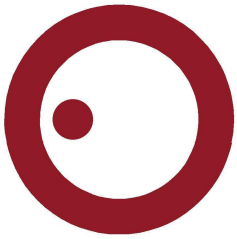


escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

RELATÓRIO DE ESTÁGIO - SIBS MULTICERT

ESTUDANTE RICARDO SILVA

Leiria, Setembro de 2024

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

RELATÓRIO DE ESTÁGIO - SIBS MULTICERT

ESTUDANTE RICARDO SILVA
Número: 2223362

Dissertação realizada sob orientação do Professor Doutor Paulo Manuel Almeida Costa (paulo.costa@ipleiria.pt).

Leiria, Setembro de 2024

AGRADECIMENTOS

Quero agradecer todo o esforço que o Professor Doutor Paulo Manuel Almeida Costa teve, bem como a sua dedicação, paciência e ajuda para que este relatório fosse entregue.

Agradeço profundamente a pessoa que posso e é uma honra chamar de amiga Cristiana Modesto por tudo o que fez por mim.

Agradeço pela oportunidade que me foi dada para realizar este curso bem como ao estágio curricular à Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria e a todos os Professores que me ajudaram a cumprir esta etapa da minha vida. Muito obrigado, ao Professor Miguel Frade, ao Professor Mário Antunes, ao Professor Patrício Domingues, à Professora Maria Piedade, ao Professor Leonel Santos, ao Professor Adail Oliveira e ao Professor Baltazar Rodrigues.

Ao meu supervisor de estágio Sr. Tiago Cardoso, ao Sr. José Inês e ao Sr. Valetim Oliveira, tanto como aos meus colegas de trabalho Nuno Fernandes e Diego, agradeço pela ajuda prestada e debate de ideias durante a realização das atividades propostas.

Por fim um agradecimento especial aos meus pais e avós, pelo apoio incondicional durante toda a minha vida académica.

RESUMO

O presente relatório tem como objetivo apresentar o trabalho desenvolvido no âmbito do estágio curricular que decorreu na empresa "SIBS Multicert - Serviços de Certificados Eletrónica S.A., localizada em Lisboa, Portugal. A área de inserção deste relatório é a cibersegurança, nomeadamente, na resposta a incidentes. A área de resposta a incidentes é crucial no quotidiano de um profissional da área de cibersegurança, pois a crescente sofisticação dos ataques, exige uma resposta rápida e eficaz das organizações. Neste contexto, os documentos DFIR emergem como ferramentas indispensáveis para responder aos incidentes, juntamente com a necessidade de existirem laboratórios digitais equipados com ferramentas adequadas, sendo um meio fundamental para o aperfeiçoamento dos métodos de resposta abordados nos documentos DFIR, como também para treinar os profissionais de cibersegurança.

Relativamente aos tópicos abordados, este relatório inicia-se com a contextualização do ambiente em que este estágio decorreu. De seguida é exposto o trabalho que foi realizado, nomeadamente, as tarefas propostas, as mudanças necessárias e as tomadas de decisões. Ainda, são detalhadas todas as tarefas e entregáveis inerentes a este estágio bem como as dificuldades sentidas ao longo da sua execução. Por último, são apresentadas as conclusões retiradas com o trabalho realizado e a bibliografia consultada.

ABSTRACT

The aim of this document is to present the work carried out as part of the curricular internship at the company 'SIBS Multicert - Serviços de Certificados Eletrónica S.A.', located in Lisbon, Portugal. This document focuses on cybersecurity, specifically incident response. The area of incident response is crucial in the day-to-day life of a cybersecurity professional, as the growing sophistication of attacks requires organisations to respond quickly and effectively. In this context, DFIR documents emerge as indispensable tools for responding to incidents, along with the need for digital laboratories equipped with appropriate tools, being a fundamental means of perfecting the response methods covered in DFIR documents, as well as training cybersecurity professionals.

With regard to the topics covered, this report begins by contextualising the environment in which this internship took place. It then goes on to describe the work that was carried out, in particular the tasks proposed, the changes required and the decisions made. It also details all the tasks and deliverables inherent in this internship, as well as the difficulties experienced during its execution. Finally, the conclusions drawn from the work carried out and the bibliography consulted are presented.

ÍNDICE

LISTA DE FIGURAS

Glossário

Plano de Reposta a Incidentes (Incident Response Plan) – PRI (IRP) - Conjunto de instruções ou procedimentos para detectar, responder ou mitigar danos estruturados numa documentação.

Resposta a Incidente (Incident Response) -RI (IR) - Ações conduzidas por organizações quando existe suspeita ou a confirmação de que sistema(s) pode(m) ter sido violado(s).

Perícia Forense Digital e Resposta a Incidentes (Digital Forense and Incident Response) – FDRI (DFIR) - Documento, denominado de playbook, com a combinação de duas áreas da cibersegurança, a resposta a incidentes e informática forense. A análise forense investiga como os incidentes aconteceram e a resposta a incidentes deteta, responde, mitiga e recupera, quando se há um incidente.

Forense Digital - Área de investigação e reconstrução de incidentes, através da recolha e análise dos artefatos achados.

Evento - Ocorrência observável numa rede ou sistema, podendo ser indicio de incidente ou não.

Vulnerabilidade - Insuficiência, de qualquer natureza, que pode ser explorada por uma ou mais ameaças.

Ameaça - Potencial causa de incidentes indesejáveis, podendo resultar em danos para a empresa ou organização. Podendo ser ameaças acidentais ou deliberadas.

Alerta - Eventos gerados automaticamente pelos SIEM a partir dos eventos recolhidos (logs), para posterior triagem.

Incidente - Evento adverso com consequência(s) negativa(s) que depois de analisados pelos profissionais de cibersegurança são considerados incidentes.

Ataque - Tentativa de expor, desativar, destruir, alterar, roubar ou obter acesso não autorizado a um ambiente digital de uma empresa, organização ou terceiro.

Ataque zero-day - Ataque nunca antes conhecido que explora vulnerabilidade(s).

Métricas de Avaliação - Existem quatro (4) tipos de possíveis incidentes, conhecido por métricas de avaliação: verdadeiro positivo, quando se confirma que de facto é um ataque, falso positivo, quando se pensa que é um ataque, mas na verdade, é um evento, verdadeiro negativo, quando se pensa que é um evento e

de facto é um evento, e falso negativo, quando se pensa que é um evento mas, na verdade, é um ataque.

Risco - Possibilidade de uma ameaça ser explorada num ambiente digital de um terceiro.

Agente da ameaça - Individuo que efetua o ataque.

Malware - software concebido para propósitos maliciosos.

Ransomware - Forma de malware. Utilizado como ferramenta para bloquear o acesso às informações de um terceiro e pedir um resgate para voltar a ter acesso.

Phishing - Tipo de ataque digital que utiliza engenharia social, que utiliza diferentes tipos de meios para chegar às vítimas, como por exemplo, websites e emails.

Engenharia social - Método de manipulação das vítimas de modo a obter as informações pessoais com o proposito de realizar ataques digitais.

Exflitração de dados - Roubo, movimentação não autorizada ou remoção de quaisquer dados de um ambiente digital

Software - componente intangível de um sistema computacional responsável por executar tarefas programadas ao hardware.

Kali Linux - Sistema operativo, com ferramentas de cibersegurança utilizado por profissionais da área.

MITRE Caldera - Plataforma de emulação de um adversário desenvolvida pela MITRE Coporation. Permite as equipas de segurança realizarem simulações de ataques digitais.

LISTA DE ABREVIATURAS

ANACOM	Autoridade Nacional de Comunicações.
bit	Digito binário.
Byte	Unidade de informação digital composta por oito bits.
CCIS	Consórcio Centro Internet Segura.
CISO	Diretor de segurança da informação.
CNCS	Centro Nacional de Cibersegurança.
CSIRT	Equipa de Resposta a Incidentes.
DFIR	Digital Forensics and Incident Response.
ENSC	Estratégia Nacional de Segurança do Ciberespaço.
IP	Internet Protocol.
NIST	National Institute of Standards and Technology.
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RCMCS	Roteiro para Capacidades Mínimas de Cibersegurança..
SIEM	Gestão de Informações e Eventos de Segurança.
SO	Sistema Operativo.

1

INTRODUÇÃO

O presente relatório apresenta o trabalho desenvolvido no âmbito do estágio curricular de mil e quatrocentas (1400) horas, com início em dezoito de setembro de dois mil e vinte e três (18/09/2023) e termino a dia três de junho de dois mil e vinte e quatro (03/06/2024), na empresa SIBS Multicert - Serviços de Certificação Eletrónica S.A.. Relativamente aos ramos de atividade, a SIBS Multicert faz prestação de serviços de certificação eletrónica, incluindo a instalação, montagem e gestão de infraestruturas técnicas adequadas, a emissão, validação e gestão de certificados eletrónicos, a formação em tecnologias de informação, comunicações e segurança, entre outros ramos de atividade.

1.1 Tarefas propostas

Este relatório pretende expor as tarefas executas no âmbito deste estágio, as metologias utilizadas, resultados obtidos e trabalhos futuros. Relativamente às tarefas executadas, estas foram acordadas entre ambas as partes e consistem nas seguintes:

- Elaboração de documentação de resposta a incidentes e análise forense (denominado por documento DFIR), com base em dois incidentes, Ransomware e Phishing;
- Elaboração do processo de recolha e manuseamento de prova digital, executando um levantamento de documentação e formação em ferramentas necessários para o trabalho dos profissionais de cibersegurança designados por First Responders;
- Preparação de modelos de relatório para apresentação de resultados, consistindo em três (3) relatórios de comunicação: um (1) para a comunicação com os colaboradores da empresa; um (1) para a comunicação com os stakeholders; um (1) para a comunicação pública; um (1) relatório relativamente à resposta ao incidentes; um (1) para a fase de análise forense e um (1) para o pós incidente especificamente para a comunicação à administração;
- Criação de laboratório virtual para análise de evidências;

- Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados.

Nas tarefas foram aplicados conhecimentos obtidos nas unidades curriculares no ano letivo transato, como é o caso da unidade curricular de Políticas e Análise de Risco na Segurança da Informação, Segurança em Rede de Computadores, Cibersegurança Ofensiva e Defensiva I (um) e II (dois), Administração Segura de Sistemas Informáticos, Análise Forense Digital I (um) e II (dois), Gestão e Análise de Relatórios de Segurança e Tratamento de Incidentes de Segurança Informática. Estas unidades curriculares forneceram bases fundamentais para a criação do documento DFIR e dos laboratórios digitais. Exemplo disto são os módulos "Métodos de Investigação", "Autopsy"e "Relatório"abordados na unidade curricular de "Análise Forense Digital".

Com o intuito de organizar o tempo por tarefa foi elaborado um gráfico de Gantt que sofreu alterações consoante as necessidades e as novas lições académicas e não académicas do quotidiano laboral. Com tal, apresenta-se o Gráfico de Gantt original:

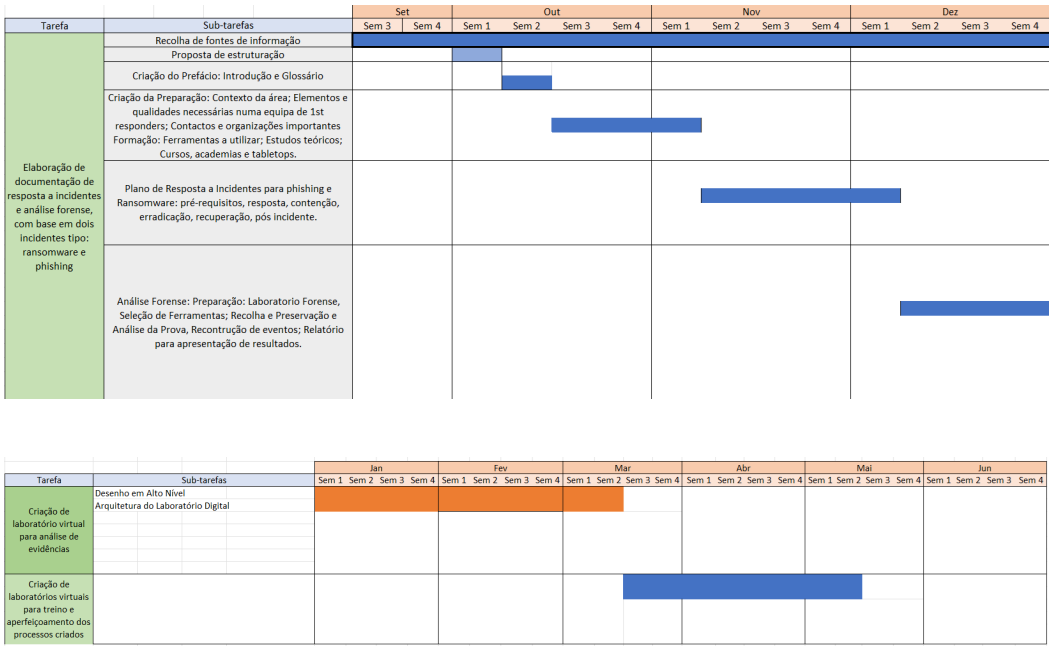


Figura 1: Gráfico de Gantt original

Na Figura 1 é apresentado o gráfico de Gantt original na íntegra, constituído por três (3) tarefas principais:

- "elaboração de documentação de resposta a incidentes e análise forense, com base em dois incidentes tipo: ransomware e phishing";
- "Criação de laboratório virtual para análise de evidências";

- "Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados";

Apresenta oito (8) subtarefas:

- "Recolha de fontes de informação";
- "Proposta de Estruturação";
- "Criação do Prefácio": "Introdução"e "Glossário";
- "Criação da Preparação": "Contexto da Área"; "Elementos e qualidades necessárias numa equipa de 1st responders"; "Contactos e Organizações Importantes";
- "Formação": "Ferramentas a Utilizar"; "Estudos Teóricos"; "Cursos, Academias e Tabletops";
- "Plano de Resposta a Incidentes para Phishing e Ransomware": "Pré-requisitos", "Resposta", "Contenção, Erradicação, Recuperação", "Pós-incidente";
- "Análise Forense": "Preparação": "Laboratório Forense", "Seleção de Ferramentas"; "Recolha e Preservação"e "Análise da Prova", "Reconstrução de eventos"; "Relatório para apresentação de resultados";
- "Desenho em Alto Nível"; "Arquitetura do Laboratório Digital".

Estas tarefes e subtarefas são constituídas por dependências, ou seja, sem a conclusão da primeira (1ª) tarefa/subtarefa não se avançaria para a seguinte.

A primeira (1ª) tarefa trata-se da criação de um documento DFIR (Resposta a Incidentes e Análise Forense) para dois tipos de incidentes: ransomware e phishing.

A segunda (2ª) tarefa “Criação de laboratório virtual para análise de evidências”, tem como objetivo a criação de um laboratório digital. Este laboratório consiste numa máquina virtual alocada no computador pessoal, onde fosse possível fazer a análise forense das evidências encontradas.

Na terceira (3ª) tarefa “Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados”, tem como objetivo a criação de um laboratório digital constituído por duas máquinas virtuais: uma que serviria de ataque e outra que serviria de vítima desse ataque, alocadas no computador pessoal. A máquina virtual de ataque foi configurada com o sistema operativo Kali e foi ainda instalado nesta o programa MITRE Caldera.

