PenTest Profissional

Por Afonso Coutinho


I'll show you the
true meaning of cool...

O que é PenTest?

Pentest, **Teste de Invasão** ou Teste de Intrusão é um conjunto de ataques cibernéticos **autorizados**, para descobrir **vulnerabilidades** de um **sistema de informação**.

Todas as vulnerabilidades são exploradas de forma cuidadosa, informando o **Cliente** sobre cada exploração.

É necessário?

É necessário?

- Relatar o nível de segurança atual da empresa
- Identificar falhas de sistemas e processos
- Descobrir a quantidade e o nível da sensibilidade de informações que podem ser perdidas em um ataque

É necessário?!

- **390k** novos malwares por **dia** (AV-TEST)

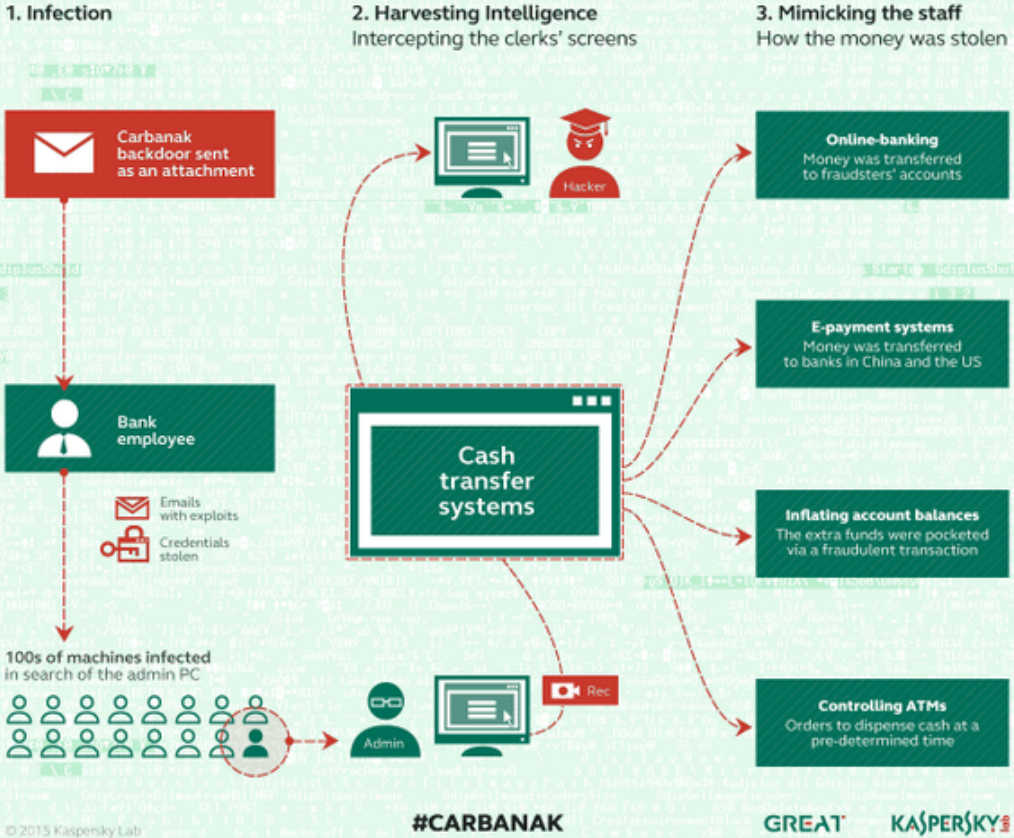
- **50%+** das empresas do mundo perderam **dinheiro** por conta de ataques **cibernéticos**.

É necessário!

- Carbanak - Bancos de 30 países sofreram o ataque, incluindo o Brasil. Mais de 1 bilhão de dólares roubados.
- Sony - Perdeu reputação depois do vazamento de dados.
- HSBC Turquia - 2.7 milhões de cartões de créditos roubados.

