

FUTURE INTERNS – TASK 3

Name: Arya Sunilkumar

Internship: Cyber Security

Email ID: asunilkumar369@gmail.com

Objective:

The objective of this task was to conduct a **Wi-Fi security assessment** on my home network to identify potential vulnerabilities, including:

- Weak passwords
- Open ports
- Unauthorized devices

By analyzing my home network, I aimed to enhance its security and reduce the risk of unauthorized access.

Skills Gained:

During this assessment, I developed expertise in:

- **Network Security Basics** – Understanding Wi-Fi encryption, security protocols, and common vulnerabilities.
- **Wi-Fi Penetration Testing** – Using tools to assess and improve wireless security.
- **Packet Analysis** – Capturing and analyzing network traffic to detect anomalies.

Tools Used:

To successfully complete this assessment, I used:

- **Wireshark** – For packet capture and network traffic analysis.
- **Aircrack-ng** – For testing Wi-Fi encryption and password strength.
- **Nmap** – For network scanning and identifying open ports or unauthorized devices.

How I Achieved It:

Step 1: Identifying Connected Devices & Open Ports (Nmap)

I started by scanning my home network to identify all connected devices and detect any unauthorized users.

Scanning for Devices:

```
nmap -sn 192.168.1.1/24 (Real IP not provided due to safety concerns)
```

Findings: I discovered **two unknown devices** connected to my Wi-Fi, which could indicate unauthorized access.

Mitigation: I immediately changed my Wi-Fi password and enabled **MAC address filtering** to restrict access.

Scanning for Open Ports:

To check which ports were open on my router and other connected devices, I ran:

```
nmap -p- 192.168.1.1
```

Findings: An open **Telnet (Port 23)** was detected, which is a security risk.

Mitigation: I disabled **Telnet access** and ensured only necessary ports were open.

Step 2: Capturing & Analyzing Wi-Fi Traffic (Wireshark)

Opened **Wireshark** and selected my **Wi-Fi interface** (wlan0).

Captured Wi-Fi packets and filtered for deauthentication attacks:

```
wlan.fc.type_subtype == 0x04
```

Analyzed the captured packets to check for any unusual network activity.

Findings: I did not detect any active Wi-Fi deauthentication attacks.

Mitigation: I enabled **AP Isolation** in my router settings to prevent device-to-device attacks.

Step 3: Checking Wi-Fi Password Strength (Aircrack-ng)

To test my Wi-Fi security, I simulated a **password cracking attempt** on my own network:

Enabling Monitor Mode:

```
airmon-ng start wlan0 (Not provided real name due to safety concerns)
```

Capturing the Handshake:

```
airodump-ng -c [channel] --bssid [BSSID] -w capture wlan0mon
```

Attempting a Dictionary Attack:

```
aircrack-ng -w rockyou.txt -b [BSSID] capture.cap
```

Findings: My Wi-Fi password was **not found** in common wordlists, confirming strong encryption.

Mitigation: I ensured my **Wi-Fi password is complex**, using a mix of **uppercase, lowercase, numbers, and symbols**.

Lessons Learned:

This hands-on experience provided me with deep insights into Wi-Fi security:

Understanding Wi-Fi Security Threats

- Learned how **attackers exploit weak Wi-Fi passwords** and encryption flaws.
- Observed how **open ports** can be exploited for unauthorized access.

Strengthening My Network Security

- Implemented **stronger encryption (WPA2/WPA3)** and disabled **WPS**.
- Closed **unnecessary ports** and **restricted unknown devices**.

Glimpses of the Task:

```

[1] # Author: Erik van der Wal
[2] #
[3] # (c) 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 2681, 2682, 2683, 2684, 2685, 2686, 2687, 2688, 2689, 2690, 2691
```

```
>root@kali:~# python3 -c "import sys; print(' '.join(sys.argv[1:]))"
```

```
[root@kali:~/]# ./simon.py
```

```
Found 8 processes that could cause trouble.
```

```
#!#! They're using --airmon-ng check kill -- before putting
```

```
the card in monitor mode, they will interfere by changing channels
```

```
and sometimes putting the interface back in managed mode.
```

```
PID Name
```

```
677 NetworkManager
```

```
Suggested device "slim" does not exist.
```

```
Run /usr/sbin/airmon-ng without any arguments to see available interfaces
```

```
[root@kali:~/]# ./simon.py
```

```
Found 9 processes that could cause trouble.
```

```
#!#! They're using --airmon-ng check kill -- before putting
```

```
the card in monitor mode, they will interfere by changing channels
```

```
and sometimes putting the interface back in managed mode.
```

```
PID Name
```

```
677 NetworkManager
```

```
Suggested device "WMI-Personal" does not exist.
```

```
Run /usr/sbin/airmon-ng without any arguments to see available interfaces
```

```
[root@kali:~/]# ./simon.py
```

Wireshark interface showing a packet capture. The top pane displays a list of packets, and the bottom pane shows the details of the selected packet (Frame 84).

No.	Time	Source	Destination	Protocol	Length	Info
80	13.639993	192.168.0.108	163.70.143.61	TCP	54	60166 → 80 [ACK] Seq=1 Ack=5776 Win=516 Len=0
81	13.631140	163.70.143.61	192.168.0.108	TCP	1446	80 → 60166 [ACK] Seq=5776 Ack=1 Win=364 Len=1392
82	13.634715	163.70.143.61	192.168.0.108	TCP	95	80 → 60166 [PSH, ACK] Seq=7168 Ack=1 Win=364 Len=41
83	13.634802	192.168.0.108	163.70.143.61	TCP	54	60166 → 80 [ACK] Seq=1 Ack=7209 Win=516 Len=0
84	13.754594	192.168.0.108	163.70.143.61	TCP	127	60166 → 80 [PSH, ACK] Seq=1 Ack=7209 Win=516 Len=73
85	13.764345	163.70.143.61	192.168.0.108	TCP	54	80 → 60166 [ACK] Seq=7209 Ack=74 Win=364 Len=0
86	16.394620	163.70.143.61	192.168.0.108	TCP	222	80 → 60166 [PSH, ACK] Seq=7209 Ack=74 Win=364 Len=168
87	16.423342	192.168.0.108	163.70.143.61	TCP	106	60166 → 80 [PSH, ACK] Seq=74 Ack=7377 Win=515 Len=52
88	16.443353	163.70.143.61	192.168.0.108	TCP	54	80 → 60166 [ACK] Seq=7377 Ack=126 Win=364 Len=0
89	20.057002	192.168.0.108	74.125.24.188	TCP	55	59293 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
90	20.124240	74.125.24.188	192.168.0.108	TCP	60	5228 → 59293 [ACK] Seq=1 Ack=2 Len=0 SLE=1 SRE=2
91	24.589225	140.82.112.26	192.168.0.108	TLSv1.2	80	Application Data
92	24.589531	192.168.0.108	140.82.112.26	TLSv1.2	84	Ignored Unknown Record
93	24.837974	140.82.112.26	192.168.0.108	TCP	54	443 → 60191 [ACK] Seq=27 Ack=32 Win=76 Len=0
94	26.232604	192.168.0.108	4.213.25.242	TLSv1.2	98	Application Data
95	26.242465	4.213.25.242	192.168.0.108	TLSv1.2	229	Application Data
96	26.293761	192.168.0.108	4.213.25.242	TCP	54	58574 → 443 [ACK] Seq=45 Ack=176 Win=514 Len=0
97	26.556354	192.168.0.108	4.213.25.240	TCP	55	60258 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
98	26.568441	4.213.25.240	192.168.0.108	TCP	66	443 → 60258 [ACK] Seq=1 Ack=2 Win=6911 Len=0 SLE=1 SRE=2

Frame 84: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface \Device\NPF{...} Ethernet II, Src: LiteonTechno_a4:4c:59 (e4:aa:aa:a4:4c:59), Dst: TendaTechnol_17:ab:2 Internet Protocol Version 4, Src: 192.168.0.108, Dst: 163.70.143.61 Transmission Control Protocol, Src Port: 60166, Dst Port: 80, Seq: 1, Ack: 7209, Len: 73

0000 e8 65 d4 17 ab 20 e4 aa ea a4 4c 59 08 00 45 00 e...LY-E
0010 00 71 0d a1 40 00 80 06 f9 4d c0 a8 00 6c a3 46 q @...M...I.F
0020 8f 3d e0 06 00 50 e1 f5 4c 9f f2 a9 5d 01 50 18 = P...L...] P
0030 02 04 5c b1 00 00 34 33 0d 0a 00 00 40 b8 d5 37 ...43...@.7
0040 f3 41 6c 8f ae f1 60 e7 ae 16 71 b6 8d 96 14 53 A...q...S
0050 21 c6 22 59 b1 44 7b 5f 8b 27 41 09 87 55 c2 76 l...Y...A-U-
0060 ab 6f 31 b2 3f 98 1a 7d 39 5d 42 fe f8 b7 73 02 o! ? } 9]B...s
0070 d6 86 54 f9 e1 70 08 04 b0 04 e6 f2 10 0d 0a ...T...p... ..

Wi-Fi: <live capture in progress> Packets: 98 · Displayed: 98 (100.0%) Profile: Default