AFD APONTAMENTOS

# Analise Forense

**Introdução**

A **analise forense** estuda técnicas para recolher, preservar, analisar e apresentar **evidências digitais** de forma legalmente válida. Esta disciplina é essencial em investigações criminais, auditorias e segurança informática.

# Objetivos da Investigação Digital

**Identificar dispositivos** envolvidos no incidente. Determinar **como** foram utilizados.

Entender **o motivo** por trás da ação. Identificar **quem** causou o incidente.

# Tipos de Evidência Digital

**Ficheiros eliminados** e seus metadados.

**Histórico de navegação** e logs do sistema. **Dispositivos conectados** (USB, cartões de memória). **Mensagens e emails**.

# Software malicioso.

**Processo de Análise Forense Digital**

**Identificação** → Determinar as fontes de evidência.

**Preservação** → Criar cópias forenses sem alterar dados.

**Análise** → Examinar ficheiros, logs, registos e atividades.

**Relatório** → Documentar descobertas e apresentar provas.

# Ferramentas Utilizadas

**Autopsy** → Investigação de discos e ficheiros apagados.

**Wireshark** → Análise de tráfego de rede.

**Volatility** → Análise de memória RAM.

**FTK Imager** → Aquisição e visualização de imagens forenses.

**Kali Linux** → Conjunto de ferramentas forenses e de segurança.

# Técnicas Anti-Forenses

**Estenografia** → Esconder ficheiros dentro de outros ficheiros.

**Encriptação** → Tornar dados ilegíveis sem chave de acesso.

**Manipulação de timestamps** → Alteração das datas de criação e modificação de ficheiros.

**Eliminação segura de dados** → Ferramentas que sobrescrevem ficheiros apagados.

# Funções de Hash e Integridade de Dados

**MD5 e SHA-1** → Já não são considerados seguros devido a colisões.

**SHA-256 e SHA-512** → Algoritmos recomendados para garantir integridade.

# Exemplo de verificação de hash:

sha256sum ficheiro.txt

**Possíveis Perguntas para Exame**

O que é a informática forense e qual a sua importância?

# Res: É a área que investiga evidências digitais de forma legalmente válida, sendo essencial para segurança e processos judiciais.

Quais são as fases do processo de análise forense digital?

# Res: Identificação, preservação, análise e documentação.

Que tipos de evidências podem ser recolhidas numa investigação digital?

# Res: Ficheiros apagados, logs, histórico de navegação, dispositivos conectados e software suspeito.

Qual a diferença entre análise live e análise a frio?

# Res: A análise live examina o sistema ligado, enquanto a análise a frio é feita com o dispositivo desligado.

O que são funções de hash e porque são importantes?

# Res: São algoritmos que geram uma assinatura única de um ficheiro, garantindo integridade e autenticidade.

Como funciona a recuperação de ficheiros apagados?

# Res: Ficheiros podem ser recuperados analisando metadados e espaços não alocados no disco.

O que é esteganografia e como pode ser identificada?

# Res: É a técnica de esconder ficheiros dentro de outros ficheiros; pode ser detectada com ferramentas como \*\*steghide\*\* .

Quais as ferramentas mais utilizadas na informática forense?

# Res: Autopsy, Wireshark, Volatility, FTK Imager, e ferramentas do Kali Linux.

**Análise de Dados Armazenados**

**Introdução**

A análise de dados armazenados envolve a **organização dos discos**, **sistemas de ficheiros** e **representação dos dados**. Estes conceitos são fundamentais para a investigação forense digital.

# Organização dos Discos

**Master Boot Record (MBR)** → Ocupa os primeiros 512 bytes do disco e contém a tabela de partições.

**GUID Partition Table (GPT)** → Método mais moderno que suporta discos maiores e mais partições.

**Partições** → Divisões lógicas do disco onde diferentes sistemas de ficheiros são aplicados.

# Sistemas de Ficheiros

**FAT (12,16,32)** → Simples, utilizado em USBs e cartões de memória.

**NTFS** → Utilizado pelo Windows, suporta permissões de ficheiros e recuperação de dados.

**EXT2, EXT3, EXT4** → Usado no Linux, inclui funcionalidades como journaling.

# Representação de Dados

**Números** → Decimal, binário, hexadecimal e octal.

# Ordem de bytes:

 **Big-endian** → O byte mais significativo vem primeiro.

 **Little-endian** → O byte menos significativo vem primeiro.

# Codificação de caracteres:

 **ASCII** → 8 bits, utilizado historicamente.

 **Unicode (UTF-8, UTF-16, UTF-32)** → Suporte a múltiplas línguas.

# Identificação de Ficheiros

**Magic numbers** → Assinaturas hexadecimais que identificam tipos de ficheiros.

# Exemplo de análise de ficheiros desconhecidos:

file nome\_do\_ficheiro

hexdump -C nome\_do\_ficheiro | head -n 10

**Possíveis Perguntas para Exame**

O que é o MBR e qual a sua função?

# Res: O Master Boot Record (MBR) é o primeiro setor de um disco, contendo a tabela de partições e código de boot.

Qual a diferença entre MBR e GPT?

# Res: O MBR suporta até 4 partições primárias, enquanto o GPT permite um número maior de partições e suporta discos maiores.

O que são magic numbers e como são usados?

# Res: São assinaturas numéricas específicas que identificam tipos de ficheiros, usadas para determinar formatos mesmo sem extensão.

Como identificar um ficheiro desconhecido?

# Res: Usando comandos como metadados e estrutura binária do ficheiro.

\*\*file\*\*

\*\*hexdump\*\*

**e**

# para analisar

O que é a Master File Table (MFT) no NTFS?

# Res: É uma estrutura que armazena informações sobre todos os ficheiros num volume NTFS, incluindo permissões e metadados.

Como recuperar ficheiros eliminados de um sistema de ficheiros?

# Res: Usando técnicas como file carving, análise da MFT (NTFS) ou FAT para identificar referências a ficheiros apagados.

O que é o journaling em sistemas de ficheiros?

# Res: É uma funcionalidade que regista alterações antes de serem aplicadas, ajudando a prevenir corrupção de dados.

Qual a importância da ordem dos bytes (endianness)?

# Res: Determina como os dados são armazenados na memória e pode afetar a compatibilidade entre sistemas diferentes.

**Investigação Digital com Autopsy**

Introdução

Autopsy é uma ferramenta gráfica para análise forense digital de imagens de discos e outros dispositivos de armazenamento. Baseado no The Sleuth Kit (TSK), é utilizado para identificar e extrair evidências digitais.

Fluxo de Trabalho no Autopsy

**Criar um caso** → Definição de nome, número do caso e investigador.

**Adicionar fonte de dados** → Imagens de disco, pastas, ficheiros individuais, ou discos virtuais.

**Executar módulos de ingestão** → Processamento automático dos dados.

**Análise e investigação** → Visualização e pesquisa de evidências.

**Relatórios e exportação** → Geração de relatórios sobre os achados forenses.

Aquisição de Imagens

Ferramentas utilizadas: **Guymager, FTK Imager**.

O processo de aquisição deve garantir a integridade dos dados, gerando um **hash SHA-256** para validação.

Montagem da imagem adquirida no Linux:

mkdir /media/pen

mount -t auto -o loop pen\_usb.img /media/pen

Análise de Conteúdos

**Tree Viewer** → Permite navegação pela estrutura de dados:

 **Data sources**: Exibe os ficheiros analisados.

 **Views**: Organiza ficheiros por tipo, tamanho, estado, etc.  **Results**: Apresenta os resultados de módulos de análise.  **Reports**: Lista relatórios gerados.

**Pesquisa de ficheiros** → Pesquisa por nome, tipo MIME, datas.

**Galeria de imagens** → Organização e análise de ficheiros gráficos.

Módulos do Autopsy

**Recent Activity** → Extrai histórico de navegação, programas usados e dispositivos conectados.

**Hash Lookup** → Compara hashes de ficheiros com bases de dados de referências conhecidas (NSRL, VirusShare).

**File Type Identification** → Verifica tipos de ficheiros e suas extensões. **Keyword Search** → Pesquisa palavras-chave relevantes nos ficheiros. **EXIF Parser** → Extrai metadados de imagens, incluindo geolocalização. **PhotoRec Carver** → Recupera ficheiros apagados do espaço não alocado.

