Relatório Técnico – Exploração de Rede Wireless com Rogue AP e Captura WPA/WPA2

Este relatório apresenta uma Prova de Conceito (PoC) demonstrando a exploração de vulnerabilidades em redes Wi-Fi por meio de um Rogue Access Point configurado com a ferramenta Wifiphisher. O objetivo foi analisar como um atacante pode induzir usuários a fornecerem a chave WPA/WPA2 através de uma página falsa de atualização de firmware.

1. Ambiente e Ferramentas Utilizadas

• Kali Linux como sistema atacante
• Placa de rede USB compatível com modo monitor
• Wifiphisher 1.4 GIT
• Dispositivo vítima (Android)
• Wireshark para captura e análise opcional

2. Configuração do Adaptador Wireless

Para habilitar o modo monitor da placa de rede, foram utilizados os seguintes comandos:

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up
```

3. Execução do Ataque com Wifiphisher

Após configurar o modo monitor, o ataque foi iniciado com:

```
sudo wifiphisher --force-hostapd
```

O SSID escolhido foi “Sineyda” (rede de laboratório).
O cenário selecionado foi “Firmware Upgrade Page”, que simula uma atualização obrigatória do roteador e solicita a senha WPA/WPA2.

4. Funcionamento do Ataque

O ataque seguiu três etapas principais:

1. Desautenticação — a vítima é removida da rede real.
2. Conexão ao Rogue AP — o Wifiphisher cria um AP falso com o mesmo SSID.
3. Phishing — a vítima recebe uma página falsa pedindo a chave do Wi-Fi.

A senha de teste enviada pela vítima foi registrada como:
wfphshr-wpa-password=teste

5. Evidências

Foram observadas requisições HTTP e o envio do formulário contendo a chave WPA simulada.
As imagens utilizadas como evidência encontram-se no repositório Git.

6. Contramedidas

• Ativar WPA3-Personal
• Desabilitar WPS
• Verificar autenticidade de páginas de roteadores
• Utilizar sistemas de detecção de Rogue AP (WIDS/WIPS)
• Conscientização dos usuários

7. Conclusão

O experimento demonstrou a eficiência do ataque Rogue AP aliado à engenharia social.
A captura da chave WPA/WPA2 foi realizada com sucesso, evidenciando a necessidade de medidas avançadas de segurança em redes wireless.