ATIVIDADE – PRÁTICA ENADE: Avaliação de Segurança com Base na NIST SP 800-115

Disciplina: Cibersegurança Ofensiva | **Referência**: NIST SP 800-115

Objetivo: Desenvolver a habilidade de leitura crítica, associação conceitual e aplicação prática da norma em contexto realista.

ALUNO: LUAN BRITO SOUSA CALAZANS 6°SEM

QUESTÃO 01

Texto-base:

A NIST SP 800-115 define um framework para avaliação técnica de segurança da informação em sistemas de tecnologia. Esse framework inclui fases distintas com objetivos bem estabelecidos que conduzem à coleta e análise de informações relevantes.

Enunciado:

Qual das alternativas representa corretamente as três fases principais de uma avaliação de segurança conforme a SP 800-115?

C) Planejamento, Avaliação, Pós-avaliação

QUESTÃO 02

Texto-base:

A SP 800-115 classifica as avaliações de segurança com base na **profundidade** (light-touch ou in-depth) e na **técnica aplicada**, como testes de penetração, varreduras de vulnerabilidades e entrevistas.

Enunciado:

Durante uma simulação controlada, um time de segurança tenta comprometer o ambiente alvo sem acesso prévio às credenciais ou à arquitetura da rede. O objetivo é avaliar se as defesas atuais podem detectar e responder à intrusão.

Essa situação é um exemplo de:

E) Teste de penetração black-box

QUESTÃO 03

Texto-base:

Segundo a NIST SP 800-115, um bom planejamento é essencial para garantir que os testes sejam realizados de forma ética, controlada e com escopo definido, evitando efeitos colaterais como indisponibilidade de serviços.

Enunciado:

I – O planejamento de uma avaliação de segurança inclui definir escopo, regras de engajamento e acordos formais de autorização. PORQUE

II – A execução sem planejamento formal pode violar leis, comprometer sistemas e deslegitimar os resultados obtidos.

A) As asserções I e II são verdadeiras, e a II justifica a I.

QUESTÃO 04

Texto-base:

As varreduras de vulnerabilidades são ferramentas essenciais no processo de avaliação de segurança e têm como objetivo identificar falhas conhecidas em sistemas e serviços expostos.

Enunciado:

Qual das opções melhor descreve o papel da varredura de vulnerabilidades, segundo a NIST SP 800-115?

D) Detectar e relatar configurações inseguras e falhas conhecidas

QUESTÃO 05

Texto-base:

A fase de pós-avaliação, conforme a SP 800-115, inclui análise dos resultados, documentação técnica, comunicação clara e

recomendações para mitigação.

Enunciado:

Com base na NIST SP 800-115, explique a importância da fase de pós-avaliação em um processo completo de teste de segurança. Em sua resposta, destaque os elementos que devem estar presentes no
relatório final e a sua relevância para o ciclo de vida da segurança da informação.

**R: A pós avalliação é a parte mais importante ,por que é com ela que na teoria vc identifica o erro e para trata-lo de maneira pratica
, é importante ter o passo a passo de cada movimento feito no sistema ate chegar aquela vulnerabilidade ,
existem ferramentas boas e práticas que entregam um visual legal a pessoa que vai tratar das falhas
como o github , obsidian etc...
isso impacta de forma positiva em varios aspectos desde a forma pratica , facilidade para resolver o problema e dai gerar outro ou adicionar no relatorio o tratamento de erro que foi usado e o passo a passo,
facilita tambem porque uma pessoa que nao pode conhecer sobre as falhas ela ve o relatorio e dai ela consegue ter uma visão de fora sendo o chefe da empresa etc...**

QUESTÃO 06

Texto-base:

A NIST SP 800-115 classifica os testes de segurança conforme os **tipos de técnica aplicada**, podendo ser: **testing (ativo)**, **examination (passivo)** e **interview (subjetivo)**.

Enunciado:

Assinale a alternativa que apresenta corretamente os três tipos de técnicas de avaliação descritas na SP 800-115:

C) Interview, Testing, Examination

QUESTÃO 07

Texto-base:

A SP 800-115 detalha que o nível de intrusividade e risco de um teste depende da técnica empregada e do grau de acesso concedido aos avaliadores.

Enunciado:

Um avaliador propõe realizar um teste de segurança com acesso administrativo parcial, em produção, com execução de scripts automatizados de exploit. Segundo a SP 800-115, essa situação exige:

C) Assinatura formal de Termo de Consentimento e definição rígida das Regras de Engajamento

QUESTÃO 08

Texto-base:

A SP 800-115 diferencia técnicas que coletam informações sem interação direta com os ativos de rede daquelas que simulam ataques reais com potencial de impacto.

Enunciado:

Analise as diferenças entre "examination" e "testing" conforme definido na NIST SP 800-115. Em sua resposta, cite exemplos práticos de ferramentas, riscos associados e aplicabilidade em

ambientes produtivos.

R: examination voce apenas examina o servidor ou dispositvo de maneira passiva
com programas que nao fazem barulho , apenas escutam o trafego da rede wire shark entre outros , e vc tbm pode fazer analise de conteudo que esta exposto de maneira facil explicita como pdf's entre outros

o testing´= é quando vc testa de maneira ativa usando ferramentas que fazem barulho
que deixam rastros nos arquivos de log , mas dai vc teria permissao pra ta fazendo isso
vc abusa das falhas que estão lá como fazer um brute force de login , ou tentar exploitar
serviço ativo.

QUESTÃO 09

Texto-base:

O planejamento da avaliação é um passo crítico para mitigar riscos legais, operacionais e de reputação.

Enunciado:

Segundo a SP 800-115, qual item NÃO é um componente necessário na fase de planejamento?

C) Tempo estimado de resposta à mitigação

QUESTÃO 10

Texto-base:

A condução de entrevistas é uma técnica útil para coletar informações qualitativas sobre práticas de segurança e conscientização dos usuários.

Enunciado:

I – A técnica de entrevista é eficaz para identificar discrepâncias entre políticas escritas e práticas reais dos usuários. PORQUE

II – A entrevista permite avaliar a superfície de ataque com base em testes automatizados de serviços de rede.

C) A asserção I é verdadeira, e a II é falsa.