Cronologias e Relatórios

**Criação de cronologias** → Baseia-se em datas de modificação, criação e acesso dos ficheiros.

**Filtragem** → Permite refinar a análise por janelas temporais ou tipos de eventos.

**Relatórios** → Gerados em diferentes formatos (TXT, KML, CSV), incluindo listas de ficheiros e tempos de modificação/acesso.

# Possíveis Perguntas para Exame

O que é o Autopsy e para que serve?

# Res: Autopsy é uma ferramenta de análise forense digital usada para investigar imagens de discos e recuperar evidências.

Quais são os principais passos na criação de um caso no Autopsy?

# Res: Criar o caso, adicionar fonte de dados, processar os dados, analisar evidências e gerar relatórios.

Como o Autopsy lida com ficheiros eliminados?

**Res: Através da vista e do módulo** \*\*PhotoRec Carver\*\* **,**

\*\*Deleted Files\*\*

# que permite recuperar dados de setores não alocados.

O que é o módulo e como ele funciona?

**Hash Lookup**

# Res: Ele compara os hashes dos ficheiros analisados com bases de dados conhecidas para identificar ficheiros suspeitos ou inofensivos.

Como os metadados de imagens podem ser úteis na análise forense?

# Res: Os metadados EXIF podem conter data, hora, modelo da câmara e coordenadas GPS, ajudando a identificar a origem de uma imagem.

Como se pode utilizar o no Autopsy?

**Keyword Search**

# Res: Esse módulo permite pesquisar palavras-chave nos ficheiros analisados, incluindo emails e documentos.

Quais são as vantagens da cronologia no Autopsy?

# Res: Permite visualizar eventos por data, facilitando a reconstrução da linha do tempo de um incidente digital.

Como gerar um relatório no Autopsy?

# Res: Através do menu \*\*Reports\*\* , onde se pode escolher diferentes formatos como CSV, KML ou HTML, dependendo do objetivo da análise.

**Análise a Sistemas Ligados (Live)**

**Introdução**

A investigação forense digital em sistemas ligados (live) foca-se na extração de informação volátil, como **dados em RAM, processos em execução e ligações de rede**. Essa abordagem é útil para obter informações que podem desaparecer após o desligamento do sistema.

# Especificidades e Limitações

**Minimizar alterações no sistema analisado**, pois qualquer ação pode modificar evidências.

**Dependência do sistema analisado**, pois algumas ferramentas podem ser bloqueadas ou afetadas por malware.

**Requer acesso ao sistema**, tornando a análise intrusiva.

# Estratégias de Investigação Live

**Execução de utilitários ou scripts** → Comandos para recolher informações sem capturar a RAM.

**Recolha de uma imagem da memória RAM (RAM dump)** → Permite análise posterior da memória volátil.

# Informação Passível de Recolha

**Lista de processos em execução** ( pslist no Linux, no Windows).

tasklist

**Lista de ficheiros abertos** ( lsof no Linux, no Windows).

handle

**Ligações de rede ativas** ( netstat no Linux/Windows).

**Dump de memória RAM** ( WinPmem para Windows, para Linux).

LiME

# Dados em RAM

Aplicações não protegem conteúdo armazenado na RAM.

Palavras-passe e informação sensível podem ser recuperadas.

Dados podem persistir mesmo após o encerramento do programa ou reinício.

# Ferramentas para Análise de RAM

**WinPmem** → Para adquirir uma cópia da memória RAM no Windows.

**LiME** → Para aquisição de RAM no Linux.

**Volatility Framework** → Para análise de dumps de memória.

# Volatility Framework

**Volatility** é uma ferramenta open-source para análise de dumps de RAM. Permite extrair **processos, passwords, ligações de rede e dados forenses**.

# Comandos úteis no Volatility:

→ Identifica o perfil do dump de memória.

imageinfo

→ Lista de processos ativos.

pslist

→ Ligações de rede ativas.

netscan

→ Extração de hashes de passwords.

hashdump

→ Mostra o conteúdo da área de transferência.

clipboard

→ Identifica processos potencialmente maliciosos.

malfind

# Possíveis Perguntas para o Exame

O que é a análise forense live e quando deve ser utilizada?

# Res: É a investigação de sistemas em execução, usada quando há risco de perder dados voláteis, como processos ativos e memória RAM.

Quais são as principais informações que podem ser recolhidas na análise live?

# Res: Processos ativos, ficheiros abertos, ligações de rede, registos do sistema e conteúdos da memória RAM.

Qual a principal limitação da análise live?

