Wi-Fi Penetration Testing

Author Gus Khawaja

Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com

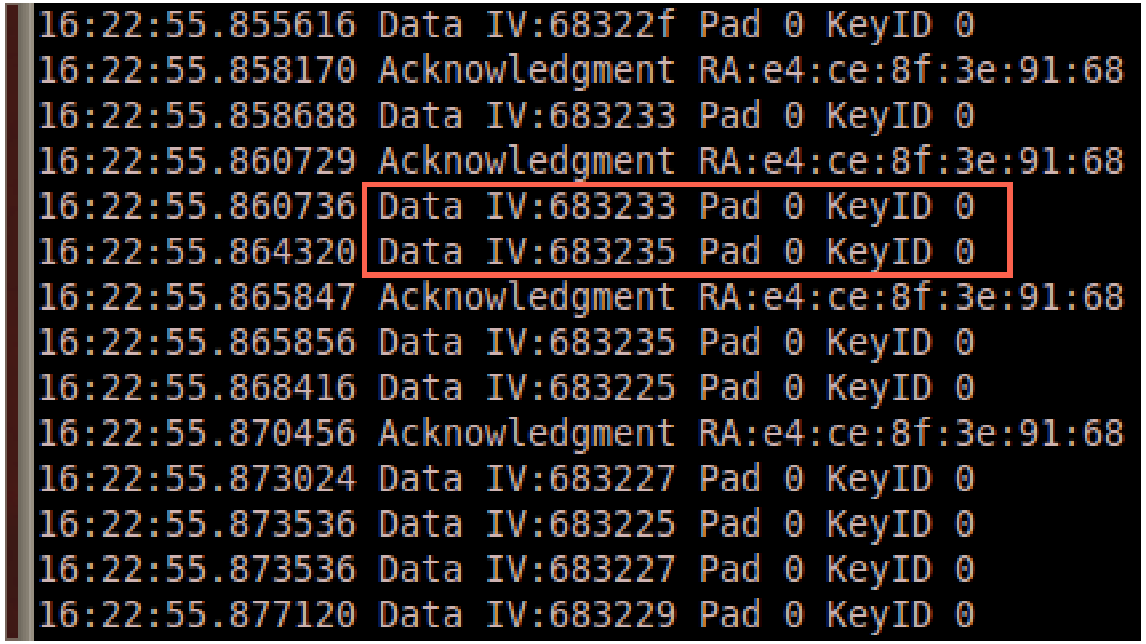
Wireless Reconnaissance

Demo Workflow

- List wireless interfaces
- Start the monitor mode
- Listing wireless networks

WEP Testing

WEP Flaw



```
16:22:55.855616 Data IV:68322f Pad 0 KeyID 0
16:22:55.858170 Acknowledgment RA:e4:ce:8f:3e:91:68
16:22:55.858688 Data IV:683233 Pad 0 KeyID 0
16:22:55.860729 Acknowledgment RA:e4:ce:8f:3e:91:68
16:22:55.860736 Data IV:683233 Pad 0 KeyID 0
16:22:55.864320 Data IV:683235 Pad 0 KeyID 0
16:22:55.865847 Acknowledgment RA:e4:ce:8f:3e:91:68
16:22:55.865856 Data IV:683235 Pad 0 KeyID 0
16:22:55.868416 Data IV:683225 Pad 0 KeyID 0
16:22:55.870456 Acknowledgment RA:e4:ce:8f:3e:91:68
16:22:55.873024 Data IV:683227 Pad 0 KeyID 0
16:22:55.873536 Data IV:683225 Pad 0 KeyID 0
16:22:55.873536 Data IV:683227 Pad 0 KeyID 0
16:22:55.877120 Data IV:683229 Pad 0 KeyID 0
```

WEP Information

- ESSID
- BSSID
- Channel
- Client’s MAC

WPA/WPA2 Testing

Bypassing Hidden ESSID

Getting ESSID

- Sniffing
- De-authentication

Summary

Wireless Reconnaissance

WEP Testing

WPA/WPA2 Testing

Bypassing Hidden ESSID