COMPARITIVE ANALYSIS OF PACKET SNIFFERS,ANALYSERS AND TOOLS

[1]ANKITA MITHAIWALA, [2]KRUPA JARIWALA

[1]Teaching Assistant, [2]Assitant Professor
S.V.N.I.T., Surat
E-mail: [1]ankitamithiwala15@gmail.com, [2]knj@coed.svnit.ac.in

Abstract- From last ten years size of the network continues to grow in terms of complexity of data, type of information and number of users. The amount and type of network traffic data flowing at each link has increased drastically. To identify and track on these links,packet sniffers, which are also called a network monitor or network analyzers are required. Many system administrator or network administrator use it to monitoring and troubleshoot the network traffic. As number of users and flow of traffic increased in past few years, it’s very important to monitor networks traffic as well as its user’s activities to keep the network smooth and efficient. For enterprise from big network it’s difficult task to maintain and monitor the network, because the large amount of information available. Packet sniffers are useful for both wired and wireless networks. The purpose of this paper is to analysis various of packet sniffers and packet analyzers how it works in Wired and wireless environment and also compare different tools available for packet sniffer and analyze and lastly make one comparative analysis based on different parameters.

Indexterms- Wire Shark, TCP Dump,Packet Filter, Network analyzer, Packet sniffer.

I. INTRODUCTION

Packet sniffing is the process of finding of the data passed through network [1]. In this process NIC capture all traffic that is flow inside or outside network. Packet Sniffing mainly used in network management, monitoring and ethical hacking. To perform sniffing we use tool named packet sniffer. A packet sniffer is also called as a network analyzer, which can be used by a network administrator to monitor and improve network traffic. Packet sniffers can be operated in both switched and non-switched environment [2]. Determination of packet sniffing in a non-switched environment is technologies that can be understood by everyone. In this technology all hosts are connected to a hub.

Network analysis is the process of capturing network traffic and inspecting it closely to determine or analyze what happened on the network. A network analyzer clear up the data packets of common protocols and displays the traffic in human-readable format. Network analysis is also called by traffic analysis, protocol analysis, packet sniffing, packet analysis, and eavesdropping to name a few [1]. Sniffing lead to be one of the most popular terms in use today. However, due to malicious users it has had a negative connotation in the past. Problem comes that how this network traffic can be eavesdrop; this problem can be solved by setting network card into a special “promiscuous mode” [2]. Currently businesses are updating their network infrastructure, replacing aging hubs with new switches. The replacement of hub with new switches that makes switched environment is widely used because “it increases security”. However, the thinking behind is somewhat flawed. It cannot be said that packet sniffing is not possible in switched environment. It is also possible in switched environment.

Network sniffer is to analyze network traffic and bandwidth utilization, so that hidden troubles in the network can be identified. Two directional control of sniffer which has coexisted since it was first produced. Positive usage of a sniffer is also its regular usage, which has as its objective the desire to maintain the network and keep it working normally [3].Not all packet sniffing software products have the same functions; some sniffers can analyze hundreds of protocols whereas others can only deal with one or two. The most typical protocols analyzed by sniffer are TCP/IP, IPX, DECNet-Ordinarily, a sniffer is used as assistant tool of the network engineer for monitoring and analyzing a network, detecting intrusion, controlling traffic or supervising network activity. IT should be noted that such features may also be utilized by hackers as a snooping tool to break into other computers [1].

II. APPLICATION OF PACKET SNIFFER

Sniffing programs have been around for a long time in two forms. Underground packet sniffers are used to break into computers. Typical uses of such wiretap programs include:

- Automatic sifting of clear-text passwords and usernames from the network.
- Conversion of data to human readable format so that people can read the traffic
- Fault analysis to discover problems in the network, such as why computer A can't talk to computer B
- Performance analysis to discover network bottlenecks

- Network intrusion detection in order to discover hackers/crackers.

III. WORKING PRINCIPLE OF PACKET SNIFFER

1. The hardware: Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyse hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth [1].
2. Capture driver: This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, and then stores the data in a buffer.
3. Buffer: Once frames are captured from the network, and it’s stored in a buffer. There are a couple captures modes: capture until the buffer fills up, or use the buffer as a "round robin" where the newest data replaces the oldest data. Some products like the BlackICE Sentry IDS from Network ICE can maintain a full round-robin capture buffer on disk at full 100-mbps speeds. This allows having hundreds of gigabytes of buffer rather than the megabyte 1-gigabyte have in a memory-based buffer.
4. Real-time analysis: Pioneered by the Network General Sniffer, this feature does some minor bit of analysis of the frames as they come off the wire. This is able to find network performance issues and faults while capturing. Many vendors have started to add minimal capabilities along this line to their products. Network intrusion detection systems do this, but they sift the traffic for signs of hacker activity rather than fault/performance issues.
5. Decode: The contents of network traffic with descriptive text so that an analysist can figure out what is going on.
6. Packet editing/transmission: Some products contain features that allow you to edit your own network packets and transmit them onto the network.

IV. PRINCIPLE OF PACKET SNIFFER

As a rule, all network interfaces on a segment have the ability to view all of the data transmitted on physical medium and each network interface is supposed to have a hardware address which is different to other existing network interfaces' on network[4].

Every network should have at least a broadcast address. In common cases, a legal network interface should respond to only these two kinds of frames. Target domain of frame has a hardware address matching to local network interface; Target domain of frame has a broadcast address. When a local network interface card is set in promiscuous mode, this network interface card has a broadcast address and produces a hardware stop to each frame it meets in order to notify the system to deal with every packet passing through. Each machine on a local network has its own hardware address which differs from other machine [4].

When a packet is sent, it will be transmitted to all available machines on local network. Owing to the shared principle of Ethernet, all computers on a local network share the same wire, so in normal situation, all machines on network can see the traffic passing through but will be unresponsive to those packets which do not belong to them by just ignoring them.

However, if the network interface of a machine is in promiscuous mode, the NIC of this machine can take over all packets and a frame it receives on network, namely this machine (involving its software) is a sniffer.

V. TYPE OF PACKET SNIFFER

A. TCPDUMP

Tcp-dump is used to find out traffic on a network. It also used search out a description of the data of packets on a network interface that match the Boolean in from of true or false expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight.

It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface [14]. In all cases, only packets that match expression will be processed by tcpdump.

When tcpdump finishes capturing packets, it will report counts of: Packets find out ``captured'' (number of packets that tcpdump has received and processed or count by)

Packets that is “received by filte” tcpdump, and possibly on the way the OS was configured - if a filter was specified on the command line, on some OS it counts packets regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether tcpdump has read and processed them yet, on other OSes it counts only packets that were matched by the filter expression regardless of whether tcpdump has read and processed [14].

Packets that id “dropped by kernel”. It is the number of packets that were dropped, due to a lack of data space, by the packet capture mechanism in the OS on which tcpdump is running, if the OS reports that information to applications; if not, it will be reported as 0.

➢ TCP Dump filters based on:

1. Type: Capture traffic by Host or web
2. Direction: From/to source
3. Protocol: TCP Traffic or UDP Traffic

1. Filtering based on Type:

- $tcpdump host 192.168.1.200 (Traffic only to/from given IP)
- $tcpdump host 192.168.1.100 and port 80
- $tcpdump net 192.168.1.0/24 and port 80

2. Filtering based on Direction:

- $tcpdump source-host 192.168.1.100 & destination-host 80

3. Filtering based on protocol:

- $tcpdump source-host 192.168.1.100 and udpdstport 53
- $tcpdump arp net 192.168.1.0

B. WIRESHARK:

Wireshark is the foremost and worldwide used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998 [13].Wireshark interface has five major components:

1. The command menus are standard pull down menus located at the top of the window.
   The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application.The Capture menu allows you to begin packet capture.