# Res: Qualquer ação pode modificar as evidências, tornando difícil garantir a integridade dos dados coletados.

Quais as ferramentas mais usadas para aquisição de RAM?

**Res:**

\*\*WinPmem\*\*

# para Windows e

**para Linux.**

Como o Volatility pode ser usado na análise forense?

\*\*LiME\*\*

# Res: Permite extrair processos, passwords, ligações de rede e identificar malware em dumps de memória.

Qual a diferença entre

**pslist**

e

no Volatility?

# Res: lista processos ativos de forma linear, enquanto

**pstree**

\*\*pslist\*\*

\*\*pstree\*\*

**exibe os processos em estrutura hierárquica.**

Como extrair passwords de um dump de memória?

# Res: Usando o comando de credenciais armazenadas.

\*\*hashdump\*\*

Como identificar malware na memória?

**no Volatility para recuperar os hashes**

**Res: Utilizando** \*\*malfind\*\* **, que identifica processos suspeitos com código injetado.**

**Investigação Digital a Telemóveis**

**Introdução**

A investigação digital forense em dispositivos móveis foca-se na **extração e análise de dados** armazenados em telemóveis, cartões SIM e cartões de memória. Esses dispositivos contêm informações valiosas como **registos de chamadas, mensagens, emails, dados de localização e redes sociais**.

# Estrutura da Investigação

**Cartões SIM** → Contém identificadores, registos de chamadas, SMS e contatos. **Telemóveis** → Armazenam IMEI, ficheiros, registos de aplicações, redes Wi-Fi e GPS.

**Cartões de Memória** → Podem conter ficheiros multimédia e backups de dados.

**Cloud e Operadoras** → Algumas informações podem ser obtidas mediante autorização legal.

# Cartões SIM e UICC

**UICC (Universal Integrated Circuit Card)** → Componente electronica que pode conter múltiplos cartões SIM.

**Evolução do SIM** → Mini SIM (2FF), Micro SIM (3FF), Nano SIM (4FF) e eSIM (MFF1/MFF2).

# Identificadores:

 **ICCID (Integrated Circuit Card Identifier)** → Número único do cartão SIM.

 **IMSI (International Mobile Subscriber Identity)** → Identifica o cliente e a operadora.

 **MSISDN (Mobile Station International Subscriber Directory Number)** → Número de telefone associado.

# Telemóveis e IMEI

**O que é o IMEI?** → International Mobile Equipment Identity, um identificador único de cada telemóvel.

# Estrutura do IMEI:

 **TAC (Type Allocation Code)** → Primeiros 8 dígitos que indicam marca e modelo.

 **Número de Série** → 6 dígitos identificando o dispositivo.

 **Dígito de verificação** → Último dígito para validação.

**Exercício**: Verificar IMEI com e validar TAC online.

\*#06#

# Métodos de Aquisição de Dados

**Aquisição Lógica** → Extrai apenas os dados acessíveis pelo sistema operativo.

 Aplicações forenses (ex.: XRY, UFED) pedem permissões ao dispositivo.  Não permite recuperar dados apagados.

**Aquisição Física** → Copia bit a bit os dados do dispositivo.

 Permite recuperação de ficheiros eliminados.

 Requer exploração de vulnerabilidades ou permissões root.

# Isolamento da Rede

**Motivo:** Evitar alterações ou eliminação remota de dados.

# Técnicas:

Ativar **modo avião**.

Remover **cartão SIM e desligar Wi-Fi**.

Usar **caixas ou sacos de Faraday** para bloqueio de sinais.

# Ferramentas Utilizadas

**XRY** → Extrai dados de telemóveis bloqueados. **Autopsy** → Análise forense de sistemas Android. **FTK Imager** → Aquisição de cartões de memória.

**SQLiteBrowser** → Análise de bases de dados de aplicações.

**strings & file** → Identificação de tipos de ficheiros e extração de texto.

# Possíveis Perguntas para Exame

Quais são as principais fontes de evidência num telemóvel?

# Res: O próprio dispositivo, cartões SIM, cartões de memória e serviços cloud.

Qual a diferença entre ICCID, IMSI e IMEI?

# Res: ICCID identifica o cartão SIM, IMSI identifica o assinante e IMEI identifica o dispositivo.

Como isolar um telemóvel antes da aquisição de dados?

