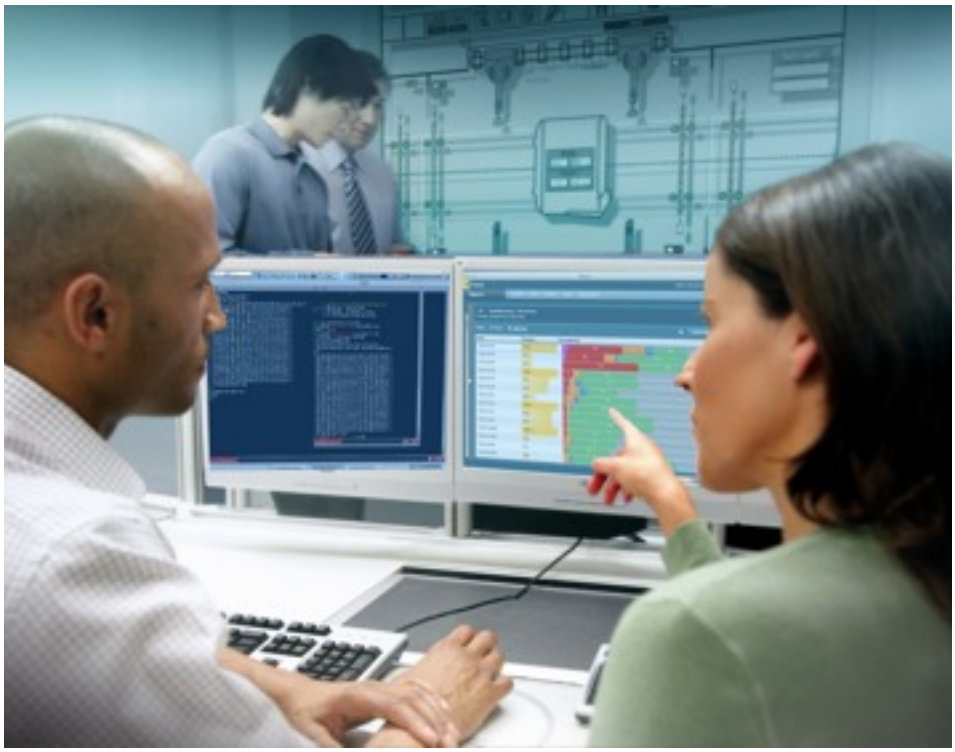
PCI-DSS PEN TEST by PenTestMe.com.br

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



A prática de Teste de Invasão (Pen Test) quando focada em conformidade com o PCI-DSS, respalda-se no requisito 11.3, que por sua vez complementa o 11.2 com foco mais específico: a tentativa efetiva de explorar vulnerabilidades afim de obter acesso não autorizado aos dados, ou qualquer outra atividade maliciosa que comprometa essa informação. O foco primário é a Confidencialidade.

PCI Security Standards

Pen Test para conformidade PCI-DSS

O escopo do Pen Test com foco em conformidade com requisitos PCI são dois: o perímetro de rede e também as camadas de aplicações. Cada qual desses alvos devem testar todos os controles e processos de segurança em duas variações, com a ameaça vindo de fora para dentro (blackbox) e ameaça interna (incluindo acesso autorizado - whitebox).

Não é necessário ser um QSA ou ASV formal a realizar o Pen Test para conformidade PCI, mas a aprovação e validação do teste deve acompanhar detalhes das falhas encontradas, evidências claras de exploração efetiva, mitigação clara e direta, priorização de ações, que respaldarão um novo Pen Test no mesmo ambiente após corrigido.

A metodologia da equipe PenTestMe.com.br adequa-se completamente aos requisitos do PCI-DSS, tanto os ítens entregáveis - são mapas de riscos e relatórios individuais para testes de perímetro de rede, testes de aplicações, discriminação de falhas TOP10 OWASP e varredura de vulnerabilidades - quanto método e processo: os testes são conduzidos em janela de tempo controlada, por profissionais capacitados, certificados e experientes. As evidências são claras e repetitíveis; o foco é a Confidencialidade.

