

Primeiro dia: coleta de informações.

Entrei no site da empresa, analisei as páginas. Encontrei uma lista de e-mails e nomes. Comecei a procurar sobre as pessoas no Google e Redes Sociais. Algumas, tinham contas públicas, outras, não consegui achar. Já tinha bastante informação sobre alguns funcionários, agora precisava arrumar um modelo de email da empresa. Me cadastrei no serviço com dados falsos e um e-mail temporário. Recebi um email de confirmação. Preparei um phishing e mandei os emails.

Segundo dia: visita à empresa.

Entrei naturalmente, procurando por Áreas restritas. Achei uma, mas precisava de um crachá para abrir a porta, provavelmente NFC. Entrei na fila de atendimento. Chegou a minha vez, ao chegar a mesa de atendimento avistei um crachá em cima da mesa. Pedi coisas razoáveis que sabia que não poderiam ser feitas e após algumas tentativas comecei a fingir ficar nervoso. Passou um tempo e parei, respirei fundo, disse com uma calma forçada: "Então, por gentileza, chame o gerente." A atendente levantou-se e saiu. O crachá tinha NFC, deu tempo o suficiente para pegá-lo, cloná-lo e devolvê-lo, sem que ninguém percebesse. Com o retorno da atendente, o gerente também apareceu. O gerente falou e explicou. Para os funcionários, acabou tudo como sendo um mal entendido. Consegui passar pela porta, havia vários corredores e portas. Não tive tempo de entrar em todas as portas, nas que procurei não achei nada.

Terceiro dia: consertando o servidor.

Verifiquei o progresso do phishing, alguns caíram, consegui credenciais do site e, provavelmente, senhas pessoais de email. Entrando no site, agora como funcionário, acabei achando telefones da empresa. Fiz uma chamada, que parecia ter vindo do setor de Recursos Humanos, para a filial, notificando que ainda hoje vai chegar um funcionário para verificar o servidor, como se fosse de rotina. Quando cheguei, me identifiquei, ganhei um crachá, e me levaram até a sala do servidor. Estava sozinho. Como o contrato não permitia derrubar o serviço, escolhi tirar uma foto do servidor, esperar por uns 40 minutos, e sai.