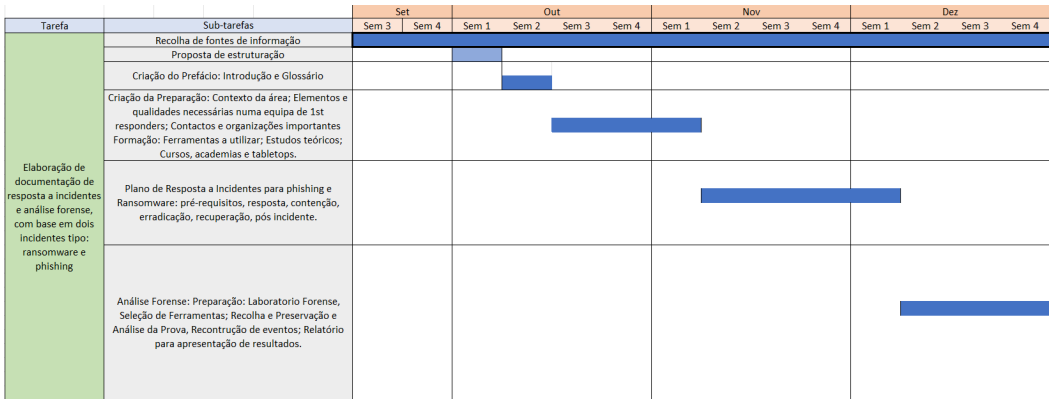


Figura 2: Gráfico de Gantt original, primeira tarefa

Separando o gráfico de Gantt, pode-se observar com mais detalhe na Figura 2, as durações de cada subtarefa. A primeira (1ª) subtarefa "Recolha de fontes de informação", foi planeada para que durasse três (3) meses e duas (2) semanas, pois a recolha de informação é um ato constante, e teve-se ainda em consideração o facto deste ser um estágio curricular para desenvolver competências teóricas, técnicas e humanas. Na segunda (2ª) subtarefa "Proposta de estruturação" que durou uma semana, foram planeadas, estudadas e organizadas todas tarefas e subtarefas e as suas durações de maneira a que tudo o que foi planeado no documento "Proposta de Estágio" fosse cumprido até ao término do estágio curricular. Na terceira (3ª) subtarefa "Criação do Prefácio: Introdução e Glossário" iniciou-se a criação do documento DFIR - Resposta a Incidentes & Análise Forense em si, começando pela introdução e pelo glossário, tendo sido planeada a sua conclusão no fim da segunda semana de outubro. A quarta (4ª) subtarefa "Criação da Preparação: Contexto da área; Elementos e qualidades necessárias numa equipa de 1st responders; Contactos e organizações importantes; Formação: Ferramentas a utilizar; Estudos teóricos; Cursos, academias e tabletops;", com duração prevista de três (3) semanas (término no fim da primeira (1ª) semana de novembro), teve como objetivo a preparação de uma boa resposta a incidentes e da sua análise forense, descrevendo-se: os tipos de elementos que uma equipa deve ter e as suas qualidades, as possíveis ferramentas a utilizar e os ensinamentos teóricos, nomeadamente cursos, academias e tabletops que podem ser frequentados. Na quinta (5ª) subtarefa "Plano de Resposta a Incidentes para Phishing e Ransomware: pré-requisitos, resposta, contenção, erradicação, recuperação, pós-incidente;" e na sexta (6ª) subtarefa "Análise Forense: Preparação: Laboratório Forense, Seleção de Ferramentas; Recolha e Preservação e Análise da Prova, Reconstrução de eventos; Relatório para apresentação de resultados;", foi planeada a preparação da resposta dos incidentes e a análise forense

a partir das diversas fases de um incidente, sendo dispendidos um (1) mês e três (3) semanas para a escrita desses mesmos capítulos.

Nas tarefas "Criação de laboratório virtual para análise de evidências" e "Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados", observa-se que estas não têm as subtarefas, uma vez que só com os conhecimentos adquiridos na execução do documento DFIR é que seria possível melhor planear as próximas fases. Note-se ainda que, foi previsto, a execução da tarefa "Criação de laboratório virtual para análise de evidências" em dois (2) meses e duas (2) semanas e a tarefa "Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados" em dois (2) meses, deixando três (3) semanas sem tarefas para que se pudesse rever tudo o que foi criado fosse possível implementar possíveis melhorias e/ou resolver possíveis imprevistos, se necessário.

1.2 Tarefas Realizadas

Abaixo, é apresentado o Gráfico de Gantt (Figura 3) com as subtarefas e as suas reais durações:

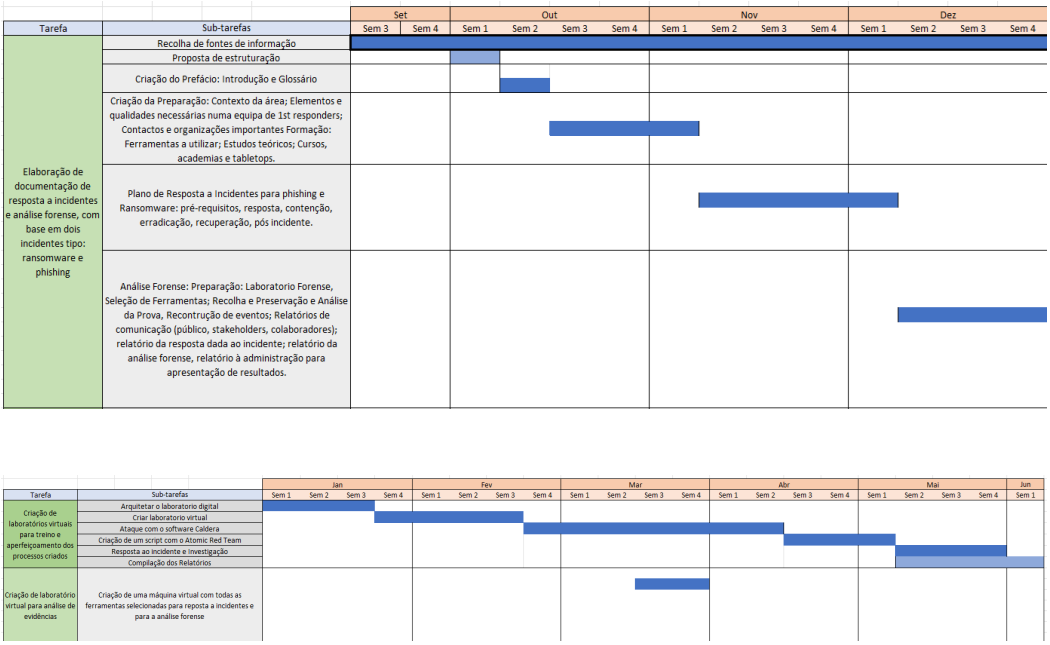


Figura 3: Gráfico de Gantt com as subtarefas e durações em que na realidade foram executadas

De seguida, apresenta-se o mesmo gráfico ampliado (Figura 4) em específico para a primeira (1ª) tarefa:

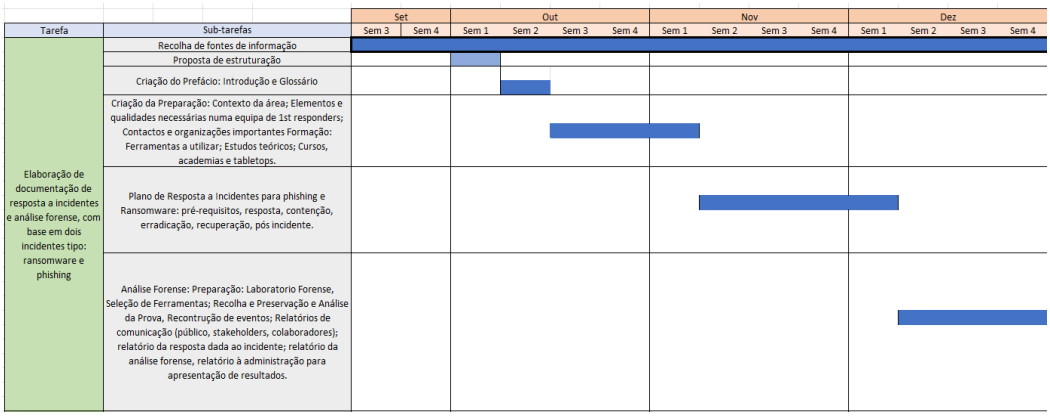


Figura 4: Gráfico de Gantt ampliado em específico na primeira (1ª) tarefa

Como se pode observar, na primeira tarefa nada mudou, ou seja, as tarefas planeadas foram executadas no tempo estipulado (Figura 5).

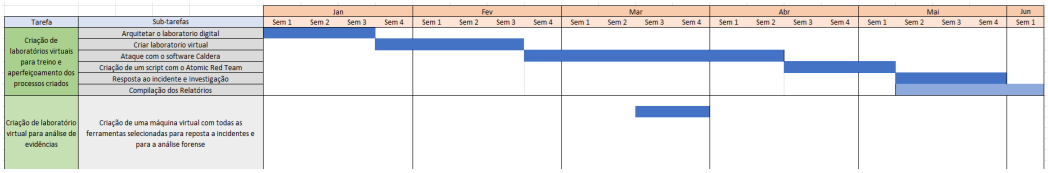


Figura 5: Gráfico de Gantt das duas ultimas tarefas complementadas e atualizadas

Já as duas (2) últimas tarefas foram completadas com as devidas subtarefas e foi mudada a ordem de execução. Assim, a segunda (2ª) tarefa passou a ser “Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados” e a terceira (3ª) “Criação de laboratório virtual para análise de evidências”. Adicionalmente, a segunda tarefa sofreu complicações e alterações que mudaram a estratégia inicialmente definida, o que será explicado com mais detalhe no capítulo de Desenvolvimento.

1.3 Síntese

Este relatório está organizado em quatro (4) capítulos: o atual faz a introdução e contextualização do trabalho; no caítulo dois (2) com o nome de "Trabalho Relacionado"onde se faz um levantamento do estado atual dos documentos DFIR e dos laboratórios digitais; no capítulo três (3), é exposto o trabalho que foi realizado, nomeadamente, as tarefas propostas, as mudanças necessárias e as tomadas de decisões e, ainda, são detalhadas todas as tarefas e entregáveis inerentes a este estágio bem como as dificuldades sentidas ao longo da sua execução; por último, no capítulo quatro (4) são apresentadas as conclusões retiradas com o trabalho realizado e a bibliografia consultada.

2

TRABALHO RELACIONADO

A evolução da documentação de DFIR (Digital Forensics and Incident Response) tem sido significativa ao longo dos últimos anos. Esta evolução foi impulsionada pelo aumento da complexidade das ciberameaças juntamente com necessidade de responder a incidentes de uma forma rápida e eficaz.

2.1. DFIRs - Desafios

Contudo, garantir a consistência e a qualidade dos DFIRs tem sido um grande desafio para organizações privadas e públicas. Outros desafios associados à documentação DFIR são os seguintes:

- Existe proliferação de Formatos: a falta de um padrão universal para a documentação DFIR, que tem uma variação tão vasta de formatos e estruturas, dificulta a colaboração entre diferentes equipas e a condução das análises;
- Escassez de detalhes técnicos: por norma, a documentação oferecida é superficial, omitindo detalhes técnicos críticos para a compreensão dos pontos abordados na documentação(como por exemplo, sobre os detalhes críticos na recolha de evidências e nas análises realizadas);
- Obstáculos com o acesso: a documentação pode estar dispersa em diferentes tipos de documentos, o que dificulta a obtenção de informação para a criação dos documentos DFIR;
- Manutenção inadequada: devido à informação não estar devidamente atualizada, tal leva a que informações obsoletas, incompletas e desatualizadas sejam utilizadas na formulação dos documentos DFIR.
- O crescente volume de dados gerados pela organizações e a complexidade da arquitetura dos sistemas torna a formulação da documentação mais elaborada e demorada;
- Tempo de resposta e a falta de recursos: havendo a necessidade de responder rapidamente a incidentes de segurança é preciso garantir a imediata disponibilidade de recursos humanos, financeiros e técnicos necessários para tal. A

falta destes recursos pode limitar a deteção e a capacidade de responder a estes incidentes.

2.1.1. Tendências e Soluções

- Utilizar ferramentas que sofreram processos de automatização, tanto na recolha como na análise de artefatos, facilita a execução dos processos referidos e, ainda, a possibilita a redução de erros humanos;
- A aplicação de inteligência artificial na análise de grandes volumes de dados permite a criação de relatórios mais precisos, mais completos e detalhados;
- O armazenamento e a partilha de documentação em plataformas Cloud facilita o acesso à mesma e a colaboração entre equipas.

2.1.2. Ransomware e Phishing

Ao especificar o tema na criação de DFIRs focados em incidentes de Ransomware e Phishing, pode-se afirmar que a documentação tem sido importante a combater a sofisticação das ciberameaças.

O estado de arte e desafios específicos de Ransomware e Phishing:

- Ransomware: como tem existido cada vez mais proliferação dos ataques de Ransomware, tem sido necessária uma documentação DFIR mais detalhada e eficaz. Por sua vez, a recolha de informação sobre as novas variantes de Ransomware e sobre os vetores de ataque e os métodos de exfiltração de dados, tornaram-se fundamentais para a investigação e a prevenção de futuros incidentes. Logo, a documentação DFIR deve conter ações técnicas e as técnicas de negociações entre os agentes de ameaça e as vítimas;
- Phishing: Os documentos relativos aos incidentes de phishing exigem uma elaboração cuidadosa sobre as engenharias sociais utilizadas, o que cativou a vítima a sofrer o incidente e os mecanismos de payload. Ou seja, a análise das campanhas de phishing é crucial na identificação das táticas, técnicas e procedimentos (TTPs), que devem ser consideradas na criação ou atualização dos documentos DFIR.

2.1.3 Empresas que proporcionam soluções comerciais de cibersegurança

- CrowdStrike: esta empresa com a sua plataforma de criptografia ponta a ponta auxilia a deteção e a resposta a ameaças;
- Palo Alto Networks: para além das reconhecidas firewalls, a Palo Alto Networks oferece uma plataforma que inclui funcionalidades DFIR;

- Tenable: esta empresa é especializada em soluções de gestão de vulnerabilidades;
- Rapid7: a Rapid7 oferece um software de segurança que encontra vulnerabilidades, gere ativos e ajuda na resposta a incidentes;
- FireEye: empresa líder em deteção e resposta a incidentes;
- Deloitte e Accenture: empresas de consultoria com amplas gamas de serviços relativos à cibersegurança;
- VirusTotal e Any.Run: Oferecem plataformas para análise de malware e identificação de ameaças.

2.2 Laboratórios Digitais

O papel desempenhado pelos laboratório digitais é crucial numa investigação. A evolução na sofisticação das ameaças digitais tem exigido que os laboratórios sejam adaptados e atualizados constantemente.

2.2.1 Desafios:

- Como abordado nos tópicos acima, a complexidade dos incidentes de ransomware e phishing tem sido intensificada, pois as técnicas são mais evasivas e automatizadas. Tal ituação exige que aos laboratórios digitais tenham à disposição ferramentas e metodologias mais avançadas;
- A escassez de profissionais qualificados em análise forense dificulta a contratação e retenção de talentos;
- Devido ao elevado volume de dados por norma recolhidos, os analistas têm dificuldades em analisá-los com precisão e dentro do tempo pedido.

2.3 Fontes de conhecimento consultadas

As tomadas de decisões ao longo deste estágio foram feitas com base no conhecimento obtido em leituras de websites e livros, cujas as fontes de informação estarão na secção "Bibliografia"deste documento. Estas fontes de conhecimentos foram utilizadas para seis (6) áreas deste estágio:

Glossário: fortinet, 2024; SANS, 2024b.

Playbook: Criação de Playbooks / recomendações - Networks, 2024; certsocietegenerale, 2024a; certsocietegenerale, 2024b; Wahnon, 2024; MITRE, 2024a; MITRE, 2024b.

Informações legais: CNCS, 2024;

Informações sobre ferramentas: Johansen, 2022; ma-insights, 2024.

Equipa de 1º responders: Axonius, 2024; Linkedin, 2024; GIAC, 2024.

Laboratório Digital: ATC, 2024; SANS, 2024a.

2.4 Síntese

Conclui-se assim que a área da resposta a incidentes está em constante evolução, devido à crescente sofisticação e complexidade dos ataques informáticos. Impõe-se assim a existência de ferramentas de resposta a incidentes e de recursos humanos que se adaptem à constante evolução destes ataques.

3

DESENVOLVIMENTO

Relativamente à primeira tarefa definido pela empresa, “Elaboração de um documento de resposta a incidentes e analise forense, com base em dois tipos de incidentes: ransomware e phishing”, este foi iniciado na terceira semana de setembro e foi terminado na última semana de dezembro.

A tarefa “Elaboração de um documento de resposta a incidentes e analise forense, com base em dois tipos de incidentes: ransomware e phishing"teve como primeira subtarefa a recolha de informações sobre documentos DFIRS,tendo sido para tal efetuadas leituras de documentos sobre o planeamento e construção de DFIRS e, ainda, observados elementos áudio visuais. O intuito desta subtarefa foi de fazer um levantamento do estado de arte e aprender os conceitos necessários à elaboração deste documento.