# Res: Ativando o modo avião, removendo cartões SIM/Wi-Fi e colocando em caixa de Faraday.

Qual a diferença entre aquisição lógica e aquisição física?

# Res: A aquisição lógica extrai apenas dados acessíveis, enquanto a física copia toda a memória, incluindo dados apagados.

Como recuperar mensagens eliminadas de um cartão SIM?

# Res: Se não sobrescritas, podem ser recuperadas com leitores de cartões SIM especializados.

Qual a importância do IMEI na investigação forense?

# Res: Permite identificar e rastrear dispositivos móveis.

Como funciona a extração de dados de aplicações móveis?

# Res: Através da análise de bases de dados SQLite e logs do sistema.

Que ferramentas podem ser usadas na análise forense de telemóveis?

# Res: XRY, UFED, Autopsy, FTK Imager, SQLiteBrowser, entre outras.

**Análise Forense de Aplicações Mobile**

**Introdução**

A análise forense de aplicações móveis foca-se na extração de informações sobre permissões, comunicações, bases de dados e código-fonte. Aplicações podem armazenar e transmitir dados sensíveis, tornando-as um alvo essencial para investigações digitais.

# Permissões em Aplicações

**Controle de permissões:** Sistemas operativos móveis (Android e iOS) impõem restrições ao acesso de funcionalidades.

# Permissões normais vs. perigosas:

 **Normais:** Baixo risco, ativadas por padrão (ex.: alterar fuso horário).

 **Perigosas:** Requerem aprovação explícita (ex.: GPS, acesso a contactos).

# Grupos de permissões importantes:

 **Localização** → Acesso a GPS e redes Wi-Fi.

 **Armazenamento** → Leitura/escrita em dispositivos.

 **SMS/Chamadas** → Monitorização de mensagens e registos de chamadas.

# Riscos de segurança:

 Aplicações podem enganar utilizadores para obter permissões desnecessárias.

 Algumas escondem comportamento malicioso por trás de permissões legítimas.

# Análise de Comunicações

**HTTP vs HTTPS** → Aplicações devem usar HTTPS para proteger dados.

# Captura de tráfego:

 Pode revelar comunicações inseguras ou dados expostos.

 Ferramentas como

mitmproxy

# Autenticação e APIs:

permitem analisar conexões cifradas.

Algumas aplicações utilizam OAuth para autenticação.

APIs sem autenticação podem permitir vazamento de dados.

# Bases de Dados Locais

**Armazenamento interno**:

 Muitas aplicações usam **SQLite** para armazenar dados.

 Algumas bases de dados não são cifradas, permitindo fácil extração.

# Análise de bases de dados:

 Ferramentas como **SQLiteBrowser** permitem visualizar conteúdos armazenados.

 Logs de atividades e mensagens podem ser recuperados.

# Análise de Código

**Ficheiros APK**:

 Aplicações Android são distribuídas como

(arquivos ZIP).

.apk

 Podem ser descompiladas para análise com ferramentas específicas.

# Ferramentas de análise:

 **APKTool** → Descompila APKs para análise do código.

 **JADX-GUI** → Permite leitura do código-fonte Dalvik/Java.

 **Bytecode Viewer** → Análise de binários compilados.

# Extração de credenciais e links ocultos:

 Muitas aplicações armazenam tokens ou URLs sensíveis em seu código.  APKs podem conter credenciais hardcoded.

# Possíveis Perguntas para o Exame

O que são permissões perigosas em aplicações móveis?

# Res: São permissões que exigem autorização explícita do utilizador e podem afetar a privacidade, como acesso à câmara e GPS.

Como pode um investigador forense analisar comunicações de uma aplicação móvel?

# Res: Utilizando ferramentas como para capturar tráfego de

\*\*mitmproxy\*\*

**rede, verificando a segurança das conexões HTTP/HTTPS.**

Qual a importância da análise de bases de dados em aplicações móveis?

# Res: Muitas aplicações armazenam dados localmente em SQLite, permitindo recuperar mensagens, registos e atividades do utilizador.

Como descompilar uma aplicação Android para análise forense?

