UNIVERSIDADE SÃO JUDAS TADEU

GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

NATASHA MELO E YASMIN VICTÓRIA

**ANATOMIA DE UM ATAQUE COMPLEXO**

SÃO PAULO – SP

2024

NATASHA MELO E YASMIN VICTÓRIA

RA:82429222 E 824210011

**ANATOMIA DE UM ATAQUE COMPLEXO**

Pesquisa e apresentação sobre o tema “Anatomia de um ataque complexo”, com foco na identificação de vulnerabilidades, tipos e técnicas de ataque, e motivação do cracker, conforme orientações fornecidas.

Orientador: Robson Calvetti

SÃO PAULO – SP

2024

Sumário

1. Vulnerabilidades................................................................................................................1
2. Tipos e Técnicas de Ataque Utilizados...............................................................................1
3. Motivação do Cracker........................................................................................................1

SÃO PAULO – SP

2024

# **Alunas: Natasha Melo e Yasmin Victória**

**RA: 82429222 e 824210011**

# **Pratica 2**

# Anatomia de um ataque complexo

**Vulnerabilidades** são fraquezas ou falhas em sistemas, redes ou aplicações que podem ser exploradas por atacantes. Essas falhas podem surgir devido a erros de codificação, configurações inadequadas ou sistemas desatualizados.

1. Vulnerabilidades

No vídeo, o ataque complexo explora várias vulnerabilidades:

**Segurança Fraca em Dispositivos de Rede:** O invasor acessou a rede da empresa através de um termostato conectado à rede, que não estava protegido adequadamente pelo firewall. Essa vulnerabilidade é um exemplo de como dispositivos aparentemente inofensivos podem ser um ponto de entrada para ataques.

**Falta de Monitoramento e Segurança em Dispositivos:** A empresa não verificou a segurança dos dispositivos conectados à rede, como o termostato, facilitando o acesso não autorizado.

**Ausência de Sub-redes e Segmentação de Rede:** A rede simples da empresa, sem sub-redes ou segmentação, permitiu ao atacante mover-se facilmente e acessar dados sensíveis.

2. Tipos e Técnicas de Ataque Utilizados

O vídeo detalha o uso de técnicas específicas para realizar o ataque:

**Injeção de I-Frame:** O invasor utilizou um ataque de injeção de i-frame para comprometer o site de um boliche, que atuava como uma porta de entrada para a rede da empresa.

**Movimentação Lateral e Exploração de Rede:** Uma vez dentro da rede, o atacante explorou a estrutura de rede simples da empresa para acessar e roubar arquivos sensíveis.

**Ransomware:** Após obter os arquivos, o invasor criptografou a unidade de armazenamento e excluiu os backups para garantir que a empresa não pudesse recuperar os dados sem pagar o resgate.

3. Motivação do Cracker

A motivação do invasor é clara e multifacetada:

**Lucro Financeiro:** O invasor visava obter lucro através da venda dos arquivos roubados. Ele recebeu 75 bitcoins como pagamento por seus arquivos.

**Impacto Competitivo:** A motivação também envolvia um aspecto competitivo, pois os arquivos foram comprados por uma empresa rival, permitindo-lhe avançar tecnologicamente à frente da empresa original que desenvolveu os projetos.

Referências

Anatomia de um ataque complexo. Produtora: CISCO Ano: 2017 Disponível em: [“Anatomia de um ataque complexo”](https://www.youtube.com/watch?v=TWX0m8bdwqQ)