Anatomia de um ataque complexo

https://video-br.cisco.com/detail/video/5620318141001

https://youtu.be/NF3w2aukgpU?si=qptzx3a_k-Bpbpyq

1. Vulnerabilidades

- **Falta de conscientização do usuário**: O phishing só funciona porque o usuário clicou em um link malicioso e forneceu credenciais;
- **Credenciais fracas ou mal protegidas:** Senhas não criptografadas ou armazenadas em planilhas do Excel tornam o acesso fácil.
- **Ausência de autenticação multifator:** Com apenas usuário e senha, o invasor consegue acesso completo;
- **Configurações inseguras de servidores:** Servidores de e-mail, arquivos ou banco de dados podem não ter restrições adequadas de acesso, permitindo que um invasor use credenciais válidas para se movimentar lateralmente;
- **Falta de monitoramento e alertas:** O invasor consegue copiar e deletar dados sem ser detectado, o que indica ausência de sistemas de detecção de intrusão (IDS/IPS) ou logs analisáveis.

2. Tipos e técnicas de ataques utilizados

- **Reconhecimento**

Técnica: Varredura ativa para identificar sistemas e serviços disponíveis.

- **Acesso inicial**

Técnica: Phishing (envio de e-mails falsos para roubar credenciais).

Técnica: Uso de contas válidas com credenciais comprometidas.

- **Escalada de privilégios / Acesso a credenciais**

Técnica: Exploração de senhas armazenadas de forma insegura (planilhas não criptografadas).

- **Coleta de dados**

Técnica: Extração de arquivos críticos do banco de dados.

- **Exfiltração**

Técnica: Transferência de dados pela rede para o invasor.

- **Impacto**

Técnica: Destruição de dados.

> Observação: Essas técnicas são frequentemente combinadas em ataques complexos e seguem os padrões de TTPs (Táticas, Técnicas e Procedimentos) documentados pelo MITRE.

3. Motivação do cracker

- **Financeira**

Roubo de informações bancárias, dados de cartões de crédito ou dados corporativos valiosos;
Venda de dados roubados no mercado negro;
Ransomware: exige pagamento para devolver acesso aos dados.

- **Política ou estratégica**

Hacktivismo: ataque motivado por causas sociais ou políticas;
Exposição de falhas de empresas ou governos para constrangê-los publicamente.

- **Satisfação pessoal / ego**

Desejo de provar habilidades técnicas, desafiar sistemas de segurança complexos;
“Destruição pelo desafio”: causar prejuízos ou caos apenas para demonstrar poder ou habilidade.

- **Competitiva**

Roubo de propriedade intelectual ou segredos comerciais para obter vantagem no mercado.