Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise

Article *in* International Journal of Computer Applications · February 2022

DOI: 10.5120/ijca2022921876

2 authors, including:

Bindu Dodiya
MAPIT
6 PUBLICATIONS **13** CITATIONS

SEE PROFILE

Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise

Bindu Dodiya
Institute of computer Science
Vikram University Ujjain

Umesh Kumar Singh, PhD
Institute of Computer Science
Vikram University Ujjain

ABSTRACT
Packet analysis is a primary trace back technique in network forensics, Packet analysis, often referred to as packet sniffing or protocol analysis, describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network. This can be used to find traces of nefarious online behavior, data breaches, unauthorized website access, malware infection, and intrusion attempts, and to reconstruct image files, documents, email attachments, etc. sent over the network .Packet analysis is typically performed using a packet sniffer, a tool used to capture raw network data going across the wire. Wireshark proves to be an effective open source tool in the study of network packets and their behavior. In this regard, Wireshark can be used in identifying and categorizing various types of attack signatures. It lets administrator to see what's happening on network at a microscopic level. The purpose of this paper is to demonstrate how Wireshark is applied in network protocol diagnosis and can be used to find some basic indicators of compromise for a malware.

Keywords
Packet analyis, Indicators of compromise IOC, wireshark, Maware

1. INTRODUCTION
In today's world, computer networks have become smarter and much more complex. At the same time, hackers across the world are designing and inflicting various types of attacks through the internet for different reasons such as information theft, machine corruption and hijacking. These attacks affect most system users including the administrators and forensic investigators [1]. All these issues impel network engineers to be able to analyze network traffic and understand its behavior. As the number Organizations must regularly check their resources for the presence of malicious components. One of the ways in which a resource may become infected is as a result of vulnerability exploitation by cybercriminals. At the time of exploitation, experts may investigate incidents related to the threat. Moreover, some findings of these investigations may already be publicly available. Such reports have practical value. A typical report on an Advanced Persistent Threat (APT) campaign also includes Indicators of compromise .By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent them or limit damages by stopping attacks in earlier stages. Of all the detailed technical information on any given Advanced Persistent Threat (APT), "indicators of compromise" have the greatest practical value for security administrators [2].Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. When a host is infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic to identify affected hosts and users. Captured packets can reveal the signatures of attacks, and this information can enable the users to recover the systems from damages caused by the attackers.

There are two aspects that make packet analysis very important. First, packet analysis is part of the baselines of anything important to a network because it allows knowing the state of a network in advance before problems arises [3]. Second, packet analysis is useful to diagnose a network in the case of attack, and it helps network administrators look into wires and know the traffic traversing them or the issues that might be present[4]. The later aspect is the foundation of network forensics with packet analysis tools like Wireshark. Analyzing packets with the goal of enforcing network security can help network users with the following [5]:

- Understanding network characteristics Learning who is on a network
- Determining who or what is utilizing available bandwidth
- Identifying peak network usage times
- Identifying possible attacks or malicious activity
- Finding unsecured and bloated applications

In this paper it has been described that how packet analysis tool like wireshark can be used to collect values for some basic indicators of compromise.The second section describes features and benefits of wireshark. The third section describes process of collecting basic indicators of compromise with example followed by discussion and conclusion.

2. PACKET SNIFFING USING WIRESHARK
There are various types of packet-sniffing programs, including both free and commercial ones. Each program is designed with different goals in mind. A few popular packet-analysis programs are tcpdump, OmniPeek, and Wireshark .tcpdump is a command-line program. OmniPeek and wireshark. Wireshark have graphical user inter- faces (GUIs).**Wireshark** is the world's foremost and widely-used network protocol analyzer. It lets us see what's happening in our network at a microscopic level. [6] .Wireshark offers several benefits that make it appealing for everyday use. It is aimed at both the journeyman and the expert packet analyst, and offers a variety of features to entice each.

