Elias Edenis

TECNOLOGIA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E CRIMES DIGITAIS

SIMULADO 04

ESTE SIMULADO FAZ PARTE DO CURSO MINISTRADO PELO PROFESSOR ELIAS EDENIS

COMO FAÇO PARA ADQUIRIR O CURSO?

ACESSE:

https://eliasedenis.com.br/ntaic/index.html

Instagram do Professor:

https://instagram.com/entenda.cibercrimes

QUESTÃO 01 Um Investigador de Polícia está analisando o histórico de recompensas da rede Bitcoin para verificar a alegação de um suspeito de que ele minerou ativos no "período inicial" da rede. Considerando o mecanismo de *Halving*, que reduz a emissão a cada 4 anos, a recompensa concedida aos mineradores por bloco no período de 2016 a 2020 foi de:

A) 50 BTC.

B) 25 BTC.

C) 12,5 BTC.

D) 6,25 BTC.

E) 3,125 BTC.

QUESTÃO 02 Uma equipe de TI da Polícia Civil está reconfigurando o endereçamento lógico de sua rede interna. Ao optar pelo protocolo IPv4, o administrador deve lembrar que o endereçamento é composto por um total de bits específico, enquanto o IPv6 oferece uma expansão significativa. Os tamanhos, em bits, dos endereços IPv4 e IPv6 são, respectivamente:

A) 16 bits e 64 bits.

B) 32 bits e 64 bits.

C) 32 bits e 128 bits.

D) 64 bits e 128 bits.

E) 128 bits e 256 bits.

QUESTÃO 03 Durante o cumprimento de um mandado de busca e apreensão, um perito identifica que os dados de um servidor estão protegidos por criptografia simétrica. Ao elaborar o relatório, ele deve explicar que este modelo é caracterizado por:

A) Utilizar exclusivamente um par de chaves complementares (pública e privada).

B) Ser mais lento que a criptografia assimétrica no processamento de grandes volumes.

C) Utilizar uma única chave para os processos de encriptação e desencriptação.

D) Depender de certificados TLS para validar a chave privada em repouso.

E) Ser utilizado obrigatoriamente apenas em comunicações de e-mail.

QUESTÃO 04 Considere que um analista de rastreamento de criptoativos observa uma transação na blockchain do Bitcoin com o objetivo de identificar o proprietário. Sobre as heurísticas de agrupamento (*clustering*), analise as assertivas abaixo:

I. A técnica de *Common Spending* (Gasto Comum) assume que, se uma transação possui múltiplos endereços de entrada (*inputs*), todos pertencem à mesma pessoa.

II. A identificação do endereço de troco pode ser feita pela precisão numérica, onde a saída com muitas casas decimais costuma ser o troco que volta ao remetente.

III. Um endereço novo que nunca apareceu na rede antes, quando surge como saída, junto com outro que já transacionou, possui alta probabilidade de ser um endereço de troco.

Está(ão) correta(s): A) Apenas I. B) Apenas II. C) Apenas I e III. D) Apenas II e III. E) I, II e III.

QUESTÃO 05 Uma empresa de Santa Catarina sofre um ataque onde o invasor não apenas criptografa os servidores, mas também ameaça vazar dados sensíveis de clientes para forçar o pagamento, usando o medo da empresa de receber multas da LGPD. De acordo com o que você estudou, essa modalidade de ataque é denominada:

A) Sequestro Lógico Simples.

B) Negação de Serviço Distribuída (DDoS).

C) Ransomware, com Dupla Extorsão.

D) Invasão de Dispositivo *Zero Day*.

E) *Defacement* Estrutural.

QUESTÃO 06 Um Agente de Polícia solicita ao provedor de conexão os registros de um suspeito. De acordo com o Marco Civil da Internet (Lei nº 12.965/2014), o prazo mínimo de

guarda de registros de conexão por parte do provedor de conexão e o prazo para o provedor de aplicações de internet são, respectivamente:

A) 6 meses e 1 ano.

B) 1 ano e 6 meses.