Ainda em relação à primeira tarefa a sua segunda subtarefa, inicia-se com uma análise à possível duração de cada uma das restantes subtarefas, criando-se assim uma estimativa que foi baseada em opiniões pessoais e pressupostos. Com base nesta análise foi então criado o primeiro (1º) gráfico de Gantt com o nome de “Proposta Gráfico Gantt 04-10-23”, com a ajuda do software Microsoft Excel, utilizando assim uma das ferramentas até à altura disponibilizadas pela empresa.

De seguida e ainda no âmbito desta segunda subtarefa, deu-se o início ao planeamento do documento word “Playbook DFIR - Resposta a Incidentes e Análise Forense”, também foi feita uma análise sobre a duração prevista para a construção do "Playbook DFIR"e sobre os conteúdos a colocar no mesmo. Esta análise foi feita com base em observação e leitura de outros documentos DFIR ("Playbook DFIR"), opiniões pessoais, documentos educativos disponibilizados nas unidades curriculares de Análise Forense Digital I (um) e II (dois), de Políticas e Análise de Risco na Segurança da Informação e Tratamento de Incidentes de Segurança Informática. À medida que a análise foi feita, desenvolveu-se um documento, apenas com alguns tópicos a serem abordados. Esta versão inicial do documento DFIR permitiu melhor estruturar e visualizar as ideias em formato digital. Findada esta análise, foi elaborado o documento “Proposta de estrutura 06-10-23”.

3.1 Documento "Proposta de Estrutura"

No início do documento será feito um resumo do conteúdo do mesmo. Depois, será feita a introdução de tópicos tais como: aspetos fundamentais do DFIR, como a deteção, análise, contenção, erradicação, recuperação e pós-incidente bem como a análise forense e as suas fases, em incidentes digitais e cibercrimes, concluindo com o objetivo do documento DFIR.

Este documento contará ainda com:

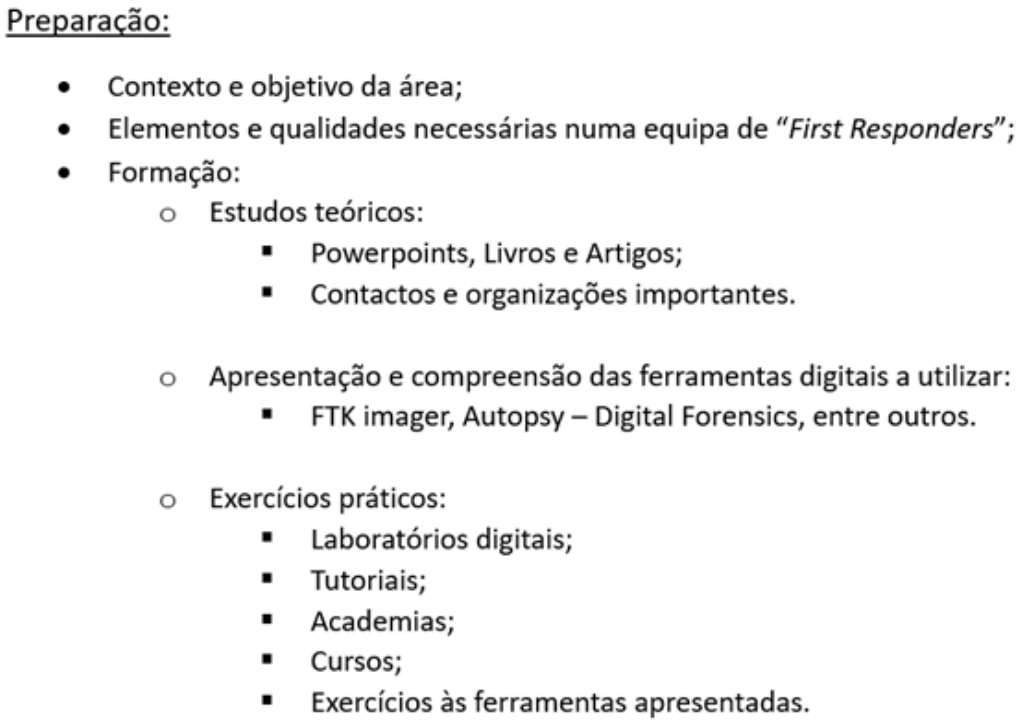


Figura 6: Estrutura planeada para o Documento DFIR, secção da preparação.

Como se pode observar na Figura 6, relativamente à "Preparação", esta foi dividida em 3 tópicos "Contexto e objetivo da área", "Elementos e qualidades necessárias numa equipa de "First Responders" e "Formação". O tópico "contexto e objetivo da área", será uma introdução ao tópico expondo a sua definição, explicando a sua importância e em que ambiente se insere no quotidiano. No tópico "Elementos e qualidades necessárias numa equipa de "First Responders"será primeiramente descrito o que são os "First Responders", que competências técnicas e humanas que estes devem ter e, ainda, serão indicados contactos digitais para reportar crimes às entidades responsáveis (Polícia judiciária e Centro Nacional de Cibersegurança) e os termos para a notificação de incidentes. O tópico "Formação" subdivide-se em "Estudo Teóricos", "Apresentação e compreensão das ferramentas digitais a utilizar" e "Cursos e academias e TableTops". O subtópico "Estudos Teóricos" tem como objetivo ensinar ou relembrar conhecimentos teóricos. O subtópico "Apresentação e

compreensão das ferramentas digitais a utilizar" apresenta os utilitários e as suas capacidades. Por fim, o subtópico "Cursos e Academias e TableTops", expõe as áreas que representam as competências técnicas e teóricas que os "First Responders"devem ter. Na secção seguinte, "Plano de Resposta a Incidentes", serão apresentadas subsecções, tais como:

- "Pré-requisitos";
- "Resposta";
- "Contenção, Erradicação e Recuperação";
- "Pós-incidente".

Detalhando mais cada subsecção, dentro de "Pré-requisitos", abordar-se-ão os subtópicos "Identificação de recursos e ativos de informação", "Definição dos ativos mais valiosos através da análise de impacto dos riscos associados aos recursos e ativos de informação", "Criação de política de resposta a incidentes", "Elaboração do processo de centro de partilha para as partes interessadas ("stakeholders")". Nesta secção espera-se que todos os pré-requisitos sejam identificados e implementados para que no caso de ser necessário a utilização do documento DFIR a empresa já esteja pronta para conseguir responder ao incidente.

Dentro da subsecção "Resposta" tem-se os subtópicos "Processos de organização para ransomware e phishing", "Mecanismos de contacto externo para comunicar ao público", "Processos de análise de vetores de ataque para melhoramento continuo da deteção e análise de incidentes", "Inventário de deteção de métodos associados a métricas de eficácia da atualidade, qualidade e relevância", "Modelo de registo de atividades de resposta a incidentes" e "Relatório de resposta a incidentes e o modelo para os relatórios sobre o estado de evolução dos incidentes". Nesta subsecção tem-se como objetivo fazer compreender o que se deve fazer caso se comprove que o incidente é um verdadeiro positivo, tornando-se assim por definição um ataque.

Dentro da subsecção "Contenção, Erradicação e Recuperação" tem-se os subtópicos "Laboratório de investigação – pesquisa e avaliação de potenciais sistemas atacantes", "Avaliação do estado de retenção de cópias de segurança ("backups") dos principais recursos". Nesta secção espera-se conseguir compilar ações de contenção, erradicação e recuperação para o normal funcionamento da empresa.

Por fim, na subscção "Pós-incidente" tem-se o subtópico "Tópicos a discutir com a equipa sobre os incidentes que ocorreram". Nesta secção espera-se conseguir colmatar possíveis erros para que não se repitam no futuro e se possível tornar

mais ações autónomas como também implementar novas soluções de segurança ou reforçar/modificar soluções defensivas.

Na secção "Análise Forense", serão apresentadas as fases que se devem percorrer para uma correta Análise Forense, começando pela preparação.

Dentro do subtópico “Preparação” tem-se:

- Identificação da origem dos indícios de provas digitais;
- Escolha da melhor abordagem para análise e apreensão da evidência.

De seguida, dentro do subtópico “Preservação do Sistema”, tem-se:

- Preservação do ambiente virtual e documentação do estado deste ambiente.

De seguida, dentro do subtópico “Pesquisa de Provas”, tem-se:

- Fundamentar com dados ideias que apoiem ou refutem as hipóteses sobre o incidente.

Por fim, a fase de "Reconstrução de Eventos"e "Relatório".

3.2 Desenvolvimento do documento DFIR

Para o desenvolvimento do próprio documento DFIR recorreu-se aos utilitários “Word” e “Google”. O primeiro (1º) foi utilizado para a criação e compilação do documento. O segundo (2º) foi utilizado para pesquisa de informação, que permitiu orientar e guiar a boa execução deste documento, que abaixo será apresentado com mais detalhe.

Começando pelo índice, consegue-se observar na Figura 7 que existem diferenças entre a estrutura planeada no início do estágio curricular e a atual.

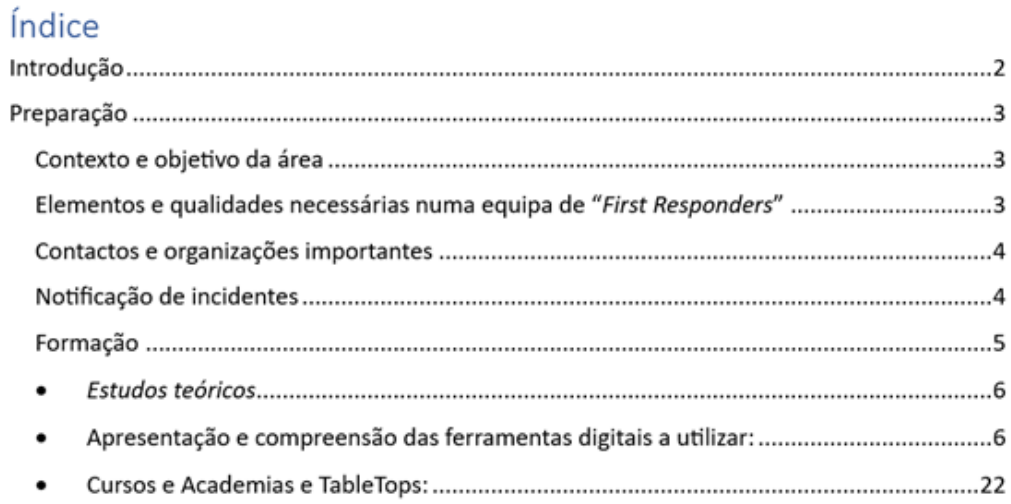

Índice

Figura 7: Estrutura real do Documento DFIR

As mudanças feitas entre a versão inicial e a imagem acima foram as seguintes:

- Não existe resumo, pois não teria utilidade neste contexto;
- O "Glossário" foi colocado antes da "Bibliografia";
- Foi acrescentado como tópico isolado "Contactos e organizações importantes", com o intuito de otimizar os processos de resposta;

- Foi acrescentado o tópico “Notificação de incidentes” com o intuito de melhorar a estrutura do documento DFIR;
- Os tópicos “Identificação de recursos e ativos de informação” e “Definição dos ativos mais valiosos através da análise de impacto dos riscos associados aos recursos e ativos de informação” foram modificados e abordados no tópico ”Lista de Ativos”, no qual se descreve que se deve fazer uma lista de ativos com uma análise de risco e impacto para cada empresa com que se trabalha.
- Os subtópicos da “Resposta” (Processos de operação para ransomware e phishing; Mecanismos de contacto externo para comunicar ao público; Processos de análise de vetores de ataque para melhoramento continuo da deteção e análise de incidentes; Inventário de deteção de métodos associados a métricas de eficácia da atualidade, qualidade e relevância; Modelo de registo de atividades de resposta a incidentes; Relatório de resposta a incidentes e o modelo para os relatórios sobre o estado de evolução dos incidentes.) passaram a estar organizados em diferentes áreas. Os subtópicos relacionados com a comunicação interna e externa, passaram para a subsecção de “Notificação de incidentes”, os tópicos relacionados com a resposta mantiveram-se no mesmo local mudando a forma como foi exposta a informação;
- Os tópicos “Laboratório de investigação – pesquisa e avaliação de potenciais sistemas atacantes;” “Avaliação do estado de retenção de cópias de segurança (“backups”) dos principais recursos.” foram retirados do documento;
- O ponto “Tópicos a discutir com a equipa sobre os incidentes que ocorreram” foi reformulado, tendo sido acrescentado mais conteúdo ao mesmo;
- A fase de “Análise Forense” foi completamente reformulada, sendo que a “Preparação” contém estes tópicos:
  - “Laboratório Forense”;
  - ”Equipa de investigação Forense”;
  - “Seleção de ferramentas”;
  - “Processo de investigação: First Responder”;
  - “Identificação da origem dos indícios de provas digitais”,
  - “Restrições da legislação portuguesa à recolha da prova”.
- O tópico “Preservação do Sistema” mudou para a designação “Recolha e Preservação do Ambiente”, tendo-lhe sido ainda acrescentado o subtópico “Preservação e documentação do estado do sistema virtual”;

- Acrescentaram-se ainda os tópicos “Análise da prova”; “Reconstrução de Eventos e Relatório”; “Fundamentar com dados que apoiem ou refutem as hipóteses sobre o incidente.”; “Relatório”.

Tendo em conta a estrutura e mudanças aqui apresentados, abordar-se-á com mais detalhe os tópicos mais pertinentes para o presente relatório.

3.2.1 Tópicos abordados - Preparação

No ramo da “Preparação” são apresentadas as qualidades técnicas e humanas que os "First Responders"necessitam de ter ou aprender para corresponderem os objetivos previstos na sua área de trabalho. No subtópico “Contactos e organizações importantes” por sua vez, são apresentados os contactos digitais e telefónicos para as Organizações responsáveis, tais como a Polícia Judiciária (PJ), Centro Nacional de Cibersegurança – (CNCS) e Centro Nacional de Cibersegurança (CERT), bem como os artigos do Decreto-Lei n.º 65/2021, de 30 de julho, com as instruções de como se deve proceder à notificação de incidentes. No Subtópico “Formação”, são apresentadas três subcategorias, nomeadamente, a subcategaria “Estudos Teóricos” onde são apresentados documentos sobre temas teóricos da área da cibersegurança:

- No primeiro (1º) powerpoint “Redes Computacionais.pdf” são abordados os seguintes tópicos: Conhecimentos em redes computacionais e protocolos de rede; Modelo OSI e TCP IP; Protocolos de segurança; Conceitos de arquitetura de segurança de rede;
- No segundo (2º) “cibersegurança.pdf”, são abordados os seguintes tópicos: Cibersegurança; Técnicas de scanning e sniffing; Fases dos ataques;
- No terceiro (3º) “Taxonomia MITRE ATT CK e RE CT.pdf” são abordados os seguintes tópicos: Definição e Objetivos; Matrizes: empresarial, móvel e ICX;
- No quarto (4º) “Noções sobre o Plano de Resposta a Incidentes.pdf” são abordados os seguintes tópicos: Necessidade de PRI; Objetivos; Benefícios; Considerações legais;
- No quinto (5º) “Análise Forense.pdf”, são abordados os seguintes tópicos: Conceitos; Métodos científicos; Princípios do tratamento de provas digitais e ética.

Ainda, a subcategoria “Apresentação e compreensão das ferramentas digitais a utilizar”, apresenta diferentes tipos de ferramentas ao dispor dos "First Reponders"e Analistas Forenses para a formulação de resposta a incidentes e para a realização de análises forenses, tais como:

Utilitários de sniffing e scanning ("Wireshark";“TCPview”; “TCP Dump”; “Network Miner”; “Netcat”.);

Utilitários multifunções (“FTK Imager”; “OSForensics”; “MXToolBox”; “Autopsy - Digital Forensics”; “Belkasoft”; “Nirsoft”.);

Utilitários de visualização (“FlareVm e Remnux”; “Oracle VM virtualBox”.);

Utilitários de verificação de alteração de estado ("Regshot”; "Sysinternal”.);

Utilitários de recolha e análise (“Volatility”; “RegRipper”; “Maltego”; “SRUM-Dump e WxTCmd”.);

Utilitários para informações sobre ameaças a domínios e IP (“Talos Intelligence”; “URLVoid”; “IPVoid”; “ThreatCrowd”; “Domain Dossier”.);

Utilitários de hash threat intel e sandbox (“AnyRun”; “URL Scan”; “Hybrid Analysis”; “Any.run”; “Joe Sandbox”; “Zeltser”; “Malwoverview”.);

Utilitários para codificar e descodificar (“Cyber Swiss Army Knife”; “Uncoder”.);

Utilitário de OSINT (“SpiderFoot”.);

Utilitários de exploração de vulnerabilidades (“Nessus”; “Metasploit”; “Legion”.);

Utilitário para DFIR (“FireEye Redline”.);

Utilitários de análise de ficheiros e Websites (“PDFID.py”; “PDF-parser.py”; “Virustotal”; “Web-Check”; “IDA Pro”; “Ghidra”; “OllyDbg”; “x64dbg”;);

Utilitário de edição de texto (“Sublitetext”).

