Ementa do curso de Wireless

Aula 1

- Sobre o curso de *Wireless*
- A lei Carolina Dieckmann
- O padrão IEEE
    - As diversas emendas
    - A emenda IEEE 802.11
        - 802.11
        - 802.11b
        - 802.11a
        - 802.11n
- Terminologia em redes sem fio
    - DS, WDS, BSS, BSA, AP, STA, ESS, ESSID, BSSID, IBSS
- Tipos de rede sem fio
    - Infra estrutura x Ad Hoc
- Modos de operação
    - Diferenças entre
        - Modo Promíscuo x Managed x Monitor
- Kali Linux
- O comando iwconfig
    - Principais opções
- O programa Airodump-ng
    - Principais campos
- Laboratório *Wireless*
    - Capturando tráfego remoto com o modo monitor

Aula 2

- Funcionamento da rede *Wireless*
- O frame *wireless*
- Estudo detalhado sobre o frame *wireless*
    - O campo Header
        - Frame Control
            - Protocol
            - Type: Data, Control, Management
            - SubType
            - ToDS
            - FromDS
            - More Fragment
            - Retry
            - Power Management
            - More Data
            - Protected Frame
            - Order
        - Duration/ID
        - Adress 1,2,3,4
        - Sequence Control
        - QOS Control
        - Frame Body
    - O campo Data
    - O campo FCS
- Laboratório Wireshark
    - Capturando os frames *wireless*

Aula 3

- Principais sistemas de criptografia
  - OPN
  - WEP
  - WPA/WPA2 Personal
- A criptografia OPN
- Laboratório Wireshark
  - Captura do processo de autenticação OPN
- A criptografia WEP
  - O algoritmo XOR
  - O processo de criptografia
  - O processo de descriptografia
- Formas de autenticação WEP
  - OPN
  - SKA
- Laboratório Wireshark
  - Captura do processo de autenticação WEP OPN
  - Captura do processo de autenticação WEP SKA
- A criptografia WPA/WPA2
  - Autenticação WPA/WPA2 Personal
    - O processo 4-way handshake
    - A chave PTK
  - Vulnerabilidade
    - Reproduzir a chave PTK usando dicionário

Aula 4

- A suíte aircrack-ng (teoria + laboratório)
  - Airmon-ng
  - Airodump-ng
  - Aircrack-ng
  - Aireplay-ng
  - Airbase-ng
  - Packetforge-ng

Aula 5

- Quebra de senhas (aircrack-ng)
  - WEP
    - O método FMS/KOREK
    - O método PTW
  - WPA/WPA2 Personal
    - Dicionário
- Laboratório WEP OPN
  - Quebra de senhas WEP OPN com clientes
    - 64 bits
    - 128 bits
    - 152 bits
  - Quebra de senhas WEP OPN sem clientes
- Laboratório WEP SKA
  - Quebra de senhas WEP SKA
- Laboratório WPA/WPA2 Personal
  - Quebra de senhas WPA/WPA2 Personal (via dicionário)

Aula 6

- Ataques específicos contra WPA/WPA2 Personal
- Geração de wordlist
  - CUPP
  - Crunch
- Quebra do WPA/WPA2 usando John the ripper + Aircrack-ng
- A chave PMK
  - Teoria
  - Pré calcular a chave PMK usando Rainbow Tables
- Quebra do WPA/WPA2 via Rainbow Tables
  - Genpmk
  - Cowpatty
  - Pyrit
- Captura do tráfego com Wireshark/airdecap-ng
  - WEP
  - WPA/WPA Personal

Aula 7

- Burlando autenticações
    - Redes ocultas (Hidden SSID’s)
    - Filtros de MAC Address (MAC Filter)
- Atacando a infra estrutura
    - Ataques contra o AP
        - Laboratório Hydra
    - Negação de serviço
        - Deauth
        - Association/Authentication Flood

Aula 8

- Ataques de clonagem (airbase-ng)
    - Evil Twin
    - MissAssociation
    - Rogue AP
    - Honeypot
- SET – Social Engineering Toolkit
    - Páginas phishing
        - Credential Harvester Attack
- Man in the Middle
    - Definição
    - Laboratório Ettercap-ng
        - Arp Spoofing
        - DNS Spoofing
- Quebra de certificados digitais
    - SSLSTRIP
- Defendendo-se contra o ARP Spoofing
    - Arpon

Aula 9

- Ataques avançados
  - WPA/WPA2 Enterprise
  - O protocolo WPS
- Redes Enterprise
  - Funcionamento
  - Servidor Radius Falso
    - FreeRadius WPE + Hostapd
  - Quebra da autenticação
    - Asleap
- O protocolo WPS
  - Definição
  - Modos de operação
    - Push-button-connect
    - PIN
  - O número PIN
    - Funcionamento
  - Quebra de senhas WPA/WPA2 PSK via WPS
    - wash + bully

Aula 10

- Documentação técnica
- Realizando um *Wireless pentest* (teoria + laboratório)
  - Realizando a captura remota de logins (nome de usuário + senha) em um sistema Hotspot
    - Escopo
    - Descoberta
    - Ataque
    - Contra medidadas
- Criptografia de dados
  - Criptografando arquivos/pendrives
    - Truecrypt