GLOSSÁRIO DE TERMOS

Versão 3.1br

Advanced Level
Security Test

Os termos deste documento são complementares ao Glossário de Termos – Núcleo Base para o exame de certificação CTAL-ST Security Test.

Tradução realizada pela WG Tradução do BSTQB baseada na versão 3.1 do *ISTQB Glossary of Testing Terms*

acurácia
accuracy

Capacidade do produto de software em fornecer os resultados ou efeitos, corretos ou acordado com o grau necessário de precisão.
Ver também: funcionalidade
Referência: ISO 9126

ambiente operacional
operational environment

Produtos de software ou hardware instalados nos locais de trabalho, residência dos usuários ou consumidores, onde o componente ou sistema sendo testado será utilizado. O software pode incluir sistemas operacionais, sistemas de gerenciamento de banco de dados e outros aplicativos.

ameaça interna
insider threat

Ameaça de segurança proveniente de dentro da organização, muitas vezes por um usuário do sistema autorizado.

análise de causa-raiz
root cause analysis

Técnica de análise que visa identificar as causas dos defeitos. Ao orientar as medidas corretivas para as causas raiz, espera-se que a probabilidade de reincidência do defeito seja minimizada.

anti-malware
anti-malware

Software usado para detectar e inibir malware.
Ver também: malware

API
API

Acrônimo para Application Programming Interface (Interface de Programação de Aplicativos)

arquiteto de teste
test architect

(1) Pessoa que fornece orientação e direção estratégica para uma organização de teste e para o seu relacionamento com outras disciplinas. (2) Pessoa que define a maneira como o teste é estruturado para um determinado sistema, incluindo tópicos como ferramentas de teste e gerenciamento de dados de teste.

atacante
attacker

Uma pessoa ou processo que tenta acessar dados, funções ou outras áreas restritas de um sistema sem autorização, com intenção potencialmente maliciosa.
Ver também: hacker

ataque de segurança
security attack

Tentativa de obter acesso não autorizado a um sistema, componente, recursos, informações ou uma tentativa de comprometer a integridade de um sistema.
Referência: pós NIST.IR.7298

auditoria de segurança
security audit

Auditoria que avalia os processos e a infra-estrutura de segurança de uma organização.

baseline
baseline

Especificação ou produto de software formalmente revisto ou acordado que servirá como base para futuros desenvolvimentos, pondendo ser alterado apenas por meio de um processo formal de controle de mudança
Referência: pós IEEE-610

botnet
botnet

Uma rede de computadores comprometidos, chamados bots ou robôs, que é controlada por terceiros e usada para transmitir malware ou spam, ou para lançar ataques.

caso de uso de abuso
abuse case

Um caso de uso no qual alguns atores com intenção maliciosa estão causando danos ao sistema ou a outros atores.
Ver também: caso de uso

CLI
CLI

Acrônimo para Command-Line Interface

cobertura de desvio
branch coverage

Porcentagem de desvios no código exercitado por uma suíte de teste. Isso significa que 100% de cobertura de desvio implica em 100% de cobertura de decisão e também em 100% de cobertura de sentença.

coleta de contas
account harvesting

Processo de obtenção de listas de endereços de e-mail para uso de envio de mensagens em massa.

complexidade ciclomática
cyclomatic complexity

O número máximo de caminhos lineares, independentes, através de um programa. A complexidade ciclomática pode ser calculada como: L - N + 2P, onde: L é o número de arestas/links em um gráfico, N é o número de nós em um gráfico e P é o número de partes desconectadas do gráfico (por exemplo, um gráfico chamado ou sub-rotina).
Sinonimos: número ciclomático
Referência: pós McCabe

computação forense
computer forensics

A prática de determinar como um ataque de segurança teve êxito e avaliar os danos causados.

cross-site scripting (XSS)
cross-site scripting (XSS)

Uma vulnerabilidade que permite aos atacantes injetar código malicioso em um site.
Referência: NIST.IR.7298

denial of service (DOS)
denial of service (DOS)

Um ataque de segurança que se destina a sobrecarregar o sistema com solicitações de tal forma que solicitações legítimas não possam ser atendidas.

