Redes Wireless

Entendendo e Invadindo

Ganesh

- Quem Somos
- Nossas atividades
- Processo seletivo

Kali Linux

- O que é?
- Por que não usaremos?
- Por que Linux?

Ferramentas

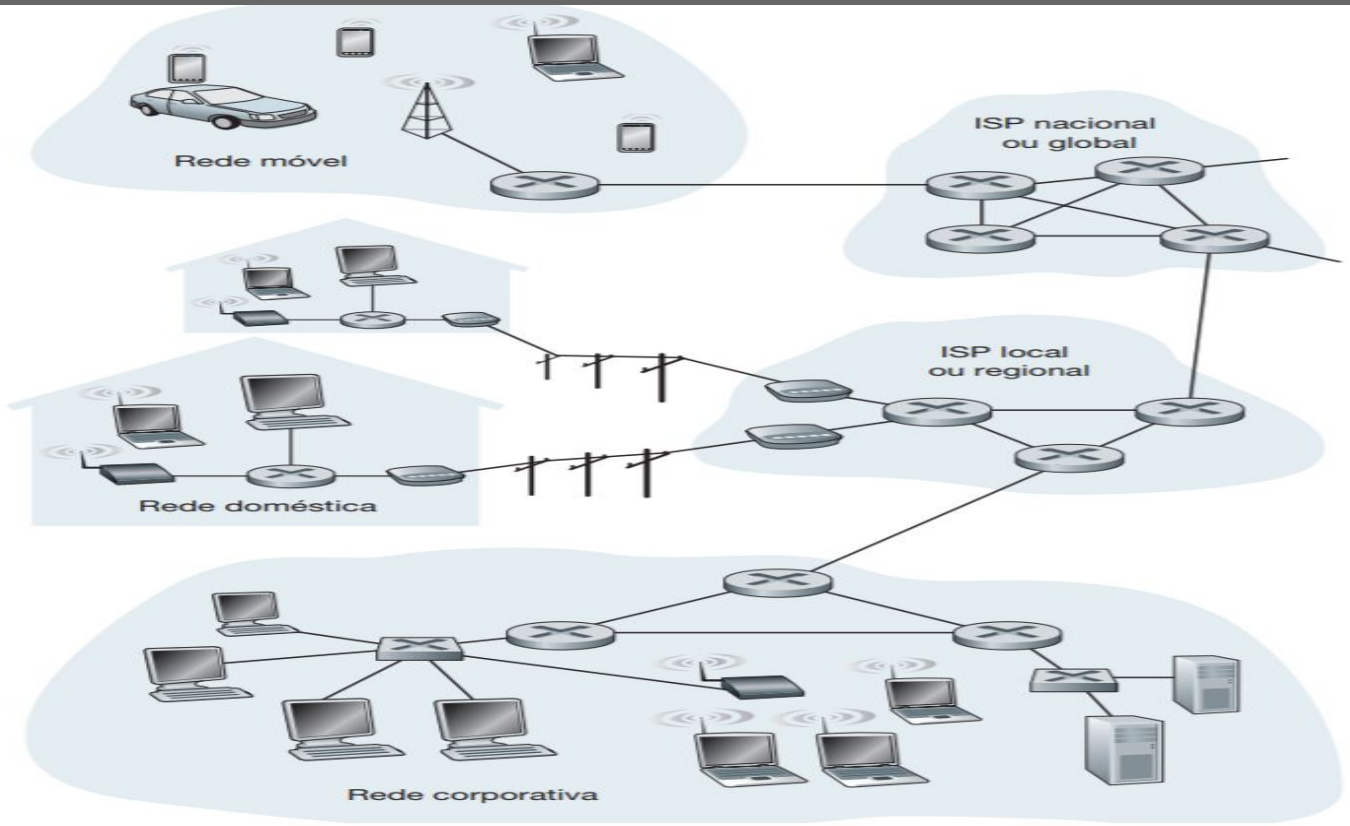
- Wireshark
- Aircrack-ng

Wireshark

Captura de pacotes

Análise da rede

Redes


Rede móvel
ISP nacional
ou global
ISP local
ou regional
Rede doméstica
Rede corporativa

Aircrack-ng

Airmon-ng

Airodump-ng

Aireplay-ng

Aircrack-ng

Mac address

Endereço único

“Imútavel”

Padronizada no hardware

O que é Wi-Fi?

- Tecnologia de comunicação sem fio
- Wi-Fi Alliance
- Baseado no padrão IEEE 802.11


Para que serve os padrões IEEE?

