Passively Eavesdropping: Reconnaissance with Sniffing Tools

Juita Tushar Raut
Research Scholar, JJT University, Rajasthan, India

Dr. Vikram Patil
Research Co-Guide, JJT University, Rajasthan, India

Dr.Yogeshkumar Sharma
Research Guide, JJT University, Rajasthan, India

ABSTRACT
With the expansion and popularization of network, the management and observing of network data is important to keep network smooth and efficient. The process of monitor and capture all the traffics passed through the network using sniffing tools. To sort all types of traffic such as protected as well as unprotected is possible through sniffing. This paper study the issue of worker misuse of computers within the work and the choice of facing employers and network directors relating to whether or not it's acceptable watch the employee's digital computer within the organizations. The paper give brief introduction of what is a packet sniffer, types and uses .Two popular packet sniffing tools are discussed and examined, Wireshark and Windump. These tools are compared on the basis of their features and qualitative parameters.

Keywords: sniffing tool, packet sniffer, Wireshark, Windump.

1. INTRODUCTION

Packet sniffing is the process of capturing and analyzing the packets contents transmitted over network. It is used to improve problems of network. To capture the network traffic device or software are used. It can monitors any traffic like web ,port sniffer, mail traffic ,infrastructure traffic ,and other UDP ,TCP traffic. Now a days technology is become integral part of our daily lives. Every organization improves their worker efficiency by using technology. Every technology comes with pros and cons, includes misused of technology by employees in a working place. This misused mostly happened into the workplace while accessing internet for non-technical purposes. This affects employees performance .Network monitoring is the best solution to observe the traffic without knowingly employees. This is done by network supervisor who observes all the inappropriate actions happened in the network.

Packet Sniffing is method which can be used to gather all packets travelled across the network. It is done by tools that called as packet sniffer. This is either software or hardware tool to intercept, log, analyze network traffic and data. It analyzes network traffic by its type .It also identify root cause. This results in improvement of bandwidth and security. In today's market numbers of packet sniffers are available in paid as well as free. In this study two tools were used to analyze the traffic over the network including Wireshark and Windump. There are two types of sniffing including Active Sniffing and Passive Sniffing.

Active Sniffing

In this sniffing traffic that is passed through the switch which regulates the data between ports and scan the MAC address. It actively injects the traffic into the LAN to enable sniffing.

Passive Sniffing

Sniffing is done through the hub. In this sniffing sniffers are activated at data link layer of the network. All traffic is sent across the network. Every machine is receives the traffic which is already connected to the LAN. Attackers passively wait for the traffic to be sent and capture those using sniffers.

2. REVIEW OF LITERATURE

Nedhal A. Ben-Eid (2015)

Now a days it is very critical to secure organization system from external hackers and employees that take misused of computers in workplace. In this paper author studied the problem of employees and

Copyright © 2020 Authors

discussed ethical and legal dimensions of decision facing employers. In this paper author discussed and examined two security tools like Wireshark and Cola soft Capsa. These tools are packet sniffer tools .By using this tools administrator can easily captures all the packets on the network and also observed irregular behaviour.

Most of the employees were used internet for their personal work in workstation also did miss used of it. So there is need of some kind of network tool in the workplace to watch their employees. Author compared network tools in terms of their features, characteristic behaviour, qualitative and quantitative parameters. After testing both tools author has been conclude that both having different qualities. Capsa is more practical and user friendly also provide detail information where as wireshark is more powerful than Capsa.

Dr.Aruna Varanasi and P.Swathi (2016)
Now a day's used of computers and internet are increasing day by day. Also sharing of data within network is growing. To handle such type of situation will required tools and application. So they can monitor and analysed data. This helps to administrators to resolve the problems which were occurred within network.

In this study, efforts were taken by authors to explain some sniffing tools which help to monitor the data which is passed through network. In that wireshark, TCP DUMP, TCP Flow, ColaSoft Capsa with their features and limitations. Authors were studied different types of tools, examined those tools with network traffic and finally concluded that every tool has special quality with their property.

Piyush Goyal and Anurag Goyal (2017)
In this article author compared two of the most widely used open source packet sniffing and network monitoring tools like Wireshark and Tcpdump. These tools are useful in cyber mitigation but are also widely used by cyber criminals to eavesdrop or gain illegal access. Though they were designed to assist the network administrators in better assessing the servers, traffic and diagnosing the issues but they have become the favourite tool of hackers to scan a particular network and sniff on unprotected data. After implementing both tools author conclude that wireshark is more capable in analyzing the packets captured and the speed of capture.

3. RESEARCH METHODOLOGY

In this study, author trying to use applied research. In applied method some practical implementation is required to achieve results. Which is a also categorized into quantitative method to collect existing data. Those data was collected from previous published articles, books and online available information.

After getting results from experimental method results are analysed through statistical method in valid manner. In this study two tool were used for analysis of network traffic. Traffic including LAN, WI-FI etc. Wireshark and Windump were used for this study to analyze the traffic.

4. KEY FEATURES OF WIRESHARK AND WINDUMP:

In today's market so many packet sniffers are available according to various organization and personal need, but of all these Windump and Wireshark are mostly used.

4.1 Wireshark

It is an open source and free sniffing tool. It is also known as tshark.Which has been run upon nearly all operating systems including windows, Linux, macOS , Solaris, FreeBSD and NetBSD. This tool is come along with GUI and command-line interface. It collect, capture and analyzes the data which is passed over network. It can capture data from many different network media including Ethernet, Wireless LAN, Bluetooth, USB and more. It displays the entire contents of the captured frame in both ASCII and hexadecimal format. It has ability to separates network protocol packets with different colour scheme like green for HTTP, blue for DNS etc.

4.2 Windump

It is the windows version of tcpdump which analyzes the network traffic to find active malware. It is command-line tool comes into two parts. First part is called as WinPcap, which captures network

Copyright © 2020 Authors

traffic. Second part is program itself, windump. This is invoked from command-line after installing WinPcap library [6].

It captures all type traffic on the specified network. By using specific protocol, host or port it can filter captured data. It provides many options where details of packets captured can be viewed in several formats like -D gives list of available interfaces, -W overwrites the file name , -U this option provide runtime output , -A shows output in ASCII format.

5. Windump versus Wireshark

5.1 Options

Windump can hide capture information while live packet captures using –H option whereas Wireshark has no such feature to hide the data.

Windump can decrypt IPSec ESP packet if compiled with cryptography. By default DES algorithm is used. For this option –E is used whereas this option is unavailable into Wireshark.

Wireshark can collect different types of statistics and display the result in the window which updated in semi-real time. This is done by –Z option. This feature is not available in Windump.

Wireshark can dump all the packets after that matching filter is apply whereas Windump use –d to dump compile packet with matching code, -dd option to dump packet matching code with c program and –ddd option is used for decimal numbers.

5.2 Memory

After analyzing Wireshark and Windump tools by running on windows 10. Virtual size of Wireshark tool is 58,647 KB means almost 58.647 MB. The virtual size of Windump tool is 556 kb it means 0.556 MB. After this analysis it is clear that Wireshark is more than 50 times. From above analysis it is clear that Windump wins this contest.

5.3 Speed of Capture

To calculate the speed of capturing packets using timers and simultaneously run both tools on same local machine and resulted with almost same output. Local machine is connected with LAN and also some handset were connected that machine via Wi-Fi. Wireshark is much faster than Windump in capturing the packets.

5.4 No. of protocols supported

After analysing the data packets within wireshark it is crystal clear that more than 1000 protocols are supported to this tool. In Windump only TCP/IP protocol supports to this tool.

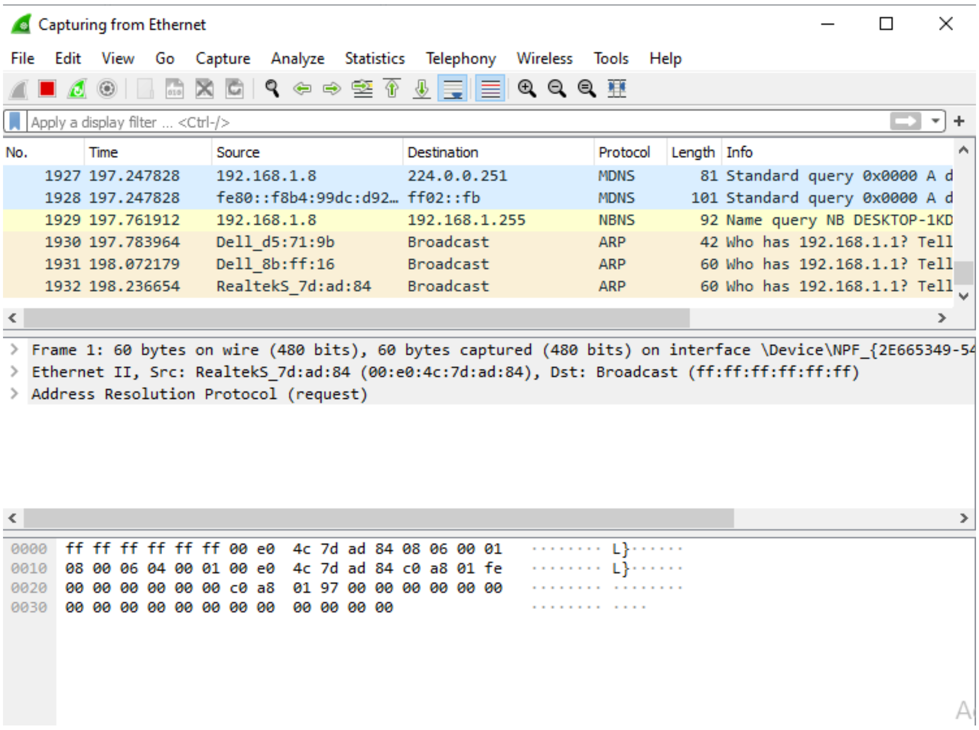
6. Network Monitoring

It constantly monitors network for slow or failing components and send alert to the network administrator in terms of email, SMS or alarms. This type of problem caused by overloaded or crashed servers, network connections. In most organizations, all staff systems are connected to the system administrator’s computer. This is allows the system administrator to obtain access to a staff’s computer, which will easy his work when a specific problem occurs. Administrator has right to monitor two types of surveillance including Internet and Desktop. In Internet surveillance user’s online data will be monitored and in desktop surveillance computer’s activity stored in hard disk.