Além da Confidencialidade e Sigilo

O suplemento ao requisito 11.3 do PCI-DSS deixa claro que o foco do PenTest é Confidencialidade e Sigilo da informação. Indica inclusive que testes de negação de serviço devem não precisam constar em relatório. Mas nós os negligenciaremos, complementamos os relatórios de Confidencialidade com ameaças a Disponibilidade e Integridade da informação, mas entregamos em Mapas de Riscos e Seções de Relatório em separado, para que você decida o que anexar ou não à documentação para seu processo de Auditoria PCI-DSS.

O reteste das falhas encontradas para validação de mitigação ou compensação é previsto.

Metodologia de Pen Test para PCI

A metodologia atual, utilizada pela equipe PenTestMe.com.br para execução dos testes é fundada nas melhores práticas do NIST - em especial a SP 800-115 - OSSTMM da Isecom e Guia de Testes OWASP. A metodologia de projeto fundada na Mehari. Em ambos os casos, projeto e execução, nossos métodos, projetos e entregáveis atendem com sobras os requisitos PCI-DSS.

Na fase de preparação, os pontos previamente mapeados serão os locais e forma de armazenamento dos dados críticos - confidenciais - a serem preservados - os dados do portador do cartão (*hardholder data*), incluindo bancos de dados, bases LDAP e dispositivos de retenção desses dados. O diagrama de rede, pre-requisito do item 1.1.2 do PCI-DSS, é imperativo, e o resultado da última auditoria PCI caso exista, desejável. Demais requisitos como resultados prévios de PenTests ou varreduras de vulnerabilidades são opcionais e avaliados no Termo de Abertura do Projeto - TAP.

Foco na Confidencialidade

Para conformidade PCI-DSS *data leak* e outros riscos à Confidencialidade, incluindo acesso não autorizado de usuários válidos (autenticados) ou usuários diversos (externos) são o principal ponto a ser testado, bem como as possíveis formas de *bypass* dos controles e processos que asseguram essa informação.

Dessa forma estendemos nossos testes também a eventos simples, tentando determinar de que forma uma falha técnica como XSS pode se tornar uma armadilha, usada como vetor de exploração de engenharia social ou para *phishing*.

Além de checklists e Auditoria PCI

Pen Test é assunto sério e técnico. Apenas o bom entendimento e domínio da especificação PCI-DSS não bastam para executar um Teste de Penetração efetivo. Nossa equipe atua como CSO em sistemas bancários, são técnicos, são Security Researchers, são Security Specialists, e Arquitetos de Segurança incluindo Firewall, BGP, IDS/IPS, WAF, e são certificados; possuem boa capacidade de avaliação e julgamento técnico e principalmente boa capacidade de definir medidas compensatórias rasoáveis, ao invés de simplesmente recomendar o óbvio - e caro - quando o nível do risco simplesmente não paga o investimento para sua mitigação.

Clientes certificados PCI-DSS

Nossos testes de penetração da PCI-DSS já foram utilizados para completar com sucesso o processo de validação e certificação PCI de bancos, empresas de crédito, construtoras e seguradoras.

Entregáveis Previsíveis

Termo de Abertura de Projeto (Pré):
- Escopo e contra-escopo; Missão;
- Objetivo, Metodologia; Cronograma;
- Stakeholders e demais envolvidos;

Resultados do Pen Test:
- Mapas de Riscos Categorizados;
- Relatórios de Vulerabilidades;
- Relatórios de Penetrações;
- Relatórios de Conformidade e DoS;
- Itens encontrados contendo:
- Nome, Descrição, Mitigação, Origem;
- Evidência, Impacto, Criticidade;
- Agravante; Origem do Risco;

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 geral. 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.