

Anatomia de um Ataque Complexo

Vulnerabilidades, Técnicas e Motivação dos Crackers

Ana Carolina Guedes - 823212037

Bruno Alves Tuckmantel - 823130276

Enzzon Gusttavo Oliveira Nascimento - 823153720

Francibelde da silva Lima - 823210292

Grazielle Gomes Da Silva Cardoso - 823116153

Leonardo de Castro Ferreira - 823110769

Thiago cordeiro - 823120734



Introdução

Os ataques cibernéticos estão cada vez mais sofisticados, explorando vulnerabilidades para comprometer sistemas e roubar dados.

O filme Takedown retrata um ataque complexo realizado por Kevin Mitnick, um dos hackers mais famosos do mundo, e sua perseguição pelo especialista em segurança Tsutomu Shimomura.

Nesta apresentação, veremos as motivações do cracker, os tipos e técnicas de ataque utilizados e as estratégias para mitigar essas ameaças.

Vulnerabilidades

Engenharia Social

Manipulação de funcionários para obter credenciais.

Sniffing e Spoofing

Interceptação e falsificação de pacotes de rede.

Exploits em Sistemas

Utilização de vulnerabilidades desconhecidas para acessar servidores.

Senhas Fracas e Falhas de Autenticação

Obtenção de acessos privilegiados sem autorização.

Tipos e Técnicas de Ataque Utilizados

Phreaking

IP Spoofing

Sniffing

MITM

Zero-Day

Engenharia Social



Motivação do Cracker

- Desafio e Reconhecimento – Ele queria provar sua superioridade técnica.
- Curiosidade e Poder – Buscava explorar sistemas para acessar informações sigilosas.
- Invasão sem fins financeiros – Diferente de outros crackers, ele não tinha como objetivo o lucro, mas sim testar os limites da tecnologia.



Passo a Passo Mitnick

-
- Reconhecimento – Coletava informações sobre alvos e sistemas vulneráveis.
 - Exploração de Vulnerabilidades – Identificava falhas em redes e softwares.
 - Invasão – Obtinha acesso não autorizado a servidores e sistemas telefônicos.
 - Escalonamento de Privilégios – Ganhava controle total dos sistemas invadidos.
 - Execução do Ataque – Interceptava comunicações e roubava códigos-fonte.
 - Cobertura de Rastros – Usava IP Spoofing e outras técnicas para se manter invisível.

Como se proteger?

Monitoramento
de Redes

Firewalls e
IDS/IPS

Treinamento
contra Engenharia
Social

Atualização
Contínua

MFA



Conclusão

O caso de Kevin Mitnick mostra como ataques complexos podem explorar múltiplas vulnerabilidades para comprometer sistemas.

A motivação dos crackers pode variar, mas as consequências são sempre graves, podendo causar roubo de dados, prejuízos financeiros e riscos à privacidade.

A segurança cibernética deve ser uma prioridade para indivíduos e empresas, com práticas preventivas e resposta rápida a incidentes.