Webamooz Wireless Penetration Testing

By Milad Kahsari Alhadi

بسم الله الرحمن الرحیم و به نستعین، انّه خیرُ ناصر و معین. خدمت تمامی دنبال‌کنندگان اندیشکده مجازی امنیت تبادل اطلاعات آیو، عرض سلام و تحیت دارم.

در این دوره که سطح آن مقدماتی تا متوسط است، مباحث امنیت شبکه وایرلس و مخابرات مانند تاریخچه توسعه شبکه و مخابرات (با نگاه نظامی)، مفاهیم پایه مخابرات (مانند سیگنال، فرکانس، موج، پروپگیشن، مدولاسیون، آنتن‌ها)، «اصول اینترنت‌کاری / Fundamental of Internetworking»، لایه‌بندی شبکه، پروتکل‌های شبکه، ارتباطات و آشکارسازی کدهای سطح ماشین، شبکه‌بندی سطح ماهواره، شبکه‌بندی سطح موبایل (هسته شبکه 2G/3G/4G)، مسائل نظامی با محوریت شبکه وایرلس، حملات ایرگپ بر علیه ساختار ICS (حملات حرارتی، صوتی و الکترومغناطیس)، ایجاد تداخل سیگنال (Signal Jamming)، حملات مردی در میان، حملات منع سرویس، حملات بر علیه سرویس بلوتوث و ... مورد بررسی قرار گرفته است.

انشالله این دوره، برای شما و تمامی عزیزان فعال در صنعت امنیت کشور مفید باشد. خواهشمند هستم، با تهیه این محتوا از این حرکت و همچنین به منظور تولید محتواهای آموزشی تخصصی مشابه دیگر، حمایت کنید. سرفصل دوره آزمایش نفوذپذیری شبکه‌های وایرلس به شرح زیر است:

1. Basic of Satellite Telecommunication
    - Orbital Altitudes of Earth
        - High Earth Orbit
        - Medium Earth Orbit
        - Low Earth Orbit

- Frequency band of Satellite Communication
  - Super High Frequency Subchannels
    - L-Band
    - S-Band
    - K-Band
  - Frequency Multiplexing
    - Frequency Division Multiplexing (FDM)
    - Time Division Multiplexing (TDM)
    - Code Division Multiple Access (CDMA)
- Satellite Communication Services
  - Fixed Satellite Service
    - Multistage Balistic Rocket
    - Simorgh-2
    - GPS
    - GLONASS
    - Galileo
    - Compass
  - Inter Satellite Service
    - Interplant Communication
    - Mars Rover Control
  - Earth Exploration-Satellite Service
  - Satellite Switching on the Ground
  - Satellite Switching on the Space
- Attacks on Satellite Communication
  - Medium Range Anti Satellite Systems
    - Speed Calculation of Object
    - Covert MM to Mach
    - ASAT Nudol Project of Russia
  - Signal Jamming

2. Computer Networks Basics

- Baseband and Passband Communication
- Network Protocol Stack
  - Network Protocol Stack – Layers
  - Network Protocol Stack – Protocols

        - Network Protocol Stack – Interfaces
    - Why Network Designed with Layered Scheme
    - Networking Protocol Stack
        - TCP/IP Protocol Stack
        - OSI Protocol Stack
        - Other Protocol Stack
        - Service Categories and Reliability
            - Transmission Control Protocol
            - User Datagram Protocol
        - Data Injection in ICMP Packets
        - Connection Oriented – TCP
        - Connectionless – UDP

3. Mobile Phone System

- Mobile Phone Evolution
    - 1s Generation – AMPS
    - 2s Generation – GSM
    - 3s Generation – UMTS
    - 4s Generation – LTE
- Mobile Communication
    - Introduction to the Mobile Communication
    - Cellular Network Communication
- Advanced Mobile Phone System – Amps
    - A-AMPS
    - D-AMPS
    - Base Transceiver Stations
    - Base Station Switching Center
    - Mobile Switching Center
    - Signaling System no. 7 – SS7
- Global System for Mobile – GSM
    - Global System for Mobile Specification
    - Digital Gaussian Minimum Shift Keying
- Network and Switching Subsystem
    - Mobile Switching Center

        - Home Location Register
        - Visitor Location Register
        - NSS Elements
        - Gateway MSC
        - GSM Call Process
    - High Speed Downlink Packet Access
    - High-Speed Uplink Packet Access
    - Long Term Evolution (LTE)
        - LTE Specification
        - LTE Forecast
        - Evolution of Mobile Standards

4. Advanced Wireless Sniffing

- Introduction to the Wireless
    - Wireless Topology
    - Wireless Range
    - Wireless Security Protocols
    - Scanning for Open and Hidden SSID's
    - Creating Password Dictionary
    - Cracking Wi-Fi Passwords
- Advanced Wireless Sniffing
    - Wireshark – Capturing Traffic
    - NetworkMiner – Extract Files and Data
    - Suricata – Analysis the Captured Traffic
    - DarkStat – Analyzing Network Traffic
    - Wireless Network Detector
    - Wireless Network Sniffer

5. Man in the Middle Attacks

- What is MiTM
    - Introduction to the MiTM Attack
    - MiTM Attack Scenario
- Man in the Middle Attack
    - ArpSpoof – Setup Between Our Victim and Router

- DriftNet – Displaying Victims Image Traffic
- URLSnarf – Capturing Website Information_Data

6. Denial of Service Attacks

- Introduction to DOS
  - What is DOS Attacks?
  - DDOS and DOS Attacks
  - DDOS and DOS Scenario
- Denial of Service Attack
  - Volume-Based DoS
    - TCP Flood
    - UDP Flood
    - ICMP Flood
  - Protocol-Based DoS
    - Syn Attack
    - Fragmented Attacks
    - Ping of Death
    - Smurf Attack
  - Application Layer Based Attacks - DoS
    - Buffer Overflow
    - Ability Server Vulnerability Analysis
    - Fuzzing