efeito de monitoração
probe effect

Efeito causado no componente ou sistema pelo instrumento de medição quando o componente ou sistema está sendo medido, por exemplo, por uma ferramenta de teste de desempenho ou por um monitor. Por exemplo, o desempenho poderá ser um pouco pior quando as ferramentas de teste de desempenho forem utilizadas.

efetividade
effectiveness

Capacidade de produzir um resultado desejado.
Ver também: eficiência

encriptação
encryption

Processo de codificação de informações de modo que somente as partes autorizadas possam recuperar as informações originais, geralmente por meio de uma chave de desencriptação específica ou processo.

endurecimento do sistema
system hardening

Processo passo-a-passo de reduzir as vulnerabilidades de segurança de um sistema, aplicando uma política de segurança e diferentes camadas de proteção.

engenharia social
social engineering

Tentativa de enganar alguém para que revele informações (por exemplo, uma senha) que podem ser usadas para atacar sistemas ou redes
Referência: NIST.IR.7298

entendibilidade
understandability

Capacidade que um produto de software tem de possibilitar ao usuário entender se ele é adequado para uso, e como pode ser utilizado em determinadas tarefas e condições de uso.
Ver também: usabilidade
Referência: ISO 9126

escalabilidade
scalability

Capacidade que um produto de software tem para sofrer um upgrade ou para acomodar aumento de cargas.
Referência: pós Gerrard

estouro de buffer
buffer overflow

Falha no acesso de memória, devido ao processo de armazenamento de dados ultrapassar os limites fixos do tamanho da área de armazenamento temporário, resultando em estouro da área de memória adjacente ou levantamento de excessão.
Ver também: buffer

firewall
firewall

Componente ou conjunto de componentes que controla o tráfego de entrada e saída da rede com base em regras de segurança predeterminadas.

garantia da informação
information assurance

Medidas que protegem e defendem os sistemas de informação assegurando a sua disponibilidade, integridade, autenticação, confidencialidade. Estas medidas incluem o restabelecimento de sistemas de informação através da incorporação de capacidades de proteção, deteção e reação.
Referência: NIST.IR.7298

gerenciamento de mudança
change management

(1) abordagem estruturada de transição de indivíduos, equipes e organizações a partir de um estado atual para um estado futuro desejado. (2) forma controlada para efetuar uma mudança, ou uma proposta de mudança, para um produto ou serviço.
Ver também: gerenciamento de configuração

gráfico do fluxo de controle
control flow graph

Representação abstrata de todas as possíveis sequências de eventos (caminhos) na execução de um componente ou sistema.

GUI
GUI

Acrônimo para Graphical User Interface

hacker
hacker

Pessoa ou organização que está ativamente envolvida em ataques de segurança, geralmente com intenção maliciosa.
Ver também: ataque

hacker ético
ethical hacker

Testador de segurança usando técnicas hacker.

hashing
hashing

Transformação de uma sequência de caracteres de comprimento variável em um valor ou chave de comprimento fixo geralmente menor. Os valores hash, ou hashes, são comumente usados em pesquisas de tabela ou banco de dados. As funções criptografadas de hash são usadas para proteger dados.

impacto de risco
risk impact

O dano que será causado caso o risco se tornar um resultado real ou evento.
Sinonimos: impacto

indicador de desempenho
performance indicator

Métrica de nível alto de eficácia e/ou eficiência utilizada para guiar e controlar o desenvolvimento progressivo, por exemplo, deslizes no acompanhamento da linha do tempo do projeto no desenvolvimento de software.
Sinonimos: indicados chave de performance
Referência: CMMI

malware
malware

Software que se destina a prejudicar um sistema ou seus componentes.

mascaramento de dados
data obfuscation

Transformação de dados que torna difícil para um ser humano reconhecer os dados originais.

modelo de ciclo de vida
lifecycle model

Particionamento da vida de um produto ou projeto em fases.
Ver também: ciclo de vida do software
Referência: CMMI

painel de controle
dashboard

Representação de medições dinâmicas de desempenho operacional para algumas organizações ou atividades, usando métricas representada por metáforas visuais, como "marcadores", "contadores" e outros dispositivos semelhantes às do painel de um automóvel, de modo que os efeitos de eventos ou atividades podem ser facilmente entendidos e relacionados com os objetivos operacionais.
Ver também: painel de controle corporativo, scorecard
Sinonimos: dashboard

pharming
pharming

Ataque de segurança destinado a direcionar o tráfego de um site para um site fraudulento sem o conhecimento ou consentimento do usuário.

