Wireless Pentesting Practical Notes

Last update: 8/7/18 - Ivan

Manually Change MAC:

```
root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 hw ether 00:11:22:33:44:55
root@kali:~# ifconfig wlan0 up
root@kali:~# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 54  bytes 10166 (9.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2304 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Specify 2.4 GHz or 5 GHz in airodump (a is the 5 GHz band):

```
root@kali:~# airodump-ng --band a mon0
```

De-Auth:

Specific Client

```
root@kali:~# aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 00:21:27:FD:61:06 mon0
```

- -a = AP MAC
- -c = Client MAC

Multiple Clients

```
root@kali:~# aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 00:21:27:FD:61:06 mon0 &> /dev/null &
[1] 14776
root@kali:~# jobs
[1]+  Running                 aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 00:21:27:FD:61:06 mon0 &> /dev/null &
root@kali:~# aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 80:E6:50:22:A2:E8 mon0 &> /dev/null &
[2] 14789
root@kali:~# jobs
[1]-  Running                 aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 00:21:27:FD:61:06 mon0 &> /dev/null &
[2]+  Running                 aireplay-ng --deauth 100000 -a 64:7C:34:A4:BB:B2 -c 80:E6:50:22:A2:E8 mon0 &> /dev/null &
```

- Use **&** at the end of the command to run it in the background
- Use **&>/dev/null** to redirect the output to null
- Use **jobs** to see commands running in the background
- Use the **kill** command to stop a specific command
    - **Kill All**
    - **Kill %**(*JOB NUMBER*)

All Clients

- Run airodump with specific AP & channel (--bssid and --channel) > launch aireplay to deauth
- In aireplay, omit the -c argument (the client argument).

Wireless Pentesting Practical Notes

Last update: 8/7/18 - Ivan

Cracking WPA/WPA2

Capturing the handshake

Handshake packets are sent every time a client associates with the target AP. So to capture it we are going to :

1. Start airodump-ng on the target AP:

```
> airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface]
Ex: airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0
```

2. Wait for a client to connect to the AP, or deauthenticate a connected client (if any) for a very short period of time so that their system will connect back automatically.

```
> aireplay-ng --deauth [number of deauth packets] -a [AP] -c [target] [interface]
Ex: aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c 00:AA:11:22:33:44 mon0
```

Notice top right corner of airodump-ng will say “WPA handshake”.

Cracking with wordlist

- Aircrack:

```
> aircrack-ng [HANDSHAKE FILE] -w [WORDLIST]
ex: aircrack-ng is-01.cap -w list
```

Advanced:

- Saving & starting from cracking progress
  - Display wordlist on screen:

```
root@kali:~# john --wordlist=wpa-wordlist --stdout
```

  - Redirect output and use it as input to aircrack-ng:

```
root@kali:~# john --wordlist=wpa-wordlist --stdout  --session=upc | aircrack-ng -w - -b 00:10:18:90:2D:EE handshake-01.cap
```

  - Restoring progress from the save above:

```
root@kali:~# john --restore=upc | aircrack-ng -w - -b 00:10:18:90:2D:EE handshake-01.cap
```

Preparation for the engagement:

GOVERNANCE

Wireless Penetration Test Process Overview:

1. Initiation / Pre-Engagement:
   a. Define scope
   b. Collect Environment Information
   c. Schedule Tests
   d. Communicate to Stakeholders
   e. Get client formal sign-off
2. Information Gathering:

. Identify wireless networks

a. Identify network segments
b. Identify technologies used
c. Identify protocols
d. Create a target list

3. Vulnerability Identification:

. Identify potential attack vectors
a. Identify exploitations

4. Exploitation (situational/optional):

. Test potential vulnerabilities without breaking anything
a. Document successful attacks and potential attacks

5. Reporting:

. Describe vulnerabilities found
a. Describe potential issues
b. Describe confirmed issues
c. Define risk
d. Propose recommendations

Initiation / Pre-engagement Process:

- Scope: Analyze all the wireless networks in the company, determine the risk of the current wireless networks, and propose improvements.
- Environmental Info (example):
  - XOXO Laptops (WPA2/WPS)
  - XOXO Cameras (WPE)
  - XOXO Guest Wi-Fi (open/portal authentication)
  - XOXO Cafeteria (open)
- Schedule Tests
  - Communicate with managers, admins, and teams and agree on dates
  - Client sign off
  - Tests are ready to begin

Information Gathering Process:

- Packet Capture:
  - Utilize monitor mode: listen to any traffic independent of the mac address
  - Utilize packet injection capable network cards:
    - Alfa AWUS036NHA
    - Alfa AWUS036NH
    - TP-LINK TP-WN722N
    - D-Link DWL-G132
  - Airmon Suite:
    - Airmon-ng: enabling monitor mode
    - Airodump-ng: enables eavesdropping & capture packets in promiscuous mode
    - Aireplay-ng: packet injection, enables replay of captured packet (i.e. replay an authentication packet to simulate a client connecting to the network)
    - Aircrack-ng: crack wireless passwords captured

Identifying Target Networks:

- Wireless mapping
  - Simple solution: walking around with airmon-ng running, document findings
  - Fancy solution:Heatmapper
- Identify Rogue APs
- Identify Hidden Wireless Networks

Identifying & Exploiting Vulnerabilities:

- Common Wireless Vulnerabilities
  - Analytic Attacks

    - Packet Injection
    - Weak Credentials
    - Eavesdropping
    - Brute-Forcing
    - Authentication Bypass
- Make sure open networks are segregated, no access to servers, Document everything.
    - If you find an open network:
        - Try to ping internal servers, DCs, etc.
            - If any response, attempt to access server
        - Wireshark to capture traffic
            - Utilize filters to extract info, find unsecure protocols, etc.
    - Utilize aircrack on any WEP findings

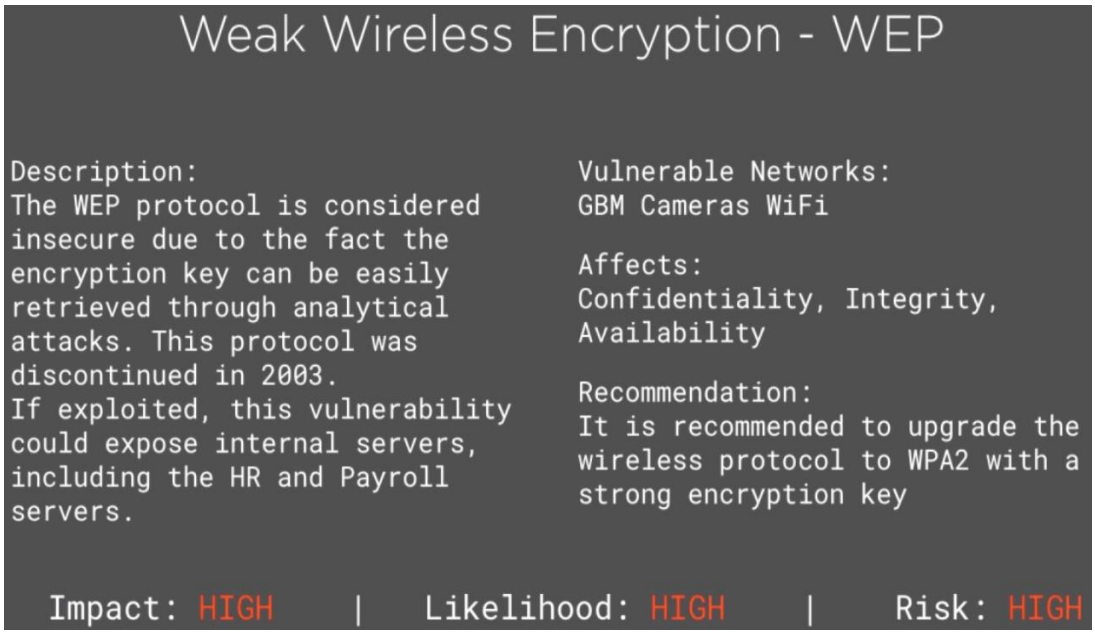
Post-exploitation

- Look for:
    - Authentication passwords
    - Network design
    - Known vulnerabilities
    - Traffic eavesdropping
    - Reachable services

Reporting

- Risk
- What to include
    - Cover page
        - Project name
        - Company name/logo
        - Client name/logo
        - Confidentiality note
    - Legal information
        - Non-liability statement
    - Executive Summary
        - Brief description
        - Scope
        - Timeline
        - Summary of findings in non-tech language
        - High level risk overview
    - Technical findings
        - Sectioned by vulnerability
            - Description of the finding
            - Impact
            - Likelihood
            - Risk
            - Recommendation

- EXAMPLE:



  - Recommendations