2.1 Benefits of Wireshark

- **Supported protocols :** Wireshark supports more than 850 protocols. These range from common protocols like IP and DHCP to more advanced proprietary protocols like AppleTalk and BitTorrent. Wireshark is developed under an open source model, new protocol support is added with each update.
- **User-friendliness :** The Wireshark interface is one of the easiest to understand of any packet-sniffing application. It is GUI-based, with very clear context menus and a straightforward layout. Wireshark provides several features designed to enhance usability, such as protocol-based color coding and detailed graphical representations of raw data. command line interface of other packet sniffing tool like tcpdump is very complicated while The Wireshark GUI is great for those who are just entering the world of packet analysis.
- **Cost :** Wire- shark is released as free software under the GPL. it can be downloaded from it's official website and can be used for personal or commercial purpose.
- **Program support :** The Wireshark web page have links which directs to several forms of support, including online documentation, a support and development wiki, FAQs, and a place to sign up for the Wireshark mailing list, which is monitored by most of the program's top developers. Paid support for Wireshark is also available from CACE Technologies through its SharkNet program.
- **Operating system support :** Wireshark supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms. complete list of supported operating systems is available on the Wire- shark home page.

2.2 Collection of IOCs using wireshark

Indicators of compromise (IOCs) are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in earlier stages[1] Monitoring for indicators of compromise enables organizations to better detect and respond to security compromises. Collecting and correlating IOCs in real time means that organizations can more quickly identify security incidents that may have gone undetected by other tools and provides the necessary resources to perform forensic analysis of incidents. If security teams discover recurrence or patterns of specific IOCs they can update their security tools and policies to protect against future attacks as well .Wireshark is a popular tool for troubleshooting network related issues. When a host is infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic . and these packet captures can be used to identify affected hosts and users. Collection of IOCs help organizations to detect and prevent attack. In this section it is explained that how to Collect following IOC for malware using wireshark.

- File Hashes
- Host IP address
- Domain Name
- Host Name
- MAC address of host

Wireshark can be used in two ways one is to perform local capture and other is to analyze packet captures already available .There are many sites that provide pcap for analysis .we have used pcap from Traffic analysis exercise Pizza Bender. [7]

(I) Finding the Hash of infected file

The fundamental goal of web analytics is to collect and analyze data related to web traffic and usage patterns. The data mainly comes from four sources[8]

- Direct HTTP request data: directly comes from HTTP request messages (HTTP request headers).
- Network level and server generated data associated with HTTP requests: not part of an HTTP request, but it is required for successful request transmissions - for example, IP address of a requester.
- Application level data sent with HTTP requests: generated and processed by application level programs (such as JavaScript, PHP, and ASP.Net), including session and referrals. These are usually captured by internal logs rather than public web analytics services.
- External data: can be combined with on-site data to help augment the website behavior data described above and interpret web usage. For example, IP addresses are usually associated with Geographic regions and internet service providers, e-mail open and click-through rates, direct mail campaign data, sales and lead history, or other data types as needed.For Collecting hash of infected file follwing steps has been followed
  - (i) apply filter http.request in wireshark .
  - (ii) from the resuts of step(i) get the affected files from http objects.
  - (iii) Save the affected file(.in this example found file is a php file).
  - (iv) Get Hash of the file saved .

In this example Obtained Hash of infected file using wireshark is : a52a1e151bf4b993efcff87b3780d731 Screenshot of above process is presented in fig1 .

