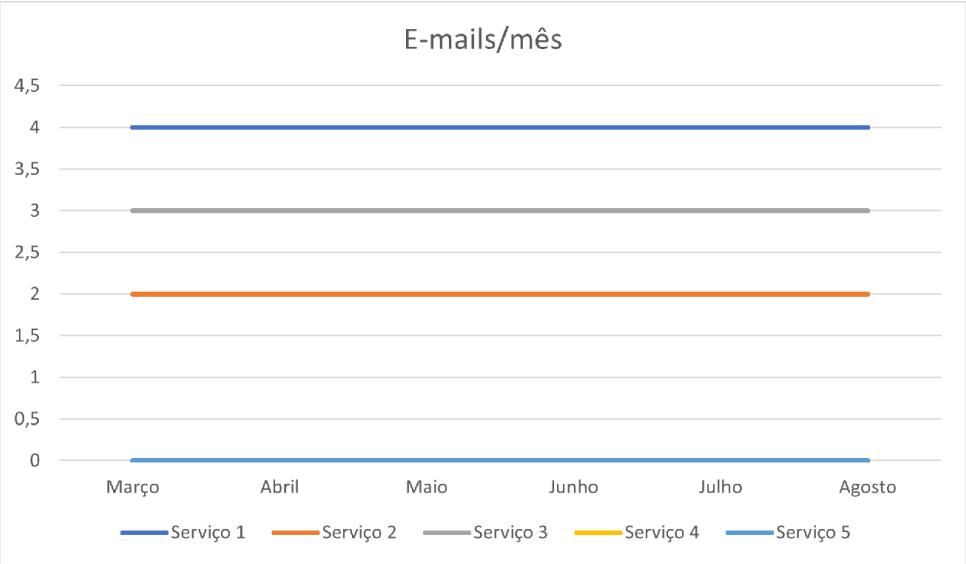
- Inoitsu

Dados expostos/comprometidos

São todos os dados sensíveis, confidenciais, copiados, roubados e/ou transmitidos por um indivíduo/grupo não autorizado.

Respeitando a Lei n.º 58/2019, de 8 de agosto (RGPD), os nomes de funcionários, dados pessoais e os nomes dos respetivos serviços, não serão identificados neste documento.

No seguimento das análises feitas com o auxílio das ferramentas utilizadas foram obtidas as seguintes conclusões representadas nos gráficos seguintes.



Com os e-mails facultados foi elaborada uma análise individual a cada um deles, obtendo assim as seguintes informações:

Serviço 1

- Funcionário 1 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Covve (fevereiro de 2020) e Nitro (setembro de 2020);
- Covve – e-mail, nome, profissão, número de telemóvel, morada, perfis de redes sociais;
- Nitro - e-mail, nome e palavra-passe.

- Funcionário 2 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

- Funcionário 3 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

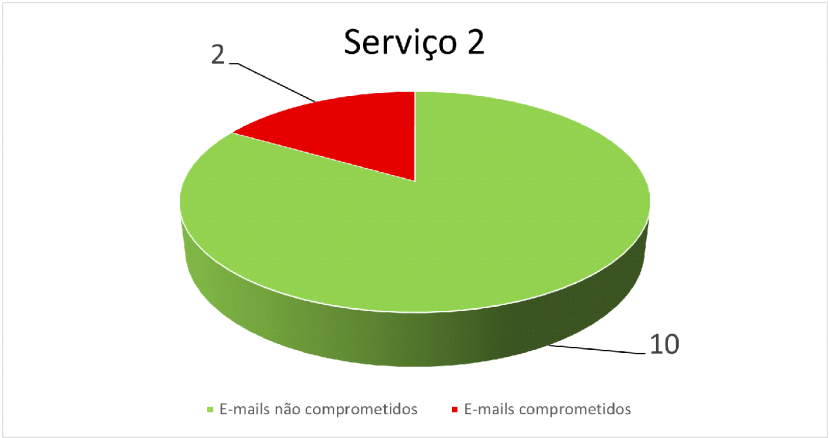
- Funcionário 4 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no PDL (outubro de 2019), LinkedIn (maio de 2016 e durante o primeiro semestre de 2021);
  - PDL - e-mail, profissão, glocalização, nome, número de telemóvel e perfis de redes sociais;
  - LinkedIn (2016) – e-mail e palavra-passe;
  - LinkedIn (2021) – e-mail, nível académico, género, glocalização, profissão, nome e perfis de redes sociais.

- Funcionário 5 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

Serviço 2

- Funcionário 1 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

- Funcionário 2 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020) e Canva (maio de 2019);
  - Nitro - e-mail, nome e palavra-passe.
  - Canva - e-mail, localização geográfica, nome, palavra-passe e nome de utilizador.

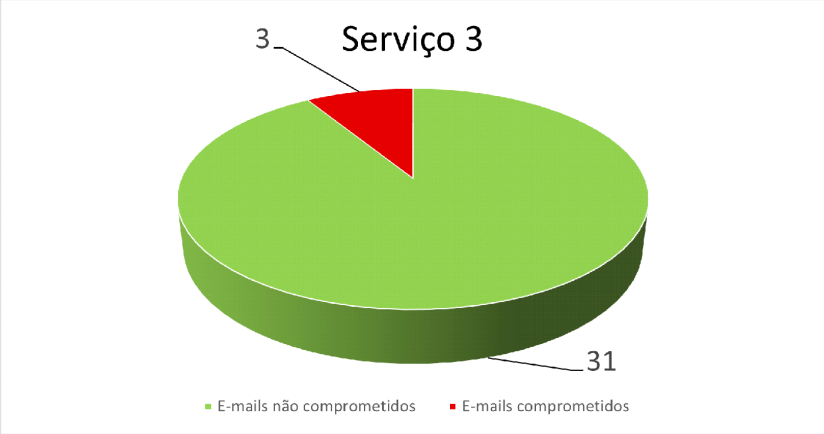


Serviço 3

- Funcionário 1 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

- Funcionário 2 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.

- Funcionário 3 (xxxxxx.xxxxx@ulsguarda.min-saude.pt) no Nitro (setembro de 2020);
  - Nitro - e-mail, nome e palavra-passe.



