VINÍCIUS VIEIRA

PÓS TECH

DEFENSIVE CYBER SECURITY BLUE TEAM OPS

TECH CHALLENGE

FASE 03

CHALLENGE - FORENSICS FUNDAMENTALS

Descreva as respostas para os questionamentos deste Tech Challenge em um relatório detalhado com prints das telas de comando e ferramentas, incluindo explicações.

PROPOSTA

Você é um(a) perito(a) forense em seu primeiro dia de trabalho. Sua unidade foi acionada para cumprir um Mandado de Busca e Apreensão na empresa fictícia ATMOSIGMA LTDA e algumas tarefas serão delegadas a você. Com base no conteúdo desta fase, responda às questões abaixo justificando suas condutas do ponto de vista das boas práticas aplicáveis em cada proposição:

Q1. Ao chegar no local de crime, foi constatada a existência de diversos computadores e notebooks desligados. Os peritos mais experientes te pediram para dar início à cadeia de custódia. Utilizando o modelo disponibilizado pelo NIST (disponível na pasta “Apoio” da Imagem **Chall_Pos_Tech_Ori.dd**), crie um extrato de documento para exemplificar como você faria o registro da aquisição inicial de **até 5 (cinco)** artefatos, explicando na sequência por que a execução correta dessa atividade é importante.

Q2. Um perito sênior começou o processo de criação de uma cópia forense a partir de um dos discos encontrados no local. De posse do artefato original (representado por **Chall_Pos_Tech_Ori.dd**) e das cópias forenses (representadas por **Chall_Pos_Tech_Img1.dd e Chall_Pos_Tech_Img2.dd**), é possível afirmar que as cópias foram realizadas com sucesso? As imagens possuem o mesmo tipo de Filesystem? Justifique suas respostas.

Q3. Antes de prosseguir com os demais discos, o mesmo perito da questão anterior solicitou que um dos drives da maleta fosse esterilizado para acomodar uma nova imagem. Qual(is) comando(s) ou ferramenta(s) você utilizaria para completar essa tarefa? Como você pode garantir que a mídia foi sanitizada adequadamente? Use um pendrive ou uma pequena partição em uma máquina virtual para demonstrar esse procedimento.

Q4. Monte a imagem **Chall_Pos_Tech_Img1.dd** em seu computador e use seu navegador de arquivos para identificar o conteúdo da pasta “Exame”**.** Na sequência, preencha a tabela abaixo, demonstrando como chegou nos resultados encontrados. O que são os tempos M, A e C encontrados?

#	Nome do Arquivo	Extensão	Modification time (mtime)	Access time (atime)	Change time (ctime)
1					
2					
3					
4					
5					

Q5. Analisando o conteúdo da mesma pasta da questão anterior (Exame), é possível afirmar que extensões apresentadas são compatíveis com o conteúdo dos arquivos? Demonstre suas conclusões por meio da linha de comando e pelo uso dos Magical Numbers.

Q6. Alguns dos discos apreendidos são do tipo SSD (solid-state drive). Discorra brevemente sobre os desafios que este tipo de tecnologia traz à Perícia Forense Computacional.

QUESTÃO BÔNUS: O mandado de Busca foi motivado por uma suspeita da Fraude Contábil na ATMOSIGMA. Um dos funcionários registrou alguns dados importantes em uma planilha protegida na pasta “Bonus” da imagem **Chall_Pos_Tech_Img1.dd**, tomando o cuidado de anotar a senha de acesso em um “lugar seguro”. Você consegue acessar esses dados?

OBJETIVOS E PONTUAÇÃO

Questão	Objetivos	Valor
1	Conceituar cadeia de custódia, associar seu correto manuseio à admissibilidade da prova (Daubert Standart) e travar contato com ao menos um dos modelos disponíveis para praticar seu preenchimento.	10%
2	Compreender que as funções hash funcionam como uma impressão digital do arquivo e que os resultados obtidos a partir de diferentes algoritmos devem ser registrados para garantir a integridade da evidência. Adicionalmente, o filesystem também precisa ser identificado e registrado.	15%
3	Compreender o que é sanitização de mídia e demonstrar a sua realização. Adicionalmente, utilizar alguma técnica como o checksum 64bits para garantir que a esterilização foi efetiva.	20%
4	Compreender o processo de exame inicial das evidências, manipulando as imagens adequadamente e extraindo informações preliminares julgadas importantes.	20%
5	Compreender que o perito nunca deve confiar apenas nos nomes dos arquivos e que tal análise é necessária assim como medida de exame preliminar das evidências.	20%
6	Demonstrar a compreensão sobre a limitação da aplicação das técnicas consagradas de perícia post mortem às novas tecnologias.	15%
Bônus	Estimular os alunos a aprofundarem a análise e encontrar soluções ainda não apresentadas no material por conta própria. Os alunos mais avançados serão estimulados pelo desafio e os iniciantes não serão prejudicados, pois não dependem dessa resolução para tirar a nota máxima.	20% extras

IMPORTANTE

Para resolver os desafios das disciplinas, o link de acesso é http://142.93.50.43:8000/challenges.


PDS TECH