Livro: Segurança de Computadores e teste de invasão - Tradução da 2ª edição norte-americana

Ler o cap. 01 e responder as “Questões de revisão” deste mesmo capítulo.

SUBMETER RESPOSTAS VIA EMAIL

ENDEREÇO: joao.gress@iesgo.edu.br

PRAZO: 17AGO25, 2359h

FORMATO: PDF

Luan Calazans

QUESTIONÁRIO DE FIXAÇÃO 01 - SEGURANÇA DA INFORMAÇÃO

QUESTÃO 01

Resposta:

Chapéu Cinza – mistura o lado ético (ensinar) com práticas duvidosas.

Opera em área moral ambígua.

QUESTÃO 02

Resposta:

Chapéu Branco – usa o conhecimento para proteger redes.

Corrige falhas e fortalece a segurança.

QUESTÃO 03

Resposta:

Chapéu Preto (Hacktivista) – invade sistemas por ideologia.

Acesso não autorizado para fins políticos.

QUESTÃO 04

Resposta:

Chapéu Preto – pratica crimes virtuais.

Rouba e vende cartões de crédito.

QUESTÃO 05

Resposta:

CIOs buscam análises técnicas e realistas.

Investem em defesa avançada, não só perfis de hackers.

QUESTÃO 06

Resposta:

Site desatualizado e não responsivo.

Não atende padrões modernos de usabilidade.

QUESTÃO 07

Resposta:

Phishing/Email Spoofing – falsifica remetente.

Envia e-mails automáticos maliciosos.

QUESTÃO 08

Resposta:

Scanner de vulnerabilidades (Burp, Nikto).

Ataca scripts e sites inseguros.

QUESTÃO 09

Resposta:

Botnet – rede de computadores zumbis.

Usada em ataques DDoS massivos.

QUESTÃO 10

Resposta:

Verdadeiro – hacker ético usa técnicas do cracker.

A diferença está na permissão e no objetivo.

QUESTÃO 11

Resposta:

Falso – firewall protege redes.

Não compromete diretamente sistemas.

QUESTÃO 12

Resposta:

Verdadeiro – ético e cracker usam métodos iguais.

O que muda é ética e legalidade.

QUESTÃO 13

Resposta:

Verdadeiro – SANS oferece GIAC.

Certificação reconhecida mundialmente.

QUESTÃO 14

Resposta:

Verdadeiro – GIAC tem GREM.

Certificação em engenharia reversa.

QUESTÃO 15

Resposta:

Falso – só é legal com autorização.

Sem permissão, é crime (CFAA).

QUESTÃO 16

Resposta:

Script Kiddies – novatos que usam scripts.

Não entendem o impacto real.

QUESTÃO 17

Resposta:

Port Scanning – varredura de portas.

Exemplo: Nmap.

QUESTÃO 18

Resposta:

Desenvolvedores de Exploits – criam códigos.

Exploram falhas de forma autônoma.

QUESTÃO 19

Resposta:

Programa/Script – instruções sequenciais.

Executadas pelo computador.

QUESTÃO 20

Resposta:

Hacker Ético/Pentester – contratado por empresas.

Pensa como invasor para testar defesas.