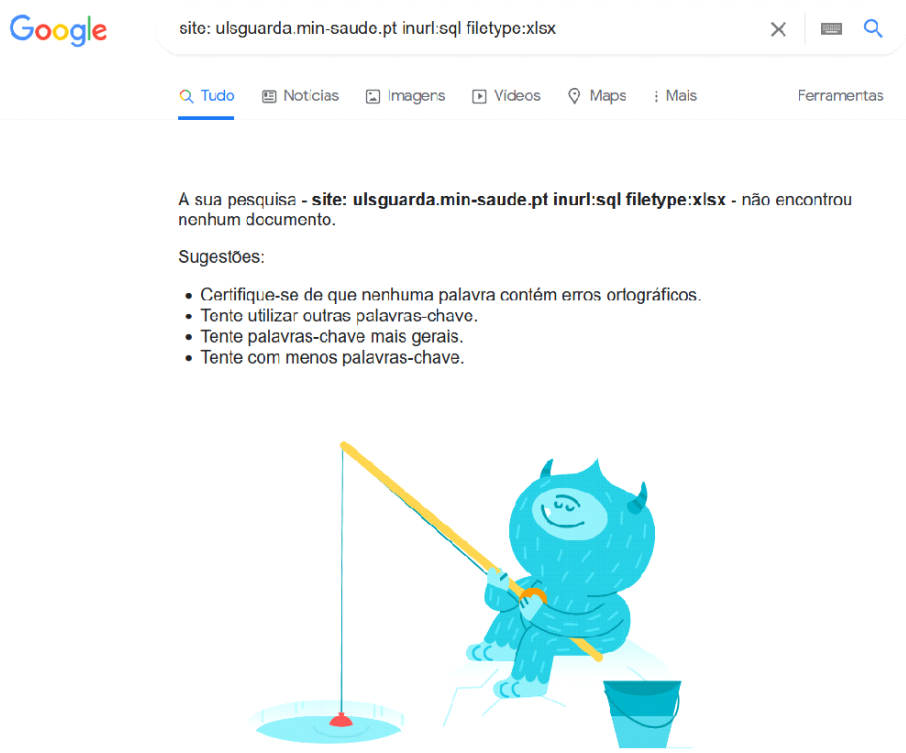
Serviço 4

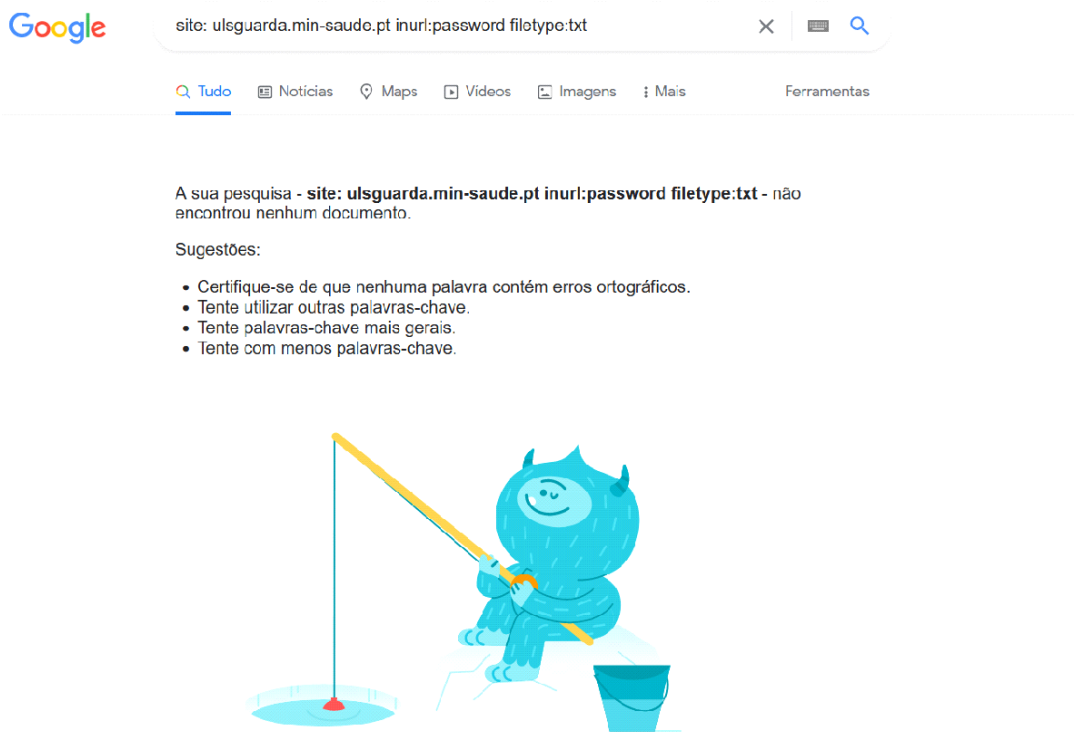
Serviço 5

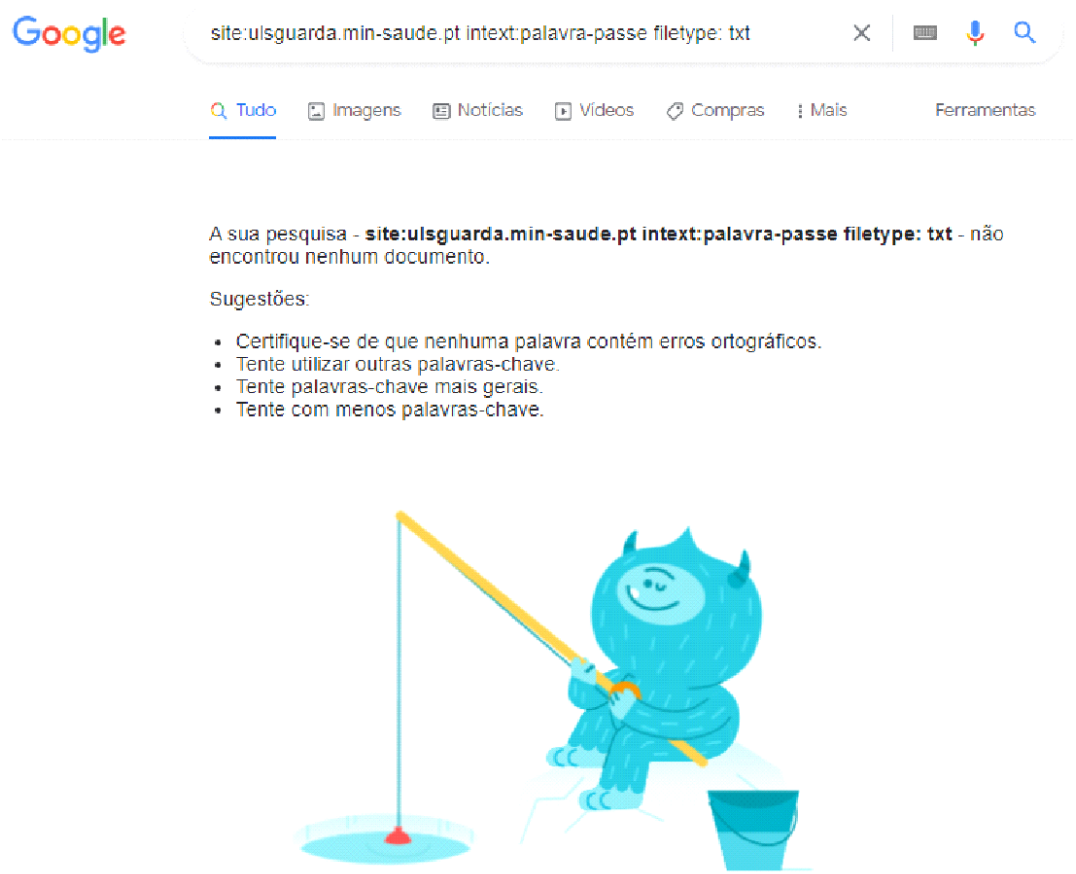
Google Dorks

É um método de procura diferente do tradicional de forma a especificar os resultados obtidos após a seleção especificada.

1) Site: - Pesquisa em *Website;*
2) inurl: - Pesquisa em *Links URL* com *keywords;*
3) intext: - Pesquisa no conteúdo dos *Websites* por k*eywords;*
4) filetype: - Pesquisa por tipos de ficheiros;
5) intitle: - Pesquisa no título dos *Websites* por *keywords*;
6) index of/: - Pesquisa por dados expostos em servidores e domínios;
7) _after: - Pesquisa por datas.




Google
site: ulsguarda.min-saude.pt inurl:password filetypo:txt
Tudo
Notícias
Maps
Vídeos
Imagens
Mais
Ferramentas
A sua pesquisa - site: ulsguarda.min-saude.pt inurl:password filetype:txt - não encontrou nenhum documento.
Sugestões:
Certifique-se de que nenhuma palavra contém erros ortográficos.
Tente utilizar outras palavras-chave.
Tente palavras-chave mais gerais.
Tente com menos palavras-chave.

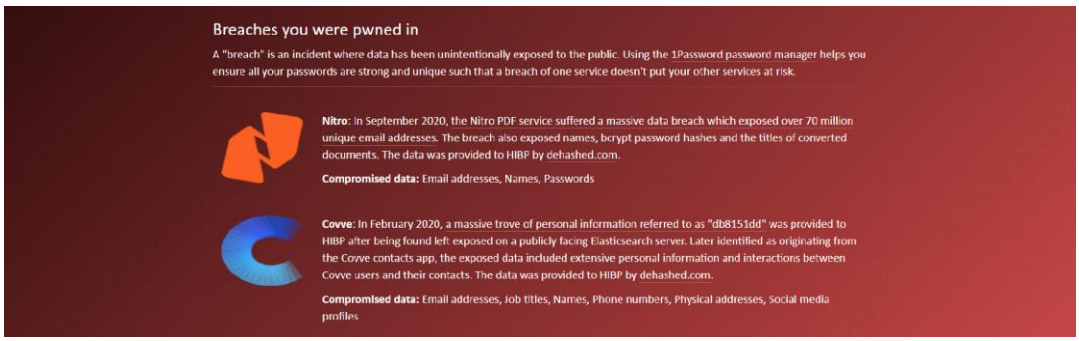

Google
site:ulsguarda.min-saude.pt intext:palavra-passe filetype: txt
Tudo
Imagens
Notícias
Vídeos
Compras
Mais
Ferramentas
A sua pesquisa - site:ulsguarda.min-saude.pt intext:palavra-passe filetype: txt - não encontrou nenhum documento.
Sugestões:
Certifique-se de que nenhuma palavra contém erros ortográficos.
Tente utilizar outras palavras-chave.
Tente palavras-chave mais gerais.
Tente com menos palavras-chave.

Medidas de mitigação

1) Mudar as palavras-passe regularmente;
2) Não utilizar o e-mail institucional fora do contexto de trabalho;
3) Verificação dos dados pessoais nos sites apresentados anteriormente;

Serviço 1

Funcionário 1



Covve
Date of Breach: 2020-02-20
Details: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles,

Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Job titles,Names,Passwords,Phone numbers,Physical addresses,Social media profiles

Identity Alerts: Names,Passwords

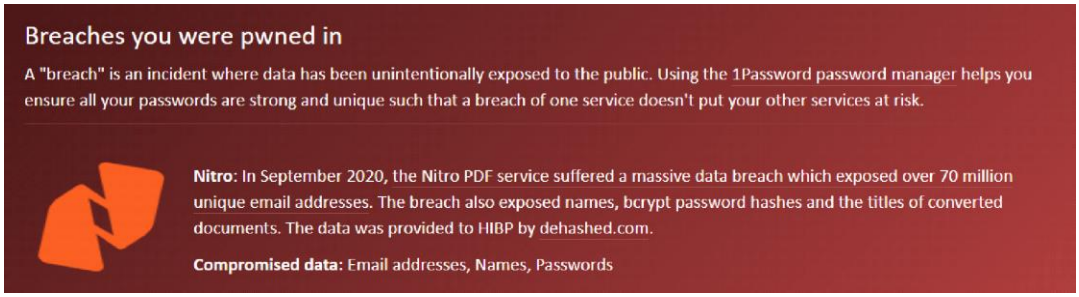
Exposed Contact Info: Phone numbers,Physical addresses,Social media profiles

Total Breaches: 2

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 2



Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

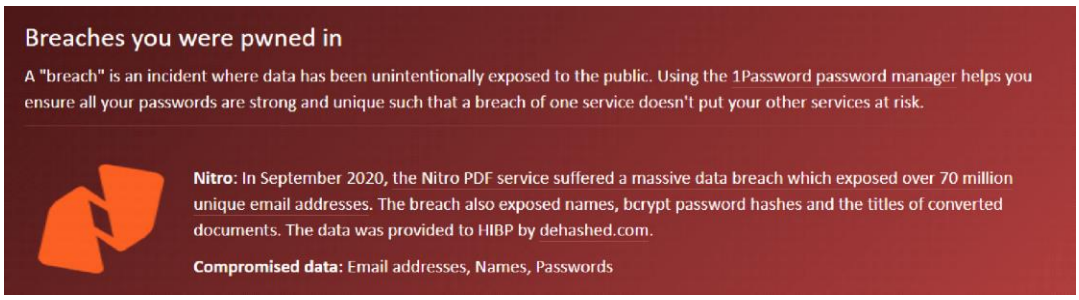
Identity Alerts: Names,Passwords

Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 3



Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

Identity Alerts: Names,Passwords

Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 4

Anti Public Combo List
Date of Breach: 2016-12-16
Details: In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Breached Data: Email addresses, Passwords,

Data Enrichment Exposure From PDL Customer
Date of Breach: 2019-10-16
Details: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.
Breached Data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles,

Exploit.In
Date of Breach: 2016-10-13
Details: In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Breached Data: Email addresses, Passwords,

LinkedIn
Date of Breach: 2012-05-05
Details: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Breached Data: Email addresses, Passwords,

LinkedIn Scraped Data
Date of Breach: 2021-04-08
Details: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.
Breached Data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles,

