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 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 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.

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, 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 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. 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.

2.3 Teste 3:

O *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 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. 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 e cupons de desconto de lojas fictícias com valores muito exorbitantes, serviços de download gratuito de vídeos e músicas providos de plataformas fictícias. Com a evolução dessa etapa, passaremos a usar ataques mais elaborados, envolvendo ofertas mais convincentes, como uma premiação relacionada a uma fornecedora de serviço vinculada ao alvo (por exemplo plano de saúde e empresa de telefonia), cupons promocionais de lojas online reais (como Amazon e Mercado Livre), espaços de entretenimento conhecidos (como Kinoplex e Vivo Rio), e até mesmo serviços de streamming conhecidos (como Netflix e Spotify).

Cada abertura de arquivo usado, 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 baiting usado nesse teste.

2.4 Teste 4:

O *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 fato dos anexos serem compostos apenas por links para páginas web usadas no teste e o contexto/intenção das mensagens.

Na etapa que simularemos 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, desatualização de softwares instalados na rede interna, alertas de falhas de segurança do sistema interno, avisos de urgência vindos de algum parceiro da instituição ou, até mesmo, de um suposto representante de um setor interno para outro.

Já etapa na qual simularemos Pretexting os e-mails serão mais elaborados e convincentes, se passando por algo enviado por um parceiro de negócios, fornecedor de serviços ou membro interno. 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, sendo as mensagens também relacionadas a área na qual o alvo pertence 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 ataques e os horários que tiveram maiores ocorrências de sucesso dos mesmo, 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.

1. **Conclusão:**