Na secção de “Cursos e Academias e Tabletops” foi sugerido aos "First Responders"executarem estes cursos para se tornarem melhores nas suas funções:

- “How to conduct a forensic investigation”;
- “Essential skills for investigating ransomware attacks”;
- “Practical Windows Forensics”;
- “Blue Team Level 1 Junior Security Operations Certification”;
- “Blue Team Level 2 Advanced Security Operations Certification”;
- “An Introduction to Digital Forensics”;
- “Introduction to Network Analysis”;
- “Learn how to analyze and defend against real-world cyber threats/attacks” ;
- “Phishing”;

- “Network Security”;
- “Nmap”;
- “Vulnerability Research” ;
- “Snort”;
- “Proactive incident detection”;
- “Processing and storing artifacts”;
- ”Artefact analysis fundamentals” ;
- “Introduction to advanced artefact analysis”;
- “Advanced artefact handling”;
- “Dynamic analysis of artefacts”;
- “Static analysis of artefacts”;
- “Forensic analysis: Local incident response”;
- “Forensic analysis: Network incident response“;
- “Digital forensics”;
- “GIAC Certified Forensic Analyst (GCFA)”;
- “GIAC Network Forensic Analyst (GNFA)”;
- “GIAC Reverse Engineering Malware Certification”;
- “GIAC Certified Forensic Examiner (GCFE)”.

Embora alguns cursos sejam gratuitos, outros são pagos, exigindo um investimento financeiro por parte da empresa para que assim possa melhorar a qualidade do trabalho dos seus funcionáios.

3.2.2 Tópicos abordados - Pré-Requisitos

Na secção “Pré-Requisitos” do “Plano de Resposta a Incidentes”, são apresentadas as recomendações a considerar para que a empresa se prepare adequadamente para esperáveis incidentes, sendo estes alguns exemplos dessas recomendações:

- Criar e manter uma lista de todos os domínios pertencentes à empresa e de todas as pessoas que podem registar domínios;
- Criar um email de template: para notificar todos os empregados de que há uma da campanha de phishing em curso contra a organização; para contactar empresas prestadoras de serviços pedindo “domain takedown”; para informar terceiros para que tomem medidas contra phishing nas suas infraestruturas;

- Assegurar que: estão implementadas soluções de correio eletrónico anti-malware/anti-spam/anti-phishing; os utilizadores sabem denunciar eventos de phishing;
- Realizar um teste Firedrill para garantir que todos os aspetos do "Playbook DFIR"estão a funcionar (pelo menos uma vez ao ano), utilizando para tal os laboratórios virtuais para treino e aperfeiçoamento dos processos criados. Ainda, deve-se testar os canais de contacto internos.

3.2.3 Tópicos abordados - Centro de partilha

Na subsecção “Centro de partilha para Administração, Stakeholders, Colaboradores, Comité e Público” são apresentados os tipos de partilha de informação, nomeadamente, interno, comité, administração, stakeholders e público. Em adição, foram criados templates para a comunicação dos incidentes para os colaboradores, para o público e para os stakeholders.

3.2.4 Tópicos abordados - Resposta - Fluxogramas

Relativamente à “Resposta” foram criados dois (2) espaços distintos, um para a Resposta a Ransomware e outro para a Resposta a Phishing. No espaço para a Resposta a Ransomware, foi primeiro apresentado o Ransomware, nomeadamente, a sua definição e, ainda, uma descrição do estado de arte em termos da importância de ter métodos para a resposta a este tipo de ataque tendo em conta o aumento dos números casos. Foi ainda apresentado o Fluxograma de Deteção, com o intuito de detetar os indicadores de ameaça, o qual se pode observar na Figura 8.

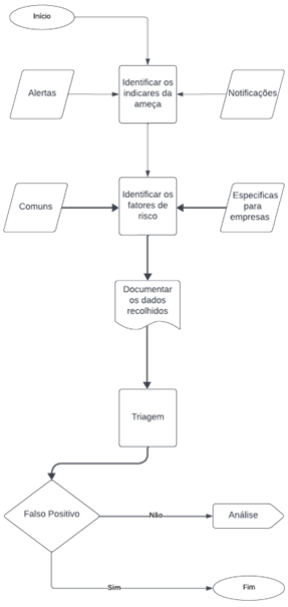


Figura 8: Fluxograma para a deteção de ransomware.

Juntamente a Figura 9, o Fluxograma de Análise:

Figura 9: Fluxograma para a análise de ransomware.

Todos os passos de cada fluxograma foram explicados no documento DFIR, seja a definição ou, em casos específicos, contactos e informações. Este processo foi repetido para o Phishing, tendo sido apresentada uma definição deste incidente e o fluxograma de Deteção e de Análise (Figuras 10 e 11).

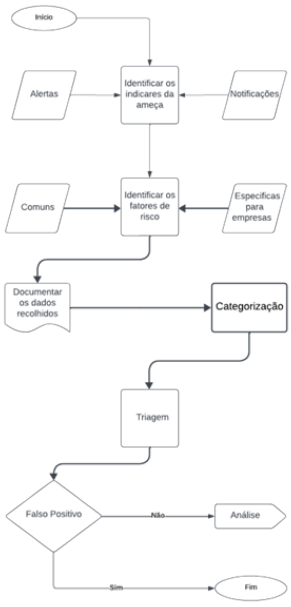


Figura 10: Fluxograma para a deteção de phishing.

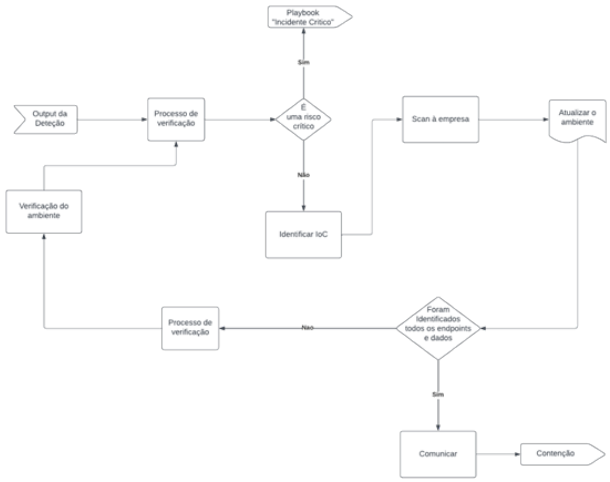


Figura 11: Fluxograma para a análise de phishing.

No tópico "Contenção, Erradicação e Recuperação" para o ataque de Ransomware foi apresentado o fluxograma (Figura 12) e detalhadamente explicados os passos do mesmo.

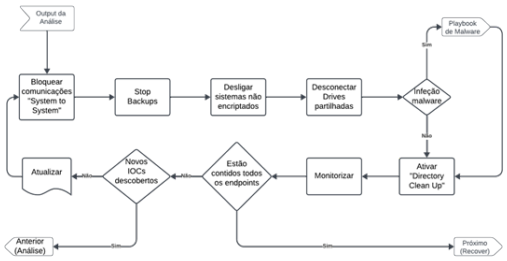


Figura 12: Fluxograma para a resposta a ransomware, Contenção, Erradicação e Recuperação.

Tal como também foi abordado o fluxograma de recuperação para ransomware (Figura 13).

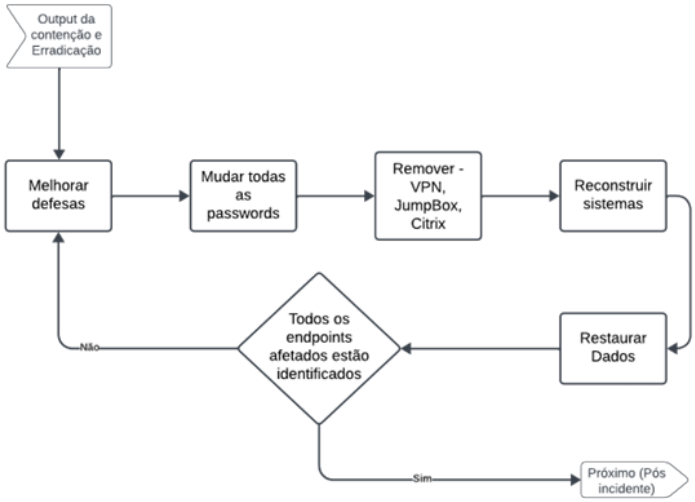


Figura 13: Fluxograma para a recuperação de um ataque de ransomware.

O mesmo processo foi feito para Phishing, apresentando o Fluxograma de Contenção e Erradicação, e o Fluxograma de Recuperação (Figuras 14 e 15).

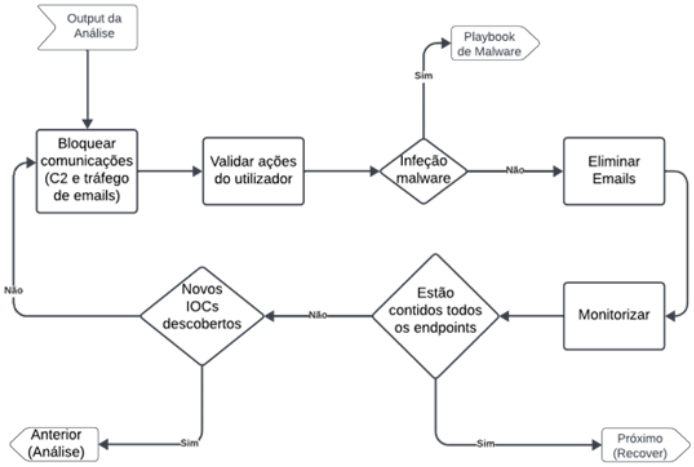


Figura 14: Fluxograma para a resposta a phishing, Contenção e Erradicação.

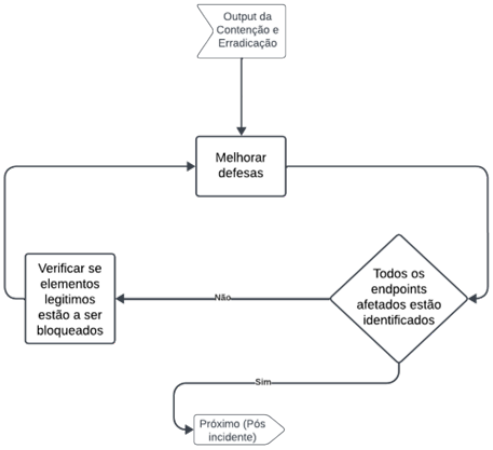


Figura 15: Fluxograma para a resposta a phishing, Recuperação.

Relativamente ao Pós-Incidente, foram apresentados os fluxogramas para Ransomware e para Phishing respetivamente(Figuras 16 e 17):

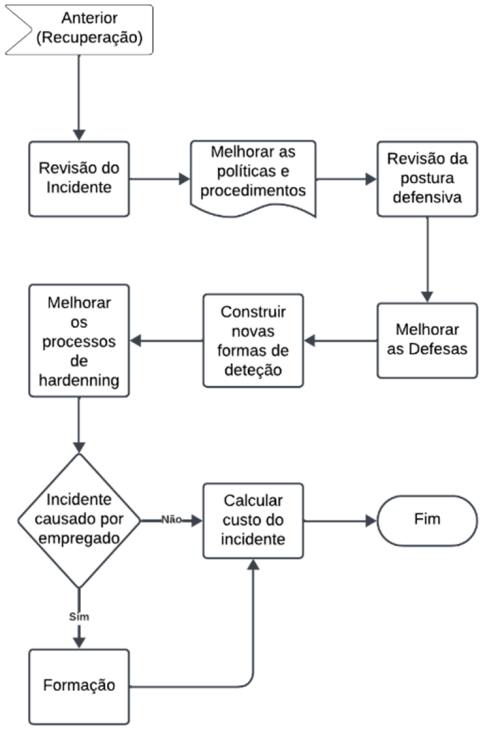


Figura 16: Fluxograma para a resposta a ransomware, pós-incidente.

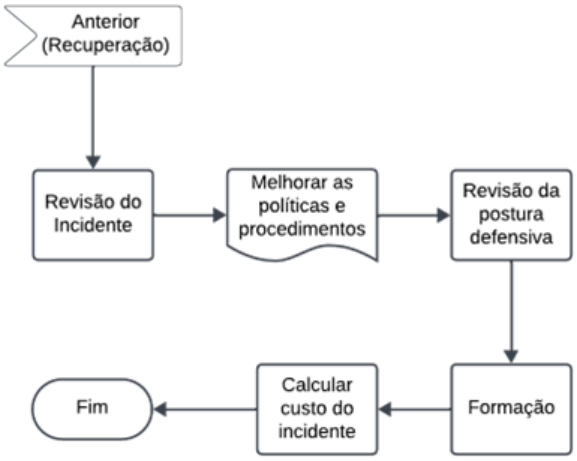


Figura 17: Fluxograma para a resposta a phishing, pós-incidente.

3.2.5 Tópicos abordados - Análise Forense

Fechando este secção, o subtópico “Análise Forense” começa com o subsubtópico “Preparação”. Neste subsubtópico aborda-se temas como:

- o “Laboratório Forense” onde se é explicado o seu propósito e como deve ser planeado;
- a “Equipa Forense” onde expõe-se a sua composição e funções;
- o “Processo de investigação:
  - "First Responders” onde se abordam as funções dos "First Responder"no processo de investigação;
  - a “Identificação da Origem dos Indícios de Provas Digitais” onde é criada a ligação entre artefactos a procurar e que ferramentas utilizar;
  - “Conhecimento de Princípios das Leis de Portugal”, onde se abordam alguns conceitos teóricos relativos à utilização da prova na justiça portuguesa, sendo eles os princípios da investigação e da verdade processual, a proibição de prova, e como as autoridades judiciarias portuguesas processam uma investigação criminal na área da informática forense;
  - “Restrições da Legislação Portuguesa à Recolha da Prova”, onde se abordam algumas restrições à recolha da prova.

No mesmo subtópico da "Análise Forense", na “Recolha e Preservação do Ambiente”, apresenta-se a “Ordem de Recolha” da prova, a “Estratégia de recolha de dados voláteis”, a “Configuração da recolha de dados voláteis”, o “Processo

de Recolha de Dados Voláteis", a "Aquisição de dados estáticos", a "Recolha de provas a partir de redes sociais", o "Processo de recolha de provas a partir de vários dispositivos e suportes", recolha por "Bit-stream disco-a-disco", "Aquisição lógica" ou "Aquisição sparse" e a "Preservação da Prova".

Ainda no subtópico "Análise da Prova", foram indicadas as fases que a análise deverá ter. No subtópico "Reconstrução de Eventos e Relatório", foi exposta a forma como se deve reconstruir eventos a partir de dados que apoiem ou refutem as hipóteses e as diretrizes para a realização da avaliação do caso. Relativamente ao subtópico "Relatório", foi dada a definição e objetivo do mesmo e, ainda, detalhes de como este deverá ser feito.

O documento DFIR conta ainda com um glossário de palavras, termos, siglas, acrónimos e nomes relevantes utilizados no documento e termina com a bibliografia a que se recorreu para a sua construção.

3.3 Laboratório Forense

O restante do tempo em estágio foi dividido entre as tarefas "Criação de Laboratórios Virtuais para Treino e Aperfeiçoamento dos Processos Criados" e "Criação de Laboratório Virtual para Análise de Evidências" como se pode observar na Figura 18.