Trik Spam Botnet
Date of Breach: 2018-06-12
Details: In June 2018, the command and control server of a malicious botnet known as the "Trik Spam Botnet" was misconfigured such that it exposed the email addresses of more than 43 million people. The researchers who discovered the exposed Russian server believe the list of addresses was used to distribute various malware strains via malspam campaigns (emails designed to deliver malware).
Breached Data: Email addresses,

Summary of Breached Data Found: Education levels,Email addresses,Employers,Genders,Geographic locations,Job titles,Names,Passwords,Phone numbers,Social media profiles

Identity Alerts: Names,Passwords

Exposed Contact Info: Employers,Geographic locations,Phone numbers,Social media profiles

Sensitive Personal Data: Genders

Total Breaches: 6

Most Recent Breach: 2021-04-08

Relative Exposure Rating: 2/10

Funcionário 5

Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

Identity Alerts: Names,Passwords

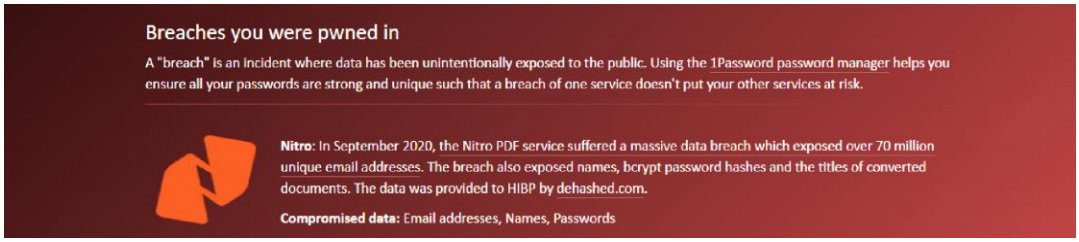
Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Serviço 2

Funcionário 1



Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

Identity Alerts: Names,Passwords

Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 2

Canva
Date of Breach: 2019-05-24
Details: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Breached Data: Email addresses, Geographic locations, Names, Passwords, Usernames,

Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Geographic locations,Names,Passwords,Usernames

Identity Alerts: Names,Passwords,Usernames

Exposed Contact Info: Geographic locations

Total Breaches: 2

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Serviço 3

Funcionário 1

Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

Identity Alerts: Names,Passwords

Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 2

Nitro
Date of Breach: 2020-09-28
Details: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Breached Data: Email addresses, Names, Passwords,

Summary of Breached Data Found: Email addresses,Names,Passwords

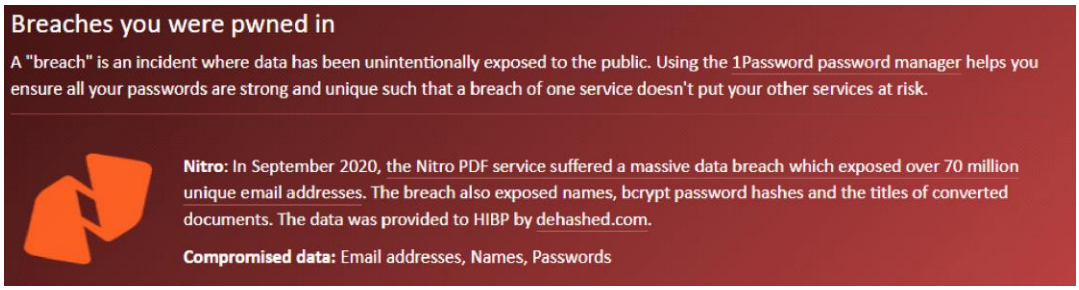
Identity Alerts: Names,Passwords

Total Breaches: 1

Most Recent Breach: 2020-09-28

Relative Exposure Rating: 2/10

Funcionário 3



8.1

Documento de Defesa

Unidade de Saúde Pública da Guarda

Andreia Santos
Bernardo Dias

Agosto de 2022

Proteção de rede

Uma vez conhecidos os tipos de criptografias sem fio (WEP/WPA/WPA2) é relativamente mais fácil proteger as redes contra estes tipos de ataques.
Esta informação mostra os pontos fracos que podem ser usados por hackers para permitir o acesso através destas criptografias.

- **WEP** - É uma criptografia antiga e é a mais fraca. Independente do tamanho e tipo da palavra-passe e mesmo que tenha dispositivos ligados à rede é possível quebrar a criptografia. Esses ataques são possíveis devido à maneira como o WEP funciona, alguns desses métodos permitem que você decifre a chave em alguns minutos.

- **WPA/WPA2** - São muito semelhantes, a única diferença entre eles é o algoritmo usado para criptografar as informações, mas ambas as criptografias funcionam da mesma maneira. WPA/WPA2 pode ser quebrado de duas maneiras:

1. Se o recurso WPS estiver ativo, há uma grande probabilidade de se obter a chave, independentemente da sua complexidade. Pode ser explorada uma falha no recurso WPS. O WPS é usado para permitir que os utilizadores se liguem à rede sem fio sem inserir a chave, isso é feito depois de se pressionar o botão WPS no router e/ou no dispositivo que eles desejam conectar.

Os hackers podem forçar brutalmente este pino num período (em média 10 horas), uma vez que eles consigam o pino correto eles podem usar uma ferramenta chamada "reaver" para fazer engenharia reversa do pino e obter a chave, tudo isso é possível devido ao facto do recurso WPS usar um pino com apenas 8 caracteres e conter apenas dígitos.

2. Se o WPS não estiver ativo, a única maneira de quebrar o WPA/WPA2 é utilizar um ataque de dicionário ("word list"), este ataque tem uma lista de palavras-passe (dicionário) e é comparada com um arquivo (arquivo "handshake") para verificar se alguma delas é a chave real da rede, se a palavra-passe não existir na lista de palavras, o invasor não poderá encontrá-la.

Medidas de prevenção

1) Não utilizar criptografia WEP, devido à facilidade em ser comprometida.
2) Utilizar WPA2 com uma palavra-passe complexa, que contenha letras minúsculas, maiúsculas, caracteres especiais e números.
3) Desativar o recurso WPS uma vez que pode ser usado para comprometer a chave WPA2 com o pino correto.

Arp Spoofing

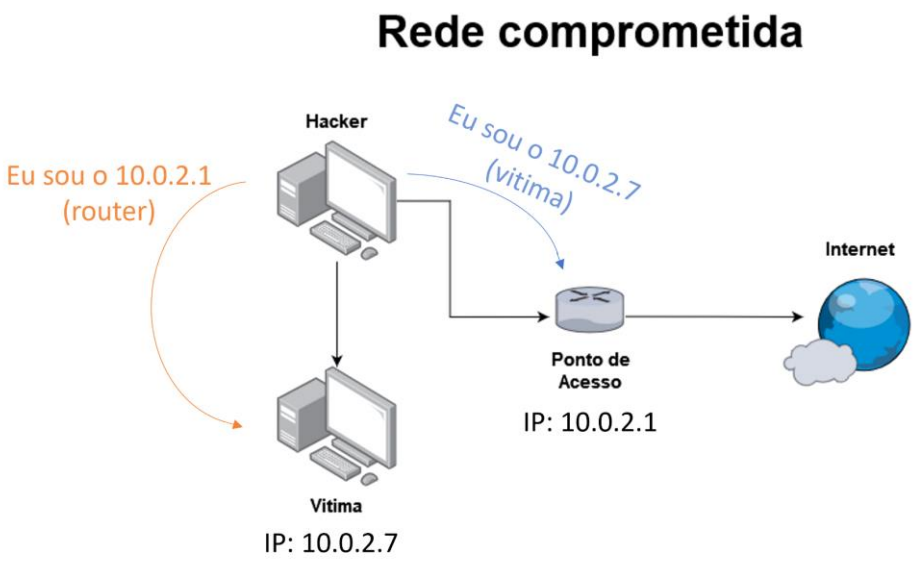
Este tipo de ataque pertence aos ataques MITM. É uma forma de ataque em que os dados trocados entre duas partes são de alguma forma intercetados, registados e, possivelmente, alterados pelo atacante sem que as vítimas se apercebam.

Para isso, o atacante manipula os MACs de cada dispositivo.

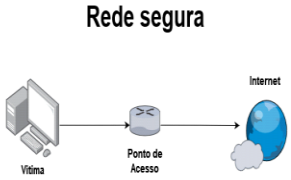
Sendo que cada manipulação tem objetivos diferentes:

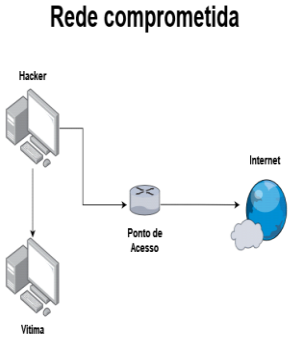
1) Manipulação do mac address do router - Ter o poder de enviar todo o tráfego à sua escolha aproveitando o facto do equipamento da vítima receber, sem hesitação, do respetivo router;
2) Manipulação do mac address da vítima - Direcionar as solicitações para a sua máquina e poder gerir todas as informações para o destinatário real.

Na imagem posterior demonstra um ataque arp spoofing em que existe a presença de um atacante no meio das comunicações na rede dando informações erradas a ambos os dispositivos.



O cenário 2 demonstra uma rede segura, em que as comunicações entre ambos os equipamentos são realizados sem a presença de um terceiro elemento e consequentemente sem qualquer interferência do atacante.





Xarp

O Xarp é um software de segurança que usa técnicas avançadas para detetar ataques.

Este tipo de software evita ataques de manipulação ARP uma vez que as firewalls não os detetam.

Faz parte da categoria de monitorização de rede e é licenciado como shareware para plataforma Windows de 32 e 64 bits e pode ser usado como uma versão gratuita até que a versão de teste acabe. O Xarp Demo está disponível para todos os utilizadores do software, mas com algumas limitações em comparação com a versão completa.

