Aluno: José Victor Medeiros Thomé da Silva
Instrutor: Franklin Martins

TAG – Engenharia Social

1. Introdução:

Nesse relatório é descrito um pentest (teste de penetração) feito dentro de uma pequena empresa utilizando técnicas de Engenharia Social. Cada um dos testes terão como foco a realização dos seguintes tipos de ações em cada um deles:

1. Acesso a dados sigilosos, tanto da empresa quanto de seus membros, indevidamente expostos na web e acessíveis através de consultas avançadas do buscador Google;
2. Acesso físico a setores da empresa feito por pessoas não autorizadas (trailgating);
3. Acesso não autorizado a rede da empresa através da invasão de aparelhos conectados a mesma usando arquivos maliciosos ou QR-Code suspeitos, sendo os mesmos anexados a e-mails com mensagens confusas ou chamativas no intuito de explorar a curiosidade do alvo em relação ao esses anexos (baiting);
4. Obtenção de informações privadas relacionadas a empresa por envio indevido das mesmas através de páginas web maliciosas, tendo seus links anexados em e-mails nos quais as mensagens tentam ou incitar uma sensação de urgência ao alvo para passar essas informações (phishing), ou enganar o alvo com um pretexto que, embora seja falso, tenta ser válido o bastante para convencer de passar esses dados (pretexting).

Por questões de eficácia, cada um desses testes de vulnerabilidade serão feitos com os funcionários da empresa durante seus expedientes de trabalho sem haver qualquer consentimento dos mesmos. No entanto, nos comprometemos a não fazer uso de nenhum dado sigiloso que acabe sendo eventualmente extraído em qualquer ataque, pois nosso objetivo é apenas fazer testes de segurança.

2. **Descrição dos testes**:

Antes de todos os testes, primeiramente faremos uma coleta de informações a respeito da rotina externa da empresa em si, analisando padrões de entrada e saída de seus membros, a interação da empresa com seus fornecedores externos e parceiros, e dados básicos de alguns funcionários, de todos os escalões, como nome e e-mail.

2.1 Teste 1:

No *teste 1* faremos algumas buscas avançadas no Google sobre empresa a procura de informações relacionadas ao seu corpo de funcionários (incluindo membros executivos) ou da própria instituição em si. Com isso, verificaremos se estão expostos na web dados sigilosos como senhas e documentos pessoais de funcionários, documentos internos da empresa e informações sensíveis de seu sistema interno.

Diante dessas buscas, qualquer ocorrência de exposição indevida desses conteúdos sigilosos serão registradas em relatório, assim como também haverão indicações de onde estão ocorrendo as exposições indevidas para que providências sejam tomadas por parte da contratante.

2.2 Teste 2:

No *teste 2* as ações se basearão em *Trailgating*. Primeiramente mandaremos um especialista que, a princípio, se passará por uma pessoa civil relacionada a algum membro de alto escalão da empresa, isto é, um civil sem nenhum vínculo profissional com a mesma. Esse especialista tentará adentrar a instituição se aproximando com conversas e interações diretas com funcionários transeuntes na entrada e, após se suceder nessa tarefa, tentará acessar outros setores internos restritos se aproximando de outros funcionários autorizados prestes a entrar no local. Nessas aproximações, algumas estratégias (envolvendo interações ou não) serão usadas, tais como: se passar por um membro de outro setor da empresa que necessita de acesso ao local com um falso pretexto, conversas envolvendo abordagem técnica ou informal (podendo inclusive fazer usos de jargões) com o intuito de distrair a pessoa enquanto adentra ao setor alvo, tentar adentrar o local usando o falso pretexto de ter sido mandado em nome de algum outro membro também autorizado ou simplesmente se aproximar na encolha sem ser percebido. Todas essas estratégias serão baseadas numa análise prévia dos padrões de comportamento e interação dos membros autorizados.