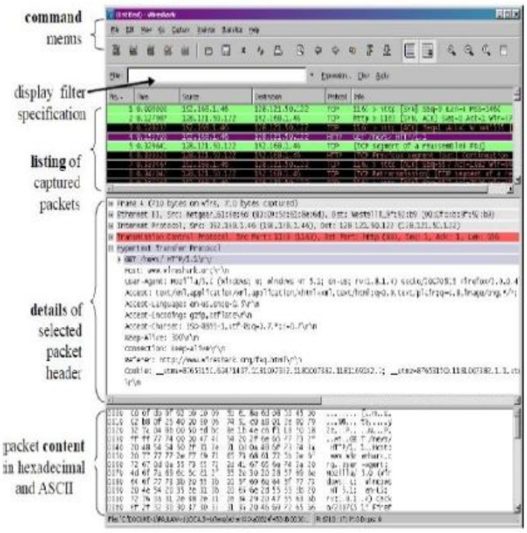

command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII

Figure 1. Wireshark GUI during packet capture and analysis [5]

2. The packet-listing window displays a one-line summary for each packet captured, including

- the packet number,
- the time at which the packet was captured,
- the packet's source and destination addresses,
- the protocol type, and protocol-specific information contained in the packet.
- The protocol type field lists the highest-level protocol that sent or received this packet.

3. The packet: header details window provides details about the packets elected in the packet-listing window.
4. The packet-contents window displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
5. Towards the top of the Wireshark graphical user interface is the packet display filter field in to which a protocol name or other information can be entered in order to filter the information [13].

C. ETTERCAP

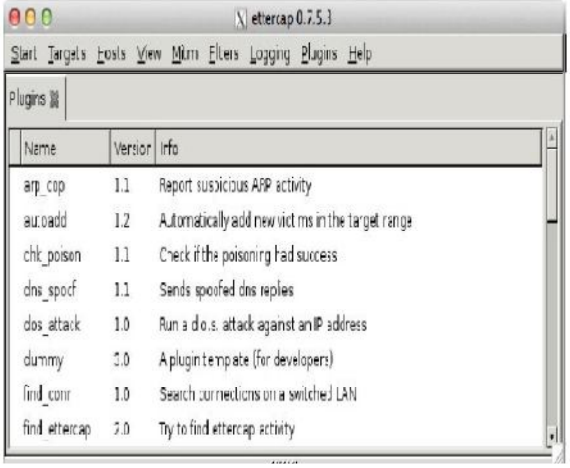
Ettercap is a suite of attack tools which do a combination of attacks based on Packet Sniffing and Packet Injection. The tools are suited for a LAN environment and rely heavily on ARP Spoofing.

Once ARP which is at Layer 2 is compromised, higher unprotected protocols such as IP, TCP and UDP can be easily tampered with. Ettercap does just that. Once Ettercap hijacks Layer 2, it allows for mangling of packets at higher layers and helps performs website redirection, on the fly content changing and even Denial of Service attack on the victim computers.

```
0 plugins
42 protocol dissectors
58 ports monitored
13861 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services
```

Figure 2. Ettercap home pages [11]

The filter internally is done packet code, which modifies the data on the fly and reinjects it back to the network. The fundamental principle is based on packet injection.



Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
dns_spoof	1.1	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity

Figure 3. Ettercap Available plug-in[11]

D. HPING

hping is a command-line oriented TCP/IP packet assembler. The interface is inspired to the ping unix command, but hping is not only able to send ICMP echo requests.

It supports TCP, UDP, ICMP and RAW-IP protocols, it has a traceroute mode which has the ability to send files between hping is named after ping because in default usage it does the same thing functionally--contacts another machine and gets it to answer [10].
While ping uses ICMP echo request to get talkback in the form of echo reply messages, hping uses tcp contact with port 0 to get talkback in the form of a TCP "nobody home" reset packet.
hping can also be used to craft and insert arbitrary byte sequences into packets. In normal usage, the packets "you" send out are usually written for you by the various software layers in the famous "network stack."