Usar a ferramenta Xarp

Algumas características deste software:

- Deteção de falsificação ARP;
- Monitorização passiva;

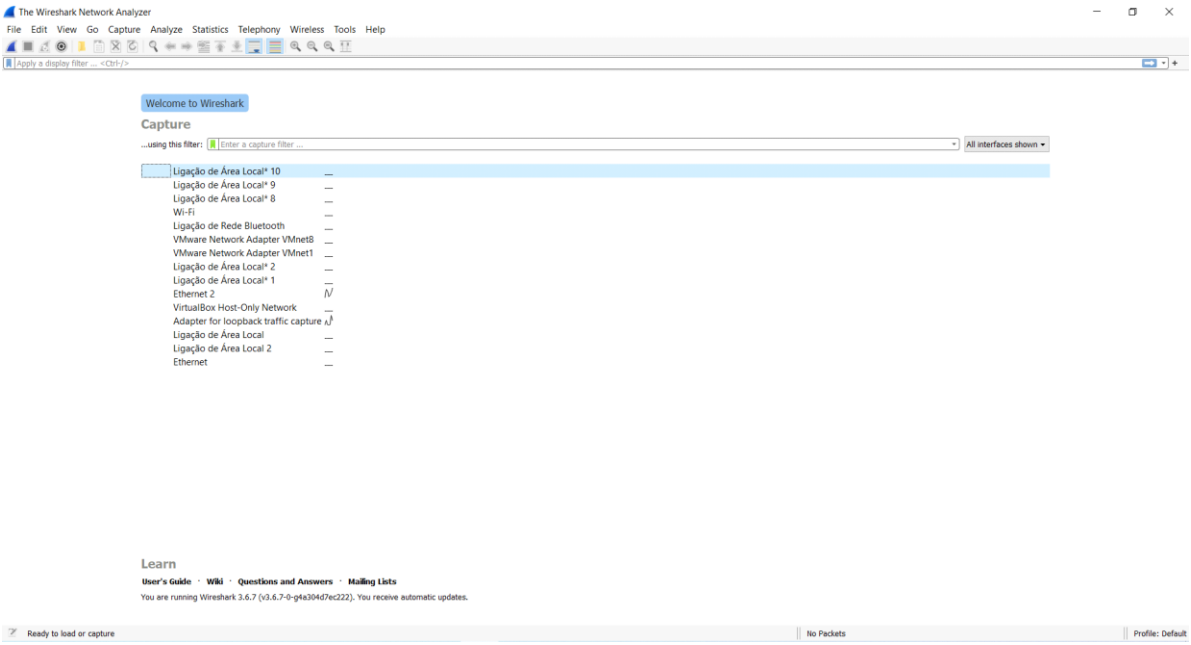
- Validação ativa;
- Níveis de segurança predefinidos;
- Monitorização de rede;
- Alerta de e-mail.

Este software envia uma notificação a alertar o utilizador das alterações feitas no caso de uma eventual deteção de um "arp spoofing". Regista e informa os MACs e IPs que foram consequentemente comprometidos.

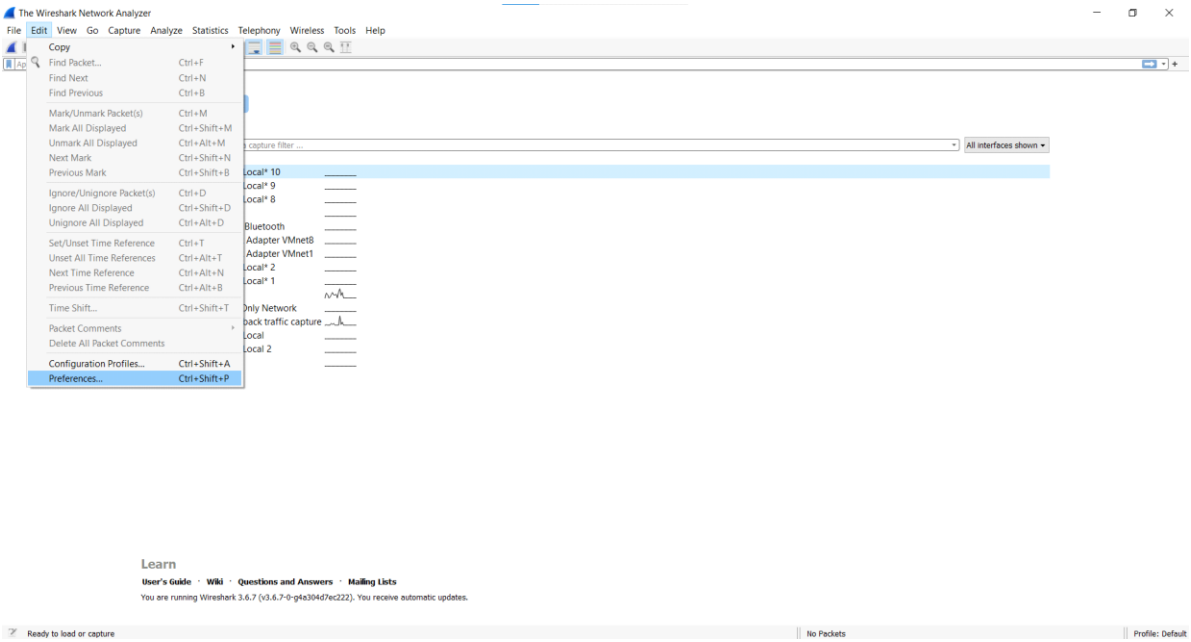
Detectar atividades suspeitas na rede com a ferramenta Wireshark

O Wireshark é um programa que analisa o tráfego de rede e organiza por protocolos e com a possibilidade da utilização de filtros com o objetivo de melhorar a análise.

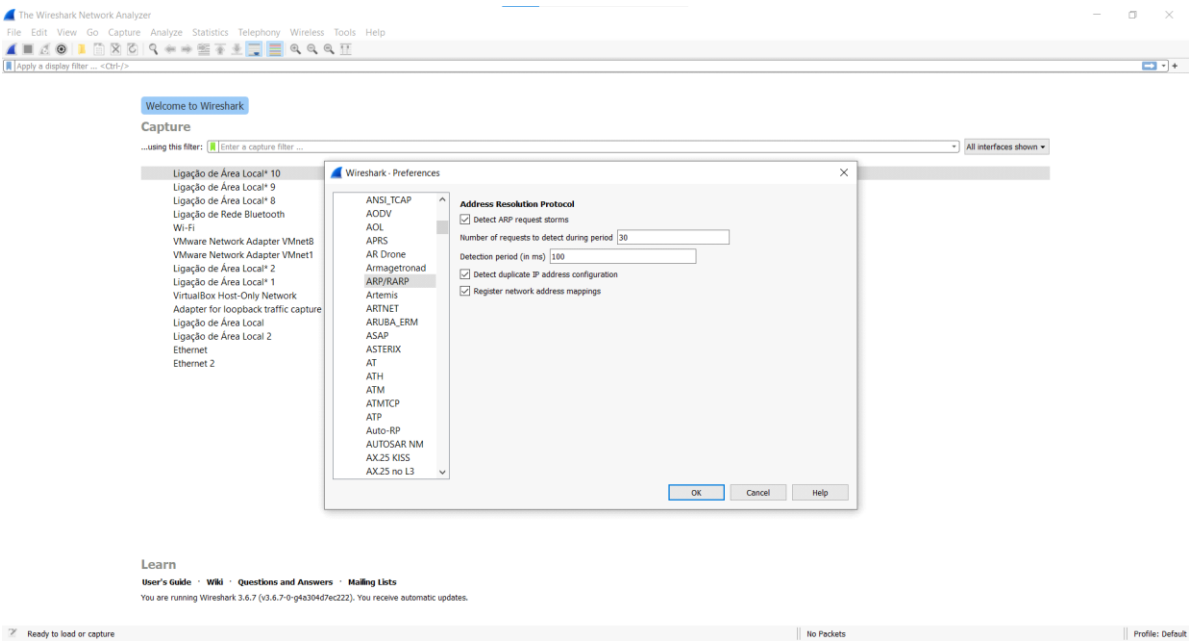
Passo 1 - Página inicial do programa.



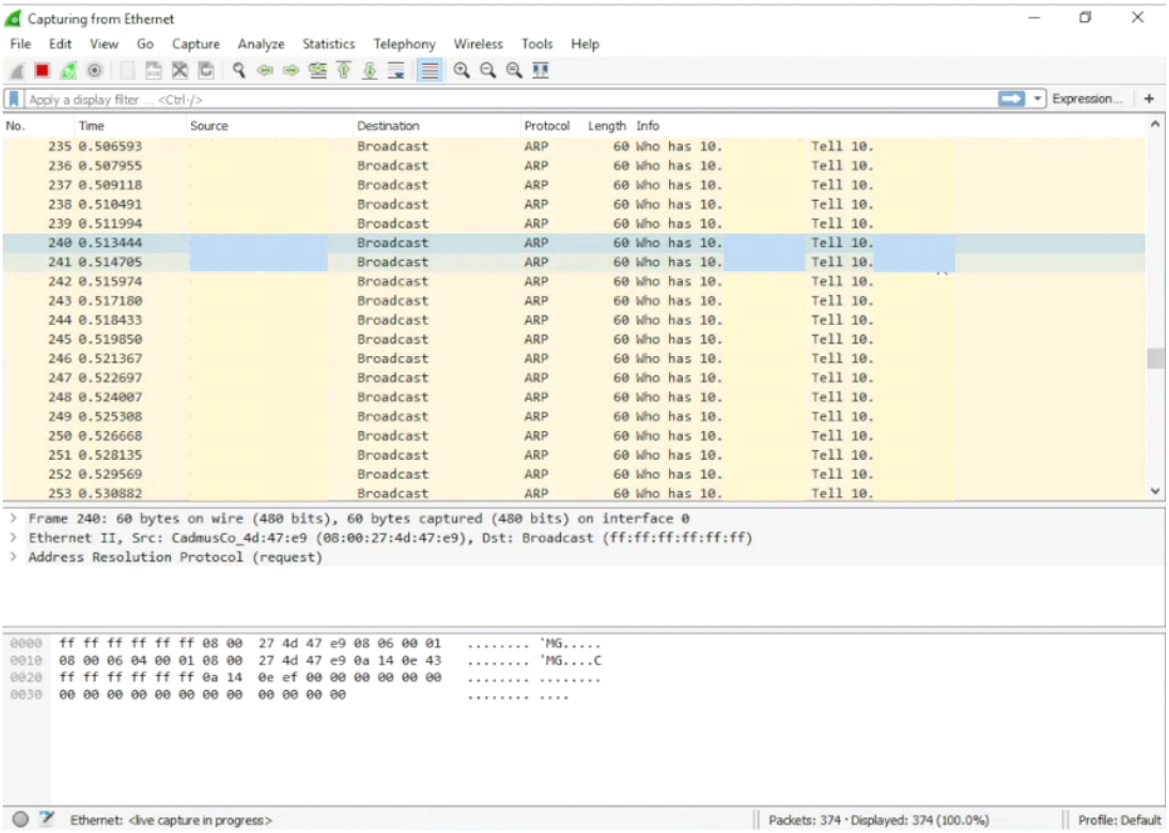
Passo 2 - Aceder às preferências do software;



Passo 3 - Localizar a opção ARP/RARP na categoria "Protocolos" e selecionar a opção de "Deteção de tempestades de solicitações ARP*"* e confirmar a alteração no botão "OK".

