Segurança básica de redes Wi-Fi

Víctor Orozco

11 de Dezembro de 2013

Agenda

Segurança

Redes sem fio

Wi-Fi

Demo

¿Como segurar uma rede sem fio?

Referencias

Segurança

Segurança

- Em um sentido amplio a segurança significa proteger os nossos ativos
  - Proteger os nossos sistemas contra atacantes
  - Proteger o nosso prédio contra desastres naturais
  - Proteger a nossa carteira de roubos na boate

Segurança informação

- Dependendo do contexto assim tem que ser as medidas de segurança
  - Ativos físicos: Computadores, carros
  - **Ativos lógicos: Arquivos de dados, código fonte de aplicativos**
  - Ativos humanos: Seres humanos a base de qualquer negocio

Redes sem fio

Sistemas de transmissão

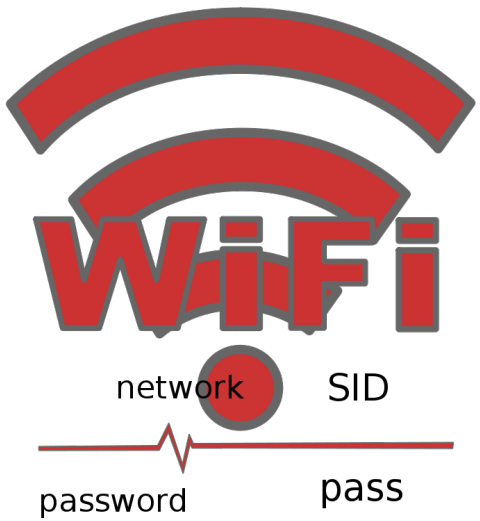
- **Rádio**
- Infravermelho
- Laser

Tipos de ondas

- **Direcional**
- Não direcional

Tecnologias

- Bluetooth
- ZigBee
- WiMax
- **Hotspot**
- **Wi-Fi**



Modelos de rede

- Fechados
  - Wpan (Bluetooth)
  - **Wlan (Wi-Fi)**
- Abertos
  - Wman (Rede de redes)
  - Wwan (GSM, LTE, 3G, etc.)

Problemas

Problemas

- A área de cobertura Wi-Fi excede os limites físicos da nossa sala

Problemas

- A área de cobertura Wi-Fi excede os limites físicos da nossa sala
- As pessoas ”ruins”tentam aproveitar estes ”excedentes”pra invadir a rede

Problemas

- A área de cobertura Wi-Fi excede os limites físicos da nossa sala
- As pessoas ”ruins”tentam aproveitar estes ”excedentes”pra invadir a rede
- Melhor cenário = pegar internet de graça

Problemas

- A área de cobertura Wi-Fi excede os limites físicos da nossa sala
- As pessoas ”ruins”tentam aproveitar estes ”excedentes”pra invadir a rede
- Melhor cenário = pegar internet de graça
- Pior cenário = pegar informação privada

Terminologia

- Claridade da sinal: Potencia, distancia, interferências, linha de visão;
- ESSID: Nome da rede;
- BSSID: Endereço MAC da rede;
- Beacon: Anuncio da presença de uma rede Wi-Fi;
- Canais: Divisões da sinal (2.4/5 Ghz) em un numero de bandas;
- Cifrado+Autenticação: OPN, WEP, WPA/WPA2 (CCMP, WRAP, TKIP, WEP, WEP40, WEP104, MGT, SKA, PSK)

WEP

- Não foi criado por expertos em cifrado e segurança.
- Algoritmo RC4 é a principal debilidade.
- 24 bits – precisam-se menos de 5000 pacotes pra ter um 50% de probabilidade de pegar a senha.
- Alem disso não existe uma comprobação de integridade de pacotes apropriada. (CRC32 linearidade não criptográfica).

WPA/WPA2

- Solução temporal da Wi-Fi Alliance.
- 802.11i da IEEE = WPA2
- Autenticação mediante PSK pra entornos domésticos (senha) e suporte pra servidores de autenticação (RADIUS).
- A principal diferença é o algoritmo WPA-TKIP(baseado RCA4) e WPA2-CCMP(baseado em AES).
- A vulnerabilidade do protocolo não radica no algoritmo mas na senha (handshake), ja que se o handshake é capturado e a senha fraca ...

