Resolução Exame 2022/2023

**“Investigação digital a sistemas ligados tentar extrair informação não volátil.”**

**Comente a afirmação, indicando também se concorda ou não com a mesma. Fundamente a sua resposta com um exemplo concreto.**

**R:**

Não concordo, pois, a investigação a sistemas ligados tenta precisamente extrair informação volátil como por exemplo *dumps* de memória *RAM* para tentar perceber o que estava a acontecer na máquina naquele momento.

**“O módulo de identificação de tipos de ficheiros do Autopsy gera output próprio.”**

**Comente a afirmação, indicando também se concorda ou não com a mesma. Fundamente a sua resposta com um exemplo concreto.**

**R:**

Concordo com a afirmação, pois o Autopsy, uma ferramenta forense digital, é conhecido por ter módulos dedicados à análise de diferentes aspectos de um caso forense.

O módulo de identificação de tipos de ficheiros do Autopsy é responsável por determinar o tipo de ficheiro com base nas suas características e assinaturas. Gera um output próprio, o que significa que fornece informações específicas sobre os tipos de ficheiro identificados durante a análise forense como por exemplo seria quando o Autopsy identifica um ficheiro como sendo do tipo JPEG, data, localização durante a análise.

**Distinga, por palavras suas, técnicas de investigação digital forense, de técnicas anti-forense.**

**Apresente exemplos de ambas. R:**

Técnicas de investigação forense digital são técnicas e ferramenta que permitem recuperar, preservar e analisar evidências digitais armazenadas em, ou transmitidas por dispositivos digitais. Exemplos disso seria o programa *autopsy* que é um programa que permite analisar discos rígidos, pens, telemóveis, entre outros dipositivos e recuperar por exemplo, ficheiros apagados.

Técnicas anti-forense é um conjunto de técnicas que impedem a análise de evidências. Exemplos disso seria por exemplo a encriptação de dados/ficheiros, estenografia (Esconder dados dentro de dados de forma a dificultar o acesso aos mesmos*.*

1. **Desenhe um esquema gráfico de um disco particionado com MBR que contenha as partições seguintes, por ordem: duas partições estendidas FAT32 e uma partição primária NTFS. As partições devem ter um tamanho igual.**



**Enumere todos os comandos necessários para espelhar, num switch Cisco, todo o tráfego de entrada nas portas Gig0/23 e Gig0/24 para a porta Gig0/1.**

En

Conf t

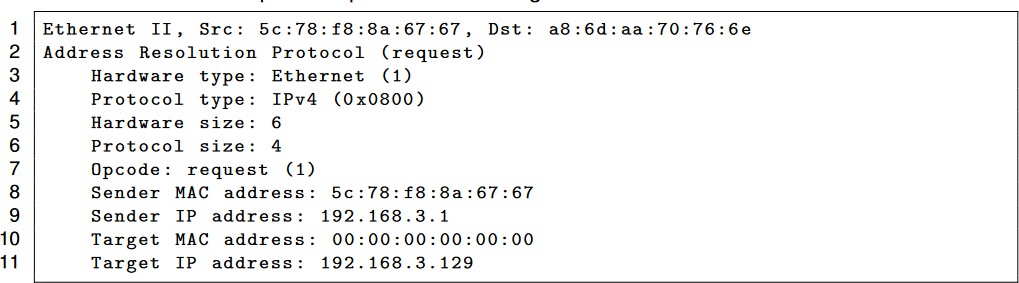
monitor session 1 source interface Gig0/23 - 24

monitor session 1 destination interface Gig0/1

exit

write memory

1. **Responda a cada uma das seguintes questões. Indique sempre a linha do resumo que lhe permitiu chegar a cada resposta.**

****

Que protocolos estão presentes no pacote? Linha 1: Ethernet

Linha 2: ARP

Linha 4: IP

Qual é o MAC do emissor?

* 5c:78:f8:8a:67:67

 Qual é o IP do destinatário?  192.168.3.129

 Qual é a aplicação geradora do pacote?

 ARP

 Qual é o propósito deste pacote?

 Descobrir endereço MAC associado ao IP  O pacote é confidencial?

 O pacote não é confidencial pois ele é enviado em uma rede local e contém informações básicas como endereços MAC e IP.

1. **Apresente uma linha de comandos que lhe permita listar as ligacões TCP efetuadas pelo PC com o endereço IP 192.168.10.12, bem assim como todas as ligacões seguras estabelecidas para o servidor web com o endereço IP 192.168.0.1, constantes de uma captura de rede guardada no ficheiro captura.pcap. Recorra ao tcpdump e filtros do tipo BPF.**

tcpdump -r captura.pcap \(src host 192.168.10.12 and tcp\)

or \(dst host 192.168.0.1 and port 443\)

Tipos de bpf e suas portas

25, 465, 587: SMTP (não cifrado e cifrado).

110, 995: POP3 (não cifrado e cifrado).

143, 993: IMAP (não cifrado e cifrado).

53, 853: DNS (não cifrado e cifrado).