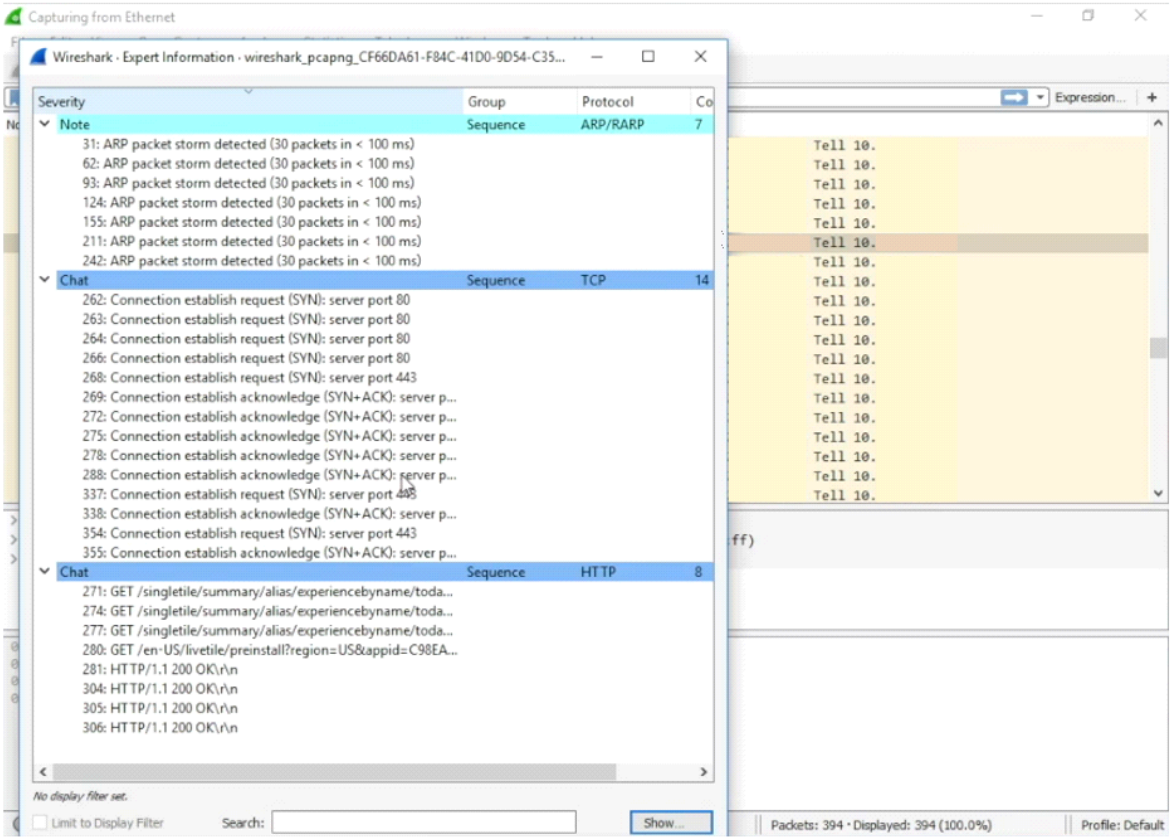


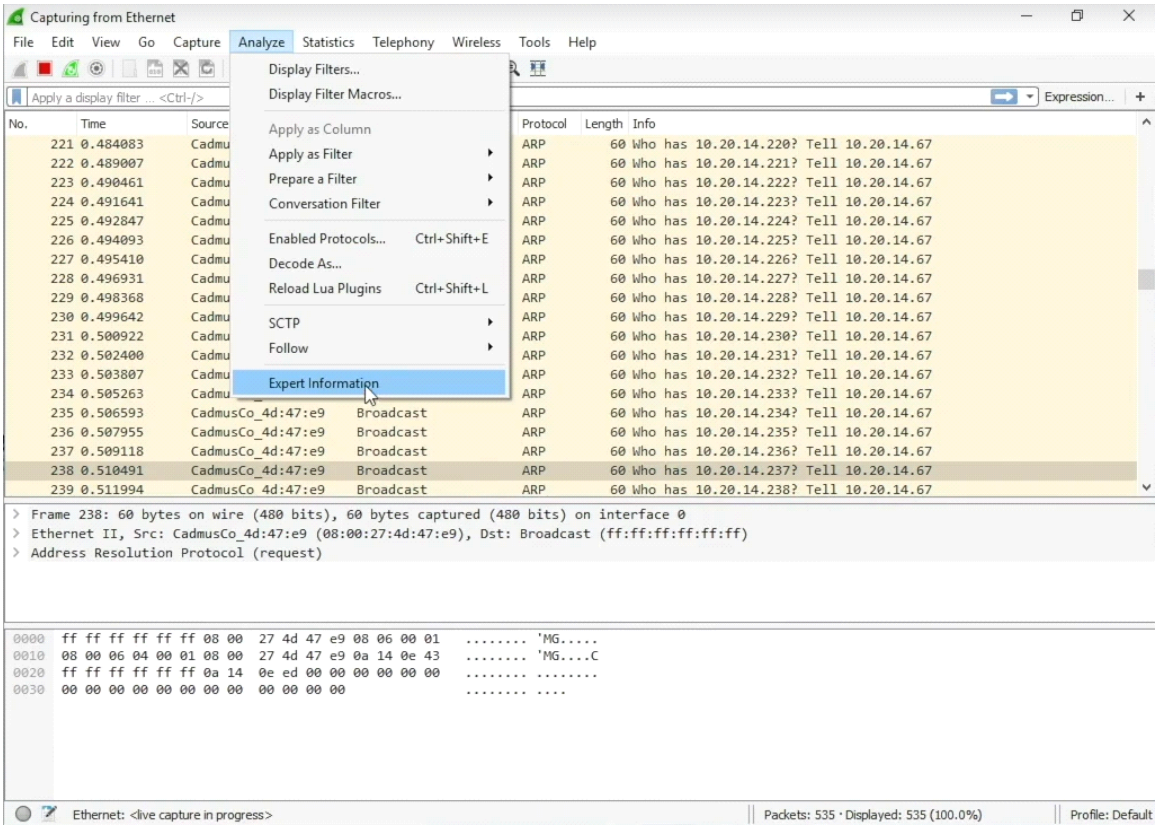
No caso de o atacante executar uma ferramenta para identificação de todos os dispositivos ativos na rede, é neste momento que o wireshark apresenta as "three-way handshake"



trocadas entre o dispositivo dele e todos os outros.

Passo 4 - Visualização de uma grande quantidade de pacotes ARP enviados de um só dispositivo e descoberta de possíveis portas abertas, é neste momento que se torna suspeito.

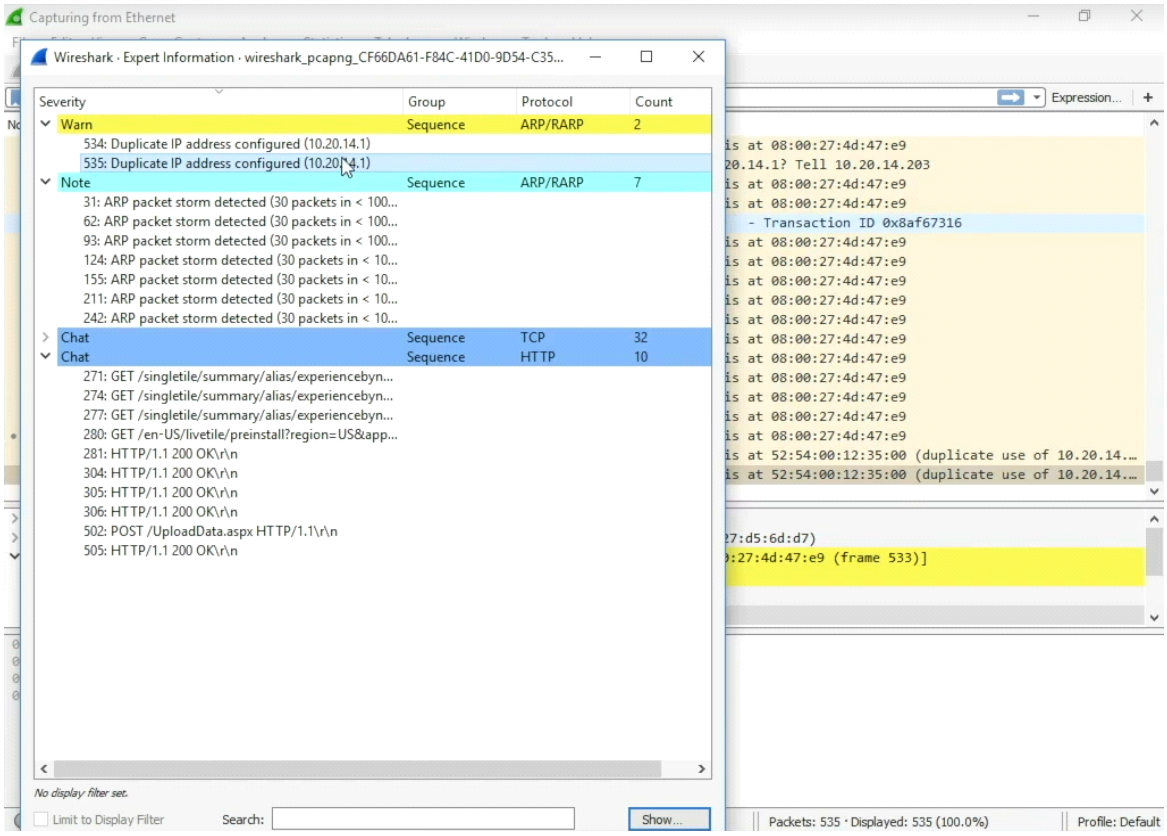




Passo 5 - Aceder a informações especializadas.