Tipos de ataque

Passivos

- Packet sniffing (captura de pacotes)
- Analise de padrões de trafego

Tipos de ataque

Passivos

- Packet sniffing (captura de pacotes)
- Analise de padrões de trafego

Ativos

- Suplantação (clonar uma PC)
- Rogue AP/Evil twin (clonar o AP para receber a autenticação)
- Modificação de pacotes (MTIM)
- Reautuação - injeção de pacotes pra simular trafego legitimo
- Denial of service - só pra incomodar
- Ataques de dicionario / força bruta

Demo

- Ferramentas: Funtoo Linux, Aircrack
- airodump: Sniffing de pacotes.
- aireplay: Injeção de pacotes (aumentar o trafego e a velocidade do ataque).
- aircrack: A partir dos pacotes recolhidos ele faz uma analise estatística (WEP), força bruta/dic (WPA)

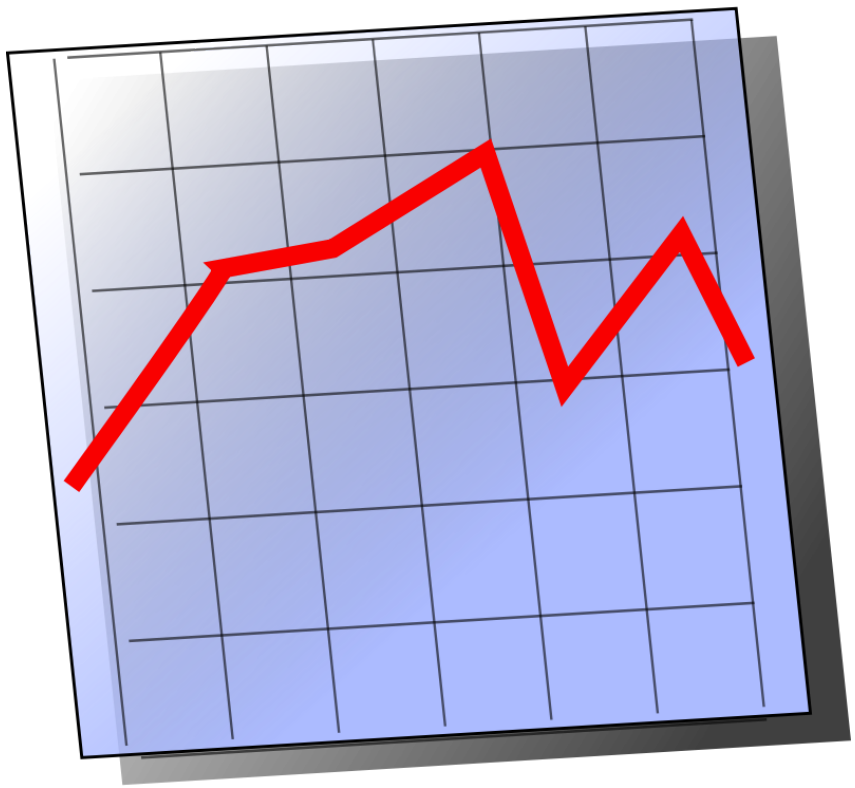
Demo WEP

1. Ativar o modo monitor na placa.
2. Descobrir os detalhes das redes por perto.
3. Iniciar a captura da rede desejada (BSSID, ESSID, canal)
4. Injetar trafego baseado nos dados capturados.
5. Pegar a senha WEP

Demo WEP

1. Ativar o modo monitor na placa.
2. Descobrir os detalhes das redes por perto.
3. Iniciar a captura da rede desejada (BSSID, ESSID, canal)
4. Injetar trafego baseado nos dados capturados.
5. Pegar a senha WEP
6. Barbada!

Demo WEP



Demo WPA

1. Ativar o modo monitor na placa.
2. Descobrir os detalhes das redes por perto.
3. Iniciar a captura da rede desejada (BSSID, ESSID, canal)
4. Forçar ou aguardar por um handshake.
5. Atacar o handshake capturado com dicionario.

Demo WPA

1. Ativar o modo monitor na placa.
2. Descobrir os detalhes das redes por perto.
3. Iniciar a captura da rede desejada (BSSID, ESSID, canal)
4. Forçar ou aguardar por um handshake.
5. Atacar o handshake capturado com dicionario.
6. Não tão barbada . . .

Demo WPA

WPA/WPA2

Segurança nível 0

- Mudar a senha original do AP.
- Mudar o SSID original.
- WPA-PSK+senha segura, nunca WSP.

WPA/WPA2

Segurança nível 0

- Mudar a senha original do AP.
- Mudar o SSID original.
- WPA-PSK+senha segura, nunca WSP.

Segurança nível 1

- Ocultar SSID (deshabilitar broadcast SSID) - Engenharia social
- Configurar filtrado MAC - Mac spoofing
- Mudar as senhas de forma regular - Furto de dispositivos, dicionario
- Desabilitar DHCP - Uma vez dentro da rede é a ultima barrera de comunicação
- Scheduler WLAN/ Desligar - Dicionario
- Diminuir a sinal do roteador ;-)

Obrigado!

- tuxtor@shekalug.org
- http://tuxtor.shekalug.org
- http://github.com/tuxtor/slides

Referencias I


Andress, J. (2011).
The basics of information security understanding the fundamentals of InfoSec in theory and practice.
Syngress, Waltham, MA.