

Segurança da informação

As três etapas iniciais

No mundo da segurança os testes de invasão ocorrem de variados tipos. Quando vamos fazer um teste é interessante ter um *modus operandi* com objetivos bem definidos para que possamos trabalhar com mais eficiência. Independente do processo de invasão existem três etapas que sempre vão existir em qualquer trabalho, elas são:

- **Conhecer**

A primeira coisa e mais intuitiva a se fazer no começo de um teste de segurança é conhecer o seu alvo, o processo de conhecer pode ser feito de várias formas, desde o trabalho manual fazendo coletas de e-mail, números de telefone, sites, sub-domínios, até coletas mais profundas usando algumas ferramentas como o The Harvester por exemplo, no processo de coleta de informações também é muito comum usar o google hacking para conseguir informações mais específicas sobre o alvo, futuramente falaremos mais desta técnica.

"Se você conhece a si mesmo e a seu inimigo, então não deve temer o resultado de 100 batalhas."

- Sun Tzu em A arte da guerra.

- **Analisar**

Esse processo é de extrema importância, é nele que você faz uso de toda a informação que coletou para extrair conteúdo útil, na etapa anterior conseguindo um número de ip, por exemplo, você poderia agora usar uma ferramenta como o Nmap para descobrir portas abertas, os serviços que elas estão rodando, a versão do serviço e até o sistema operacional a fim de encontrar alguma vulnerabilidade.

- **Explorar**

Essa é a etapa onde você ativamente tenta fazer a invasão do sistema juntando tudo que você coletou, seja tentando engenharia social, usando um exploit ou de qualquer outra forma.



 [Instagram](#)

 [Github](#)

Obrigado!