Após a conclusão dessa primeira etapa do teste 2, aprimoraremos a tentativa de invasão mandando outro especialista que, dessa vez, se passará por um representante de algum fornecedor ou parceiro da instituição que tem seu acesso ao interior da empresa restrito apenas aos setores nos quais condizem com os seus objetivos propostos. Esse especialista, caso tenha um membro supervisor o acompanhando, tentará se aproveitar ou se afastar do mesmo para acessar outros locais do estabelecimento, dependendo da conveniência do momento. Para se suceder nas infiltrações indevidas, ele poderá adotar as mesmas estratégias de aproximação do primeiro especialista ou usar estratégias próprias usando sua suposta posição de representante para isso.

Todas as tentativas de acesso indevido feitas por ambos os especialistas que forem bem sucedidas serão registradas em relatório, apontando como obtiveram acesso aos setores e se encontraram nos locais que entraram quaisquer aparelhos que estivessem suscetíveis a acesso de terceiros (como computadores fora da tela de proteção de login). Além disso, também conterá no relatório ocorrências de falhas de inspeção tanto das credenciais quanto da veracidade dos argumentos usados e falhas de vigilância por parte da segurança da empresa.

2.3 Teste 3:

No *teste 3* as ações se basearão em Baiting. Faremos esse teste enviando e-mails para diversos membros da instituição. Nesses e-mails, como o objetivo aqui é atiçar a curiosidade do alvo diante dos seus anexos maliciosos, suas mensagens estarão focadas nisso, fugindo do âmbito empresarial.

Nas mensagens passadas terão conteúdos como: falsos anúncios de plataformas de vídeos e músicas, com possibilidades de downloads de filmes recentes e melhores hits da atualidade com ótima qualidade e sem pagar nada por isso; ganho

cupons premiados duvidosos com créditos referentes a lojas (reais ou fictícias) ou espaços/eventos de entretenimento; fake-news sensacionalistas de famosos; premiações duvidosas relacionadas a planos de serviço vinculados ao alvo (como bancos, serviço de telefonia móvel e plano de saúde); ou simplesmente uma mensagem confusa que induza o alvo de baixar ou acessar os anexos. Os anexos dos e-mails podem ser links suspeitos, arquivos para download ou um QR-Code.

Para realizar as ações desse teste usaremos a feramenta SET (Software-Engineering Toolkit). Nessas ações geraremos spear-phishing attack vectors, sendo uns com arquivos anexados (tais como PDF e RAR), outros com QR-Code customizados na tentativa de invadir aparelhos móveis conectados a rede e outros contendo links para páginas web usadas nessa etapa de teste. Quanto as mensagens dos e-mails, apesar do mecanismo de teste usado ser um tipo de spear-phishing, estarão condizentes a de um baiting, que é o tipo de ataque simulado nesse teste.

A princípio, espalharemos e-mails mais simples, isto é, com conteúdo envolvendo suspeitas não muito difíceis de se detectar, como por exemplo fake-news sensacionalista bem surreal, mensagem confusa anexada com um QR-Code aleatório, cupom de desconto de uma loja fictícia com valore muito fora da realidade, e serviço de download gratuito de vídeos e músicas providos de uma plataforma fictícia. Com a evolução dessa etapa, passaremos a usar ataques mais elaborados envolvendo mensagens mais convincentes, como uma oferta relacionada a uma fornecedora de serviço vinculada ao alvo (por exemplo plano de saúde e empresa de telefonia), cupons promocionais vindos ou de lojas online reais (como Amazon e Mercado Livre) ou de espaços de entretenimento conhecidos (como Kinoplex e Vivo Rio), promoções de serviços de streamming conhecidos (como Netflix e Spotify), ou premiações vindos de instituições financeiras de aposta (como Loterias da Caixa e Loterj).

Cada abertura de arquivo anexado feita e acesso as páginas web de teste via link ou QR-Code anexado serão contabilizados e, no relatório final, registraremos toda essa contagem mostrada em um gráfico que apresentará a taxa de sucesso de cada tipo de baiting usado nesse teste.