    - Understand technical issues
    - Understand the client environment
    - Research best practices
    - Propose improvements
  - Appendix
    - Proof of findings
      - Screenshots
      - Data found (obfuscated)
      - Additional information
- What NOT to include
  - Sensitive data
    - Passwords
    - Confidential documents
    - Network traffic dumps

PRACTICAL

Information Gathering Process:
Using Airmon Suite:

- airmon-ng start wlan0 ------ enables monitor mode
- airodump-ng wlan0mon ------ detecting wireless traffic
  - Ctrl + C to stop
- airodump-ng wlan0mon --bssid (MAC ADDRESS) -c (CHANNEL) ------ captures traffic for specific target
  - I.e. airodump-ng wlan0mon --bssid 5A:73:51:12:BB:2E -c 11
- airodump-ng wlan0mon --bssid (MAC ADDRESS) -c (CHANNEL) -w (PATH, name for file) ------ writes captured traffic to files
  - I.e. airodump-ng wlan0mon --bssid 5A:73:51:12:BB:2E -c 11 -w ~/packets/wirelessaudit
  - airodump will create .cap, .csv, kismet.csv, kismet.netxml files for reporting

Identifying Hidden Networks & Deauth Attack:

- In airodump, hidden wireless networks appear with no ESSID, just the amount characters: I.e. <length: 9>
- Filter in on <length: x> to see connected devices (clients need to know the name of the hidden network in order to connect). We need to capture the initial client handshake packet to reveal the SSID name.
- 2 options, wait for someone to connect then capture the traffic OR utilize a deauth attack.
- aireplay-ng -a (MAC of AP) -c (MAC of connected Client) --deauth (#of injected packets) wlan0mon ----- starts a deauth attack
    - I.e. aireplay-ng -a 00:21:5C:1D:2D:13 -c E8:B1:FC:97:C2:82 --deauth 200 wlan0mon
    - Once client reconnects initial handshake will be automatically captured and ESSID will be revealed

Identifying & Exploiting Vulnerabilities:

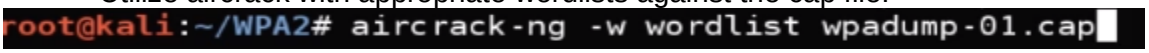
Attacking WEP Password

- Use airodump-ng, filter on WEP: airodump-ng --encrypt=WEP
- Filter on BSSID and channel, use -w to write to file
    - Watch the data packets increase, the more the easier to crack
    - In another terminal, try to use aircrack-ng on cap file while waiting:
        - I.e. aircrack-ng filename.cap

Attacking WPA Password

- Password is transmitted in the encrypted form during the initial handshake, utilize deauth attack via aireplay to capture client handshake.
- airodump will reveal handshake once captured:

- Utilize aircrack with appropriate wordlists against the cap file:



- Allow passwords to try cracking for 1-2 days, if no crack, then consider successful pass.

Mis-Configurations

- Captive Portals
    - They are web applications
        - Sql injection
        - Authentication bypass
        - Http eavesdropping
- MAC restriction bypass
    - Implemented to restrict access to devices
    - Used in whitelists of guests networks
        - Very easy to spoof/change your mac address
- Insecure management interface
    - Look for telnet/http, lack of patching, weak/default credentials

Advanced Techniques:

Red Teaming Concepts (wireless):

- Main goal is to break into the network
- Social Engineering
- Rogue APs
- Fake Captive Portals
- MiTM
- DoS

Test Prep:

- Technology:
    - Identify wireless networks
    - Identify technologies

- Create a map of wireless networks
- People:
  - Identify key personnel
  - Identify shift hours
  - Create a map of departments

Non-disruptive Attacks:

- Eavesdropping
  - Goal: capture passwords, sensitive data, and cookies
  - Tools:
    - Airmon suite (capture & decrypt)
    - Kismet (alternative to Airmon suite)
    - Wireshark (analysis)
  - Use airdecap to decrypt packets:

```
root@kali:~/demo# airdecap-ng -w 5A:34:30:34:41:30:33:37:42:33:46:42:45 capture-01.cap
```

    - Then use wireshark to analyze, check insecure protocols
- Rogue AP (MANUAL)
  - Utilizing hostapd & dnsmasq:

```
root@kali:~/ap# apt-get install -y hostapd dnsmasq wireless-tools iw wvdial
```

  - Back up the dns configuration file:

```
root@kali:~/ap# mv /etc/dnsmasq.conf /etc/dnsmasq.conf_bkp
```

  - Create custom config file:

```
root@kali:~/ap# vim /etc/dnsmasq.conf
```

  - Create hostapd configuration file:

```
root@kali:~/ap# vim /etc/hostapd/hostapd.conf
```

  - Start dnsmasq:

```
root@kali:~/ap# service dnsmasq start
```

  - Tail the logs:

```
root@kali:~/ap# tail -f /var/log/dnsmasq.log
```

  - Run the access point: hostapd (conf file)
- Fake Captive Portal
  - Create page with SET toolkit: Page Cloner, or Apache + PHP
  - For manual page: Edit the dnsmasq config file, allow redirects
  - Using setoolkit:

```
root@kali:~# setoolkit
```

    - Choose option 1: Social Engineering Attacks
    - Choose option 2: Website Attack Vectors
    - Choose option 3: Credential Harvester Attack Method
    - Choose option 2: Site Cloner
    - Use your machine IP
    - Choose your URL to clone
      - Data should save to /var/www/html

Disruptive Attacks:

- MITM
  - Basic Process:
    - Create rogue ap
    - Connect rogue ap to a real network
    - Wait for users to connect
    - monitor/eavesdrop (wireshark)
    - Modify/inject packets (MITMf)
  - Basic Manual Creation:
    - Start hostapd (also make sure dnsmasq is configured)

- Flush NAT & Routing configs to start fresh:

```
root@kali:~# iptables -t nat -F
root@kali:~# iptables -F
```

- Create NAT rule for the interface connected to the output network:

```
root@kali:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- Create a rule to forward packets from the user to the destination network:

```
root@kali:~# iptables -A FORWARD -i wlan0mon -o eth0 -j ACCEPT
```

- Enable ip forwarding on linux:

```
root@kali:~# echo '1' > /proc/sys/net/ipv4/ip_forward
```

- Observe traffic in wireshark

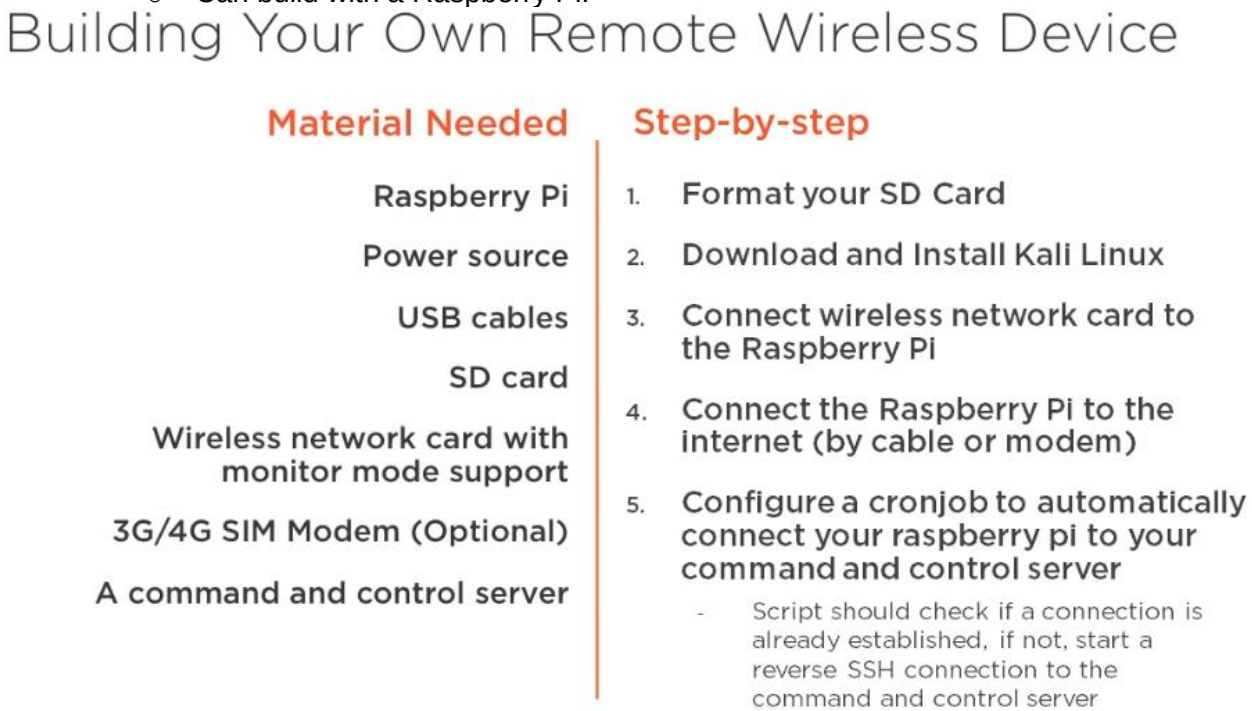
Covering Your Traces:

- Disposable VMs Good Practices
  - One virtual machine per engagement
  - Provides client segregation
  - Easy data construction
  - Utilize virtual machine templates
  - Encrypt hard drive of VM / encrypt files of VM
  - Create off-device backups
- Utilize mac address changing

Wireless Penetration Accessories:

****Before utilizing tools, make sure you know how to it all manually

- Remote Wireless Devices
  - Small device with wireless capabilities
  - Allows you to connect to wireless network remotely
  - Wireless backdoors
  - Can build with a Raspberry Pi:



- Out-of-the-box solutions: i.e. WiFi Pineapple