phishing
phishing

Tentativa de adquirir informações pessoais ou sensíveis mascarando-se como uma entidade confiável em uma comunicação eletrônica.

política de segurança
security policy

Documento de alto nível que descreve os princípios, a abordagem e os principais objetivos da organização em matéria de segurança.

privacidade do dado
data privacy

A protecção de informações de identificação pessoal ou de informações sensíveis de divulgação indesejada.

procedimento de segurança
security procedure

Conjunto de ações necessárias para implementar a política de segurança e as etapas a serem tomadas em resposta a um incidente de segurança.

quebra de senha
password cracking

Ataque de segurança que recupera senhas secretas armazenadas em um sistema de computador ou transmitidas através de uma rede.
Referência: pós NIST.IR.7298

reconhecimento
reconnaissance

Exploração de uma área alvo com o objetivo de obter informações que podem ser úteis para um ataque.

relatório de defeito
defect report

Documento que relata qualquer falha em um componente ou sistema que possa fazer com este componente ou sistema deixe de desempenhar sua função requisitada.
Sinônimos: relatório de erro, relatório de problema
Referência: pós IEEE-829

salting
salting

Técnica criptográfica que adiciona dados aleatórios (sal) aos dados do usuário antes do hash.

script kiddie
script kiddie

Pessoa que executa ataques de segurança que foram criados por outros hackers em vez de criar os próprios.
Ver também: hacker

segurança da informação
information security

Proteção dos sistemas de informação contra o acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados a fim de proporcionar confidencialidade, integridade e disponibilidade.
Sinonimos: cybersecurity
Referência: NIST.IR.7298

sensibilização de caminho
path sensitizing

Escolha de um conjunto de valores de entrada para forçar a execução de um dado caminho.

sistema de detecção de intruso (IDS)
intrusion detection system (IDS)

Um sistema que monitora as atividades nas 7 camadas do modelo OSI da rede ao nível da aplicação, para detectar violações da política de segurança.
Ver também: varredura de malware

SQL injection
SQL injection

Ataque de segurança inserindo instruções SQL mal-intencionadas em um campo de entrada para execução.

teste baseado em ataque
attack-based testing

Uma técnica de teste baseada na experiência que usa ataques de software para induzir falhas, principalmente falhas relacionadas à segurança.
Ver também: ataque de falha

teste baseado no modelo (MBT)
model-based testing (MBT)

Testes baseados ou envolvendo modelos.

teste de caminho
path testing

Técnica de modelagem de teste caixa-branca na qual os casos de teste são modelados para executar caminhos.

teste de CLI
CLI testing

Testes realizados enviando comandos para o software em teste usando uma interface de linha de comando dedicado.

teste de penetração
penetration testing

Técnica de teste com o objetivo de explorar vulnerabilidades de segurança (conhecidas ou desconhecidas) para obter acesso não autorizado.

teste de segurança
safety testing

Teste que determina a segurança de um produto de software.

teste fuzz
fuzz testing

Técnica de teste de software usada para descobrir vulnerabilidades de segurança introduzindo quantidades maciças de dados aleatórios, para o componente ou sistema.
Sinonimos: fuzzing

varredura de malware
malware scanning

Análise estática com o objetivo de detectar e remover códigos maliciosos recebidos em uma interface.
Ver também: sistema de detecção de intruso

varrredura de vulnerabilidades
vulnerability scanner

Analisador estático que é usado para detectar vulnerabilidades de segurança específicas no código.

vetor de ataque
attack vector

Um caminho ou meio pelo qual um intruso pode obter acesso a um sistema para fins maliciosos.

vulnerabilidade de segurança
security vulnerability

Fraqueza no sistema que poderia permitir um ataque de segurança bem-sucedido.

zona de rede
network zone

Uma sub-rede com um nível de confiança definido. Por exemplo, a Internet ou uma zona pública seria considerada não confiável.

zona desmilitarizada (DMZ)
demilitarized zone (DMZ)

Subrede física ou lógica que contém e expõe os serviços externos voltados para uma rede não confiável, comumente a Internet.
Ver também: zona de rede