\*\*JADX-

# Res: Utilizando ferramentas como para visualizar o código-fonte.

\*\*APKTool\*\*

GUI\*\*

**para desmontagem e**

O que é um ataque Man-in-the-Middle (MITM) e como pode ser usado na análise forense?

# Res: É um ataque que intercepta comunicações entre um dispositivo e um servidor, permitindo analisar dados transmitidos.

Como identificar credenciais armazenadas em código de aplicações?

# Res: Descompilando o APK com sensíveis como tokens e URLs.

\*\*JADX-GUI\*\*

**e pesquisando por strings**

Como um investigador pode verificar se uma aplicação está vazando dados?

# Res: Capturando tráfego de rede e analisando conexões com servidores

**externos usando ou** \*\*mitmproxy\*\* **.**

\*\*Wireshark\*\*

O que são bases de dados SQLite e qual sua relevância na forense mobile?

# Res: SQLite é um formato de BD usado por muitas aplicações para armazenar dados localmente, permitindo recuperar informações apagadas.

**Análise Forense a Redes de Computadores**

**Introdução**

A análise forense de redes investiga **tráfego de rede, logs e dispositivos conectados** para identificar ataques, fugas de informação e atividades maliciosas. Permite a captura e interpretação de pacotes de dados.

# Fases da Investigação Forense de Redes

**Identificação da Rede** → Reconhecimento de dispositivos, endereços IP e topologia.

tcpdump

Wireshark

**Captura de Tráfego** → Uso de ferramentas como registar pacotes.

e

para

**Análise Protocolar** → Verificação de protocolos suspeitos (HTTP, SMTP, POP3, etc.).

**Filtragem e Extração** → Aplicação de filtros BPF para encontrar pacotes relevantes.

**Correlação de Eventos** → Comparação com logs e outros sistemas de monitorização.

# Técnicas de Captura de Tráfego

**Port Mirroring** → Reencaminha pacotes de uma porta de switch para um dispositivo de monitorização.

**Network Taps** → Dispositivos físicos que duplicam tráfego de rede.

**Packet Sniffing** → Captura passiva de pacotes em redes Wi-Fi e com fio.

# Ferramentas de Captura e Análise

**Wireshark** → Captura e análise gráfica de pacotes. **Tcpdump** → Captura de pacotes via linha de comandos. **Nmap** → Descoberta de dispositivos e serviços ativos. **ngrep** → Pesquisa de padrões em pacotes de rede.

**tshark** → Versão CLI do Wireshark para filtragem e análise rápida.

# Berkeley Packet Filters (BPF)

**BPF permite filtrar pacotes durante a captura.** Exemplos:

Capturar tráfego HTTP:

tcpdump -i eth0 port 80

Capturar apenas pacotes de um IP:

tcpdump -i eth0 src host 192.168.1.10

Capturar pacotes DNS:

tcpdump -i eth0 port 53

# Técnicas de Análise Forense

**Identificação de sistemas operativos** →

nmap -O [IP]

**Monitorização de tráfego suspeito** → Análise de conexões inesperadas. **Deteção de ataques** → Análise de pacotes anómalos ou tentativas de exploração de vulnerabilidades.

**Reconstrução de comunicação** → Extração de credenciais e mensagens de pacotes não encriptados.

# Possíveis Perguntas para Exame

O que é a análise forense de redes?

# Res: É a investigação do tráfego e logs de rede para detetar ataques, vazamentos de dados e comportamentos suspeitos.

Quais são os principais métodos de captura de tráfego?

# Res: Port mirroring, network taps e packet sniffing.

Qual a diferença entre

**tcpdump**

e **Wireshark** ?

**Res: O**

\*\*tcpdump\*\*

# pacotes, enquanto o

\*\*Wireshark\*\*

**é uma ferramenta de linha de comandos para capturar permite análise gráfica detalhada.**

O que são Berkeley Packet Filters (BPF) e como são usados?

# Res: BPF são filtros aplicados a capturas de pacotes para reduzir a quantidade de dados processados.

Como identificar sistemas operativos numa rede?

# Res: Usando para análise de fingerprints do sistema.

\*\*nmap -O [IP]\*\*

Que tipo de informações podem ser obtidas através da análise de pacotes?

# Res: Endereços IP, protocolos utilizados, conteúdos não encriptados e tentativas de acesso suspeitas.

Como capturar apenas pacotes HTTP numa rede?