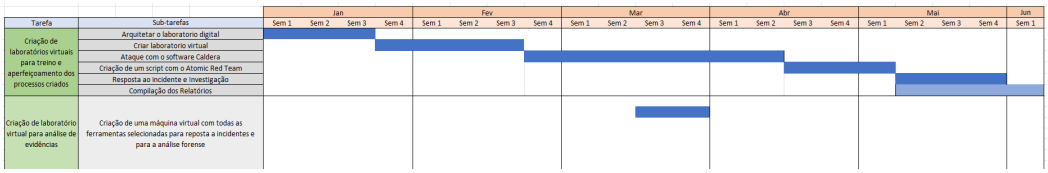


Figura 18: Tarefas restantes.

Inicialmente, planeou-se a criação de um ambiente onde estariam presentes três (3) máquinas: uma (1) que faria o ataque chamada de "Máquina de ataque", uma (1) que sofreria o ataque chamada de "Máquina Vítima" e uma (1) que serviria para máquina de análise criando assim laboratório virtual. A "Máquina de ataque" teria como Sistema Operativo (SO) o Kali Linux e nesta estaria ainda instalado o software "MITRE Caldera" que faria o ataque de modo remoto à "Máquina Vítima". Este ataque seria composto por técnicas apresentadas no website do MITRE ATT CK.

A "Máquina Vítima" tem como Sistema Operativo (SO) o Windows 11 da Microsoft, e seria atacada pela "Máquina de Ataque" e alvo de recolha de evidências para análise na "Máquina de Análise".

A “Máquina de Análise”, tem o Sistema Operativo (SO) Windows 11 da Microsoft, e instaladas todas as ferramentas necessárias para a análise da máquina afetada.

As únicas mudanças em relação ao plano inicial foram na “Máquina Vítima”. Devido ao inesperado não funcionamento do software "MITRE Caldera"mudou-se a estratégia, e assim esta máquina passaria a ser uma máquina inutilizável para o ataque remoto, porém útil na criação de um documento Script que iria ser executado na "Máquina Vítima". O Script foi criado com a ajuda da Red Canario e do seu programa Atomic Red Team.

A tarefa “Criação de Laboratórios Virtuais para Treino e Aperfeiçoamento dos Processos Criados” começou com a subtarefa “Arquitetar o Laboratório Digital”. Esta iniciou-se com a criação de um documento PDF com a arquitetura inicialmente idealizada do laboratório digital, como se pode observar na Figura 19.

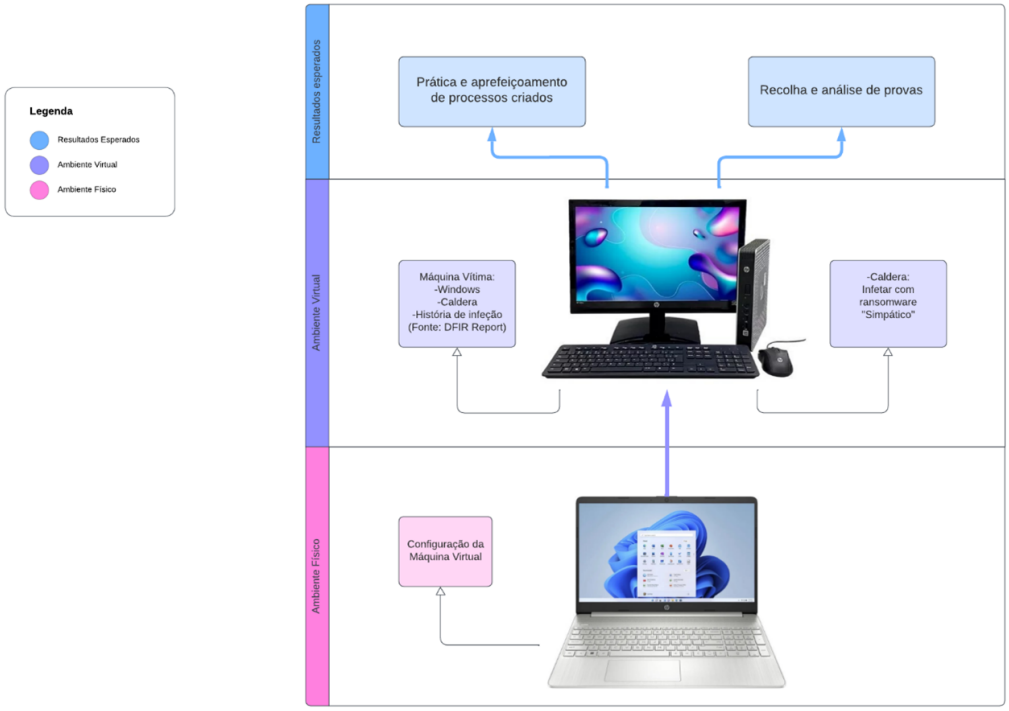


Figura 19: Arquitetura Inicial.

Inicialmente o laboratório seria formado por uma máquina física capaz de suportar a “Máquina Vítima” e a “Máquina de Ataque”, executar o ataque e por fim analisar as evidências na máquina que suportava as máquinas virtuais. Após posterior análise preferiu-se criar uma máquina virtual de análise, que pode ser vista na Figura 20:

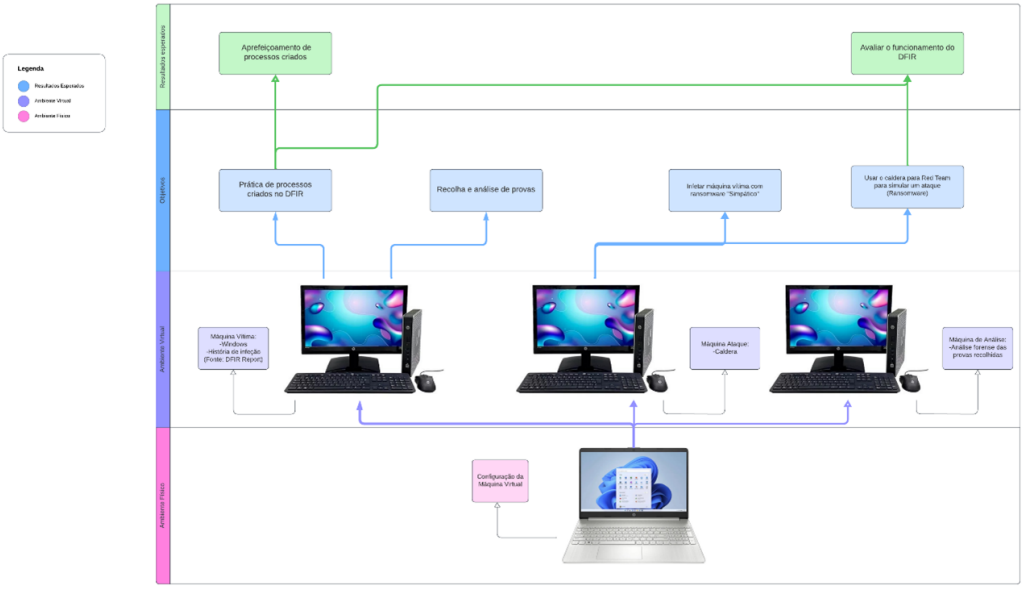


Figura 20: Arquitetura real.

3.3.1 Criação das Máquinas Virtuais

Concluída esta primeira subtarefa, foram criadas as máquinas virtuais no âmbito da segunda subtarefa "Criar Laboratório Virtual". A "Máquina Vítima" tem as seguintes configurações (Figura 21):

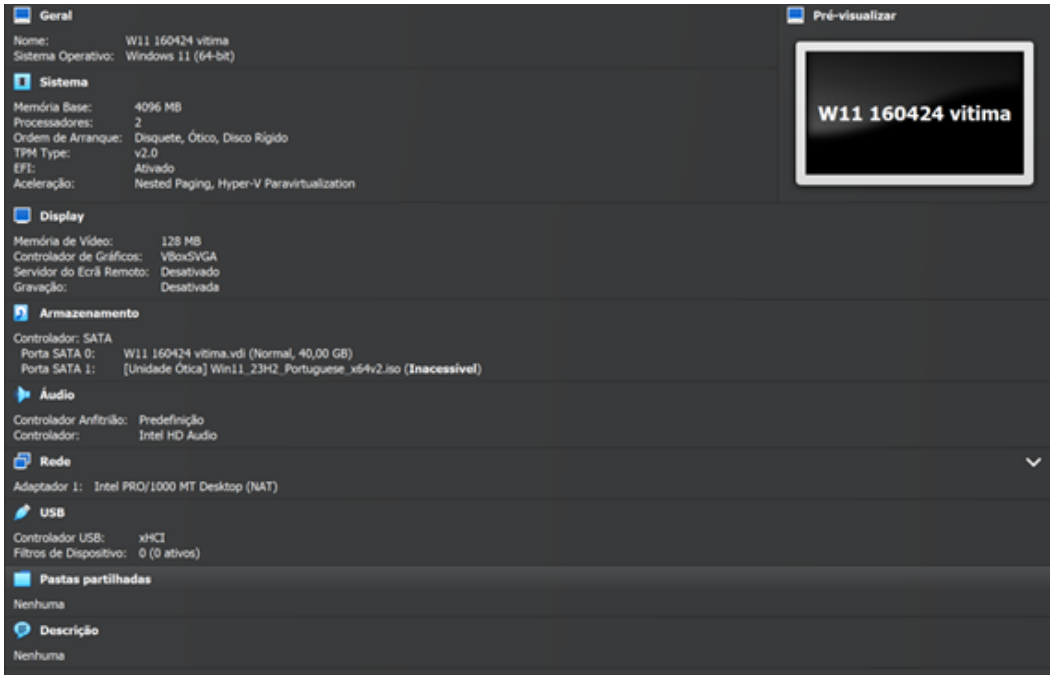


Figura 21: configurações da "Máquina Vítima".

A "Máquina de Análise" tem as seguintes configurações (Figura 22):

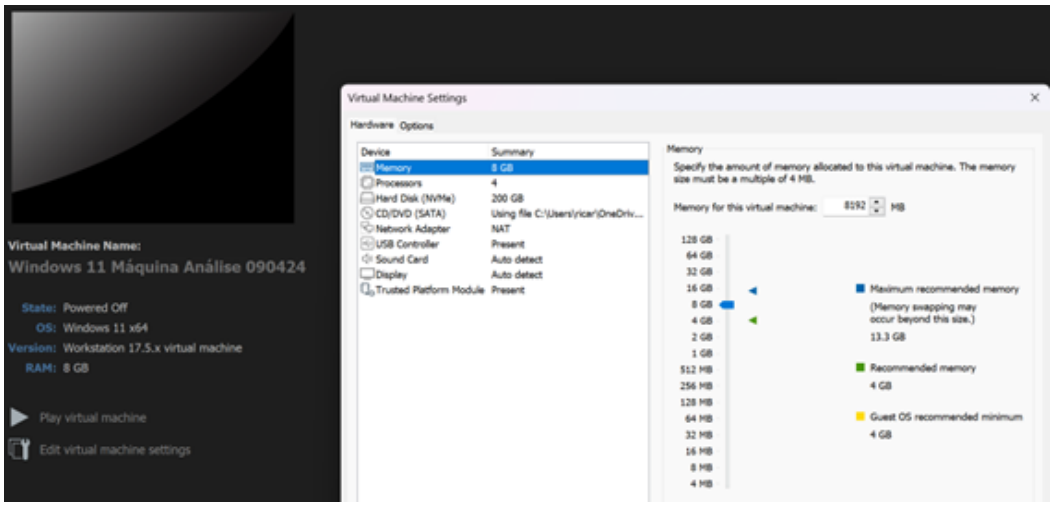


Figura 22: configurações da “Máquina de Análise”.

A “Máquina de Ataque” tem as seguintes especificações (Figura 23):

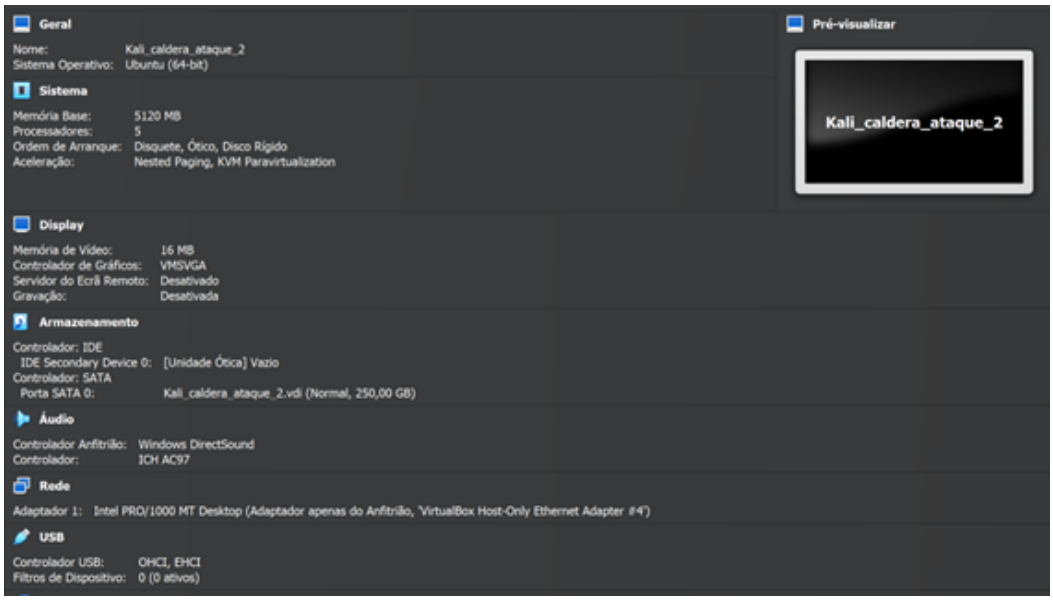


Figura 23: configurações da “Máquina de Ataque”.

3.4 Testes e Resultados - Conteúdo do Script "Cyberwatch ART-attack.ps1"

Após várias tentativas falhadas com o MITRE Caldera, mudou-se a estratégia e foi criado o Script “Cyberwatch ART-attack.ps1”. O Script tem o seguinte conteúdo (Figura 24):

```
Set-ExecutionPolicy ByPass -Scope CurrentUser
#Install NuGet
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Figura 24: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

O documento começa com a linha "Set-ExecutionPolicy ByPass -Scope CurrentUser", que dá a possibilidade do script ser executado na conta do utilizador corrente. A linha "Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force" instala o NuGet, que é um software necessário para a correta utilização do Atomic Red Team.

A linha "IEX (IWR 'https://raw.githubusercontent.com/bluecapesecurity/ invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing); Install-AtomicRedTeam -RepoOwner bluecapesecurity -Force" vai instalar o Atomic Red Team na "Máquina Vítima". Já as linhas abaixo Vão instalar a pasta "AtomicsFolder", que tem todos os ataques disponíveis da Atomic Red Team, na "Máquina Vítima":

- "IEX(IWR `'https://raw.githubusercontent.com/bluecapesecurity/invoke-atomicredteam/master/install-atomicsfolder.ps1'` -UseBasicParsing);
- Install-AtomicsFolder -Force -Branch 724cb3f50dcdd341815d5d2f34cbf90168017404".

```
# Discovery

#T1057 Process Discovery
"T1057 Atomic Test #2 - Process Discovery - tasklist"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1057/T1057.md#atomic-test-2---process-discovery---tasklist
Invoke-AtomicTest T1057 -TestNumbers 2
Start-Sleep -s 9


#T1082 System Information Discovery
"T1082 Atomic Test #1 - System Information Discovery"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1082/T1082.md#atomic-test-1---system-information-discovery
Invoke-AtomicTest T1082 -TestNumbers 1
Start-Sleep -s 9


#T1033 System Owner/User Discovery
"T1033 Atomic Test #1 - System Owner/User Discovery"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1033/T1033.md#atomic-test-1---system-owneruser-discovery
Invoke-AtomicTest T1033 -TestNumbers 1
Start-Sleep -s 9
```

Figura 25: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

O Script começa com algumas técnicas de Discovery (Figura 25), nomeadamente de "Process Discovery", "System information Discovery" e "System Owner/User Discovery", com as quais se espera obter informações sobre os processos abertos, o sistema e o utilizador.

