PEN TEST by PenTestMe.com.br

PenTestMe.com.br
pen test, vulns scan & ISO 27002 audit

Agente: FreeBSD Brasil LTDA & DC Labs
Telefone: PABX: (31) 3516-0800
FAX: (31) 3516-0801
Site: http://www.PenTestMe.com.br

Penetration Test ou Teste de Invasão de Segurança, é um método para avaliar a segurança de um sistema computacional ou de uma rede, através da reprodução efetiva de um ataque realizado por um indivíduo mal intencionado. O teste permite que as organizações identifiquem e entendam os pontos mais frágeis de sua infra-estrutura ou sistemas de T.I. e planejem correções ou mitigações.

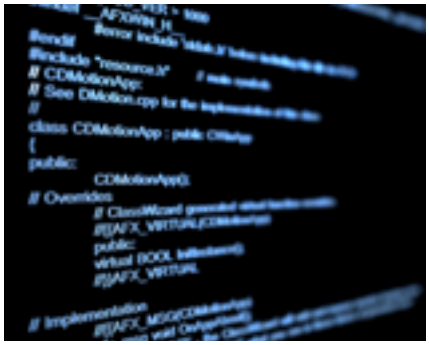
Pen Test & Validação de Segurança

A prática de Teste de Invasão (Pen Test) atende requisitos de conformidade com PCI-DSS, ISO 27002, melhores práticas e *frameworks* de gestão de T.I. e oferece respostas reais as dúvidas levantadas pelo processo da Avaliação de Vulnerabilidade. É um componente de grande valor para a compreensão técnica do processo de Validação de Segurança de T.I. Na prática além de conformidade normativa, melhores práticas, obrigações contratuais ou ainda que motivado pelo risco avaliado do seu negócio, um Pen Test executado pela equipe PenTestMe.com.br te dará uma visão estratégica valiosa: a visão das possíveis falhas que podem ser usadas para prejudicar seu negócio. A visão de um risco que pode ser mapeado pelo seu concorrente direto ou simplesmente qualquer outro indivíduo mal intencionado, e, que portanto, você precisa conhecer primeiro, e conhecer em detalhes.

A iniciativa PenTestMe.com.br é composta por experientes profissionais, com mais de uma década de atuação na área de segurança da informação, atendendo e apoiando empresas privadas e governos a conhecer e melhorar a segurança de seus ambientes. Nossa proposta é oferecer uma forma rápida, direta e efetiva de Pen Test. Num formato confiável, previsível e prático, a um custo amigável para a iniciativa privada e também para governos - abaixo do limite da Lei 8.666/93.

Resultados Esperados do Pen Test

- Relatório de vulnerabilidade;
- Mapas de risco;
- Impacto classificado do risco;
- Criticidade do dano;
- Mitigação para o risco;
- Agravante adicional ao risco;
- Probabilidade de exploração;
- Origem do risco (humana, jurídica, etc);
- Descrição detalhada do risco;
- Pilares NBR ISO/IEC 27002 afetados;
- Pilares TCSEC/DoD afetados;
- Metodologia Mehari;
- Melhores práticas OSSTMM, OWASP;
- Melhores práticas NIST SP 800-115;
- Varredura de vulnerabilidade;
- Target survey;



Desmistificando Pen Test

Um Pen Test é um método de avaliação da segurança de um sistema computacional ou uma rede, através da realização efetiva de um ataque, sob circunstâncias controladas. Esse ataque é realizado por uma equipe autorizada, mas reproduz na prática as ações de um indivíduo mal intencionado. É como colocar um cracker (*hacker* do mal, um quebrador) de fato, com autorização para testar seu ambiente. É uma prática de contra-inteligência: o agente de ameaça é seu contratado, e vai praticar os atos de destruição, invasão, evasão, adulteração ou comprometimento da sua infra-estrutura ou aplicação, dentro de um escopo autorizado e controlado. O Pen Test comprova e valida a eficácia de suas proteções ou legitimidade dos riscos e vulnerabilidades, tanto conhecidas como não mapeadas. A equipe PenTestMe.com.br vai validar o impacto da invasão, apresentar detalhes dos problemas encontrados e propor planos e estratégias de mitigação ou correção das falhas, respaldando seu negócio meio e fim.

Blackbox & Whitebox

Um teste do tipo Blackbox, também conhecido como Pen Test Externo, as vezes chamado de *Ethical Hacking* é na prática, algo mais próximo a um *Ethical Cracking*, onde a metodologia e taxinomia do teste é similar a abordagem de um *cracker* mal intencionado. A maneira de conseguir informações, as estratégias de varredura, *survey* e *numbering* do alvo, são as mesmas, e os resultados esperados também. Já, em um teste Whitebox - Pen Test Interno - o vetor de ameaça reproduzido é de um funcionário da própria organização, um convidado ou algum parceiro mais próximo, com acesso diferenciado, sob alguns aspectos, mais privilegiado.

Cego e não-cego

A equipe PenTestMe.com.br, em um teste cego, não tem acesso válido aos sistemas. Mas no teste não-cego, credenciais como usuário e senha de sistemas, websites, portais e servidores são conhecidos. O teste tenta realizar ações além das previstas, testando os limites da autenticação e autorização implementados no ambiente.

Benefícios para a Organização

A redução da exposição ao risco. A proteção da reputação e imagem da organização. Como benefício direto, a proteção da informação, incluindo a validação das medidas existentes de segurança, o conhecimento dos vetores de ataque e uma estratégia para melhoria das defesas. Complementam ainda a elevação das garantias legais e regulatórias, além de atender requisitos PCI-DSS, ISO 27002, NIST, DISA, ITIL, CobIT entre outros que prevêem testes periódicos de segurança como estratégia de gestão eficiente de T.I.

Escopo Previsível de Pen Test e Custo

O valor do Pen Test é imprevisível. Mas o custo por teste é acessível. Cada teste da equipe PenTestMe.com.br tem um escopo bem definido e delimitado:

★ 1 aplicação web*;
★ ou 1 perímetro de rede*;
★ ou 1 servidor*;

* até outros 2 servidores, serviços ou sistemas de apoio são esperados (como servidores DNS, roteadores, firewall ou banco de dados)

A EQUIPE PenTestMe.com.br é composta por profissionais com mais de uma década de experiência na área de segurança. Com formação *Lato Sensu* e MBA em Segurança da Informação; certificados CISSP, Security+, CISA, RHCE, BSDA, LPI, Auditor Leader, Ethical Hacking, Cisco, Juniper, Solaris, FreeBSD, Linux, Windows, garantindo não só experiência em Seg Info, como em tecnologia de forma ampla. A equipe é composta por profissionais da FreeBSD Brasil LTDA - especialistas em *Open Source* BSD e Apple - e DCLabs, conhecido grupo de Security Research com dezenas de *advisories* e ferramentas publicados.