How the Carbanak cybergang stole $1bn

A targeted attack on a bank



#CARBANAK

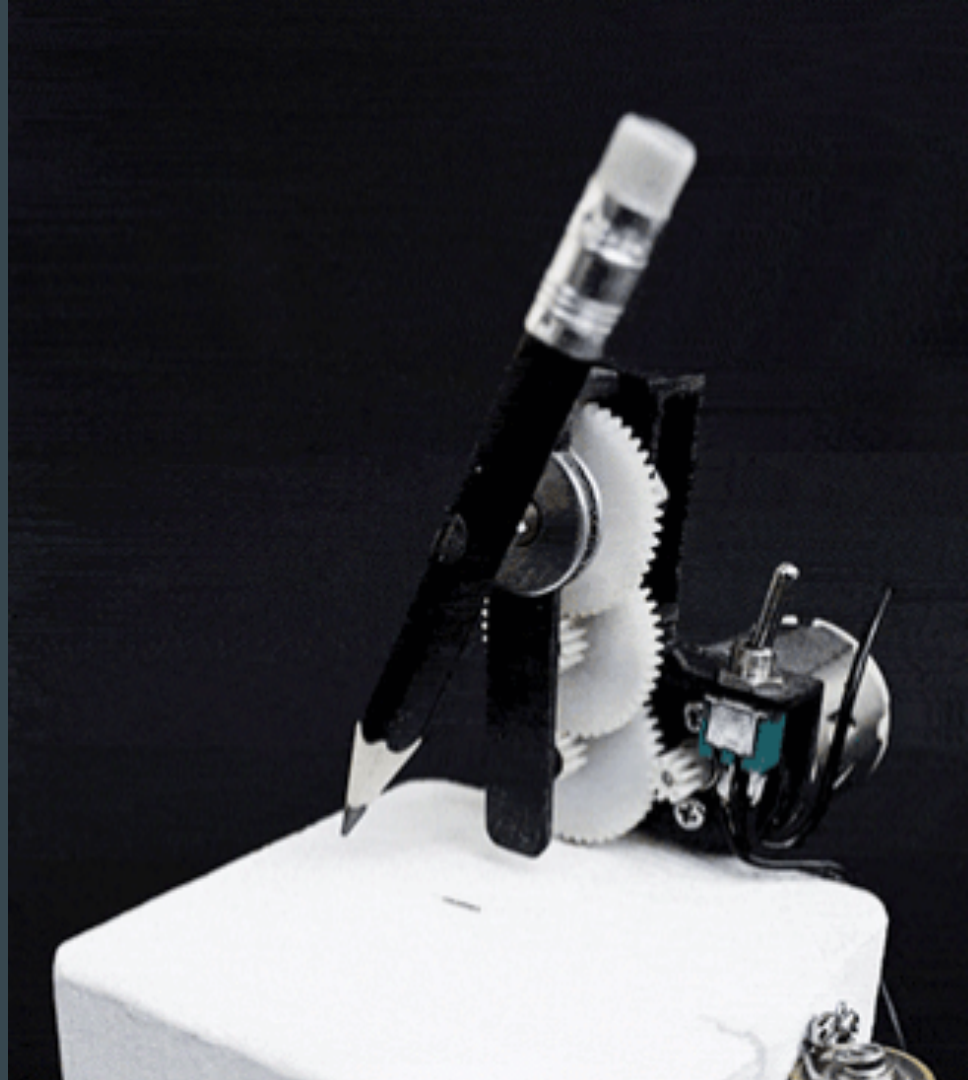
GREAT KASPERSKY

Benefícios?

Benefícios?

- Descobre vulnerabilidades expostas
- Facilita a análise de riscos reais
- Ajuda na sustentação da continuidade do negócio
- Diminui a possibilidade de ataques reais
- Ajuda a ficar em conformidade com a ISO27000, PCI, etc
- Ajuda a preservar a reputação da empresa
- Aumenta o conhecimento para análises de ataques reais

Como é feito?



Como é feito - Determinando o escopo

- Web
- Engenharia Social
- DDoS e Performance
- Infraestrutura
- Rede Interna ou Externa
- Mobile
- Database
- Virtualização

Como é feito - Realizando os testes

1. Recon e OSINT
2. Análise do alvo e planejamento de ataques
3. Encontrar vulnerabilidades
4. Explorar vulnerabilidades
5. Ganhar acessos
6. Escalação de privilégios
7. Análise de riscos e criação do relatório
8. Retestes

Como é feito - Dicas

- Nunca enviar resultados de scans pro cliente
- Nunca dá pra fazer tudo sozinho, dependendo do escopo é preciso ter um time
- O relatório precisa ter os riscos e também potenciais riscos

Alvos

Alvos

- Domínios que possam ter leaks e falha de sistema
- Erros em aplicações em desenvolvimento
- Falhas de configuração
- Falta de conscientização dos funcionários
- Nível de segurança de infraestrutura e sistema

Atacantes?
Invasores?
Ameaças?

Mindsets

- Acesso anônimo externo ou interno
- Usuário normal com ou sem informação interna
- Usuário não autorizado com informações internas
- Usuário autorizado com informações internas
- Administrador
- Funcionário infeliz ou desapontado

Quando fazer?

Quando fazer?

- Antes e depois de um momento importante, como compra de outras empresas
- Depois de contratar ou demitir pessoas que tinham trabalhos críticos
- Quando achar que o sistema está seguro ou não
- Pelo menos 1 vez por ano
- Depois de mudanças significativas no sistema ou novas integrações

Relatório

Relatório

- Mostrar tudo que foi encontrado nos testes, com detalhes, inclusive recomendações de mitigação
- Categorizar os pontos encontrado por nível de risco

Relatório

Avaliação

Avaliação - Entrega

- Apresentar para o executivos o sumário narrativo dos testes, mostrando o status geral do que foi testado

- Geralmente é uma reunião para discutir o relatório

Verificação

Verificação - Retestes

- Depois de explicar sobre todos os pontos e validar eles, é esperado que a empresa resolva os pontos
- Depois da empresa resolver os pontos, é definido um trabalho para verificar se foi realmente resolvido
- Cria-se novamente outro relatório com novas evidencias

Checklist

Telegram: @tilt4

Amanhã tem oficina de Pentest

...

Obrigado pela atenção