```
#Inicial Access
"T1078.003 Atomic Test #1 - Create local account with admin privileges"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.003/T1078.003.md#atomic-tests
Invoke-AtomicTest T1078.003 -TestNumbers 1
Start-Sleep -s 9
```

Figura 26: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

Posteriormente, é indicada uma (1) técnica de Inicial Access, através da qual se espera criar um utilizador administrador (Figura 26).

```
#Persistence
"T1547.001 Atomic Test #6 - Suspicious bat file run from startup Folder"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1547.001/T1547.001.md#atomic-test-6---suspicious-bat-file-run-from-startup-folder
Invoke-AtomicTest T1547.001 -TestNumbers 6
Start-Sleep -s 9
```

Figura 27: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

Ainda é indicada uma (1) técnica de Persistence, com a qual se espera criar um ficheiro bat na pasta de startup (Figura 27).

```
#Command and Control
"T1219 Atomic Test #1 - TeamViewer Files Detected Test on Windows"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1219/T1219.md#atomic-test-1---teamviewer-files-detected-test-on-windows
Invoke-AtomicTest T1219 -TestNumbers 1 -TimeoutSeconds 1000
```

Figura 28: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

De seguida é indicada uma (1) técnica de Command and Control, com a qual se espera conseguir instalar o "TeamViewer"sem a autorização ou input do utilizador (Figura 28).

```
#T1113 Screen Capture
"T1113 Atomic Test #7 - Windows Screencapture"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1113/T1113.md#atomic-test-7---windows-screencapture
# Add the necessary assembly
Add-Type -AssemblyName System.Windows.Forms
# Create a Bitmap object to store the screenshot
$bitmap = New-Object System.Drawing.Bitmap([System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Width, [System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Height)
# Create a Graphics object from the Bitmap
$graphics = [System.Drawing.Graphics]::FromImage($bitmap)
# Capture the screen
$graphics.CopyFromScreen([System.Windows.Forms.Screen]::PrimaryScreen.Bounds.Location, [System.Drawing.Point]::Empty, $bitmap.Size)
# Dispose of the Graphics object
$graphics.Dispose()
# Save the screenshot to a file
$bitmap.Save("C:\Users\screenshot.png", [System.Drawing.Imaging.ImageFormat]::Png)
# Dispose of the Bitmap object
$bitmap.Dispose()
Start-Sleep -s 9
```

```
#T1125 Video Capture
"T1125  Atomic Test #1 - Registry artefact when application use webcam"
# https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1125/T1125.md#atomic-test-1---registry-artefact-when-application-use-webcam
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam\NonPackaged\C:#Windows#Temp#atomic.exe /v LastUsedTimeStart /t REG_BINARY
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam\NonPackaged\C:#Windows#Temp#atomic.exe /v LastUsedTimeStop /t REG_BINARY
Start-Sleep -s 9
```

Figura 29: Conteúdo do ficheiro Cyberwatch ART-attack.ps1.

Por fim, são indicadas duas (2) técnicas de Collection, através das quais se espera conseguir um screenshot do ecrã atual e uma gravação da webcam (Figura 29).

3.5 Modificações na Máquina Vítima

Após a conclusão do Script, na “Máquina Vítima” foram feitas algumas operações, nomeadamente a execução do comando “Set-ExecutionPolicy ByPass -Scope

CurrentUser" no powershell em modo de administrador e a desativação das opções de segurança de forma a que fosse possível executar o ataque (Figura 30):

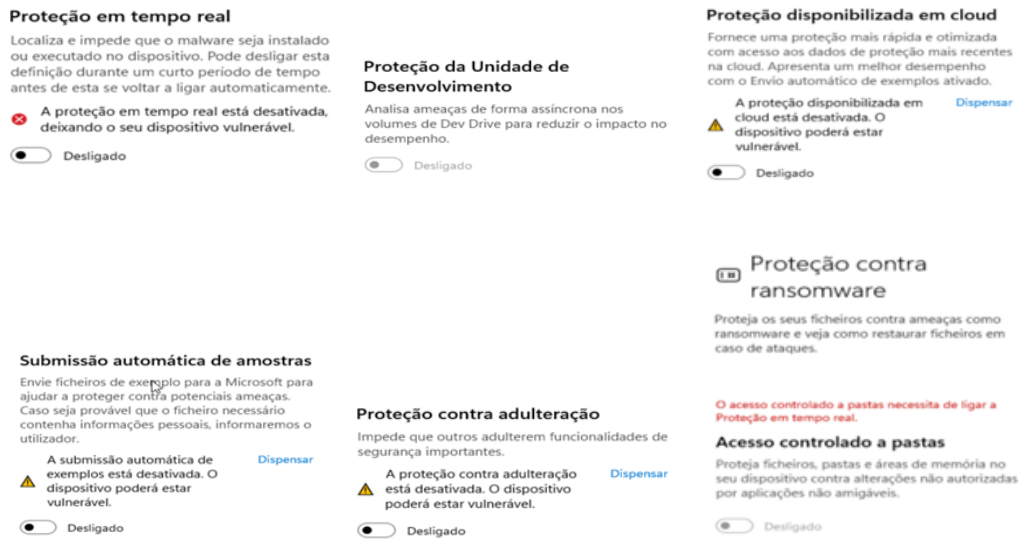


Figura 30: Modificações nas defesas da Máquina Vítima.

3.6 Execução do Script na Máquina Vítima

Por fim, este Script foi executado na "Máquina Vítima"através do comando "Set-ExecutiotionPolicy ByPass -Scope CurrentUser", no powershell em modo de administrador. De seguida entra-se na diretoria onde está o Script e faz-se a execução do Script.

Este começa por instalar o Nuget e o Atomic Red Team (Figura 31):

```
PS C:\users\vitima\Desktop> & '.\Cyberwatch_ART-attack_inicial 080424.ps1'

Name                           Version          Source           Summary
----                           -------          ------           -------
nuget                          2.8.5.208        https://onege... NuGet provider for the OneGet meta-package manager
A instalar o Atomic Red Team
==========================
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/bluecapesecurity/invoke-atomicredteam/wiki for complete details
A instalar...pode demorar algum tempo.
```

Figura 31: Início da execução.

De seguida, as técnicas começam a ser aplicadas e os outputs das mesmas são revelados:

```
T1057 Atomic Test #2 - Process Discovery - tasklist
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1057-2 Process Discovery - tasklist
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        144 K
Registry                        88 Services                   0     18 552 K
smss.exe                       388 Services                   0      1 240 K
csrss.exe                      512 Services                   0      5 652 K
wininit.exe                    584 Services                   0      6 904 K
csrss.exe                      592 Console                    1      5 912 K
winlogon.exe                   676 Console                    1      9 792 K
services.exe                   692 Services                   0     10 172 K
lsass.exe                      736 Services                   0     23 544 K
svchost.exe                    848 Services                   0     30 440 K
fontdrvhost.exe                856 Console                    1      8 200 K
fontdrvhost.exe                864 Services                   0      3 476 K
svchost.exe                    964 Services                   0     15 920 K
svchost.exe                   1020 Services                   0      8 196 K
svchost.exe                    312 Services                   0     16 232 K
dwm.exe                        596 Console                    1    109 640 K
```

Figura 32: Resultado da Técnica T1057-2.

A técnica T1057 revelou as informações dos processos abertos (Figura 32).