C) 1 ano e 1 ano.

D) 2 anos e 1 ano.

E) 5 anos e 2 anos.

QUESTÃO 07 No laboratório de perícia, um técnico utiliza a ferramenta Cellebrite UFED. Ao lidar com um dispositivo Android, ele tenta realizar uma extração física para recuperar arquivos deletados. Para que essa cópia integral de todos os bits da unidade de armazenamento seja bem-sucedida, o técnico necessita de:

A) Acesso de administrador (*root*).

B) Apenas a ativação do modo avião.

C) Acesso exclusivo via API do iTunes.

D) Conexão via protocolo SNMP na porta 161.

E) Uso obrigatório da técnica de *Chip-Off* em aparelhos desligados.

QUESTÃO 08 Um perito criminal está operando um *software* que calcula o "resumo matemático" de uma evidência digital para garantir sua integridade. Ao utilizar o algoritmo SHA-256, ele deve saber que o comprimento desse hash em base hexadecimal é de:

A) 32 caracteres.

B) 64 caracteres.

C) 128 caracteres.

D) 256 caracteres.

E) 512 caracteres.

QUESTÃO 09 Uma delegacia decide implementar o monitoramento automático de fóruns na *Dark Web*. Sobre as ferramentas de raspagem (*scraping*), analise os itens:

I. A biblioteca *Instaloader* é usada para simular navegadores e baixar informações de perfis e *stories* do Instagram.

II. O *BeautifulSoup* (BS4) é uma biblioteca Python focada na leitura e organização de dados extraídos de códigos HTML.

III. O monitoramento automatizado permite que o agente interaja ativamente com criminosos infiltrados em grupos.

Está(ão) correto(s):

A) Apenas I.

B) Apenas III.

C) Apenas I e II.

D) Apenas II e III.

E) I, II e III.

QUESTÃO 10 Ao investigar um crime de interrupção de serviço público (Art. 266, CP), a polícia identifica que o suspeito utilizou uma rede de computadores "zumbis" infectados para sobrecarregar um servidor governamental. Essa infraestrutura e o tipo de ataque são chamados, respectivamente, de:

A) *Phishing* e *Smishing*.

B) *Botnet* e DDoS.

C) *Trojan* e *Backdoor*.

D) *Worm* e *Exploit*.

E) *Keylogger* e *Spyware*.

GABARITO COMENTADO

---

01 – ALTERNATIVA CORRETA: C

- **Por que a C está correta:** No Bitcoin, o *Halving* ocorre a cada 4 anos, reduzindo a recompensa pela metade. O período de 2016 a 2020 corresponde ao segundo Halving, onde a recompensa caiu de 25 BTC para 12,5 BTC.
- **Revisão das incorretas:** A alternativa **A (50 BTC)** refere-se à Era Inicial (2009-2012). A **B (25 BTC)** foi a recompensa do primeiro Halving (2012-2016). A **D (6.25 BTC)** refere-se ao terceiro Halving (2020-2024). A **E (3.125 BTC)** é a recompensa da fase atual, iniciada em 2024.

02 – ALTERNATIVA CORRETA: C

- **Por que a C está correta:** A literalidade técnica define o IPv4 como um endereço de 32 bits (dividido em quatro octetos) e o IPv6 como um endereçamento de 128 bits, permitindo undecilhões de combinações.
- **Revisão das incorretas:** As alternativas **A, B, D e E** trazem valores numéricos incorretos que não correspondem à arquitetura de bits dos protocolos TCP/IP. Lembre-se: IPv4 = 32 bits; IPv6 = 128 bits.

03 – ALTERNATIVA CORRETA: C

- **Por que a C está correta:** Na criptografia simétrica, utiliza-se apenas uma única chave (segredo) para os processos de encriptar e desencriptar a informação.
- **Revisão das incorretas:** A **A** descreve a criptografia *assimétrica* (par de chaves pública/privada). A **B** está invertida; a simétrica é mais *rápida* para grandes volumes. A **D** associa simetria a certificados TLS de forma errônea, pois o TLS usa inicialmente assimetria para trocar a chave simétrica. A **E** impõe uma restrição ("obrigatoriamente") inexistente, já que a simetria é usada em diversos cenários, como dados em repouso.

