Alok Bhawankar
PA06
Panel E

Date / /
Page
STUDY BUDDIES

WMS Assignment 4

Aim :-

Install, configure and demonstrate any one wifi traffic analyzer using sniffing tools such as wireshark, Aircrack, Airsnort, etc.

Objective :-

- To install, configure and demonstrate wifi traffic analyzer using sniffing tool
- To learn use of tools such as wireshark, Aircrack, Airsnort, etc.

Theory :-

Wireshark :-

- Wireshark is a free and open source packet analyzer.
- It is used for network troubleshooting analysis, software and communication protocol development and education.

Kismet Linux :-

- Kismet Linux fans know that Kismet is a wifi swiss Army knife; it discovers APs and clients, capture wifi packets from local Nic or remote drones and can generate alerts for finger printed recon activities.

Date / /
Page
STUDY BUDDIES

Ettercap :-

- Ettercap is a suite for man in the middle attacks on LAN.
- It features sniffing of live connections, content filtering on the fly and many other interesting tricks and support active and passive dissection.

PRTG :-

- PRTG is a open source network monitor where PRTG stands for passior Router Traffic Graphes.
- It is a network monitoring software from passior AG. PRTG runs on windows and monitor network availability and network usage using SNMP, Packet sniffing, WMI, IP, SLA, & NetFlow.

Nagios :-

- Nagios is the definitive open source n/w monitoring solution.
- It can be used from simply checking to see if a network host is still up, all the way up to monitoring specific services on remote hosts and even to trigger corrective action if a problem is detected.

Date / /
Page
STUDY BUDDIES

* Protocol analyzer:
It is mostly a tool for seeing the bits and bytes flowing from end to end network in a human understandable format.

* wireshark misconceptions:
There is a combine misconception about wireshark to recognize what wireshark is not.
1) Wireshark is not a packet generator or packet dropper. It captures packets & analyze.
2) Wireshark will never advise if any suspicious packets or mischievous connections. Thus, it cannot use as an alarm any notification for packets.

* conclusion:-
Thus, we studied the configuration of wireshark and analyzation of wifi traffic using the analyzing tool wireshark.

* FAQ:
1) List the different open source tools to capture packet. also, write it features
packets are -
- PRTG - Fiddler - Ethereal CAPS
- tcpdump - Packet capture - Solar winds
- kismet - Network miner

Date __/__/__
Page _____
STUDY BUDDIES

PRTG :-
- It filters according to IP addresses protocols and type of data
- It offers a dashboard which shows complete information about which application uses the most bandwidth

Solarwinds :-
- offers many types of IT management tools including Deep packet Inspecting and Analytics.
- It inspects all the contents of the packet to determine even the smallest detail including what application causes more traffic

Q2 Which mode NIC uses for Ethercap / packet sniffing ?
- When you are running a sniffer, the packet capture driver that we mentioned earlier will put computers NIC into what is known as promiscous mode

- This means the sniffing computer will be able to see all the traffic on the segment regardless of who is being sent to.

Date / /
Page
STUDY BUDDIES

Q3 which wireshark filter can be used to monitor outgoing packets from a specific system on the network?

→ outgoing packets would contain the IP address of the system as it is a source address.

- So assuming that the IP address of the system is 192.168.1.2. The filter would be IP Src == 192.168.1.2