```
T1082 Atomic Test #1 - System Information Discovery
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1082-1 System Information Discovery
Host Name:                 USER
OS Name:                   Microsoft Windows 11 Pro
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Vitima
Registered Organization:
Product ID:                00330-80000-00000-AA963
Original Install Date:     16/04/2024, 15:56:55
System Boot Time:          20/09/2024, 16:11:01
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 154 Stepping 3 GenuineIntel ~2496 Mhz
BIOS Version:              innotek GmbH VirtualBox, 01/12/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
Input Locale:              pt;Português (Portugal)
Time Zone:                 (UTC+00:00) Dublin, Edimburgo, Lisboa, Londres
System Locale:             pt;Português (Portugal)
Total Physical Memory:     4 080 MB
Available Physical Memory: 1 334 MB
Virtual Memory: Max Size:  4 976 MB
Virtual Memory: Available: 2 460 MB
Virtual Memory: In Use:    2 516 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5036620
                           [02]: KB5027397
Logon Server:              \\USER
                           [03]: KB5036212
                           [04]: KB5036893
                           [05]: KB5037020
Network Card(s):           1 NIC(s) Installed.
```

Figura 33: Resultado da Técnica T1082-1.

A técnica 1082-1 revelou as informações do sistema (Figura 33).

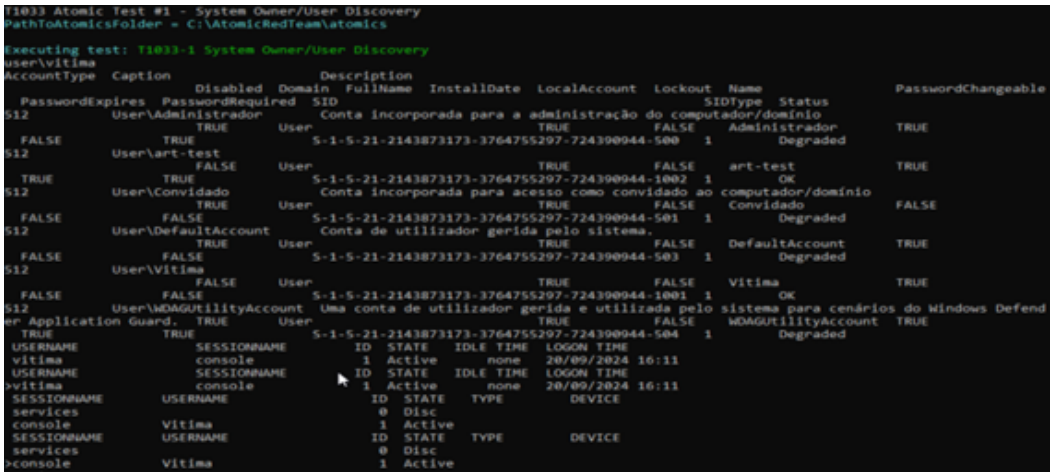


Figura 34: Resultado da Técnica T1033-1.

A técnica T1033 revelou as informações dos utilizadores (Figura 34).

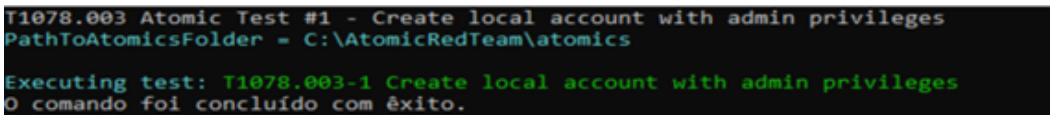


Figura 35: Resultado da Técnica T1078.003-1.

A técnica T1078.003-1 criou um utilizador (Figura 35).

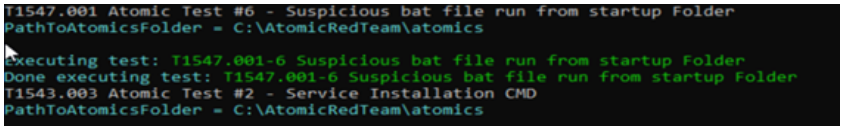


Figura 36: Resultado da Técnica T1547.001-6.

A técnica T1547.001-6 criou e colocou um ficheiro bat na pasta "startup"(Figura 36).

Figura 37: Resultado da Técnica T1219-1.

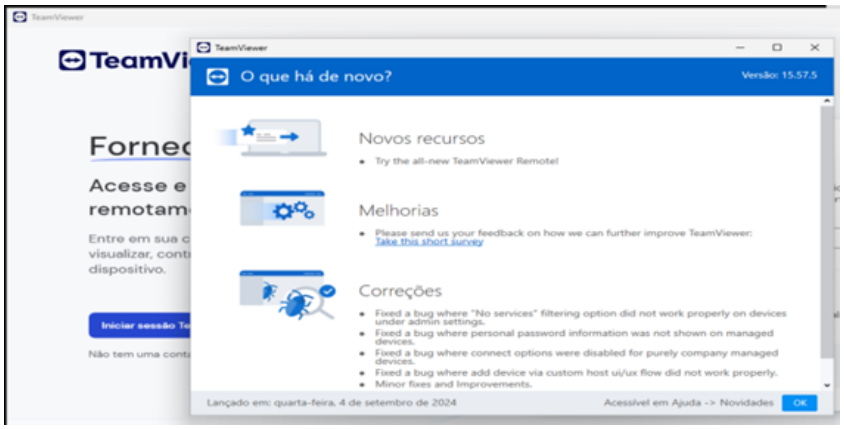


Figura 38: Resultado da Técnica T1113.

A técnica T1219-1 fez o download e instalou o software "TeamViewer"(Figuras 37 e 38).

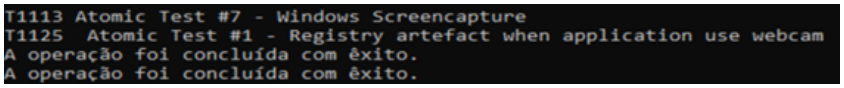


Figura 39: Resultado da Técnica T1125.

As técnicas T1113 e T1125 foram executadas com sucesso (Figura 39).

3.7 Análise Forense - Recolha de artefactos

Concluído o ataque, começa a fase de investigação, esta por sua vez inicia o caso "Aa24.SIBSMulticert". Nesta fase, as primeiras evidências recolhidas foram a foto ao ecrã da "Máquina Vítima" e o "memory dump"da informação volátil, a partir da aplicação Volatility, com os nomes de "Aa24.SIBSMulticert - 0000A - Foto do Ecrã" e "Aa24.SIBSMulticert - 0001A - memdump", como pode ser observado nas Figuras 40 e 41:

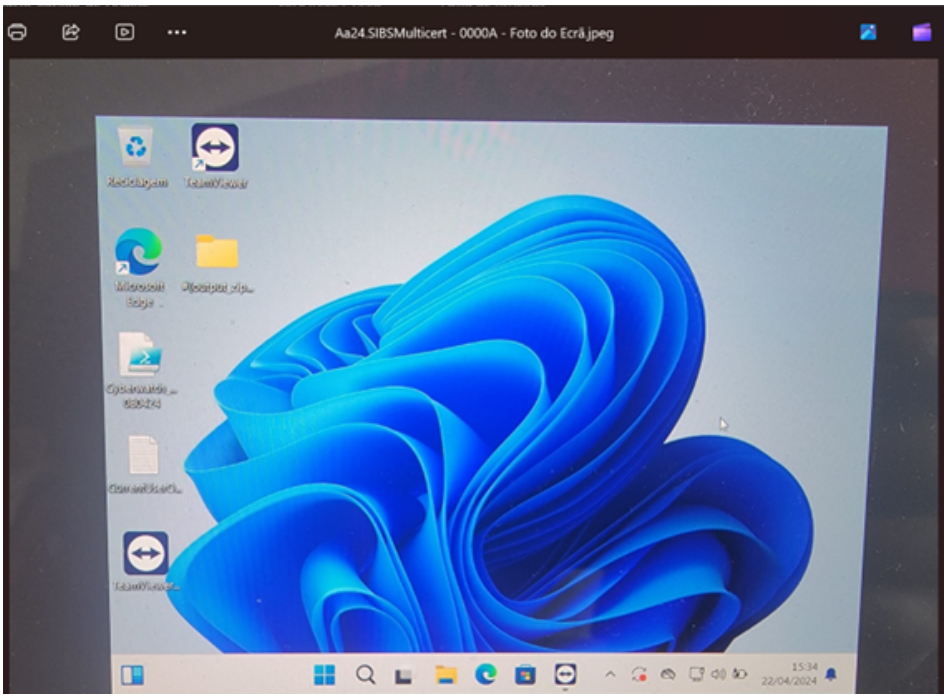


Figura 40: Aa24.SIBSMulticert - 0000A - Foto do Ecrã.

Figura 41: Aa24.SIBSMulticert - 0001A - memdump.

De seguida, foram retiradas três cópias da imagem do disco: a original, que não foi utilizada para qualquer tipo de investigação “Aa24.SIBSMulticert - 0002A -

Máquina Artefacto Original"; uma segunda de backup "Aa24.SIBSMulticert - 0004A - Máquina Artefacto Backup de Análise" e a terceira cópia foi usada para fazer as investigações, recolhas e análises necessárias "Aa24.SIBSMulticert - 0003A - Máquina Artefacto Cópia para Análise" (Figura 42).

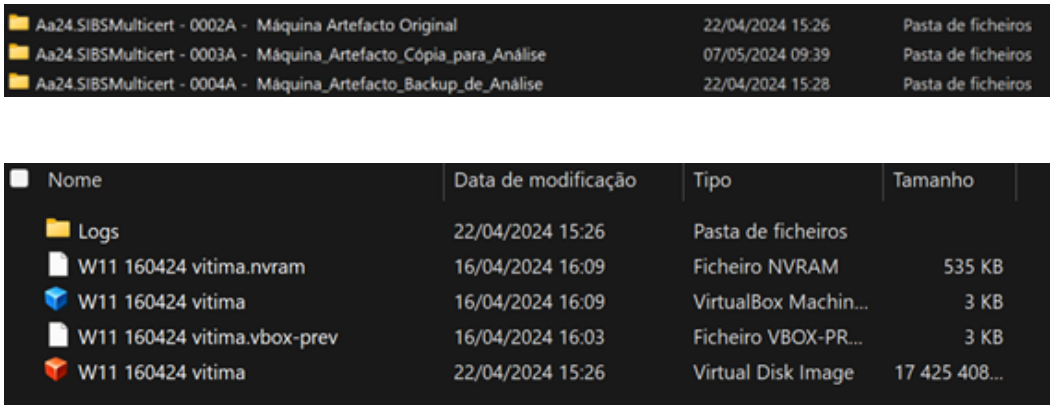


Figura 42: Cópias do disco.

Posteriormente, foram retiradas as evidências "Aa24.SIBSMulticert - 0005A - FTK Imager - ficheiros Temp", "Aa24.SIBSMulticert - 0006A - Recolha Kape", "Aa24.SIBSMulticert - 0007A - FTK Imager - Users - Public", "Aa24.SIBSMulticert - 0008A - FTK Imager - Users - Vítima - Desktop", "Aa24.SIBSMulticert - 0009A - FTK Imager - Windows - Diagnostics - Maintenance". Estas evidências foram obtidas a partir da Máquina de Análise onde se utilizou o FTK imager, com exceção da prova "Aa24.SIBSMulticert - 0006A - Recolha Kape" onde foi utilizado, como o nome indica, o software "Kape"(Figura 43).

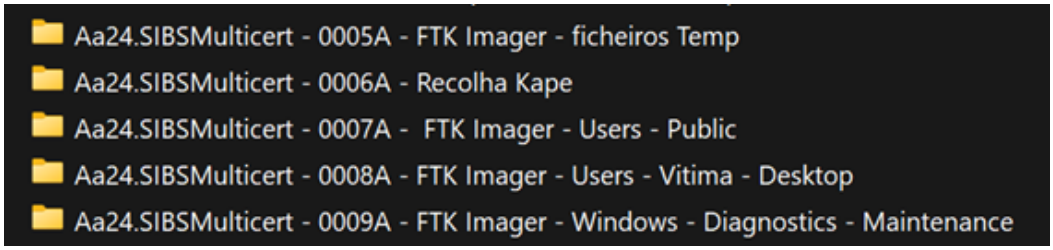


Figura 43: Evidências.

Vários outros artefactos foram encontrados (por exemplo, ficheiros instalados do "TeamViewer", informações sobre o utilizador criado, ficheiros do AtomicRedTeam, histórico do "browser", ficheiros eliminados, histórico da linha de comandos, entre outros.), a partir do software Autopsy, como se pode observar na Figura 44:

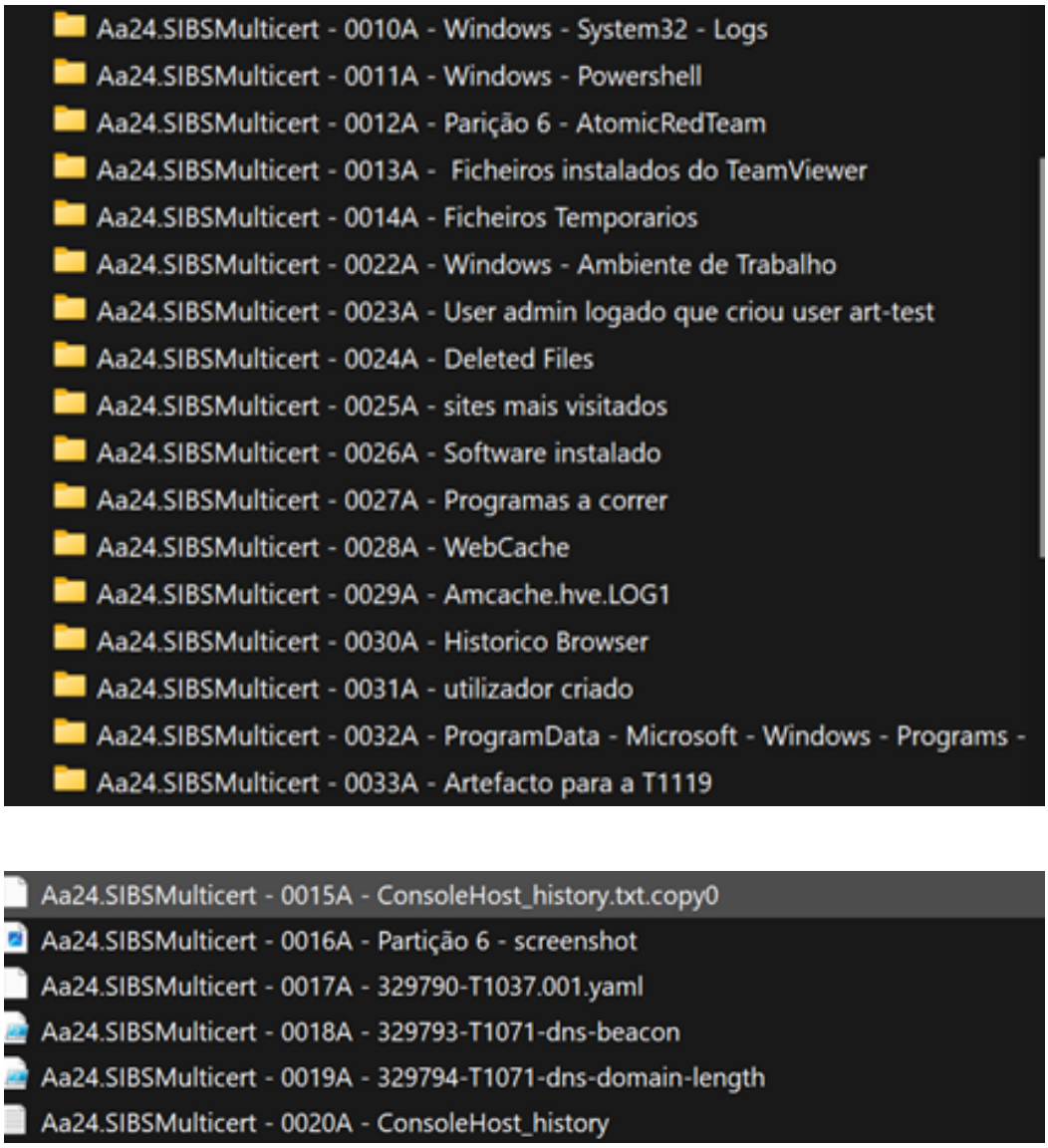
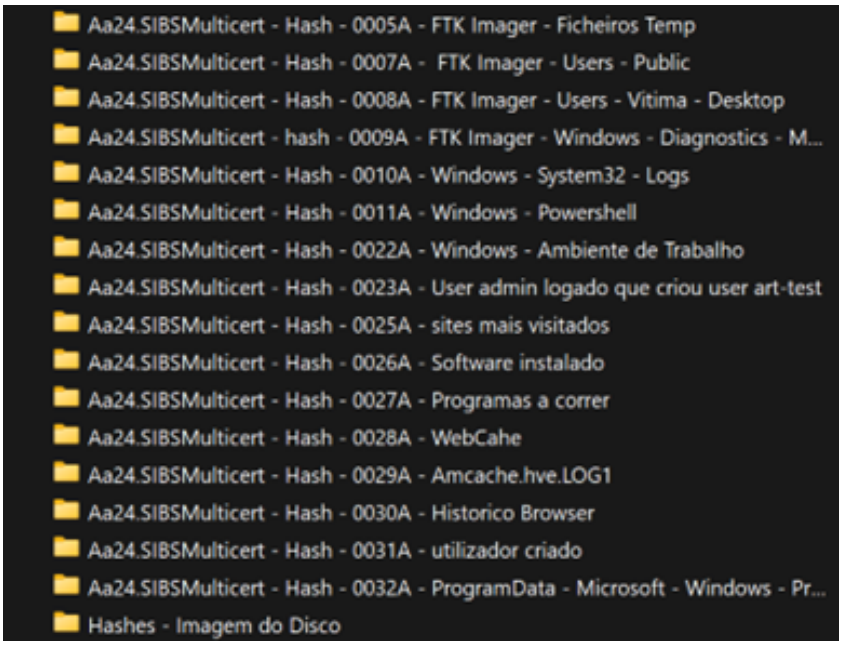


Figura 44: Exemplos das Evidências econtradas pelo Autopsy.

Todos os artefactos passaram pelo processo de se guardar a hash para garantir a integridade da prova (Figura 45):



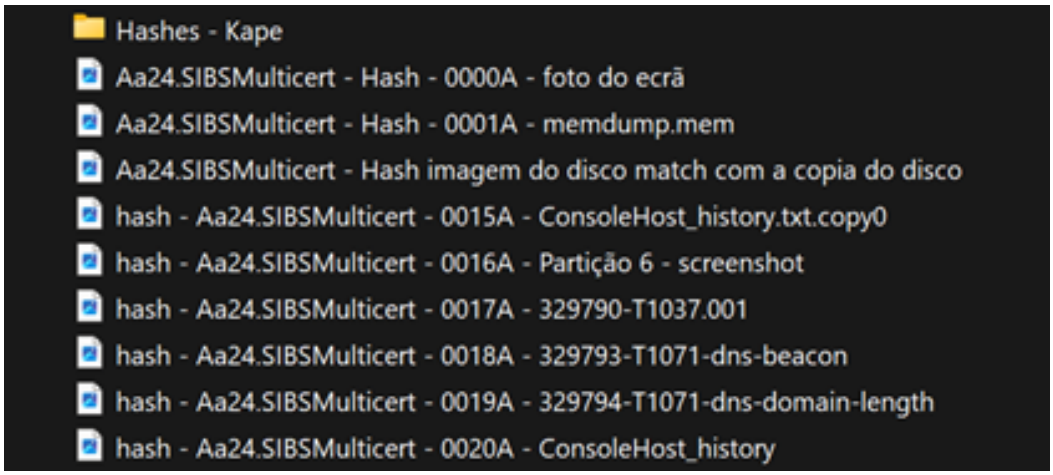


Figura 45: Exemplos dos hashes em Evidências econtradaos pelo Autopsy.

Para obter o hash do ficheiro, escreve-se na linha de comandos o seguinte comando: "get-filehash (diretoria) nome do ficheiro"(Figura 46).

Figura 46: Exemplo da obtenção do hash.

3.7.1 Análise

Na fase de "Análise" começa-se por tentar perceber quais os registos que a linha de comandos guardou. Ao abrir a evidência "Aa24.SIBSMulticert - 0020A - ConsoleHost

history", consegue-se observar que três (3) comandos foram executados e que o ataque foi feito a partir de um script, porém, não se sabe o que foi executado no script (Figura 47).

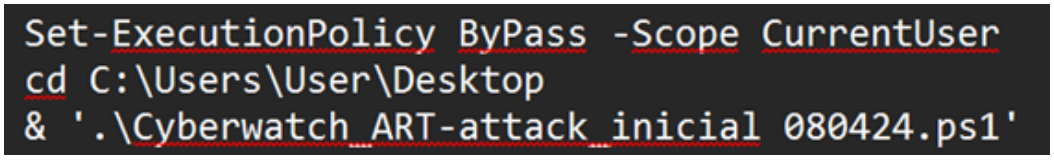


Figura 47: Fase de análise, console history.

A partir das evidências recolhidas pode-se comprovar que existiu o auxílio do software da Red Canario, o "Atomic Red Team", pois foi encontrado instalado na máquina (a partir do artefacto "Aa24.SIBSMulticert - 0012A - Parição 6 - AtomicRedTeam"), juntamente com as duas pastas que este software instala na "Máquina Vítima"(Figura 48):

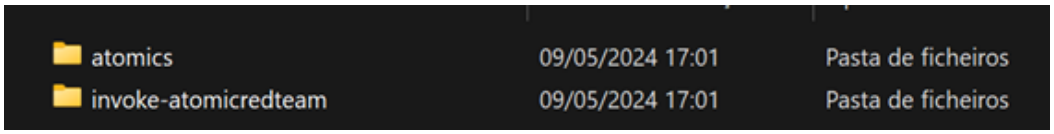


Figura 48: Fase de análise, pastas do ART.

Dentro da pasta "atomics", podem ser encontradas as possíveis técnicas, eis alguns exemplos (Figura 49):

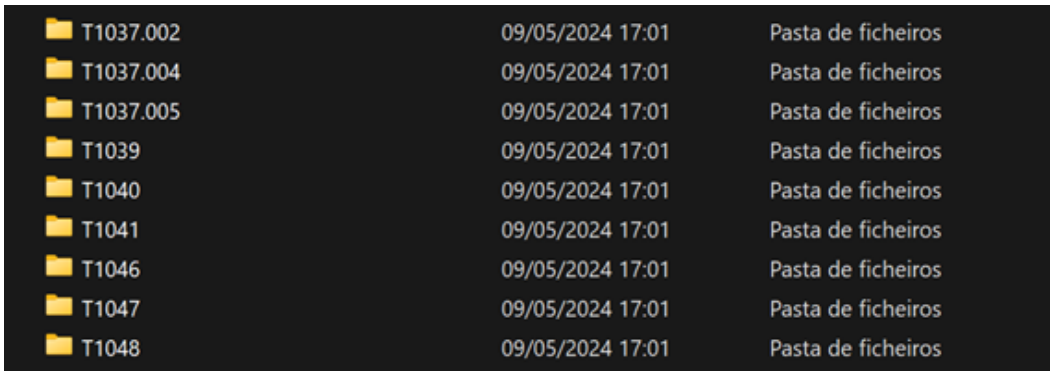


Figura 49: Fase de análise, exemplos de técnicas.

Dentro da pasta "invoke-atomicredteam" estão os diversos métodos e procedimentos utilizados pelo software Atomic Red Team para chamar determinada técnica, eis alguns exemplos (Figura 50):

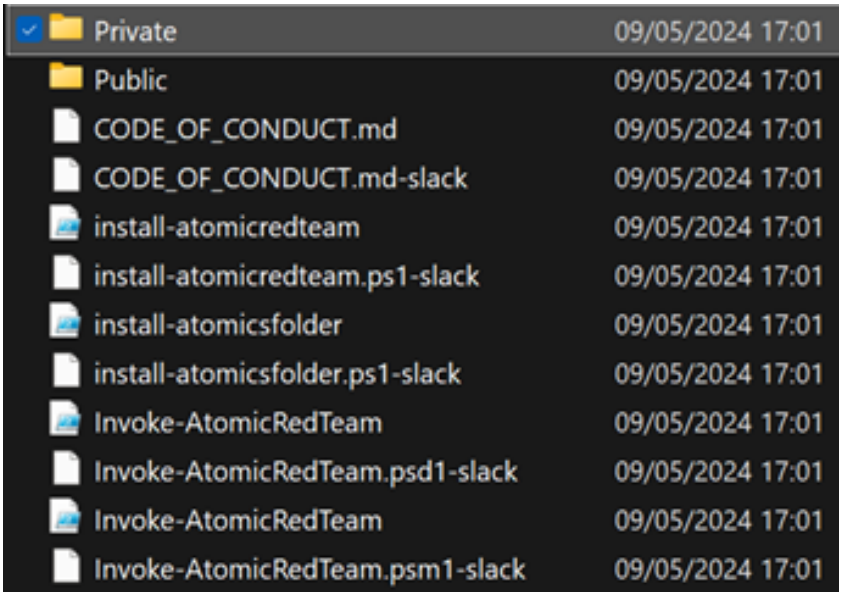


Figura 50: Fase de análise, conteúdo da pasta “invoke-atomicredteam”.

A partir deste momento pode se comprovar, devido às provas encontradas e já referenciadas, quase tudo o que foi feito neste ataque (com exceção das técnicas de “Discovery”, pois estas utilizaram a linha de comandos e, como se pode observar, a linha de comandos não guardou o código utilizado) como, por exemplo:

- Aplicação da técnica T1078.003 de Incial Access. Era esperada a criação de um utilizador administrador. Como o sistema operativo Windows da "Máquina Vítima"estava em português, a técnica não encontrou o grupo “Admin” e colocou o “art-test” como utilizador normal. Sabe-se também que o utilizador foi criado às 17 horas 19 minutos e 54 segundos da tarde do dia 15 de abril de 2024 e que o utilizador que sofreu o ataque é um administrador chamado “vitima” (Figura 52).