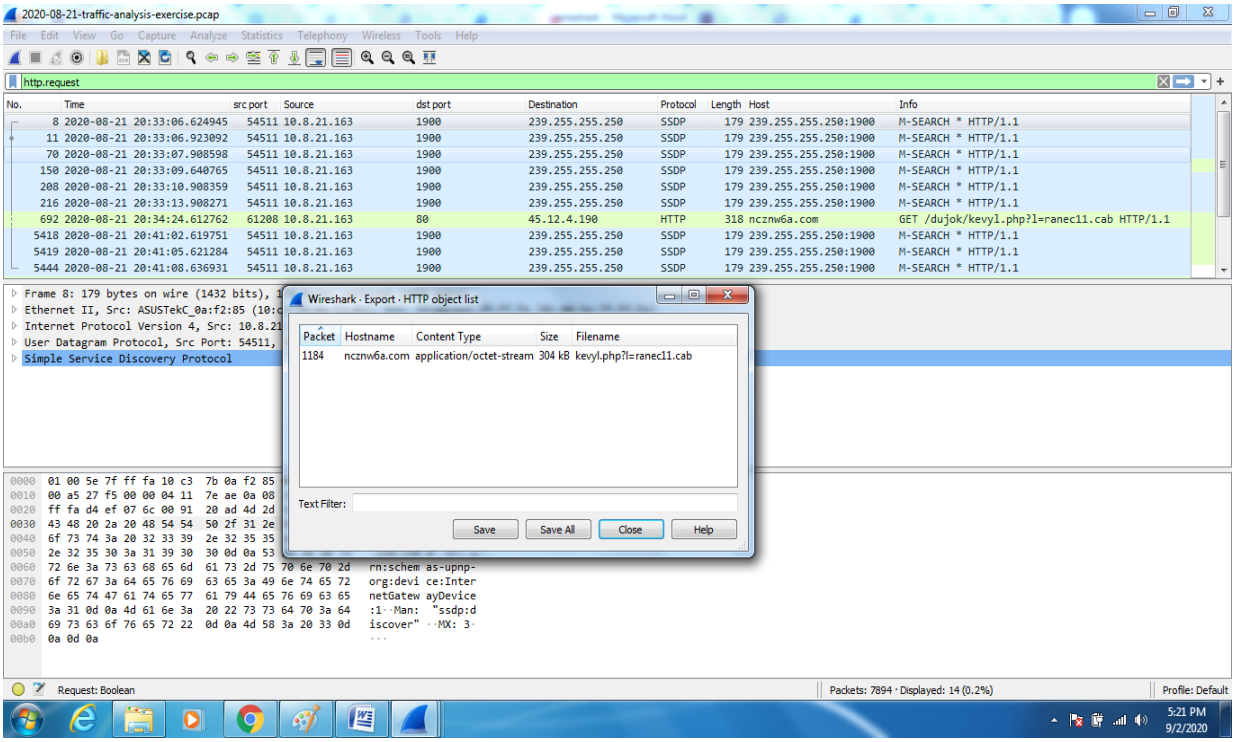

Fig 1 finding hash of an infected file using wireshark

(Ia) Checking whether the file is infected or Not:

By applying filter http.request a file and its hash can be found in(*I*). In next step it has to be checked whether the file is malicious or not .For this obtained file hashes has been checked at virustotal.com. VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004. VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.Files up to 650 MB can be uploaded to the website, or sent via email (max. 32MB). Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and, by extension, VirusTotal's own capability. Suspected URL's can be scanned and search through the VirusTotal dataset. VirusTotal for dynamic analysis of malware uses the Cuckoo sandbox.[9].

After scanning obtained file hashes on virustotal it has been found that file hashes are infected results are depicted in fig2.