2.4 Teste 4:

No *teste 4* as ações se basearão em Phishing (mais especificamente Spear-Phishing) e Pretexting. Nesse teste, assim como no anterior, faremos as ações usando e-mails simulando operações maliciosas, sendo as únicas diferenças o contexto/intenção das mensagens e o fato dos anexos serem compostos apenas por links de páginas web usadas no teste.

Na etapa que simularemos ataques de Spear-Phishing os e-mails terão o intuito de passar uma sensação de alerta e apreensão no alvo. Para isso, usaremos mensagens como: alertas de invasão da conta bancária da empresa e extravio de dinheiro da mesma, desatualização de softwares instalados na rede interna, alertas de falhas de segurança do sistema interno, avisos de urgência vindos de algum parceiro/fornecedor da instituição ou, até mesmo, de um suposto representante de um setor interno da empresa.

Já na etapa que simularemos ataques de Pretexting os e-mails serão mais elaborados e convincente, se passando por algo enviado por um parceiro de negócios, um fornecedor de serviços ou um membro interno da empresa, tendo como intenção explorar a confiança do alvo nesses indivíduos. As mensagens terão conteúdos com

pretextos que tenta ser válidos de acordo com a situação, tais como: um pedido de atualização de dados no sistema, informações para auxiliar na manutenção da rede e periféricos, efetuação de entrega de suprimentos ou transações internas entre setores.

Em ambas as etapas faremos uso do SET para gerarmos os e-mails maliciosos de teste usando a opção Spear-Phishing Attack.

A primeira etapa a ser executada será a de ataque Spear-Phishing na qual dispararemos uma série de e-mails para membros de diversos setores da empresa, sendo que padrões de mensagens contidas nos e-mails serão condizentes com a área da instituição na qual o alvo pertence, como por exemplo alertas de invasão de conta bancária vai para alguém do setor de TI e atraso de fornecimento vai para alguém do setor de logística.

Na segunda etapa o esquema de ação seguido será o mesmo da primeira, sendo as mensagens também relacionadas a área do alvo na empresa. Quanto aos horários de disparos, eles serão distribuídos ao longo do dia e servirão como ferramenta de análise.

A contabilização e análise de Spear-Phishing e Pretexting bem sucedidos serão feitas separadamente. No relatório final apresentaremos índices dos tipos de Spear-Phishing e Pretexting mais bem sucedidos, os setores da empresa mais afetados pelos respectivos tipos de ataque e os horários que tiveram maiores ocorrências de sucesso dos mesmos, isto é, os momentos do dia em que os alvos estavam mais suscetíveis a desestabilização emocional provocada por um Spear-Phishing ou a serem enganados pelo falso contexto de um Pretexting.

3. Conclusão:

Todos os quatro testes propostos nesse pentest tem como objetivo detectar determinados tipo de vulnerabilidade exploráveis via Engenharia Social no cotidiano da empresa. Abaixo estão descritos os objetivos centrais de cada teste:

1. Teste 1: Detectar qualquer informação privada relacionada a empresa (seja por parte de seus funcionários ou da instituição em si) que esteja exposta na web e possa ser encontrada via motores de buscas como o Google;
2. Teste 2: Detectar falhas graves da segurança interna da empresa, sejam por políticas não adotadas ou negligências da equipe de vigilância, relacionadas verificação de credenciais de funcionários autorizados, monitoramento da movimentação de pessoas externas dentro dos espaços internos, proteção contra acesso de terceiros a dispositivos internos conectados ao sistema e controle de entrada e saída dos espaços da instituição;
3. Teste 3: Detectar acessos imprudentes e indevidos por parte dos membros da instituição a anexos de e-mails suspeitos dentro do ambiente de trabalho, podendo expor a rede interna a invasões de malwares tanto por dispositivos fixos (como PCs e terminais de trabalho) quanto dispositivos móveis conectados a mesma;
4. Teste 4: Detectar falhas de inspeção e de confirmação da veracidade do conteúdo de e-mails por parte dos membros da empresa, seguida de eventuais exposições indevidas de informações privadas da instituição por meio de acesso a possíveis sites maliciosos com links anexados a esses e-mails.