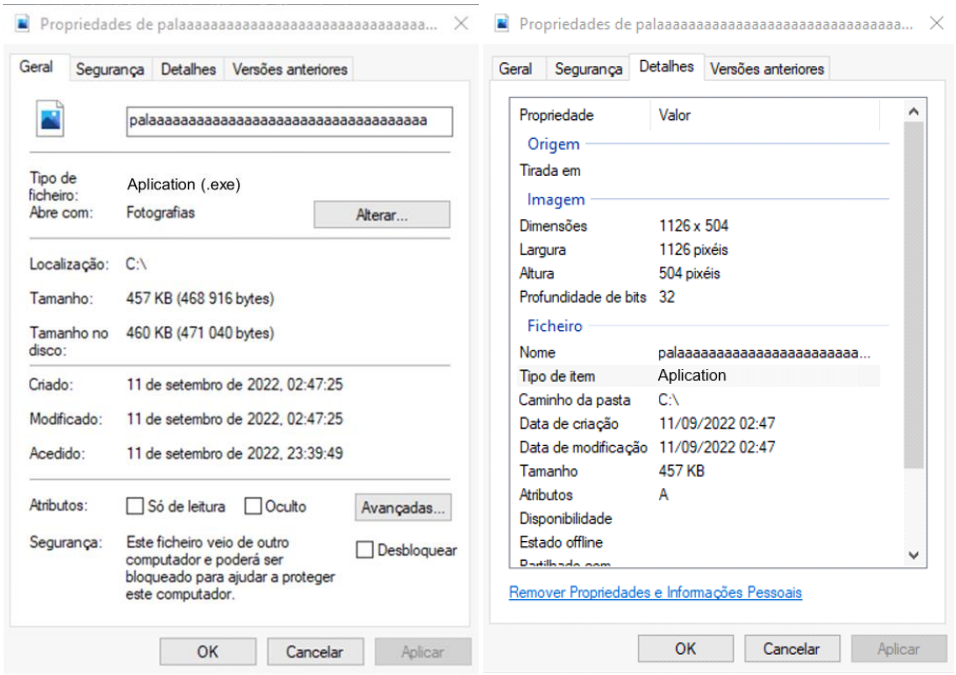
Passo 6 - Visualização do alerta.

É neste momento que o Wireshark informa que há dois dispositivos com o mesmo endereço IP sendo que têm MACs diferentes e se confirma a tentativa de manipulação da tabela ARP.



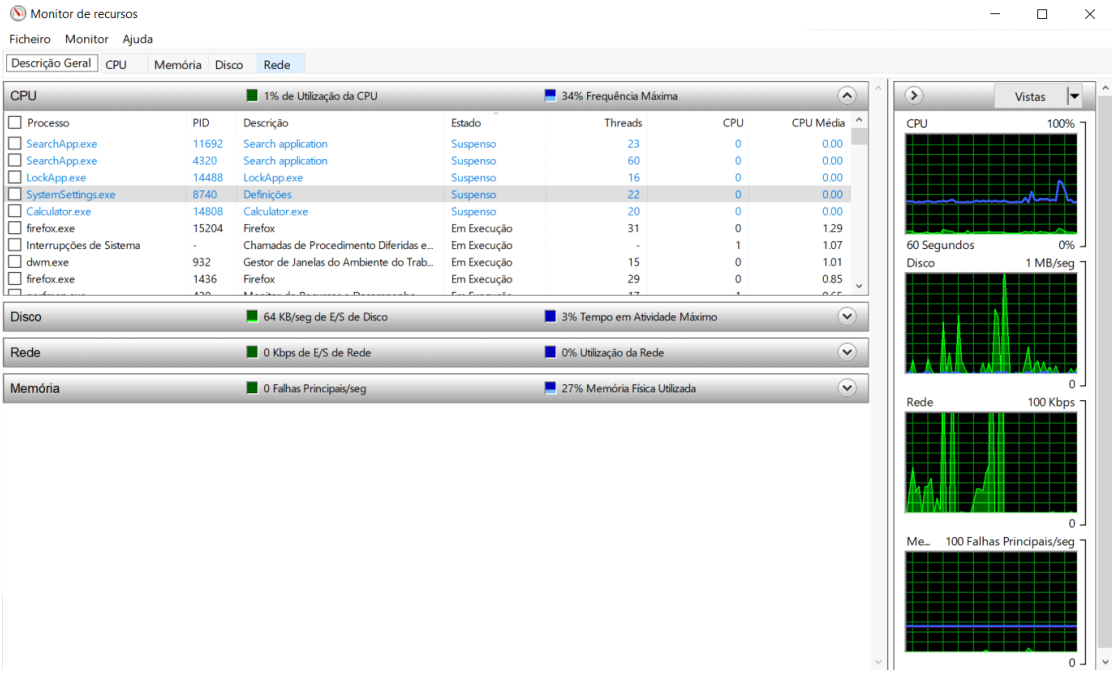
Detectar Trojans Manualmente

Passo 1 - Retificar o tipo de ficheiro nas propriedades do mesmo.

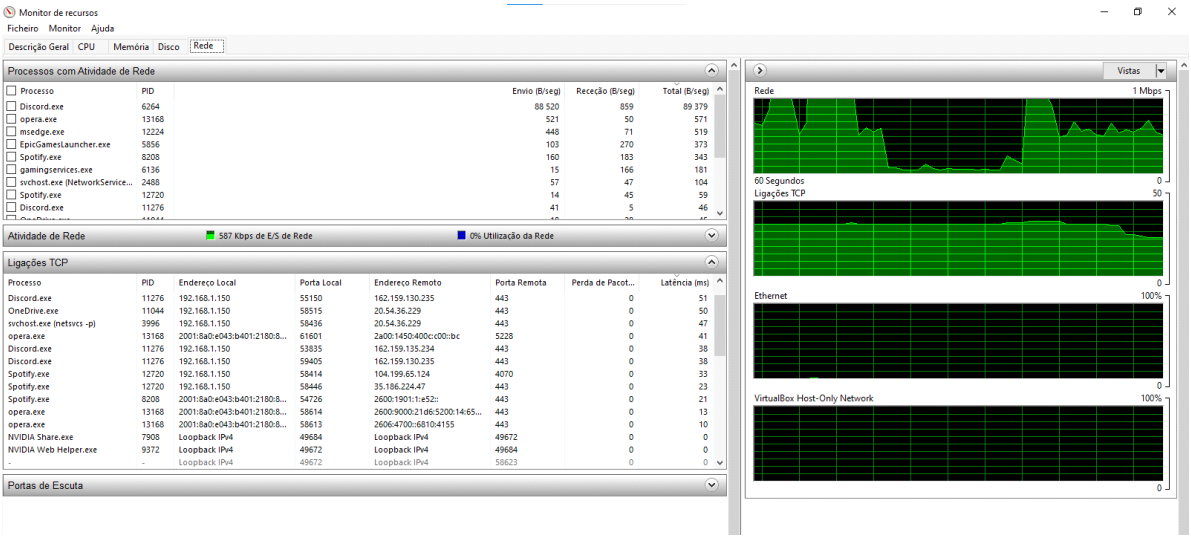


Como é possível verificar nas capturas de ecrã apresentadas, o tipo de ficheiro não corresponde ao esperado. O esperado seria um ficheiro ".png" e na realidade é um executável.

Passo 2 - Aceder à opção de Rede do Monitor de recursos.



Passo 3 - Retificação dos IPs e portas abertas nas ligações TCP.



Passo 4 - Efetuar um ping para o endereço desconhecido.

Passo 5 - Verificação do endereço no browser.

No caso dos endereços IPs serem desconhecidos, a melhor solução passa por realizar uma procura no browser de forma a confirmar a correspondência ao site/aplicação em utilização. Com a ajuda de um site de DNS reverso, é possível detetar a presença de um terceiro dispositivo nas comunicações trocadas.

Exemplo de um site para a deteção de DNS reverso:

https://mxtoolbox.com/ReverseLookup.aspx

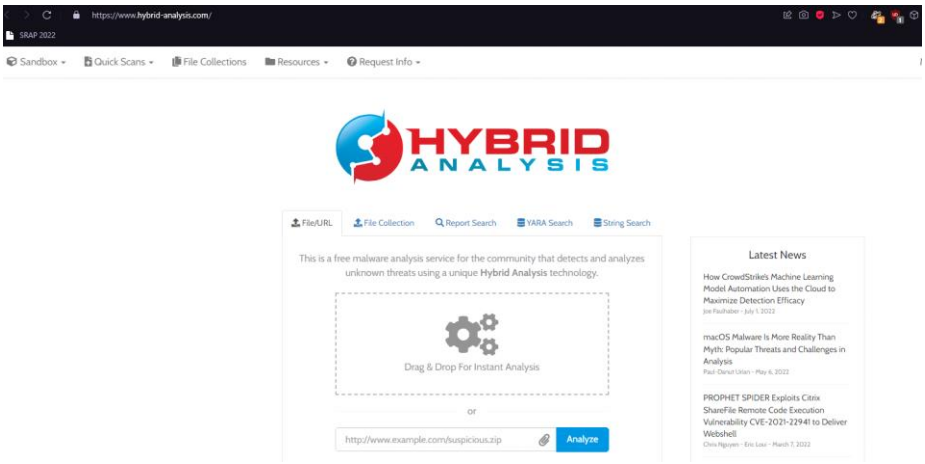
Detectar Trojans com Sandbox

Um sandbox, é um local onde qualquer ficheiro irá ser executado e posteriormente analisado.

