

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP) POLÍCIA FEDERAL

CARGO 4: PERITO CRIMINAL FEDERAL – ÁREA 3: INFORMÁTICA FORENSE

Prova Discursiva

Aplicação: 27/7/2025

PADRÃO DE RESPOSTA DEFINITIVO

A sofisticação dos *malwares* atuais exige do perito o domínio de técnicas e estratégias de evasão, como, por exemplo, *malwares fileless*, que operam inteiramente na memória RAM, evitando gravação em disco e dificultando a detecção por antivírus tradicionais. O polimorfismo altera dinamicamente a estrutura do código, o que produz instâncias diferentes a cada execução. A ofuscação, por sua vez, encobre a verdadeira lógica do programa, o que dificulta tanto a análise humana quanto automatizada, **sendo a criptografia uma das técnicas mais utilizadas e que se adequa ao comportamento de ofuscação**. Em ambientes críticos, como redes industriais SCADA, essas técnicas representam sérias ameaças à segurança nacional.

A atuação do perito nesse contexto exige conhecimento técnico aprofundado, precisão metodológica e sensibilidade jurídica, com vistas à produção de provas digitais robustas e à proteção de sistemas estratégicos da administração pública e do país como um todo.

Ao se deparar com essa situação, o perito deve iniciar sua análise, identificando as principais características do *malware*, com soluções e tipo de ferramentas, como IDA Pro, Ghidra e Radare, que são amplamente utilizadas para interpretar códigos compilados, enquanto *debuggers* (ex.: x64dbg, OllyDbg) são empregados para observar a execução em tempo real e identificar chamadas de sistema, manipulações de memória e desvios lógicos.

Muitas ferramentas atuais possuem componentes de interpretação e *debug* associadas. *Sandboxes* fornecem ambiente controlado para executar o código sem riscos, o que permite observar e registrar todos os comportamentos maliciosos de forma segura. Já a análise em Assembly torna-se imprescindível quando o código apresenta compressão, empacotamento ou ofuscação além de criptografia, muito comum nesse tipo de artefato.

O processo forense envolve o isolamento da amostra, o cálculo de *hash*, para garantir a integridade e a cadeia de custódia, a análise estática com descompiladores, a fim de se obter o código fonte, incluindo, em alguns casos, o código *assembly*, a análise dinâmica com *sandbox* e *debugger*, na qual o artefato é executado em ambiente controlado e seu comportamento é analisado, incluindo *dump* de memória do artefato em execução. Essas etapas permitem reconstruir a lógica do funcionamento do *malware*, mesmo quando protegido por camadas de ofuscação e criptografia, identificar funções maliciosas e extrair evidências para atribuição e responsabilização e possíveis comunicações de rede além de persistência nos sistemas afetados.

QUESITOS AVALIADOS

Quesito 2.1 – Principais técnicas antioforenses que grupos criminosos utilizam na criação de *malwares*

Conceito 0 – Não citou nem explicou nenhuma técnica ou o fez de forma totalmente equivocada.

Conceito 1 – Apenas citou as principais técnicas sem explicá-las.

Conceito 2 – Explicou corretamente apenas uma das seguintes técnicas: polimorfismo, *fileless malware*, criptografia e ofuscação.

Conceito 3 – Explicou corretamente apenas duas das técnicas enumeradas.

Conceito 4 – Explicou corretamente apenas três das técnicas enumeradas.

Conceito 5 – Explicou corretamente as quatro técnicas enumeradas.

Quesito 2.2 – Papel de métodos de análise como *debuggers*, descompiladores, *sandboxes* e análise de código Assembly no exame técnico

Conceito 0 – Não abordou o papel de métodos de análise ou o fez de forma totalmente equivocada.

Conceito 1 – Apenas mencionou que existem métodos de análise, sem indicar seu papel.

Conceito 2 – Mencionou corretamente o papel de métodos de análise, mas sem aplicação ao exame técnico.

Conceito 3 – Mencionou corretamente o papel de métodos de análise.

Quesito 2.3 – Processo de utilização dessas soluções e suas principais funções

Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.

Conceito 1 – Apenas descreveu corretamente um processo de utilização dessas soluções, mas não indicou suas principais funções.

Conceito 2 – Descreveu um processo de utilização dessas soluções e indicou suas principais funções, de forma insuficiente, tendo demonstrado pouco domínio técnico e capacidade de articular conceitos avançados de engenharia reversa.

Conceito 3 – Descreveu corretamente um processo de utilização dessas soluções e indicou suas principais funções, com domínio técnico e capacidade de articular conceitos avançados de engenharia reversa.