```
Username        : art-test [1002]
SID             : S-1-5-21-748454400-3796715826-3808751716-1002
Full Name       :
User Comment    :
Account Type    :
Account Created : Mon Apr 15 16:19:54 2024 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Mon Apr 15 16:19:54 2024 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account
```

Figura 51: Informações do utilizador criado.

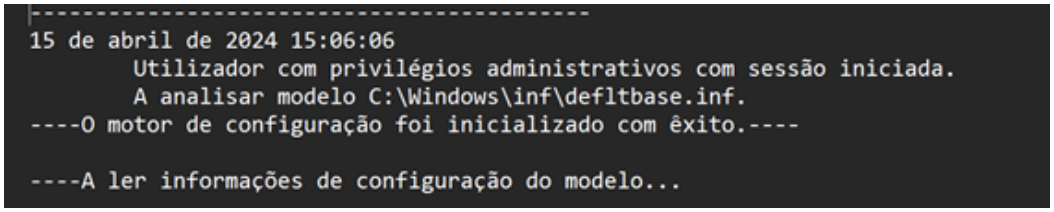


Figura 52: Utilizador que estava logado na hora do ataque.

- Com a aplicação da técnica T1547 “Suspicious bat file run from starup Folder”, previa-se a colocação de um ficheiro bat pasta “startrup” (Figura 53).

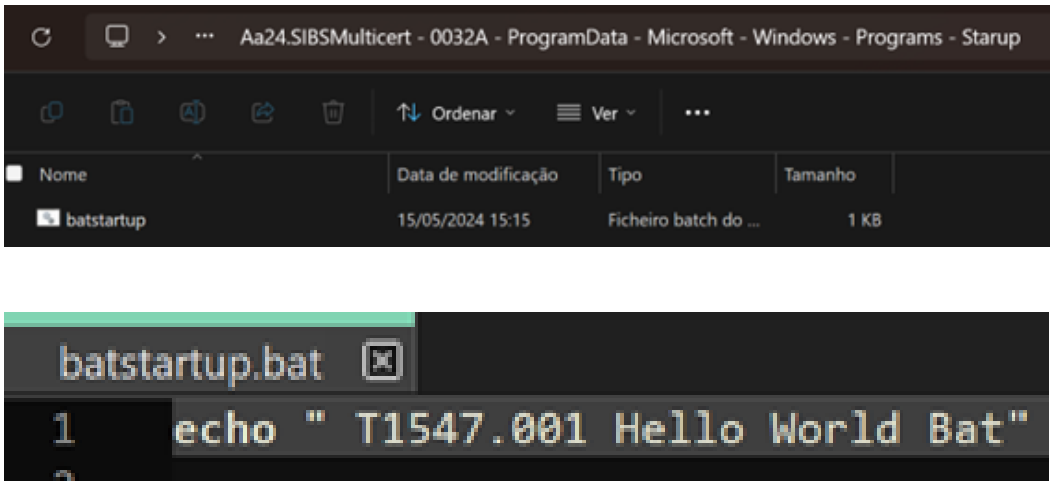


Figura 53: Ficheiro bat encontrado e seu conteúdo.

- Com a aplicação da técnica T219 “TeamViewer Files Detected Test on Windows”, esperava-se encontrar os ficheiros instalados do "TeamViewer"(Figura 54):

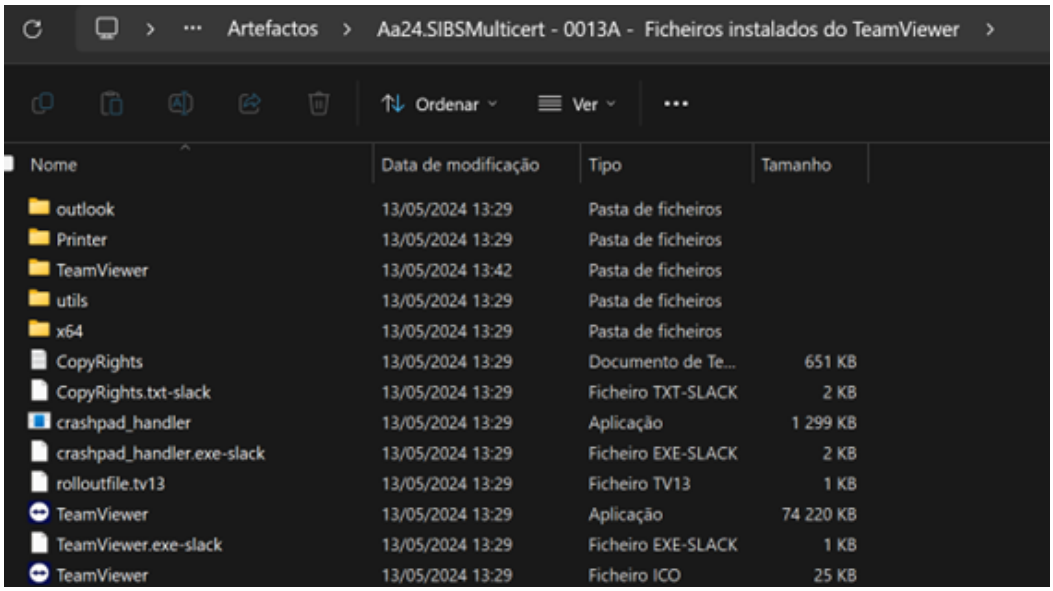


Figura 54: Ficheiro instalados do Teamviewer.

- As técnicas de “Coleção”:
- O screenshot foi encontrado (Figura 55):

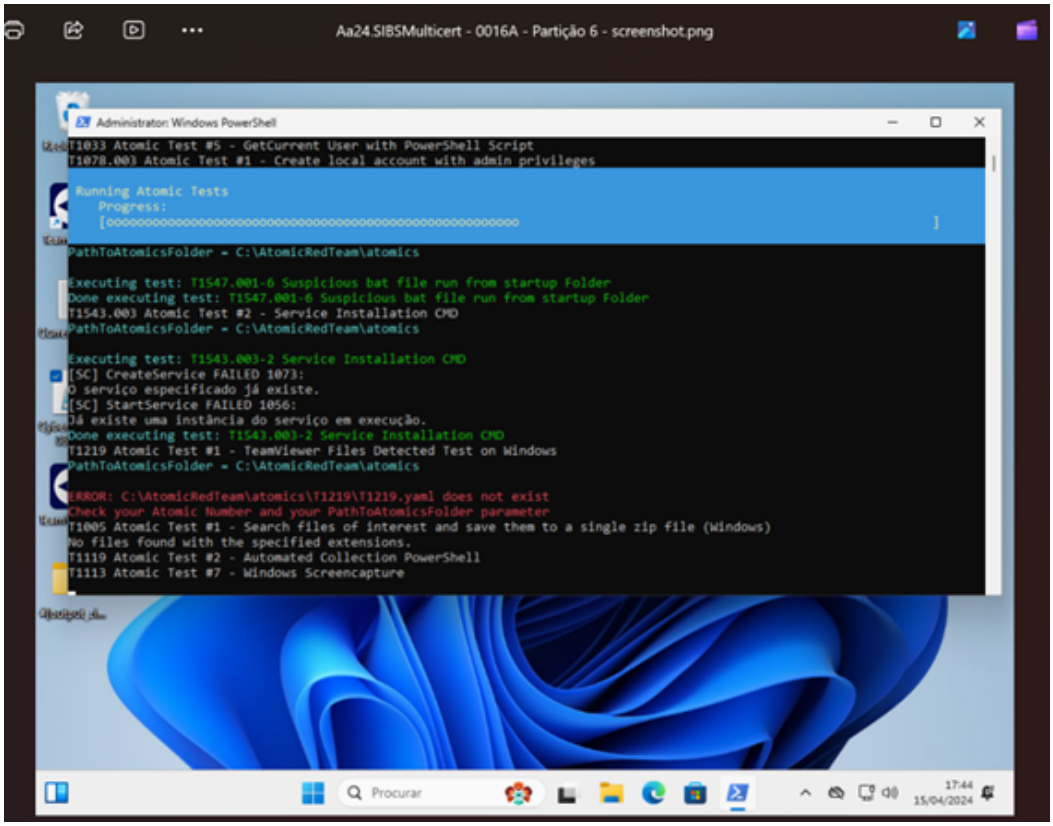


Figura 55: Ficheiro instalados do Teamviewer.

Em relacão à técnica T1125 "Resgistry artefact when application use webcam"consegue-se perceber que não foi aplicada, pois a máquina virtual não possuía câmara.

Terminando a fase de “Análise”, o relatório do incidente foi produzido.

3.7.2 - Reconstrução de Eventos

O relatório é constituido pelos seguintes tópicos: “Enquadramento”, “Investigação”, ”Análise Forense”, “Reconstrução de Eventos”, “Conclusões e Recomendações”. Na fase de “Enquadramento”, foi explicado qual o propósito do relatório, como a investigação começou e a razão pela qual se abriu essa investigação. Na fase de "Investigação"mostrou-se como foram recolhidas as provas, a análise das mesmas e a reconstrução de eventos. Por fim, nas "Conclusões e recomendações", recomendou-se, para além de medidas para melhoria da segurança, que os comandos executados pelo powershell e pela linha de comandos fossem guardados.

3.8 - Síntese

Neste capítulo foram abordados os pontos cruciais do DFIR como:

- A organização do DFIR;
- As mudanças do plano original para o resultado final;
- Os powerpoints entregáveis na secção de estudos teóricos e os cursos aconselhados;
- Templates de partilha de informação;
- Fluxogramas desenvolvidos para Ransomware e Phishing;
- A análise forense;
- A arquitetura planeada e a real do laboratório Forense;
- As configurações das máquinas virtuais;
- O conteúdo do script "Cyberwatch ART-attack.ps1";
- As modificações nas configurações de defesa da "Máquina Vítima";
- A execução do Script;
- A análise forense da "Máquina Vítima".

Todos estes pontos foram cruciais para o desenvolvimento e conclusão das tarefas planeadas. com exceção da tarefa "Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados” pois esta teve de ser modificada como já referido.

4

CONCLUSÕES

Este estágio teve como objetivos:

- Elaboração de documentação de resposta a incidentes e análise forense, com base em dois incidentes tipo: ransomware e phishing;
- . Construção do processo de recolha e manuseamento de prova digital;
- Criação de laboratório virtual para análise de evidências;
- Preparação de modelos de relatório para apresentação de resultados;
- Levantamento de documentação ou formação em ferramentas para First Responders;
- Criação de laboratórios virtuais para treino e aperfeiçoamento dos processos criados.

Concluí-se assim que cerca de 83% das atividades propostas foram cumprindas com sucesso, este resultado advém das seis (6) tarefas propostas das quais cinco (5) foram realizadas sem alterações e da tarefa restante que, embora com alterações, foi também concretizada. Estes números espelham-se na concretização, sem alterações, das subtarefas:

- Recolha de fontes de informação;
- Proposta de estruturação;
- Criação do Prefácio: introdução e Glossário;
- Criação da Preparação;
- Plano de Resposta para Phishing e Ransomware;
- Análise Forense: Preparação; Recolha, Preservação e Análise da Prova, reconstrução de eventos e Relatórios;
- Arquitetar o Laboratório digital;
- Criar o Laboratório digital;
- Criação de um Script com o Atomic Red Team;
- Resposta ao incidente e investigação;

- Compilação do Relatório.

Relativamente aos produtos/entregáveis criados, resultaram os seguintes:

- O documento DFIR para os ataques de Ransomware e incidentes de Phishing;
- Os templates criados para a comunicação e para a formulação do relatório do incidente;
- Os powerpoints de estudos teoricos;
- O laboratório digital com todas as máquinas virtuais.

Para trabalho futuro, podem ser apontadas medidas, tais como:

- Melhorar o documento DFIR, complementando com outros casos de uso;
- Aumenta a capacidade e âmbito dos laboratórios digitais para dar resposta a outras necessidades.

BIBLIOGRAFIA

ATC (2024). *ATT&CK® Navigator*. URL: https://atc-project.github.io/react-navigator/ (acedido em 26/09/2024).

Axonius (2024). *6 Essential Skills for Incident Responders | Axonius*. en. URL: https://www.axonius.com/blog/6-essential-skills-for-incident-responders (acedido em 26/09/2024).

certsocietegenerale (2024a). *IRM/EN/IRM-16-Phishing.pdf at main · certsocietegenerale/IRM*. en. URL: https://github.com/certsocietegenerale/IRM/blob/main/EN/IRM-16-Phishing.pdf (acedido em 26/09/2024).

— (2024b). *IRM/EN/IRM-17-Ransomware.pdf at main · certsocietegenerale/IRM*. en. URL: https://github.com/certsocietegenerale/IRM/blob/main/EN/IRM-17-Ransomware.pdf (acedido em 26/09/2024).

CNCS (2024). *CNCS - Regime Jurídico*. URL: https://www.cncs.gov.pt/pt/regime-juridico/ (acedido em 26/09/2024).

fortinet (2024). *What is a DDoS Attack? DDoS Meaning, Definition & Types*. en. URL: https://www.fortinet.com/resources/cyberglossary/ddos-attack (acedido em 26/09/2024).

GIAC (2024). *GIAC Battlefield Forensics and Acquisition Certification | Cybersecurity Certification*. URL: https://www.giac.org/certifications/battlefield-forensics-acquisition-gbfa/ (acedido em 26/09/2024).

ma-insights (2024). *MA - insights*. URL: https://ma-insights.vercel.app/adversaries/teamtnt (acedido em 26/09/2024).

Johansen, Gerard (dez. de 2022). *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response*. en. Packt Publishing Ltd. ISBN: 978-1-80323-025-2.

Linkedin (2024). *(11) Building a Successful Incident Response Team: Essential Skills and Traits | LinkedIn*. URL: https://www.linkedin.com/pulse/building-successful-incident-response-team-essential-skills-engole/ (acedido em 26/09/2024).

MITRE (2024a). *MITRE ATT&CK®*. URL: https://attack.mitre.org/ (acedido em 26/09/2024).

— (2024b). *MITRE D3FEND Knowledge Graph*. en. URL: https://d3fend.mitre.org/ (acedido em 26/09/2024).

Networks, Palo Alto (2024). *Digital Forensics and Incident Response (DFIR)*. en-US. URL: https://origin-www.paloaltonetworks.com/cyberpedia/digital-forensics-and-incident-response (acedido em 26/09/2024).

SANS (set. de 2024a). *sans-blue-team/DeepBlueCLI*. original-date: 2016-09-20T16:06:06Z. URL: https://github.com/sans-blue-team/DeepBlueCLI (acedido em 26/09/2024).

— (2024b). *What is OSINT (Open-Source Intelligence?) | SANS Institute*. URL: https://www.sans.org/blog/what-is-open-source-intelligence/ (acedido em 26/09/2024).

Wahnon, Meir (set. de 2024). *meirwah/awesome-incident-response*. original-date: 2015-11-10T22:10:58Z. URL: https://github.com/meirwah/awesome-incident-response (acedido em 26/09/2024).

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Relatório de Estágio - SIBS Multicert"*, é original e foi realizado por Estudante Ricardo Silva (2223362) sob orientação de Professor Doutor Paulo Manuel Almeida Costa (paulo.costa@ipleiria.pt).

Leiria, Setembro de 2024

Assinado por: **Ricardo Tiago Gregório da Silva**
Num. de Identificação: 15983769
Data: 2024.11.12 15:37:28+00'00'

CHAVE MÓVEL

Estudante Ricardo Silva