The application doesn't build packets; it only generates the to-be-packetized data but hands it off to others to manufacture the actual packets. But you can roll your own with packet injection tools like hping[10].
Functions of hping:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

E. KISMET

Kismet is a wireless "detector, sniffer, and intrusion detection system," and one of the growing list of essential open source tools for computer network security professionals.
Kismet runs on any POSIX-compliant platform, including Windows, Mac OS X, and BSD, but Linux is the preferred platform because it has more unencumbered RFMON-capable drivers than any of the others.
Monitor mode ability is critical to fully utilizing Kismet, because it allows Kismet to examine all the packets it can hear, not just those of whatever access point (AP) that are associated with.
Almost as important to police, intelligence agencies, and black hat hackers is the fact that it allows Kismet to work passively, intercepting and collecting packets without leaving any fingerprints of its own behind [12].
The point is that if you want to investigate Kismet fully, the first step is to ensure that you have a driver that supports RFMON -- monitor mode -- for your wireless network interface card (NIC).
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic [15].
Kismet features the ability to log all sniffed packets and save them in a tcpdump/Wireshark or Airsnort compatible file format. Kismet can also capture "Per-Packet Information" headers [15].

VI. COMPARATIVE ANALYSIS

Based on this an extensive review of literature on Packet sniffer and analyzer available tools was done.

Parameters based Security requirements	Tcp-Dump [14]	Wire shark[5]	Ettercap [11]	Hping[10]	Kismet [15]
Integrity	Available	Available	Available	Available	Available
Authentication	Not Available	Available	Not Available	Not Available	Not Available

Table 1. Comparative Analysis based Security

Parameters based on functionality	Tcp-Dump [14]	Wire shark[5]	Ettercap [11]	Hping[10]	Kismet [15]
GUI	Not Available	Available	Not Available	Not Available	Not Available
VOIP Facility	Not Available	Available	Not Available	Not Available	Not Available
Decode Message	Not Available	Available	Not Available	Available	Not Available

Table 2.Comparatives analysis based on functionality

CONCLUSION

In this paper we reviewed on available packet sniffer and analyzer in term of different parameters. Basically, the task of packet sniffer is used to analysis the traffic on network and find out particular attack happened in network on not. For detection of attack packet sniffer check out incoming and outgoing of packet in network and also find out the performance of network. For analysis we take five different tools for packet analysis and take it comparative analysis. With Comparative analysis we can say that Wire shake provide more functionality and detection of attack is easy compared to any other tool.

REFERENCES

[1] Rupam AV, Singh A. An Approach to Detect Packets Using Packet Sniffing. International Journal of Computer Science & Engineering Survey (IJCSES) Vol. 2013;4.

[2] Santos, M. J. C. (2016). Automated Scalable Platform for Packet Traffic Analysis.

[3] Saxena, P., & Sharma, S. K. (2017). Analysis of Network Traffic by using Packet Sniffing Tool: Wireshark.

[4] EtherealPacketSniffing,Available:netsecurity.about.com/od/readbookreviews/gr/aapro52304.htm.

[5] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158- 162(2007).

[6] BoYu"Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 7, 2010, Page(s): V7-1-V7-3(2010).

[7] Osvaldo Rein, José Antônio Jardini, Wagner Seizo Hokama, Luiz Carlos Magrini, "Advantages of adopting Web Services in smart grids", Innovative Smart Grid Technologies Latin America (ISGT LA) 2013 IEEE PES Conference On, pp. 1-5, 2013.

[8] Deepak D. Kshirsagar, Sachin S. Sale, Dinesh K. Tagad, Ganpat Khandagale, "Network Intrusion Detection based on attack pattern", Electronics Computer Technology (ICECT) 2011 3rd International Conference on, vol. 5, pp. 283-286, 2011.

[9] Jiujun Cheng, Liufei Hu, Junjun Liu, Qingyang Zhang, Chendan Yan, "A New Mechanism for Network Monitoring and Shielding in Wireless LAN", Mathematical Problems in Engineering, vol. 2014, pp. 1, 2014, ISSN 1024-123X.

[10] http://homepage.smc.edu/morgan_david/cs75/abs/packet-injection-hping.htm (View on 22 Jan-2018)

[11] http://www.securitytube.net/video/136(View on 22 Jan-2018)

[12] https://www.linux.com/news/introduction-kismet-packet-sniffer. (View on 22 Jan-2018)

[13] https://www.wireshark.org/. (View on 22 Jan-2018)

[14] http://www.tcpdump.org/ (View on 22 Jan-2018)

[15] https://www.kismetwireless.net/ (View on 24 Jan-2018)

★★★