SISTEMAS COMPUTACIONAIS E SEGURANÇA

Atividade Aula 02 - 03/09

Universidade São Judas Tadeu
2025

Integrantes

Eduardo Irineu de Araújo Santos de Souza - **RA: 825153123**

Fabrício dos Santos Sampaio - **RA: 825142856**

Juan Pablo Silva dos Santos - **RA: 825163816**

Lauanda Jones Almeida da Silva - **RA: 825164056**

Rayanne Raquel Nascimento da Silva - **RA: 825155393**

Kauã Barbosa - **RA:**

Sistemas e segurança Vulnerabilidades

1- O funcionário usa o mesmo notebook para trabalho e para lazer,

2- a empresa permite o funcionário trazer seu próprio notebook á empresa, ao invés de fornecer um especificamente para o trabalho, e o deixando em um local fixo

3- Usar a mesma rede para todos os dispositivos, já que nem todos os dispositivos wi-fi conseguem ter um alto nível de proteção, como foi o caso do termostato mostrado no vídeo, permitindo ele ter acesso a um aparelho de dentro da rede.

4- Por estarem todos os aparelhos em uma mesma rede principal, nem sub-redes, fez com que ao conseguir acesso por meio do termostato, ele conseguisse acessar desde documentos jurídicos, até os projetos em que eles estavam trabalhando.

5- Dados transmitidos sem criptografia (HTTP, Telnet, FTP). tanto para arquivos individuais quanto para cada setor.

Tipos e técnicas de ataque utilizados

Ataque de injeção de i-frame, uma técnica usada para enganar os usuários e fazê-los com que cliquem em um botão inofensivo, mas na verdade estão clicando em algo malicioso e que como consequência faz com que os usuários adicionem o malware em seus computadores. As consequências desta prática são:

● roubos de credenciais;
● autorização de ações sem consentimento;
● disseminação de malware.

Uma das maneiras de injetar um i-frame malicioso são:

● Cross-site Scripting (XSS);
● SQL injection + Defacement;
● comprometendo o servidor;
● CMS e plugins mal desenvolvidos.

Empresas protegem sua rede principal com firewall, mas dispositivos conectados algumas vezes acabam sendo esquecidos e não são monitorados. O invasor acaba explorando essa parte esquecida para entrar por dentro do firewall.

Shadow IT ou exploração de IoT são nomes que são denominados quando um dispositivo esquecido/dentro do firewall é explorado e o ataque seguinte é de movimento lateral (pivoting) para comprometer a rede maior.

Após a shadow IT para obter os arquivos e documentos sigilosos o invasor em alguns casos pode cometer o chamado Ransomware Attack.

● O invasor invade a rede;
● Ganha privilégios de administrador;
● Antes de criptografar os servidores principais, exclui os backups (locais, em rede ou snapschots).;
● Em seguida, criptografa as unidades (arquivos, banco de dados, sistemas).;
● E muitas vezes, deixa notas de resgate exigindo pagamento em criptomoedas.

Há variações de Ransomware que são executados atualmente:

● Ransomware com destruição de backups - impede a recuperação interna e força a negociação;
● Dupla extorsão - além de criptografar e excluir backups, o invasor rouba os dados e ameaça publicá-los se não houver pagamento;
● Tripla extorsão - também ataca clientes fornecedores ou expõe os dados publicamente para aumentar a pressão.

Motivação do cracker

A expressão “motivação do cracker” se refere às razões, interesses ou objetivos que levam uma pessoa a praticar atividades de invasão, quebra de sistemas ou exploração de vulnerabilidades de forma ilegal ou antiética.

Um cracker é diferente de um hacker ético: enquanto o hacker pode usar seus conhecimentos para testar a segurança e até fortalecer sistemas, o cracker busca explorar falhas para benefício próprio ou para causar prejuízos.

Principais motivações do cracker:

Financeira - roubo de dinheiro, dados bancários ou venda de informações.

Pessoal - vingança, disputa, prova de poder contra uma empresa ou indivíduo.

Ideológica/política (hacktivismo) - atacar sistemas para protestar contra governos ou instituições.

Reconhecimento - busca de fama em comunidades clandestinas.

Curiosidade/desafio - prazer em superar barreiras tecnológicas, mesmo sem lucro direto.

Observando atentamente podemos notar que a motivação inicial do hacker em questão era o desejo de desafio e a fraca segurança que o deixou ainda mais animado. Mas quando ele percebeu quanto dinheiro ele poderia ganhar com aquilo que achou, se tornou muito mais motivado.