**Universidade São Judas Tadeu  
  
Sistemas Computacionais e Segurança  
  
Prof° Robson Calvetti  
  
Definição do Grupo**  
Lucas Gabriel Hora Benetti – RA: 825134041  
Matheus Ortiz de Jesus – RA: 825149730  
Yago Henrique- RA: 825140992

**Vídeo analisado:**

“Anatomia de um Ataque Cibernético: Como um Invasor Pode Deixar Você Sem Nada”  
(https://youtu.be/NF3w2aukgpU?si=sKJ0IUwtwud2k30g)

**Objetivos**

Identificar:   
- Vulnerabilidades;  
- Tipos e técnicas de ataques utilizados;  
- Motivação do Cracker.

**Cenário**

- Servidor Web conectado ao banco de dados;

- Servidor de e-mail;

- Sistema de compartilhamento de arquivos;

- Cracker mal-intencionado.

**Etapa 1: Acesso inicial**

- **Técnica de Ataque:** Phishing. O cracker envia um e-mail falso se passando por uma empresa legítima ou pessoa de confiança.

- **Vulnerabilidade:** O usuário desprevenido, que clica no link malicioso fornecido no e-mail, permitindo que suas credenciais sejam roubadas.

**Etapa 2: Movimentação e Escalada de Privilégios**- **Técnica de Ataque:** Uso de contas válidas e escalada de privilégios. Com as credenciais roubadas, o invasor tem acesso inicial aos sistemas. Em seguida, ele procura por senhas não criptografadas em arquivos e sistemas de compartilhamento para acessar sistemas mais importantes e obter privilégios de administrador.

- **Vulnerabilidade:** Armazenamento de senhas sem criptografia, o que permite ao invasor ganhar acesso a sistemas críticos e escalar seus privilégios facilmente.

**Etapa 3: Coleta e Exfiltração de Dados**

- **Técnica de Ataque:** Coleta e infiltração de dados. O invasor, já com acesso privilegiado, vasculha os sistemas para encontrar informações valiosas, como dados de clientes, propriedade intelectual ou informações financeiras. Ele então envia esses dados para fora da rede da empresa.

- **Vulnerabilidade:** Acesso privilegiado obtido por meio de senhas não criptografadas e a falta de monitoramento adequado de dados sensíveis.

**Etapa 4: Destruição e Danos**

- **Técnica de Ataque:** Destruição de dados. Como parte final do ataque, o cracker pode apagar os dados do sistema para causar o máximo de dano à empresa.

- **Motivação:** Causar prejuízo à empresa, além de roubar dados.

**Motivação e objetivo do invasor (Cracker)**

- Obter dados críticos: O principal objetivo é ter acesso a informações valiosas da empresa;

- Destruir dados e causar danos: O invasor destrói dados para prejudicar a empresa.

**Tipos e técnicas de ataque utilizados durante a invasão:**

- **Ataque de Phishing:** O cracker envia e-mails falsos para roubar credenciais.

- **Uso de contas válidas:** Com as credenciais em mãos, o invasor pode ter acesso a outros sistemas e aplicativos.

- **Acesso às credenciais e escalada de privilégios:** Ao acessar o sistema de compartilhamento de arquivos e obter as senhas não criptografadas, o invasor pode ter acesso a sistemas mais importantes.

- **Coleta e infiltração de dados:** O invasor coleta dados importantes e os envia para si mesmo.

- **Destruição dos dados:** O invasor apaga os dados, causando danos significativos à empresa.

**Vulnerabilidades identificadas ao longo do ataque:**

- **Usuário desprevenido:** O usuário clica em um link malicioso, o que expõe suas informações de login e facilita o acesso do invasor.

- **Senhas não criptografadas:** O armazenamento de senhas em arquivos simples e sem criptografia permite que o invasor acesse sistemas críticos.  
**- Falta de barreiras de autenticação de usuários:** Como autentificação de dois fatores ou perguntas de segurança.