Universidade Federal do Rio de Janeiro (UFRJ)
Processo Seletivo do Grupo de Resposta a Incidentes de Segurança (GRIS)
Tag de Engenharia Social
Avaliador: Franklin Martins
Candidato: Felipe de Jesus

Objetivo: Explicar ataque de engenharia social para conseguir informações e mostrar como aprimorar este ataque.

Phishing é um tipo de ataque hacker, em que o invasor cria uma cópia falsa de um site para obter informações confidenciais de empresas ou pessoas, como logins e senhas. Dessa forma, ele pode invadir o sistema e fazer quase tudo o que desejar, como por exemplo, mudar o login e a senha do sistema e deletar informações importantes. Este é um tipo de invasão, na qual o hacker utiliza ferramentas de engenharia social para descobrir o comportamento e caracteristicas da pessoa e assim criar uma situação falsa para tentar manipular pessoas e empresas com intuito de obter informações sigilosas. Irei utilizar este tipo de ataque para obter informações importantes de uma escola.

Vamos supor que eu ainda esteja no ensino médio na mesma escola em que estudei. Durante este curso, a partir do momento que conclui o curso de programação no laboratório de informática e virei monitor do laboratório, comecei a me envolver de forma recíproca com todos os departamentos do colégio, como a direção, secretaria e coordenação. Sempre que ocorria algum problema relacionado à informática nestes departamentos, como queda de internet ou problemas no computador, eu e o pessoal do laboratório de informática era chamado para resolver os problemas. Dessa forma, construi uma relação de amizade com todos os órgãos administrativos do colégio.

Essa escola possui um sistema de gerenciamento online fornecido pela SEEDUC (Secretária de Estado de Educação). Todas as informações dos alunos, como os dados pessoais estão nesse sistema. Eu quero entrar no sistema e conseguir todas essas informações, porém o sistema possui login e senha, os quais nenhum aluno pode saber. Dessa forma, irei utilizar um pouco de engenharia social e phishing para descobrir as credenciais do sistema em um dos departamentos da escola. Analisando os órgãos da escola, percebi que o mais legal, carinhoso e afetivo é a secretaria. As secretárias desempenham trabalhos que necessitam de acesso ao sistema, como por exemplo a matrícula de alunos e produção de relatórios, como históricos escolares e certificados de conclusão. Portanto, inicialmente irei utilizar a ferramenta SetToolkit do Kali Linux para clonar o site de acesso ao sistema da escola. Logo após isso, irei fazer uma ligação para a funcionaria principal da secretaria me passando pelo diretor do colégio e dando permissão para que o aluno/monitor, Felipe, do laboratório de informática possa imprimir algum documento importante e pessoal na secretária. Com isso, irei na secretaria e peço para entrar em um dos computadores para acessar o documento, aproveito para imprimir uma cópia do meu cpf, por fim deixo o computador com a página falsa do sistema aberta e invento uma história para a secretária, como “Me inscrevi em um esporte no Centro Esportivo aqui perto, mas eles estão pedindo uma declaração escolar, preciso dela para levar ao centro até amanhã, no máximo, se não irei perder a vaga”. Desse modo, ela vai entrar no sistema através da página falsa e os dados de acesso irão ser enviados para o meu computador que é o servidor deste site falso. Enfim, irei pegar a declaração, agradecer e sair da secretaria. Portanto, utilizando um pouco de persuasão e Phishing, eu conseguiria o login e a senha do sistema da escola e poderia invadi-lo e extrair

o máximo de informações possíveis dos alunos e professores, além de explorar outras falhas de segurança.