ESET CYBERSOC

ETHICAL HACKING

Serviços de EH confiáveis para manter os sistemas corporativos seguros

Mobile Penetration Test

Mobile Penetration Test

Um Mobile Penetration Test é um conjunto de técnicas utilizadas para avaliar a segurança dos recursos e ativos da organização desde o ponto de vista da matéria de segurança, orientado especificamente para aplicativos móveis.

Esse conjunto de técnicas não apenas identifica as vulnerabilidades existentes na infraestrutura da empresa, mas também executa a análise com maior profundidade. Específicamente, busca-se além da identificação, a exploração das vulnerabilidades e, dessa maneira, observa-se o impacto real sobre a organização.

Este tipo de serviço pode ser executado tanto a partir de um ponto de vista interno como externo da organização. No primeiro caso, busca-se identificar e explorar as vulnerabilidades que sejam visíveis num cenário com acesso aos recursos e ativos da organização, enquanto no segundo, é realizada a avaliação a partir do ponto de vista de um atacante externo sem nenhum tipo de informação adicional.

Objetivos principais

- ✓ Obter uma fotografia do estado da segurança da organização, por meio do aplicativo móvel em um momento determinado.
- ✓ Visualizar sua empresa a partir do ponto de vista do atacante, localizando fraquezas, vulnerabilidades e pontos de acesso não autorizados, antes que os atacantes o façam.
- ✓ Comprovar o verdadeiro impacto das vulnerabilidades em seu ambiente particular (dispositivo) ou além do ambiente.
- ✓ Comprovar se o nível de proteção existente condiz com a política de segurança estabelecida pela organização.
- ✓ Comprovar a efetividade de suas medidas de proteção, políticas e processos de detecção de intrusos e resposta a incidentes.

Por que realizar um Mobile Penetration Test?

- ✓ Para conhecer o estado da segurança dos aplicativos móveis de uma organização (especialmente se nunca foi realizada uma auditoria dessas características).
- ✓ Para estabelecer um ponto de partida para começar a gerir a segurança da organização.
- ✓ Para constituir um ciclo de revisão e melhoria para a segurança.

As etapas associadas a este serviço são:

- ✓ Reconhecimento
- ✓ Análise e detecção de vulnerabilidades
- ✓ Exploração de vulnerabilidades
- ✓ Montagem e apresentação de relatórios

Relatórios

Neste serviço, são gerados 2 entregáveis ou relatórios que ajudam e orientam o cliente no processo de correção de vulnerabilidades.

O primeiro deles, o **relatório executivo**, descreve o nível de risco da empresa sem entrar em detalhes técnicos, evidenciando os problemas por meio de conceitos claros e gráficos.

O segundo relatório, o **relatório técnico**, direcionado para a área técnica da empresa, visa ajudar a equipe de TI a solucionar os problemas detectados.

Neste relatório, são mostradas todas as evidências dos testes executados de tal forma que todas as tarefas sejam escaláveis e transparentes para o cliente.

O relatório está baseado na metodologia de análise do OWASP TOP TEN 2014 e 2016, onde OWASP Top 10 é um documento dos dez riscos de segurança mais importantes em aplicativos web e móveis de acordo com a organização OWASP (em inglês, Open Web Application Security Project; em português, Projeto Aberto de Segurança em Aplicações Web) esta lista é publicada e atualizada a cada três anos por essa organização.


ESET CYBERSOC