IEEE 802.3 e IEEE 802.11

- Definem métodos de acesso e controle para redes
- Camada física e camada Enlace

Monitor mode

- Iwconfig
- Manage mode/ monitor mode

Começando a prática!

Airmon-ng

Troca a funcionalidade da placa de rede para monitor mode

Airodump-ng

Captura de pacotes de frames brutos 802.11

Aireplay-ng

Verificar a possibilidade de injetar pacotes

Fake access point

- Wi-Fi pumpkin

WPS

Possível método de quebra

Deauth

- Desafio

ICMC USP SÃO CARLOS

GANESH

Redes Wireless

Um pouco mais seguras

WEP

- Primeiro protocolo ratificado.
- Consistia em 24 bits de IV, e 40 bits de senha
- Autenticação por desafio:

Falhas de segurança

- IV inseguro
- IV pequeno
- Autenticação falha

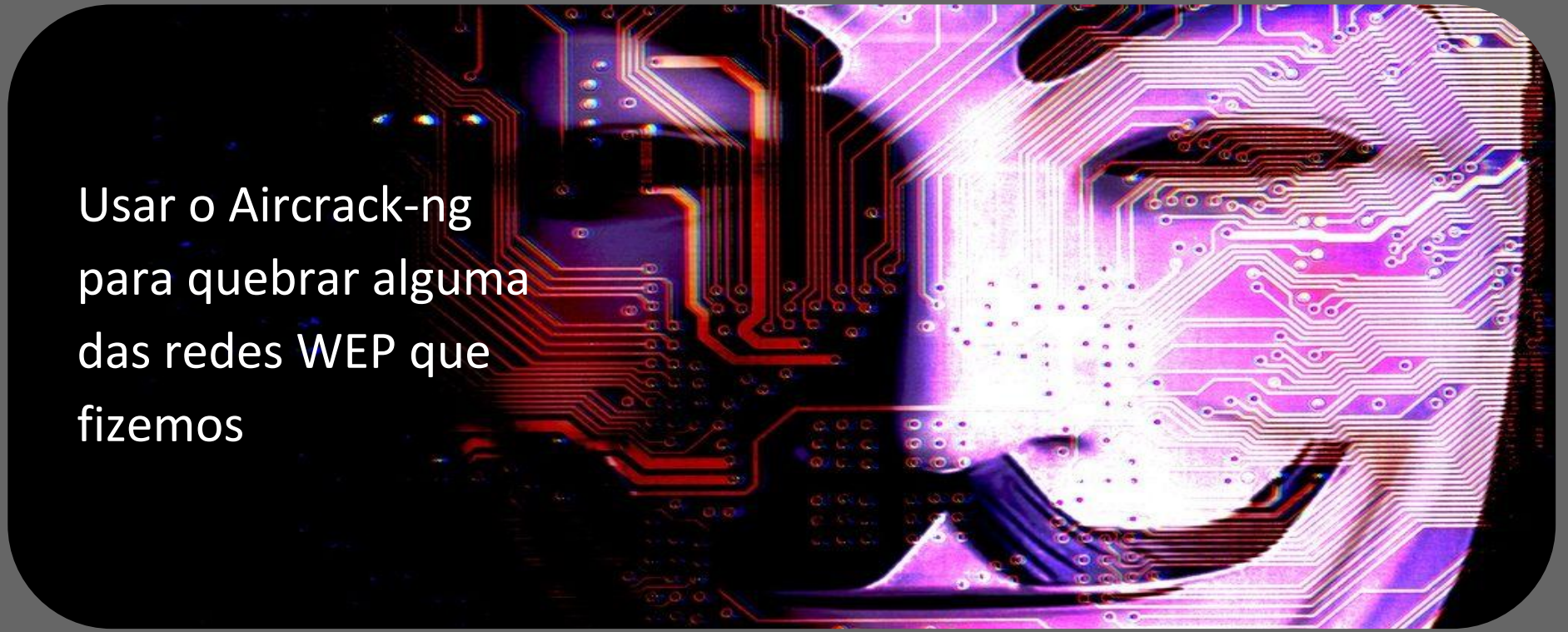
Falhas de segurança

Como se aproveitar delas?

1. Chopping attack

2. FMS

Mãos a massa



Usar o Aircrack-ng para quebrar alguma das redes WEP que fizemos


Como deixamos WI-FI protegida?

Solução temporaria

O novo protocolo (mais seguro) ainda não está pronto para ser homologado

E o que fazer com todos os hardwares que já foram vendidos?