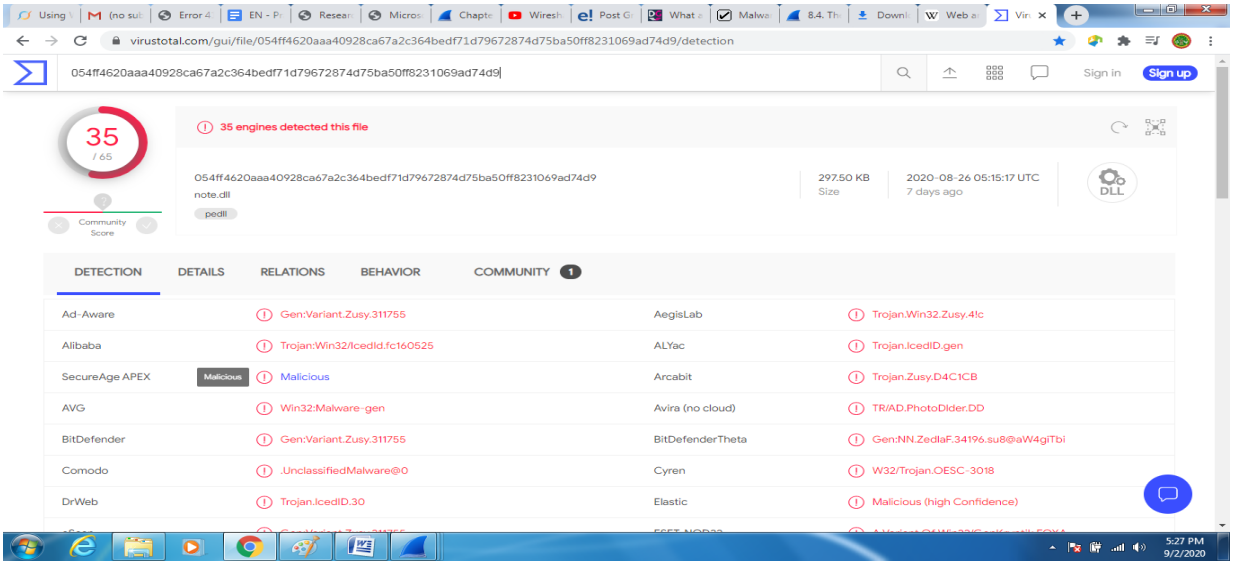

Fig2.Sacnning results on virustotal.com

(II) Finding the host name, Domain name, IP address and MAC address:

Any host generating traffic within the network should have three identifiers: a MAC address, an IP address, and a hostname. In most cases, alerts for suspicious activity are based on IP addresses.[10] If the access is avaiable to full packet capture of the network traffic, a pcap retrieved on an internal IP address should reveal an associated MAC address and hostname. Host information can be found using Wireshark by applying filter on two types of activities: Dynamic Host Configuration Protocol (DHCP) or NetBIOS Name Service (NBNS). DHCP traffic can help identify hosts for almost any type of computer connected to the network. DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network [11]. NBNS traffic is generated primarily by computers running Microsoft Windows or Apple hosts running MacOS.. Depending on how frequently a DHCP lease is renewed, DHCP traffic might not be there in pcap. Fortunately,in this case NBNS traffic can be used to identify hostnames for computers running Microsoft Windows or Apple hosts running MacOS .

In experiment presented in this paper host details have been found from NBNS traffic steps for obtaining host name , domain name,IP address and MAC address are as follows

(i) apply nbns as filter as depicted in fig3
(ii) for given source IP obtained the host DESKTOP-OF4FE8A<20> and
(iii) Domain Name can be found under hyper text transfer protocol in second window of wireshark as depicted in fig4 .
(iv) Obtained Domain is ncznw6a.com.
(v) Ger IP address of the host under Internet protocol in same window
(vi) Obtained IP addrees of host is 10.8.21.163.
(vii) IP address of infected machine is 45.12.4.190
(viii) MAC address of infected machine is 10:c3:7b:0a:f2:85 as depicted in fig5.

