Aluno: José Victor Medeiros Thomé da Silva

Instrutor: Franklin Martins

TAG – Engenharia Social

1. **Introdução:**

Nesse relatório é descrito um conjunto de testes de penetração utilizando Engenharia Social, sendo feitos dentro de uma pequena empresa. Esses testes, respectivamente usando busca avançada e as estratégias de invasão trailgating, baiting, phishing e pretexting, terão como foco a verificação dos seguintes tipos de vulnerabilidade em cada um deles:

* + 1. Acesso a dados sigilosos da empresa expostos em seu sistema através de consultas do buscador Google.
    2. Acesso físico a locais da empresa feito por uma pessoa não autorizada a áreas restritas a funcionários;
    3. Acesso não autorizado a computadores por conta de conexão de Hardware ao sistema.
    4. Acesso não autorizado ao sistema através de e-mails maliciosos no qual se passa por um aviso legítimo de algum alerta do sistema;
    5. Acesso não autorizado ao sistema através de e-mails que se passa por algum fornecedor legítimo.

Por questões de eficácia, cada um desses testes de vulnerabilidade serão feitos com os funcionários da empresa durante seu cotidiano de trabalho sem o consentimento dos mesmos. No entanto, em virtude de segurança, em nenhum desses ataques serão extraídas informações dos funcionários ou da empresa, sendo feitos apenas para testes.

1. **Ações**:

Antes de todos os testes, faremos uma coleta de informações a respeito da rotina da empresa em si externamente, analisando padrões de entrada e saída de funcionários, a interação da empresa com seus fornecedores externos 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 em busca de informações relacionadas ao corpo de funcionários da empresa, incluindo membros executivos, ou da própria empresa em si. Com isso, verificaremos se estão expostos online dados sigilosos como senhas e documentos pessoais de funcionários, documentos internos da empresa e dados do sistema interno. Diante dessas buscas, qualquer ocorrência desses dados sigilosos registrada em relatório indicará onde são expostos os conteúdos sigilosos.

O teste 2 simulará um Trailgating. Mandaremos dois especialistas em dias diferentes, um se passando por representante de um fornecedor e outro como uma pessoa civil relacionada a algum membro de alto escalão da empresa. Ambos os especialistas, baseando-se na rotina externa da empresa, tentarão ter acesso ao interior da empresa através de conversas e interações com funcionários e, a medida que se sucederem, tentarão acessar outros locais internos restritos usando diferentes tipos de abordagem, inclusive usando alguns jargões (sendo técnicos ou não). Todos os percursos de acesso indevido bem sucedido serão registrados em relatório.

O teste 3 simulará um Baiting. Através de uma ferramenta de testes (o Social-Engineering Toolkit), serão enviados a alguns membros da empresa e-mails com informações passadas de modo que tentem induzir o usuário a verificar um QR-Code anexado com seus aparelhos móveis; em outras mensagens desse teste também usaremos como isca arquivos em anexo e links falsos. Com isso, analisaremos quantos desses membros realizaram a ação pretendida.

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: