

Every Tool Depend on the Users

M.sathishkumar¹P.Prabhakaran²

¹Student, Computer Applications, PSG College of Arts & Science, Coimbatore, India

²Assistant professor, Computer Applications, PSG College of Arts & Science, Coimbatore, India.

Submitted: 10-03-2021

Revised: 27-03-2021

Accepted: 31-03-2021

ABSTRACT: The current digital world network is one of the most advanced one. The Cyber industry is can attack and use some common technique is called network scanning. Network scanning is the process of discovering active herbs on the network. The network scanning to use lots of the tools available so we want to see the most popular tools in the network scanning. They are Nmap, solar winds and Wireshark widely used for network scanning. The work aim to review some books, journal and review website. Finally, the paper the conclude with a summary of Pros and cons, use cases and deployment scope, like hood to Recommend and alternative considered.

Keywords: Network scanning, Nmap, solar winds, Wireshark.

I. INTRODUCTION:

Cyber Security evolves over time as technology evolves to find out the vulnerabilities with the new types of tools. Network scanning involves many procedures that help to identify the ports, services and live hosts. The three efficient tools in my views are discussed below. Every tool depends on the users. I have selected the tools NMAP, SOLAR WINDS AND WIRESHARK because these are my favorite tools.

II. WHAT IS NETWORK SCANNING?

Network scanning is the process of discovering active hosts on the network and information about the hosts, such as operating system, active ports, services, and applications. Network scanning is comprised of the following basic techniques:

- **Network mapping** Sending messages to a host that will generate a response if the host is active.
- **Host discovery** The first part of network scanning is identifying active hosts, known as host discovery. Network scanners perform host discovery by attempting to solicit a response from a host. You can perform host discovery on a single IP address, a range of IP addresses, or a comma-separated list of IP address.

- **Port Scanning** Sending messages to a specified port to determine if it is active.
- **Service and Version Detection** Sending specially crafted messages to active ports to generate responses that will indicate the type and version of service running.
- **OS Detection** Sending specially crafted messages to an active host to generate certain responses that will indicate the type of operating system running on the host.
- **Evasion and Spoofing** A secure network blocks scanning techniques and alerts when a scan is detected. Firewalls block scanning attempts or drop responses to request packets. Intrusion detection systems (IDS) monitor network and host activity and create alerts when traffic matches predefined signatures. Most scanning techniques are easy to detect and will easily trigger IDS alarms. Attackers therefore use a variety of techniques to scan in stealth mode to evade firewalls and IDSs.

2.1. Common Network Scanning Tools

There are numerous network scanners available including free, open source and commercial products. The following list contains a few of the more popular scanners:

- **Nmap**("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- **Solar winds** Orion network performance monitor(NPM) is a scalable, easy to use, cost-effective network monitoring system that provides a complete overview of network environments by monitoring performance and availability.The Orion Platform's modular infrastructure enables NPM users to connect with and correlate Net Flow, configuration, virtual, server and application data to diagnose and resolve complex hybrid network performance issues.

- **Wireshark** is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

2.2 Who Uses Network Scanning?

Network, system, and security professionals use network scanning for a variety of administrative functions such as security auditing, compliance testing, asset management, and network and system inventory.

Network scanning may be used to manage patching and upgrades, monitor system uptime, assess policy compliance, verify firewall filter operation, and discover unauthorized devices and applications.

Attackers use network scanning to identify active hosts, open ports and services on a target device. The attacker may then exploit discovered vulnerabilities.

III. HISTORY OF NMAP:

This section provides a timeline of the most important milestones over 16 years of Nmap history.

- Many ancient and well-loved security tools, such as Netcat, tcpdump, and John the Ripper, haven't changed much over the years.
- Others, including Wireshark, Metasploit, Cain and Abel, and Snort, have been under constant development since the day they were released.
- Nmap is in that second category. It was released as a simple Linux-only port scanner in 1997.

- Over the next 16+ years it sprouted a myriad of valuable features, including OS detection, version detection, the Nmap Scripting Engine, a Windows port, a graphical user interface, Ncat, Nping, Ndiff, and more. We plan to continue this rapid development pace in the future as well!

3.1. Nmap features:

Nmap is packed with features. It has the capacity to perform basic, bare-bones scans, such as a simple ICMP pings to determine if hosts are up or down.

It also has the means to command advanced scans containing a multitude of options and scanning across a huge spectrum of IP address space while logging to specific file types or systems.

3.2. Nmap User Interface

Nmap is utilized as a command-line driven, UNIX-based tool. This is the way it was originally written and since command-line based applications have an advantage when it comes to creating batch scripts, geeks have flocked to this version for years.

From the command-line, Nmap is executed by simply calling the name of the application (nmap or nmap.exe) and applying the appropriate parameters or switches. It is very helpful, especially for the new user or for advanced configuration, to have a copy of the help instructions close-by. These can be easily accessed from the command-line by typing nmap -h.

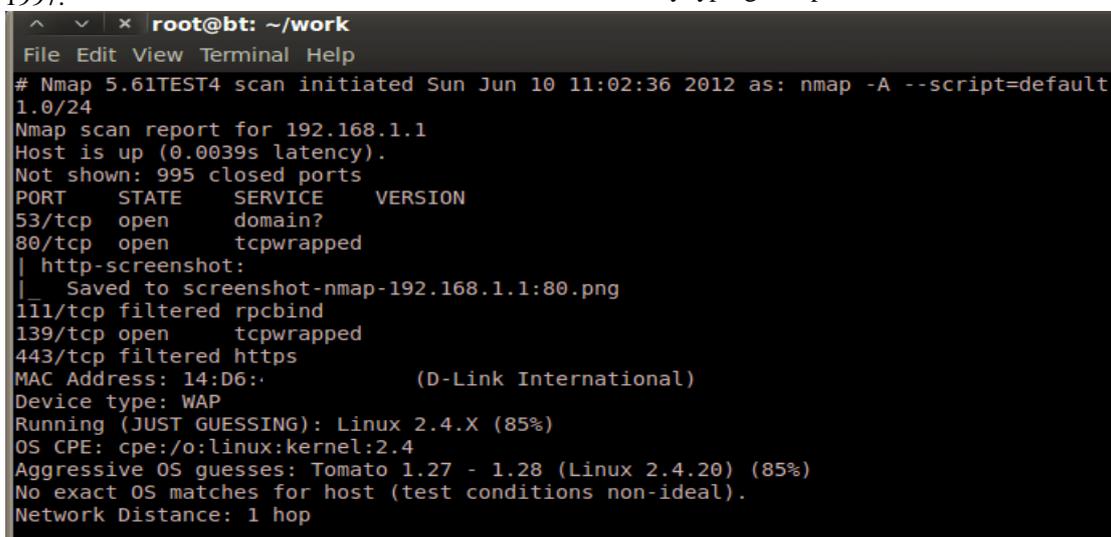


Fig: Nmap user interface

Fortunately for us now, this has all been replaced with Zenmap. In November 2007

Once installed, a Zenmap icon appears on the desktop and when double-clicked, the user is presented

with the ability to work with all Nmap configuration options and parameters.

