31/8/23

Experiments

Wireshark

→ wireshark captures network packets from various interfaces. It enables us to capture specified types of traffic based protocols, source and destination addresses and all keywords within packet payload.

→ Its real time monitoring capability is invaluable for observing ongoing network activities. This feature helps in detecting any sudden traffic spikes, and unusual protocol behaviours.

→ It also decrypts and encrypted protocols.

→ In command prompt : type ipconfig.

> ipconfig
> Windows IP configuration

Ethernet adapter Ethernet:

Connection-specific DNS suffix :
Link-local IPv6 Address . . . . : fe80::e587:29fd:2u8:4edb%2
IPv4 Address . . . . . : 10.124.2.84
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.124.0.11

→ it shows us IPV6, IPV4 addresses, subnet mask and default gateway.

→ the selected protocol appears at the bottom with all source and destination addresses and all keywords within packet payload

Bafna Gold
Date: Page:

→ when user clicks on the keywords for example destination address the destination address will be highlighted.
→ for example when we select a TCP protocol it shows:
Source port : 5228
Destination port : 58545
Sequence Number : 1
Sequence Number (raw) : 4247385453.
Acknowledgement Number : 1
Acknowledgement Number : 2
Acknowledgement number (raw) : 3944402357.
Flags : 0x010 (ACK)
window : 265.
checksum : 0x9d08.
→ Raw USB traffic can be captured.
→ various settings timers and filters can be set that ensure only triggered traffic appear.
→ Information of packet include SID number, time, source IP address, destination IP address, protocol name, length and other important information.

31/8/23