“Engenharia Social é o método de ataque que visa extrair informações através da maior falha existente num mundo tecnológico: a humana.”

O ataque de engenharia social a ser apresentado consiste em descobrir as informações de usuário e senha do Facebook de funcionários da empresa X. Sabe-se que o setor de tecnologia bloqueou o acesso ao site do Facebook em toda rede corporativa, assim sendo, alguns funcionários ficam ansiosos por encontrar uma maneira alternativa.

Dada a audácia humana, escolhe-se um ataque de phishing. A nova página falsa do Facebook é colocada como “página inicial” dos navegadores em alguns dos computadores da rede e como atalho na área de trabalho. Assim, as pessoas se interessam na oportunidade de dar uma simples checada em suas contas pessoais e acabam entregando seus dados, sendo redirecionadas, posteriormente à coleta dos mesmos, para a página do Facebook verdadeira que encontra-se bloqueada.

Visto que os computadores são autenticados pela rede, ou seja, qualquer usuário pode entrar em qualquer computador, precisa-se de uma forma alternativa de consolidar o objetivo do parágrafo anterior. Dado que temos acesso ao ambiente por meio de um colega funcionário, um dispositivo USB com qualquer distribuição Linux seria suficiente para alterar os arquivos do Windows ou, por exemplo, substituir o arquivo do

teclado virtual pelo do terminal para acesso do próprio terminal na tela de login do Windows, já que temos ferramentas para acessibilidade disponíveis antes da autenticação. Feito isso, temos acesso administrativo e conseguimos fazer a troca da página inicial.

Constatando a necessidade de parecer que o próprio usuário esteja logado a fim de aprimorar o ataque, o objetivo agora é carregar a página inicial do Facebook **logado** no servidor de phishing, dado que temos tais credenciais, e redirecionar o conteúdo para o site de phishing que a vítima está observando, criando a ilusão de que o login foi efetivamente realizado. Caso o usuário tente continuar com a navegação, a mesma será interrompida quando esta for redirecionada para a página real do Facebook.

Portanto, por este método, espera-se conseguir um número relativamente grande de contas do Facebook devido à rotatividade de usuários na empresa e, dado que eles não têm acesso ao Facebook, espera-se que a curiosidade seja uma das falhas humanas para o sucesso deste ataque.