‹ Dashboard

WiFi Pentesting Bootcamp

These video recordings are from our live online bootcamp

Session I

The following topics are covered

- WiFi protocols, standards and amendments
- Bands and Channels
- Packet Analysis
- WiFi trafficking sniffing
    - Local Capture
    - Remote Capture
- WiFi Network/device Recon
- Basic Attacks on Open WiFi
- Creating honeypot with Hostapd
- Interacting with WiFi system using Linux CLI

3:28:47

List of labs covered during the session (and homework):

- WiFi Security: Traffic Analysis I (https://attackdefense.com/challengedetails?cid=1141)
- WiFi Security: Traffic Analysis II (https://attackdefense.com/challengedetails?cid=1143)
- WiFi Security: Traffic Analysis III (https://attackdefense.com/challengedetails?cid=1142)
- WiFi Recon I (https://attackdefense.com/challengedetails?cid=1264)
- WiFi Recon II (https://attackdefense.com/challengedetails?cid=1254)
- Preferred Network List (PNL) Basics (https://attackdefense.com/challengedetails?cid=1264)
- Bypassing MAC Filter (https://attackdefense.com/challengedetails?cid=1267)

The following topics are covered

- Working of WEP Security scheme
- WEP Cracking
- WPA/WPA2-Personal security scheme
- 4-way handshake
- Cracking WPA/WPA2-PSK passphrase
- Optimizing dictionary Attack
- AP-less attacks

2:29:51

List of labs covered during the session (and homework):

- WEP Cracking (https://attackdefense.com/challengedetails?cid=30)
- WPA PSK Cracking (https://attackdefense.com/challengedetails?cid=31)
- WPA2 PSK Cracking (https://attackdefense.com/challengedetails?cid=41)
- WPA2 PSK Cracking II (https://attackdefense.com/challengedetails?cid=42)
- WEP Cracking Advanced (https://attackdefense.com/challengedetails?cid=66)
- WPA2 PSK Cracking III (https://attackdefense.com/challengedetails?cid=67)
- Live Cracking: WPA-PSK (https://attackdefense.com/challengedetails?cid=1255)
- Pivoting over WiFi: WEP (https://attackdefense.com/challengedetails?cid=1330)
- Pivoting over WiFi: WPA PSK (https://attackdefense.com/challengedetails?cid=1329)
- Live Cracking: WPA2-PSK (https://attackdefense.com/challengedetails?cid=1256)
- AP-less WPA2-PSK Cracking (https://attackdefense.com/challengedetails?cid=1257)

Session III

The following topics are covered

- EAP and 802.1x
- Authentications and Encapsulation methods
- Working of PEAP-MSCHAPv2 and TTLS-PAP
- Honeypot attacks on Enterprise networks using
  - Hostapd-mana
  - EAPHammer
- Karma Attacks
- Privacy issues of active probing (and PNL)

2:27:41

List of labs covered during the session (and homework):

- WPA/WPA2 PEAP Cracking (https://attackdefense.com/challengedetails?cid=43)
- Evil Twin (https://attackdefense.com/challengedetails?cid=1269)
- Evil Twin - WPA Enterprise (Mana) (https://attackdefense.com/challengedetails?cid=1290)
- Evil Twin - WPA Enterprise (EAPHammer)(https://attackdefense.com/challengedetails?cid=1291)
- Mana: Attacking PEAP-GTC (https://attackdefense.com/challengedetails?cid=1285)
- Karma Attacks (Mana) (https://attackdefense.com/challengedetails?cid=1301)
- Mana: Attacking PEAP-MSCHAPv2 (https://attackdefense.com/challengedetails?cid=1286)
- Karma Attacks (EAPHammer) (https://attackdefense.com/challengedetails?cid=1302)
- Mana: Attacking TTLS-PAP (https://attackdefense.com/challengedetails?cid=1287)
- Mana: Attacking TTLS-CHAP (https://attackdefense.com/challengedetails?cid=1288)
- Mana: Attacking TTLS-MSCHAPv2 (https://attackdefense.com/challengedetails?cid=1289)

Session IV

The following topics are covered

- WiFi Pivoting
- Approaches to target WiFi Access Point
- PEAP-Relay Attack
- Introduction to WPA3 Security scheme
- Improvements: OWE, SAE and DPP
- How DHE and Dragonfly handshake works
- Possible Attacks on WPA3
- Overview of FragAttacks

3:01:44

List of labs covered during the session (and homework):

- Pivoting over WiFi: WPA Enterprise (https://attackdefense.com/challengedetails?cid=1332)
- Pivoting over WiFi: PEAP Relay (https://attackdefense.com/challengedetails?cid=1341)