# Res: Usando para filtrar pacotes HTTP.

\*\*tcpdump -i eth0 port 80\*\*

O que fazer se um ataque for identificado numa análise de rede?

# Res: Isolar o tráfego suspeito, analisar logs, identificar origem e implementar medidas de contenção.

**Exame Simulado - Informática Forense**

Grupo I

[10 min] (2,5 valores)

“A tabela de partições GPT é mais segura e eficiente que o MBR.” Comente a afirmação, indicando se concorda ou não com a mesma. Justifique a sua resposta com exemplos.

[10 min] (2,5 valores)

“A análise de tráfego de rede é essencial na informática forense, mas pode ser afetada por técnicas anti-forenses.” Comente a afirmação, indicando se concorda ou não com a mesma. Justifique a sua resposta com exemplos.

Grupo II

[10 min] (2,0 valores)

Distinga a aquisição de dados lógica da aquisição de dados física em dispositivos móveis, dando exemplos concretos de situações onde se deve usar cada uma.

[10 min] (2,0 valores)

Desenhe um esquema gráfico de um disco com uma partição primária NTFS, outra partição primária FAT32 e uma partição estendida EXT4. Todas as partições têm um tamanho igual e o disco serve como unidade de arranque do sistema.

[10 min] (2,0 valores)

Enumere os comandos necessários para capturar todo o tráfego HTTP e HTTPS de entrada e saída de um PC numa rede utilizando tcpdump .

Grupo III

[25 min] (3,0 valores)

Analise o seguinte resumo de um pacote de rede:

1 Ethernet II, Src: 00:1A:2B:3C:4D:5E, Dst: 11:22:33:44:55:66

1. Internet Protocol Version 4, Src: 192.168.1.10, Dst: 10.0.0.5
2. Transmission Control Protocol, Src Port: 443, Dst Port: 50932, Seq: 310, Ack: 200, Len: 150
3. Secure Sockets Layer
4. TLSv1.2 Record Layer: Application Data Protocol: HTTPS
5. Content Type: Application Data (23)
6. Version: TLS 1.2 (0x0303)
7. Length: 120
8. Encrypted Application Data: a7d3e6f981b0...

Responda às seguintes questões, justificando suas respostas e indicando sempre a linha do resumo onde se baseou:

* 1. Que protocolos estão presentes no pacote?
  2. Qual é o endereço MAC do equipamento emissor e do destinatário?
  3. Qual é o endereço IP do equipamento emissor e do destinatário?
  4. Qual é a aplicação geradora do pacote?
  5. Qual é o propósito deste pacote?

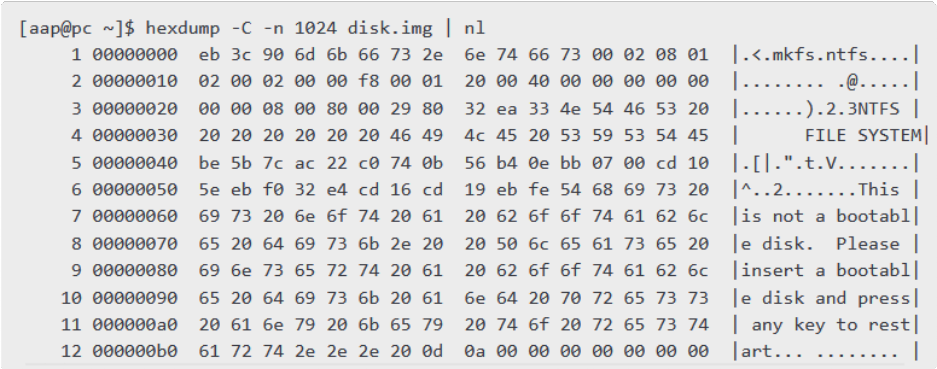
[20 min] (3,0 valores)

Apresente uma linha de comandos que permita listar todos os acessos a servidores de email (POP, IMAP, SMTP, cifrados ou não) e todas as consultas de DNS feitas pelo IP

192.168.1.50 num ficheiro de captura usando tcpdump .

rede.pcap

[25 min] (3,0 valores)

Analise a seguinte sessão de terminal e interprete os dados extraídos:

Que informação consegue extrair do ficheiro disk.img ? Analise o seu conteúdo e explique o que pode ser inferido a partir dos dados apresentados.