Como é um ambiente isolado é possível realizar testes sem arriscar danos ao dispositivo ou à rede. No final também oferece um relatório sobre o ficheiro.

Com o relatório é possível obter informações úteis em termos de segurança informática, em relação ao comportamento do mesmo, podendo saber se tem a capacidade de abrir portas, ou modificar entradas de registo e atividades suspeitas, se possui trojans, etc.

Caso em estudo: “HybridAnalysis”.



Prevenir vulnerabilidades SQL Injection

Vulnerabilidade - SQL Injection

- A maioria dos sites usa uma base de dados para armazenar os dados.
- A maioria dos dados armazenados são nomes de utilizadores, palavras-passe, … etc;
- Aplicação web lê, atualiza e insere dados na base de dados;
- Interação com base de dados é feita usando SQL.

O porquê de serem tão perigosos?

1. Permitem dar acesso à base de dados → dados confidenciais.
2. Pode ser usado para fazer login como administrador e explorar ainda mais o sistema.
3. Pode ser usado para fazer upload de arquivos.

SQL injection (SQLi)

● Tentativa de danificar a página web;

● Utilização de caracteres e palavras "e", "ordenar por" ou " ";

● Testagem de caixas de texto e parâmetros de URL no formulário "http://target.com/page.php?something=something".

Prevenção SQLi

● Usar uma lista negra de comandos;

● Usar lista de permissões;

- Usar instruções parametrizadas, dados separados do código sql.

SQLMAP

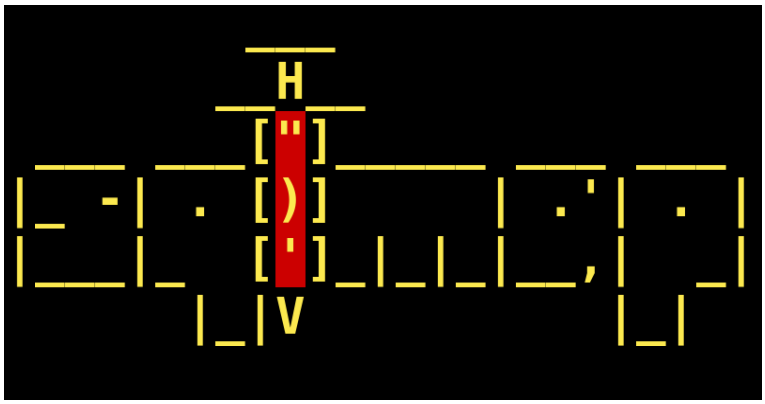
Sqlmap é uma ferramenta de teste de penetração de código aberto que automatiza o processo de detecção e exploração de falhas de injeção SQL. Com essa ferramenta é possível assumir total controlo de servidores de base de dados em páginas web vulneráveis, inclusive de base de dados fora do sistema invadido.

Outro ponto forte desta ferramenta é o facto de funcionar com muitos tipos de base de dados (mysql, mssql, … etc.).

Exemplos de comandos:

> sqlmap --help

> sqlmap -u [url de destino]



Formas de garantir segurança nos sites e nas aplicações

Os ataques informáticos causam um enorme impacto negativo nas empresas, desde a perda de confiança e financeira, espionagem industrial, dados expostos e questões legais. Além dos conselhos apresentados no documento de sensibilização serão apresentados alguns pontos importantes com o objetivo de melhorar a segurança dos sites e aplicações das empresas.

1 - Programação segura;
2 - Revisões constantes às aplicações;
3 - Contratar um serviço de "Pentest" ou criar um posto;
4 - Aderir a plataformas de "Bug Hunt" ou "Bug bounty";

Intervenções	Vantagens	Desvantagens
Programação segura	Muito completo.	Nível académico e experiência profissional exigida de um programador são elevados.
Revisões constantes às aplicações	Muito completo.	Tamanho do código. Dispendioso.
Serviço de pentest	Dá uma boa interpretação das vulnerabilidades da empresa/site.	Dispendioso.
Programas de Bug Hunt ou Bug bounty	Muita procura e oferta. Mais provável que se encontrem falhas.	Não garante uma análise total. Difícil gestão.

Aspetos a melhorar

Redes

- Implementar o syslog-ng;
- Implementar servidor radius;
- Implementar sistema por mac address;
- Evitar usar servidores dhcp;
- Usar hids e nids;
- Bastidores:
  - Melhorar a organização dos cabos de rede;
  - Organizar as ligações dos cabos por cores;
- ARP - trocar para estático todos os IP e MAC de dispositivos de rede de forma a impedir a manipulação de tabelas ARP.

Respostas a Incidentes

Unidade de Saúde Pública da Guarda

Andreia Santos
Bernardo Dias

Agosto de 2022

Índice

Glossário

Ciberataque – Ato ou ação iniciada no ciberespaço para causar dano através do compromisso das comunicações da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas.

Ciberdefesa – Os meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas.

Ciberespaço – Um domínio global e virtual criado pela interligação de todas as redes de Comunicações, informação e sistemas eletrónicos.

Cibersegurança – Estratégia, política e normas com vista à segurança das operações no ciberespaço, abrangendo missões de redução da ameaça, de vulnerabilidades, de compromisso internacional, de resposta a incidentes, resiliência, e políticas de recuperação, incluídas operações em rede, garantia da informação, ações judiciais, diplomáticas, militares e de inteligência relacionadas com a segurança e estabilidade da infraestrutura global de informação e Comunicações.

Incidente – Uma ocorrência que coloca em risco a confidencialidade, integridade ou a disponibilidade de um Sistema de Informação ou dos seus processos, armazenamento ou transmissão.

Resposta a Incidentes

Sempre que um incidente é detetado, devem ser prontamente registados todos os elementos disponíveis e a partir daí, todos os eventos com ele relacionado. A informação recolhida durante a investigação deve ser igualmente armazenada, registada e assinada pelo responsável pela investigação. A validade destas informações como provas usadas em tribunal ou no âmbito de processos disciplinares internos depende do correto dos procedimentos do tratamento dos mesmos.

Deve ser utilizada uma base de dados de registos dos incidentes, que deve conter informação sobre o "estado do incidente", um sumário, o registo de todas as ações realizadas, o contacto dos intervenientes (utilizadores e gestores), a lista das evidências recolhidas e comentários dos gestores. Finalmente, nesta fase há ainda que considerar a classificação do incidente.

Esta poderá ser uma das ações mais importantes, uma vez que os incidentes não são todos iguais e afetam a organização de diferentes formas. É importante fazer uma correta classificação de modo que o incidente seja abordado com a respetiva prioridade.

A priorização a atribuir ao incidente está muito dependente do negócio da organização, ou seja, do impacto que o incidente pode ter do ponto de vista funcional, na segurança da informação. Esta priorização poderá traduzir-se num valor numérico que traduza a severidade e o impacto que o incidente tem para a organização.

Normas e Metodologias para resposta a incidentes

Com o objetivo de contribuir para a Segurança da Informação, nomeadamente no esforço de garantir a qualidade da informação através das premissas de confidencialidade, integridade, autenticidade e disponibilidade, em sistemas cada vez mais abertos e complexos, têm surgido várias normas com recomendações das melhores práticas, especialmente dedicadas aos procedimentos e às políticas a adotar ao nível das tecnologias de informação e comunicação.

As normas existentes são muito abrangentes e acompanham em detalhe todos os processos nas várias fases do desenho da arquitetura de um Sistema de Informação. Considerando o âmbito deste trabalho, será analisado o contributo de algumas normas mais relevantes, no capítulo específico da gestão de incidentes.

Relato de eventos de segurança da informação

O controlo associado a este objetivo foca-se na necessidade de os eventos de segurança serem reportados através dos canais definidos para o efeito, tão depressa quanto possível. Os colaboradores têm de ser capazes de reconhecer um evento de segurança, saber o que fazer e compreender a mais-valia para a organização da existência de uma política de gestão.

O guia de implementação associado a este controlo aponta para a existência de mecanismos de notificação simples e acessíveis à disposição dos colaboradores, fornecedores ou outros utilizadores. O procedimento de notificação deve de incluir:

- Mecanismos apropriados de resposta que garantam o acompanhamento das ações desenvolvidas, até o assunto se encontrar resolvido;
- Um formulário para realizar a notificação do evento de modo a ajudar o colaborador a não se esquecer das ações necessárias;
- Indicação do comportamento esperado perante um evento de segurança;
- Um ponto de contacto, um procedimento formal de notificação de forma que todos os colaboradores devem ter conhecimento da sua existência;
- Referência para um processo disciplinar formal para os colaboradores, fornecedores ou outros, que cometam violações de segurança.

Gestão de Incidentes

Qualquer resposta a incidentes relacionados com cibersegurança deve seguir a orientação "OODA LOOP", este que se predomina, observar, orientar, decidir e agir, seja qualquer tipo de ameaça a uma organização, ou sistema informático.

Todos os incidentes seguindo a lei portuguesa deverão ser reportados pelas entidades às autoridades competentes, tais como, polícia judiciária (PJ), Centro Nacional de Cibersegurança (CNCS).

Os seis passos de qualquer resposta a incidentes subdividem-se nos seguintes:

- ➔ Passo 1 - Preparação;
- ➔ Passo 2 - Identificação;
- ➔ Passo 3 - Contenção;
- ➔ Passo 4 - Erradicação;
- ➔ Passo 5 - Recolha;
- ➔ Passo 6 - Aprendizagens.

Fase da Preparação - Tem como objetivos principais a edificação de uma equipa de resposta a incidentes devidamente treinada e equipada para conseguir limitar o número de incidentes que ocorrem através da seleção dos controlos de segurança adequados a implementar.

A equipa de resposta a incidentes deve possuir um kit portátil, com um computador com software apropriado e ferramentas que permitam a captura de tráfego de rede e a sua análise forense, a realização de backups e algum equipamento básico de rede.

