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 no qual suas mensagens passam ou uma sensação de urgência ao alvo para passar essas informações (phishing), ou um pretexto falso porém que tenta ser convincente o bastante para o alvo passar esses dados (pretexting).

Por questões de eficácia, cada um desses testes de vulnerabilidade serão feitos com os funcionários da empresa durante seu cotidiano de trabalho sem consentimento. 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.

1. **Descrição das ações**:

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.

No *teste 1* faremos algumas buscas avançadas no Google a respeito da 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.

O *teste 2* simulará um *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, a medida que se suceder, tentará acessar outros setores internos restritos se aproximando de outros funcionários autorizados a entrar no local. Nessas aproximações, algumas estratégias (envolvendo interação 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 com 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 o pretexto de ter sido mandado em nome de algum outro membro também autorizado ou simplesmente se aproximar na encolha sem ser percebido. Essas estratégias serão elaboradas se baseando numa análise prévia dos padrões de comportamento e interação dos membros autorizados.

Após a conclusão dessa primeira etapa do teste 1, 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. Para as infiltrações indevidas, ele poderá adotar as mesmas estratégias de aproximação do primeiro especialista, tendo inclusive em mãos um pequeno relatório com os padrões de comportamento e interação analisados na primeira etapa, ou usar sua própria posição de representante/parceiro para isso.

Todas as tentativas de acesso indevido bem sucedida feitas por ambos os especialistas serão registradas em relatório, apontando como obtiveram acesso aos setores e se encontraram nos locais que entraram computadores e aparelhos suscetíveis a acesso de terceiros (fora da tela de proteção de login). Além disso, também conterá no relatório ocorrência de falhas de averiguação de credenciais ou da veracidade dos argumentos usados e falhas de vigilância por parte dos funcionários da empresa.

O *teste 3* simulará um 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 exorbitantes referentes a lojas 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. Esses anexos 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.

O teste 4 simulará um Phishing/Pretexting. Assim como o teste 3, também usaremos uma ferramenta de testes para esse. Os e-mails simulados se passarão como enviados por algum fornecedor ou parceiro da empresa e conterão mensagens que passem sensação de urgência, como bancos afirmando supostas invasões de contas bancárias e empresas de serviços de TI notificando atualização urgente de algum serviço fornecido, ou mensagens mais elaboradas com pretextos convincentes, como pedidos de dados necessários faltantes para uma compra realizada. Esses e-mails também acompanharão de um link que levará a uma página também simulada que pedirá informações sigilosas da empresa. Tanto o acesso a esses links quanto a passagem dos dados serão contabilizadas em relatório.

1. **Conclusão:**

aaa