Protocolo Wifi Protected Acess (WPA)

Melhoria da WPA

Temporary Key Integrity Protocol (TKIP):

Pacotes podem ser ordenados temporalmente

Melhorias com o IV

Melhora na autenticação de mensagem

Novo Handshake

- AP manda um número aleatório único (ANonce)
- Cliente responde com outro número aleatório único (SNonce) e uma confirmação de integridade de mensagem (MIC), calculada usando a senha da internet e ANonce
- Se o MIC estiver correto, o AP manda a chave da sessão atual, junto com outro MIC
- Cliente confirma que recebeu a mensagem (ACK)

Novo Handshake

Como se aproveitar disso?

Quase todas as informações para conseguir acesso são passadas, assim como o resultado.

Novo Handshake

Problemas:

- Hashes não podem ser desfeitas.

Novo Handshake

Problemas:

Hashes não podem ser desfeitas.

Solução:

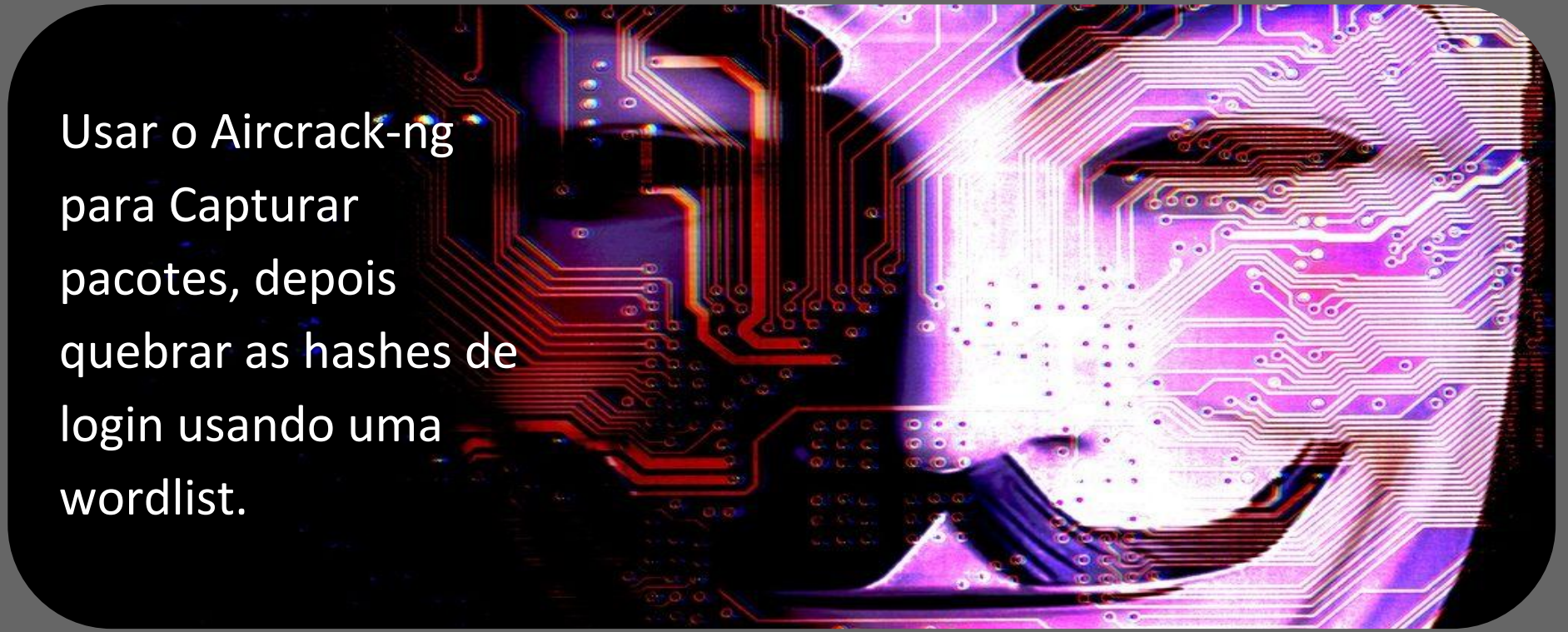
Testar todas as possibilidades!

Wordlists

- Crunch:
  - Gerar wordlists simples

- Wordlists reais:
  - Portable-Wordlists

Maos a massa



Usar o Aircrack-ng para Capturar pacotes, depois quebrar as hashes de login usando uma wordlist.

Wordlists++

Senhas parecidas, mas não iguais as wordlists?

Rule Engines

- Hashcat

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br