Grupo de Resposta a Incidentes de Segurança.

Trabalho de Engenharia Social.

Professor:Franklin Martins.

Aluno: Samuel Silva de Oliveira Filho

DRE: 098223587

Licenciatura em Filosofia – Faculdade de Educação.

A Engenharia social se refere, ao meu ver, a busca de informações básicas para que, uma pessoa: jurídica eu física, tenha seus dados e informações digitais hakeadas.

Após iniciar os preparativos para um ataque o haker precisa de informações sobre o alvo, para só após esta coleta iniciar o pentest.

Com isto em mente, inicia a segunda fase do processo que é a engenharia social propriamente dita.

O haker deve estar disposto a: revirar o lixo do seu alvo. seguir seus hábitos, conseguir detalhes sobre suas rotinas diárias, etc.

Em muitos casos, chega até a trabalhar, na empresa ou para a empresa, da qual busca obter dados.

Com estas informações inicia a análise das vulnerabilidades e a exploração das mesmas.

A próxima faze é executar as diversas ferramentas a sua disposição para executar a tarefa: uso de programas específicos para se obter uma senha, neste caso, costuma ser apenas uma questão de tempo para a senha ser quebrada, um detalhe, quantos mais dígitos a senha tiver, mais tempo será necessário para um programa descobrir a senha, o ideal, é uma senha com mais de dez dígitos

Ou também, o uso do recurso conhecido como “força bruta” que consiste, basicamente, em tentativas de erro e acertos até descobrir a senha correta, neste caso, a engenharia social bem feita, deve ser a chave para um resultado satisfatório.

Análise de um caso.

Na época do Orkut uma pessoa que se sentia segura atráz de um teclado de computador costumava ser extremamente grossa em seus comentários feitos nos grupos nos quais participava.

Um programador incomodado com tanta grosseria resolveu demonstrar que o anonimato de um perfil fake não é tão seguro quanto seu detrator pensava.

Sabendo que seu projeto era localizar uma pessoa que morava na Tijuca – informação fornecida durante uma conversa de grupo – ele criou um programa que buscava determinar quem na Tijuca entrava e saía do Orkut – na época era discagem por linha telefônica – sempre ao mesmo tempo, ou seja, sempre que a pessoa entrava no Orkut a linha telefônica ficava ocupada, quando determinou qual linha correspondia a esta constante , obteve a identidade do usuário.

Durante uma conversa de grupo onde a tal pessoa iniciou seu costumeiro mal humor o programador informou: (in box) o número do telefone e, o que havia obtido através de Engenharia Social.

Atualmente,as mídias sociais são muito mais diversificadas, fornecendo, portanto, muito mais informações sociais, acredito que: seguindo uma pessoa no: facebook, instagram, twitter, etc.

Por si só já se pode obter várias informações sobre a empresa onde ela trabalha, empresa estaque contrata pessoas para um pentest.

Lembrando que há leis que regulamentam estas atividades e, que estas técnicas só podem ser usadas de forma ética na atividade de PENTEST devidamente autorizada.