04 – ALTERNATIVA CORRETA: E

- **Por que a E está correta:** Todas as heurísticas são tecnicamente válidas. **I:** O gasto comum presume que múltiplos *inputs* exigem assinaturas privadas da mesma carteira. **II:** O troco costuma ter precisão numérica inferior (muitas casas decimais) comparado ao valor "redondo" enviado ao destino. **III:** Endereços novos gerados automaticamente pela carteira para receber saldo remanescente são fortes indícios de endereços de troco.

05 – ALTERNATIVA CORRETA: C

- **Por que a C está correta:** A Dupla Extorsão é uma evolução do Ransomware onde, além da criptografia (sequestro), o criminoso ameaça vazar dados sensíveis para causar danos reputacionais e multas da LGPD.
- **Revisão das incorretas:** A **A** ignora a ameaça de vazamento. A **B** foca em indisponibilidade por sobrecarga, não em dados. A **D** refere-se a vulnerabilidades desconhecidas, não ao modelo de extorsão. A **E** trata de pichação de sites, sem sequestro de dados.

06 – ALTERNATIVA CORRETA: B

- **Por que a B está correta:** Conforme o Marco Civil da Internet (MCI), o prazo para Provedores de Conexão (quem dá o acesso) é de 1 ano. Para Provedores de Aplicação (sites/apps), o prazo é de 6 meses.
- **Revisão das incorretas:** As alternativas **A, C, D e E** invertem ou alteram os prazos literais estabelecidos pela Lei 12.965/2014. Grave: Conexão = 1 ano; Aplicação = 6 meses.

07 – ALTERNATIVA CORRETA: A

- **Por que a A está correta:** Para uma extração física em dispositivos Android, que copia bit a bit toda a unidade, é indispensável o acesso administrativo (*root*) para elevar os privilégios da ferramenta UFED.
- **Revisão das incorretas:** A **B** é medida de preservação, não habilita extração física. A **C** refere-se ao ecossistema iOS/Apple. A **D** trata de protocolo de gerência de rede, irrelevante para extração de celular. A **E** afirma ser "obrigatório", mas o Chip-Off é uma técnica de exceção e ineficaz em celulares com criptografia ativa.

08 – ALTERNATIVA CORRETA: B

- **Por que a B está correta:** O algoritmo SHA-256 gera um resultado de 256 bits, que em base hexadecimal (notação comum em perícias) é representado por uma sequência fixa de 64 caracteres.
- **Revisão das incorretas:** A **A (32 caracteres)** refere-se ao hash MD5. As demais (**C, D, E**) trazem comprimentos incorretos para o padrão SHA-256.

09 – ALTERNATIVA CORRETA: C

- **Por que a C está correta: I:** O *Instaloader* é uma biblioteca específica para baixar dados do Instagram. **II:** O *BeautifulSoup* (BS4) é a ferramenta padrão em Python para raspagem e organização de códigos HTML.

- **Revisão da incorreta:** O item **III** está incorreto porque o monitoramento automatizado deve ser neutro (espectador); a interação caracteriza "infiltração", que exige protocolos jurídicos e operacionais distintos.

10 – ALTERNATIVA CORRETA: B

- **Por que a B está correta:** A infraestrutura de computadores "zumbis" infectados é denominada *Botnet*. O ataque que sobrecarrega sistemas via múltiplas requisições dessas botnets é o DDoS (Negação de Serviço Distribuída).
- **Revisão das incorretas: A** e **E** referem-se a roubo de dados e espionagem. **C** e **D** tratam de vetores de infecção e propagação, não do ataque de sobrecarga.

Bons estudos! Este material revisa alguns dos pontos mais críticos do seu edital. Resolva a maior quantidade de questões possíveis em simulados. Adquira o curso completo em https://eliasedenis.com.br/ntaic/index.html