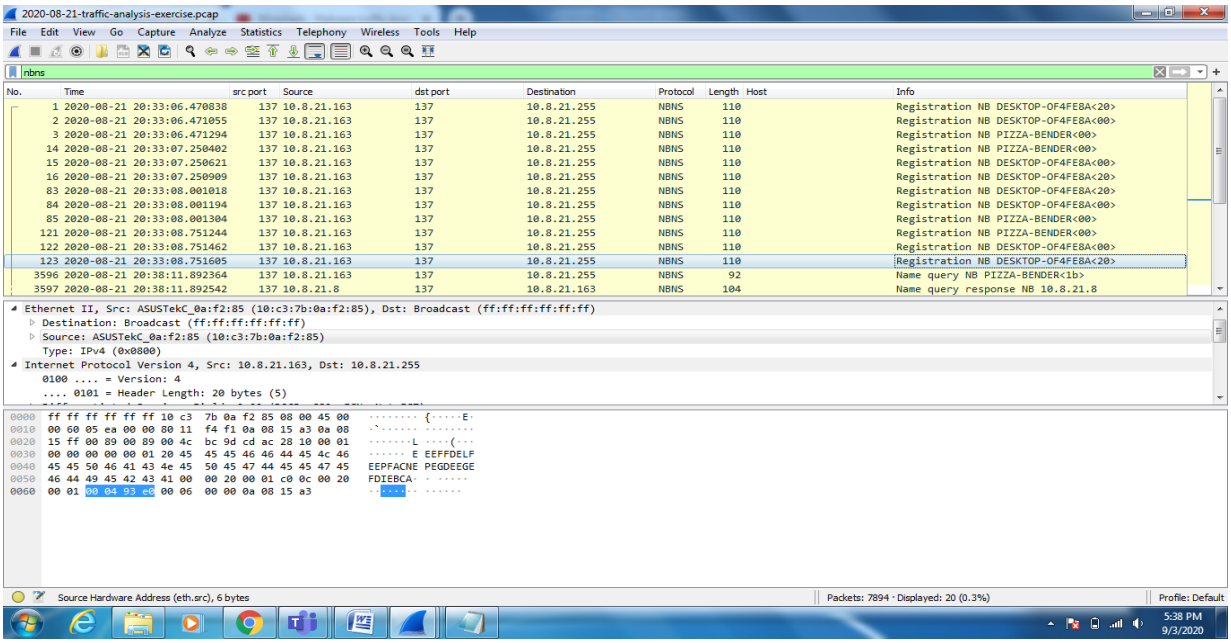

Fig3.Finding hostname from NBNS traffic using wireshark

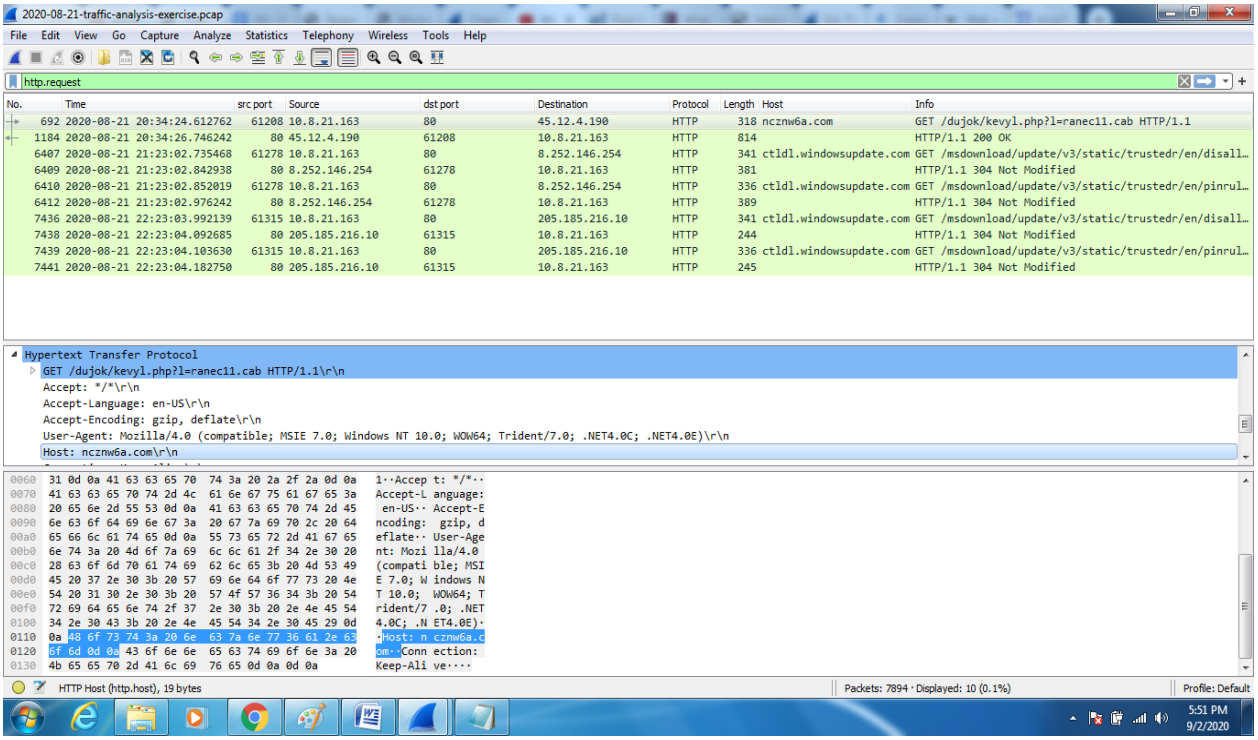

Fig 4 finding domain address using wireshark

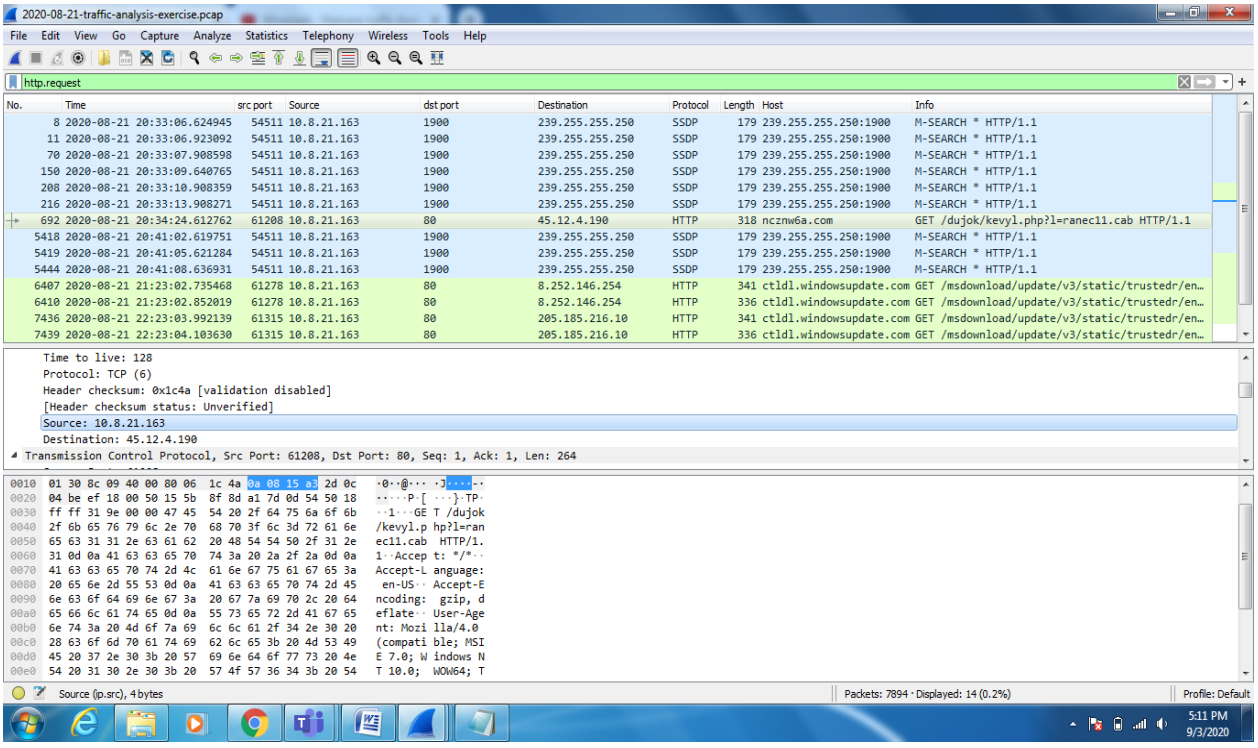

Fig5 finding IP address of infected Host

3. DISCUSSION

In section 3 procedure for finding answer for following questions using Wireshark has been explained

1. What are the infected file downloaded and their Hashes?

2. What is URL Domain of infected site?

3. What is the IP address of infected Machine?

4. What is the Host Name of infected Machine?

5. What is the MAC address of infected Machine?

The first part infected file hashes can be blocked inside network using virus guard .Access to the infected sites and their addresses can be blocked. Investigation on infected

PC whose MAC address can be made. infected files can be cleaned. In this way wireshark can be used to protect System.