Fase da Identificação - Os tipos de incidentes e o modo como podem atingir a organização são muito variados, e dessa forma não é possível estabelecer um procedimento para cada tipo de incidente. A caracterização deve ser de acordo com o seu modo de transmissão e comportamento, assim como os sinais do incidente (indicações e indícios).

As indicações, como sendo o sinal que um incidente ocorreu ou poderá estar a ocorrer, e os indícios são sinais de que um incidente poderá vir a acontecer. Sempre que um indício seja detectado a organização deverá tomar medidas necessárias visando prevenir o incidente.

Fase da Contenção - A contenção é extremamente importante uma vez que após a deteção de um incidente que tenha ocorrido, ou esteja ainda a ocorrer, é necessário responder de modo a limitar ao máximo os seus efeitos. Para isso devem existir previamente, estratégias e procedimentos de contenção para os diversos tipos de incidentes.

Fase da Erradicação - Em alguns casos este passo apenas pode ser feito em conjunto com a recuperação, como é frequente nos casos dos incidentes de malware, pois a eventual destruição dos ficheiros infetados implica a necessária reposição dos ficheiros afetados, o mesmo se passando perante o compromisso de credenciais de utilizadores, que numa primeira fase poderá passar pela eliminação da conta do utilizador nos sistemas e posteriormente a criação de novas contas.

Esta relação é particularmente importante quando os sistemas são afetados a nível dos seus sistemas operativos. A erradicação passa muitas vezes por se fazer uma nova instalação do sistema, recuperando, no entanto, as informações de customização anteriormente existentes.

Fase da Aprendizagens - Após o encerramento de um incidente, toda a equipa deve ser reunida e o processo deve ser analisado de modo a averiguar o que aconteceu, como aconteceu e porque aconteceu. Na ausência de incidentes, a equipa deve reunir-se periodicamente e analisar o conjunto de vários incidentes, sempre com o objetivo de identificar melhorias e propô-las para que sejam incorporadas na fase de preparação. No final deve ser elaborado um relatório do incidente com toda a informação sobre o mesmo e com as conclusões resultantes da reunião da equipa e com as sugestões de melhoria.

Capacidade de resposta a Incidentes

Pessoal - O fator humano é determinante, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão.

Monitor de Incidentes - Estes elementos têm por principal função a monitorização dos eventos nas plataformas de segurança, na plataforma de eventos e a receção das notificações recebidas por correio eletrónico. Todos os eventos detetados e notificações recebidas devem ser registados na plataforma de gestão de incidentes.

Gestor de Incidentes - Estes indivíduos têm a responsabilidade de gerir o incidente desde que este é introduzido na plataforma até a uma resolução do mesmo. Cada um dos incidentes registados na plataforma deve ser assumido por um gestor de incidentes.
Compete ao Gestor do Incidente fazer uma primeira triagem para confirmar que se está perante um incidente.
O Gestor de Incidentes pode solicitar apoio aos Analistas Forenses para a resolução do incidente ou para análise de vulnerabilidades e proposta de mitigação.
Analista Forense - O Analista Forense tem por principal função ajudar na investigação de incidentes quando esta exige um conhecimento técnico. O seu conhecimento técnico permite-lhe fazer um estudo mais aprofundado, recorrendo à análise forense na área de redes e sistemas, das vulnerabilidades que permitiram a ocorrência do incidente e propor ações de mitigação dessas vulnerabilidades. Deve colaborar diretamente com o Gestor do Incidente, para realizar uma reavaliação das medidas estabelecidas.
Coordenador - O Coordenador tem como principal função a gestão diária do funcionamento da resposta a incidentes. Este deve acompanhar o desempenho dos níveis de operação, garantir uma distribuição de tarefas e que os incidentes estão a ser geridos pelos indivíduos mais adequados às funções a desempenhar. Deve-se garantir um planeamento adequado de formação para os diversos elementos do grupo responsável.

Recomendações de Segurança

Política de Logging - Consolidação dos "log" das diversas plataformas numa plataforma centralizadora. Definição de uma política de retenção de "log".
Correlação de eventos - Capacidade de correlacionar os "log" de diferentes equipamentos (firewall, IDPS, outros) detetando assim indícios de incidentes.
Sincronização de relógios - Utilização do protocolo NTP permite uma efetiva correlação de eventos ocorridos em várias máquinas da organização.
Base de dados conhecimento e informação - Documentação sobre a infraestrutura e vulnerabilidades conhecidas. Informação relativa a softwares e domínios maliciosos.

Tecnologias Usadas em investigações

Sift Workstation

A Sans Investigative Forensics Toolkit (SIFT) é uma distribuição de computação forense criada pela equipe SANS Forensics para realizar análises forenses digitais. Esta distribuição inclui a maioria das ferramentas necessárias para análise forense digital e exames de resposta a incidentes. O SIFT é de código aberto e está disponível publicamente gratuitamente na internet. SIFT fornece ferramentas forenses para sistemas de arquivos, memória e investigações de rede para realizar investigações forenses aprofundadas.

Volatility

Em 2007, a primeira versão do The Volatility Framework foi lançada publicamente na Black Hat DC.

O software foi baseado em anos de pesquisas académicas publicadas em análise avançada de memória e forense. Até aquele momento, as investigações digitais concentravam-se principalmente em encontrar fraudes nas imagens do disco rígido.

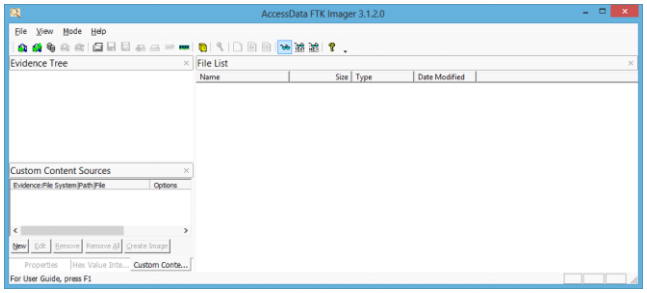
A volatilidade apresentou às pessoas o poder de analisar o estado do tempo de execução de um sistema usando os dados encontrados no armazenamento volátil (RAM).

Desde então, a análise de memória tornou-se num dos tópicos mais importantes para o futuro das investigações digitais e a Volatility tornou-se a plataforma forense de memória mais usada no mundo. Tornou-se uma ferramenta de investigação digital indispensável,

utilizada por policias, militares, académicos e investigadores comerciais em todo o mundo.

FTK Imager

O FTK Imager é uma ferramenta de elaboração de cópias perfeitas (imagens forenses) de dados de computador sem fazer alterações nas provas originais. É também possível visualizar arquivos e pastas em discos rígidos locais ou numa unidade de rede, exportar arquivos e pastas de imagens forenses, ver e recuperar arquivos que foram apagados, criação de hashes de arquivos e gestão de relatórios de hash para arquivos regulares e imagens de disco.



Método de pensamento

Ao realizar uma investigação, é importante lembrar as opções disponíveis para o investigador. Este documento pretende ser uma referência às ferramentas que podem ser usadas. Cada um desses comandos são executados localmente num sistema.
A famosa expressão "**O que sabemos sobre este incidente?**" é o primeiro pensamento que qualquer investigador deve ter. Dessa forma, o investigador pode planear melhor a análise forense.

Exemplo:
Foi dada uma imagem de um computador oriundo de uma empresa que sofreu um ataque de DDoS (serviço negado de rede), e com essa informação o investigador pode assim seguir um percurso de investigação forense mais focada em redes.

Comandos do Sift Workstation

Para a análise da imagem ser mais completa, são analisados vários parâmetros, podendo ser divididos nos seguintes:

1. Montagem de Imagens

pslist - visão geral dos processos a correr;
pstree - mostra as relações entre os processos e a "timeline" dos processos;

2. Análise de Processos

dlllist - Lista de ddls carregados através de processos;
-P - conseguimos procurar por PIDs específicos;

3. Verificação das ligações de rede

netscan - scan às ligações TCP e sockets;
Nota importante: usar os comandos "*connscan*" e "*sockscan*" em sistemas baseados em Windows XP.

4. Procura de evidências de código injetado

malfind - Encontra código injetado;
-P - Mostra apenas informações em PIDS específicos;

5. Sinais de Rootkits

psxview - Descobre processos escondidos através do crooss-view;
modscan - Faz verificações da memória carregada e não carregada.

Documento Informativo ULS da Guarda

Unidade de Saúde Pública da Guarda

Andreia Santos
Bernardo Dias

Agosto de 2022

ATENÇÃO!

O Serviço de Sistemas e Tecnologias da Informação e Comunicações da Unidade Local de Saúde da Guarda apela à sensibilização de todos os utilizadores com o objetivo de proteger não só os seus dados pessoais assim como o nosso hospital e os centros de saúde.

Para evitar o pior basta seguir os conselhos apresentados posteriormente nos diferentes contextos.

Phishing/Smishing - Técnica usada para enganar utilizadores e obter informações confidenciais.

Prevenção->

- Desconfiar de links e anexos de origem desconhecida;
- Confirmar a veracidade do remetente e o respetivo conteúdo;
- Verificar com o remetente em caso de dúvida.

- 

Ransomware - Ataque informático com o objetivo de bloquear o sistema alvo e posteriormente exigir um resgate do mesmo.

Prevenção->

- Não abrir/executar ficheiros de origem desconhecida;
- Contactar o Departamento Informático o mais rápido possível.

- 

Palavras-passe -

Prevenção->

- Incluir letras maiúsculas e minúsculas, números e caracteres especiais;
- Utilizar no mínimo 8 dígitos;
- Usar diferentes palavras-passe nos websites/serviços;
- Não pronunciar em voz alta ou partilhar palavras-passe com terceiros;
- Não associar a dados pessoais;
- Mudar a palavra-passe regularmente.

E-mails -

Prevenção->

- Não utilizar o e-mail institucional fora do contexto de trabalho.

Independentemente do departamento a que pertença é muito importante adotar todos estes hábitos. Passos simples que fazem toda a diferença.

Proteja-se, por si e por to