Christian Batista de Lima Rego

RA: 824126605

Professor Calvetti USJT – Butantã

Atividade 2 – Identificar no vídeo tema as informações solicitadas.

O cracker invadiu um banco de dados de um centro de pesquisa na Pensilvânia chamado ***Aupticon***, que trabalha com câmeras de rastreamento óptico para carros sem motoristas, através de um site de uma pista de boliches em que os funcionários da empresa participavam.

- Vulnerabilidades: O sistema automatizado de termostato da empresa é eletrônica e conectado a rede, sendo assim, necessitava de defesa. Toda a configuração e senhas de acesso ao termostato foram encontradas pelo cracker no site do próprio fabricante.

Os arquivos não eram criptografados, isso deu liberdade para que o cracker pudesse excluir os backups e criptografar as unidades.

Redes simples, sem sub-redes, tendo todos os arquivos da empresa (Projetos, RH, Documentos jurídicos etc.) em uma só rede.

- Tipos e técnicas de ataques utilizados: O cracker utilizou um ataque de injeção de ***i-frame***, que é um malware antigo que ataca os visitantes do site alvo. Depois de uma semana, um funcionário da empresa acabou tendo o malware instalado em sua máquina ao visitar o site da pista de boliche. Ao levar o notebook a empresa e conectá-lo na rede corporativa, o alvo da acesso total ao cracker através do malware.

- Qual a motivação do Cracker: Ele recebeu 75 bitcoins para realizar os ataques, provavelmente de uma empresa concorrente anunciada ao fim do vídeo.