Millions of new virus signatures are released yearly, and an antivirus can only detect viruses for known valid signatures and the unknown signatures escape the detection. today's networks are facing threats more than virus, such as malware, denial of service, port scanning covert channels, and information theft.however, antivirus software can only take very limited action on these various threats. Hackers can also target the antivirus software running on a machine, leading to multiple vulnerabilities of the system without the awareness of the user. For these different reasons, network traffic analysis at the packet level is necessary, and it can identify many different threats and attacks that could remain unnoticed by antivirus software. In the past, packet analyzers were very expensive and patented. Wireshark has changed all that. Wireshark is one of the best open source packet analysers available today, and it displays packet data as detailed as possible.

4 .CONCLUSION

The cases of packet analysis demonstrated in this paper by collecting values for Indicators of compromise will help to realize packet analysers, especially WireShark which is crucial to network forensics. "Indicators of compromise" helps to use threat data effectively, identify malware and quickly respond to incidents. Packet analyzer like wireshark can be used for security. However, despite its rich toolset, it is important to keep in mind that Wireshark is not an intrusion detection system. WireShark will not warn us when someone does strange things on network that he is not allowed to do, and it will not manipulate things on the network such as sending packets. The usefulness of Packet analyzer is that it is a convenient and effective tool that can help network security professionals figure out what is really happening in the network if strange things happen. As it has demonstrated in the paper, packet analysis in WireShark can discover a broad range of security threats and attacks against networked Computer systems.

5. REFERENCES

[1] Takahashi, D., Xiao, Y. and Meng, K. (2011) 'Virtual flow-net for accountability and forensics of computer and network systems', (Wiley Journal of) Security and Communication Networks, Vol. 7, No. 12, December, pp.2509–2526.

[2] Denis Makrushin" Indicators of Compromise as an Instrument for Threat Intelligence " Research article available online at https://www.researchgate.net/publication/349211330, Published in august 2015.

[3] Thor, J. (2009) Why You Need a Network Analyzer, online available http://www.technewsworld.com/story/67411.html

[4] Meng, K., Xiao, Y. and Vrbsky, "Building a wireless capturing tool for WiF", Wiley Journal of Security and Communication Networks, Vol. 2, No. 6, November–December S.V. (2009), pp.654–668.

[5] Vivens Ndatinya, Zhifeng Xiao, Vasudeva Rao Manepalli, Ke Meng and Yang Xiao "**Network forensics analysis using Wireshark"** Article in International Journal of Security and Networks · Vol. 10, No. 2, 2015.

[6] Chris Sanders "Practical Packet Analysis Using Wireshark to solve Real-World Network Problems" 2nd Edition

[7] https://www.malware-traffic-analysis.net/training-exercises.html 2020-08-21 -- Traffic analysis exercise - Pizza-Bender.

[8] Jack G Zheng, Svetlana Peltsverger "Web Analytics Overview" In book: Encyclopedia of Information Science and Technology, Third Edition Chapter: 756 Publisher: IGI Global January 2015

[9] https://en.wikipedia.org/wiki/VirusTotal.

[10] Richard Sharpe, Ed Warnicke, Ulf Lamping" Wireshark User's Guide Version" 3.7.0 available online at https://www.wireshark.org/docs/wsug_html/.

[11] Allied Telesis "Dynamic Host Configuration Protocol - DHCP Feature Overview and ConfigurationGuide"availableonlineathttps://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/dhcp_feature_overview_guide.pdf