Copyright © 2020 Authors

ISSN: 2394-3114
Vol-40-Issue-35-February-2020

Post Capture

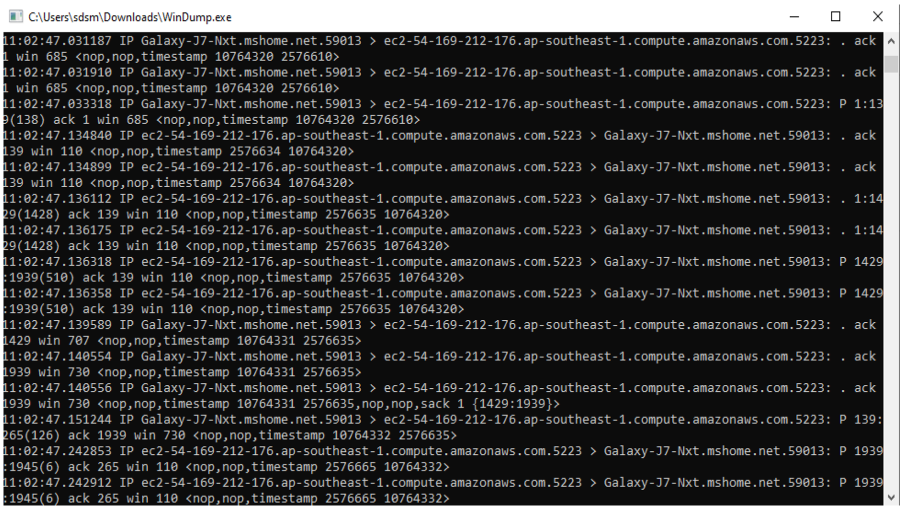

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source                 Destination    Protocol Length Info
 1927 197.247828  192.168.1.8            224.0.0.251    MDNS        81 Standard query 0x0000 A d
 1928 197.247828  fe80::f8b4:99dc:d92…   ff02::fb       MDNS       101 Standard query 0x0000 A d
 1929 197.761912  192.168.1.8            192.168.1.255  NBNS        92 Name query NB DESKTOP-1KD
 1930 197.783964  Dell_d5:71:9b          Broadcast      ARP         42 Who has 192.168.1.1? Tell
 1931 198.072179  Dell_8b:ff:16          Broadcast      ARP         60 Who has 192.168.1.1? Tell
 1932 198.236654  RealtekS_7d:ad:84      Broadcast      ARP         60 Who has 192.168.1.1? Tell
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2E665349-54
> Ethernet II, Src: RealtekS_7d:ad:84 (00:e0:4c:7d:ad:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 e0  4c 7d ad 84 08 06 00 01   ········ L}······
0010  08 00 06 04 00 01 00 e0  4c 7d ad 84 c0 a8 01 fe   ········ L}······
0020  00 00 00 00 00 00 c0 a8  01 97 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Fig.1 Wireshark Sample Capture



```
11:02:47.031187 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: . ack
1 win 685 <nop,nop,timestamp 10764320 2576610>
11:02:47.031910 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: . ack
1 win 685 <nop,nop,timestamp 10764320 2576610>
11:02:47.033318 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: P 1:13
9(138) ack 1 win 685 <nop,nop,timestamp 10764320 2576610>
11:02:47.134840 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: . ack
139 win 110 <nop,nop,timestamp 2576634 10764320>
11:02:47.134899 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: . ack
139 win 110 <nop,nop,timestamp 2576634 10764320>
11:02:47.136112 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: . 1:14
29(1428) ack 139 win 110 <nop,nop,timestamp 2576635 10764320>
11:02:47.136175 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: . 1:14
29(1428) ack 139 win 110 <nop,nop,timestamp 2576635 10764320>
11:02:47.136318 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: P 1429
:1939(510) ack 139 win 110 <nop,nop,timestamp 2576635 10764320>
11:02:47.136358 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: P 1429
:1939(510) ack 139 win 110 <nop,nop,timestamp 2576635 10764320>
11:02:47.139589 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: . ack
1429 win 707 <nop,nop,timestamp 10764331 2576635>
11:02:47.140554 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: . ack
1939 win 730 <nop,nop,timestamp 10764331 2576635>
11:02:47.140556 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: . ack
1939 win 730 <nop,nop,timestamp 10764331 2576635,nop,nop,sack 1 {1429:1939}>
11:02:47.151244 IP Galaxy-J7-Nxt.mshome.net.59013 > ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223: P 139:
265(126) ack 1939 win 730 <nop,nop,timestamp 10764332 2576635>
11:02:47.242853 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: P 1939
:1945(6) ack 265 win 110 <nop,nop,timestamp 2576665 10764332>
11:02:47.242912 IP ec2-54-169-212-176.ap-southeast-1.compute.amazonaws.com.5223 > Galaxy-J7-Nxt.mshome.net.59013: P 1939
:1945(6) ack 265 win 110 <nop,nop,timestamp 2576665 10764332>
```

Fig.2 Windump Sample Capture

From above figures , it is clear that Wireshark has powerful graphical interface due to this it has ability to separate different types of packets with different colour codes.Every colour code is dicided by types of packets. For example ,light purple is used for TCP data,light blue is UDP data and black means packet has an error.

On the other hand ,Windump has no special ability to differentitae the packets . It can be done by user itself.

During the capturing the packets it is very difficult to group and sepaprate out in Windump,whereas in wireshark it is easily done on real time .

In wireshark captured packets can be easily save,whereas in Windump it has no option is available to save caputerd data ,the packets will reamin in terminal window only.

Copyright © 2020 Authors

After getting the results it will conclude that Wireshark is more capable than Windump in terms of analyzing the packets and capturing the speed.

7. CONCLUSION

Maintaining a safe and well organised workplace requires organizations to observe the staff's computer at office. Every employee enough educated that someone monitors their online and offline data. It's duty of every employer to explain to employees what they monitor. So they can understand their privacy and their work capabilities. Although many employees and companies believe that employee sniffing is wrong or unethical, there is clear need for such practice.

In this study efforts are taken to show that sniffing is not always used as hacking purposes sometimes it used for monitoring, analyzing, troubleshooting and many useful purposes. In market many sniffing tools are available for sniffing data. In this study, two tools were used Wireshark, Windump.

8. REFERENCES

1] Dr. Aruna Varanasi & P. Swathi(2016)," Comparative Study of Packet Sniffing tools for HTTP Network Monitoring and Analyzing", IJCSET(www.ijcset.net), ISSN :2231-0711,Vol 6, Issue 12,406-409.

2] Mohammed Abdul Qadeer, M.et al.(2010)," Network Traffic Analysis and Intrusion Detection using Packet Sniffer", Second International Conference on Communication Software and Networks, 2010 IEEE.

3] Nedhal A. Ben-Eid(2015)," Ethical Network Monitoring Using Wireshark and Cola soft Capsa as Sniffing Tools", International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) 2278-1021, ISSN (Print) 2319-5940, Vol. 4, Issue 3.

4] Pallavi Asrodia & Hemlata Patel (2012)," Network Traffic Analysis Using Packet Sniffer", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3 pp.854-856.

5] Piyush Goyal & Anurag Goyal (2017)," Comparative Study of two Most Popular Packet Sniffing Tools- Tcpdump and Wireshark", 9th International Conference on Computational Intelligence and Communication Networks.

6] [Online] https://www.wireshark.org/

7] [Online] https://www.dnsstuff.com/packet-sniffers

8] [Online]https://searchenterprisedesktop.techtarget.com/tip/WinDump-The-tcpdump-tool-for-Windows

Copyright © 2020 Authors