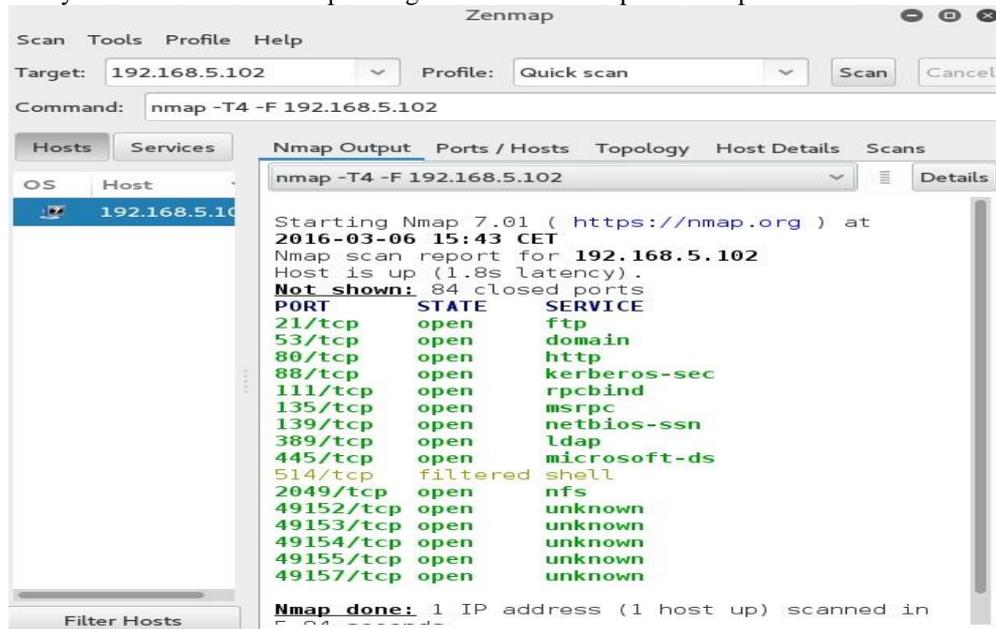


Fig: -zenmap user interface

3.3. What is Zenmap ?

Zenmap is a multi-platform, user-friendly, front-end GUI for Nmap. Like Nmap, Zenmap is free and open source. Zenmap allows you to perform all of the same usage options as in the command line version of Nmap.

Command wizard An interactive method to create Nmap commands.

Profile creation Zenmap includes several default profiles for common scan configurations. You can also save your own scans as profiles so you can run them repeatedly.

Scan tabs Zenmap allows you to run and display more than one scan at a time by using scan tabs.

Scan results saving Scan results can be saved to a file and viewed later.

Results comparison Saved scan results can be compared with each other to look for differences.

Searchable database Scan results are stored in a searchable database.

In this chapter you will learn how to use the Zenmap GUI and its various features for robust scanning management in the enterprise.

3.4. Use cases and deployment scope :

We use Nmap to both scan our network from time to time as well as to validate scan results from other platforms such as Nessus or Nexpose. One of the perks of NMAP is the built-in scripts that not only will look for weaknesses but also validate them by performing the exploit to see if the vulnerability can be exploited or not.

Nmap is a tool that I would say is always required in network testing. It's literally the first step to enumerating a network host. It's also extremely useful for non-intrusive testing as well. I would use Nmap before I use any other major scanner just to get a good idea of the open ports, then I would nail those with another test. It's only being used by our IS department. Mainly for scanning of open ports on devices. Looking for possible security holes using Nmap's scripting engine.

3.5. Pros and Cons

- + Very user-intuitive.
- + Built-in scripts allow for vulnerability testing.
- + Enumeration
- + Port Scanning
- + Network scans
- + Vulnerability checks
- + Open/Closed ports.
- + OS detection.
- Better GUI for ZenMap.
- Can be difficult to learn and master.
- They do not make modules fast enough! More moremore!
- I would say it's hard for new people using it as there are too many switches.

- Better/faster **UDP** scanning. I know that **UDP** is best effort but something better would be great instead of waiting for timeouts.

3.6.Likelihood to Recommend

As a blue/red team member, NMAP is crucial to my day and I would highly recommend it to other users needing the same type of tool for scanning. This tool is a key program to use for enumeration and port-scanning a network. One of the caveats though is if you do not have network connectivity then this tool will not be able to provide any results.

Nmap should be used in any network environment, but can even be used to scan the local host. There is a myriad of uses for it though, I frequently use it when deploying cloud servers to audit ports, or check if traffic is getting through. I also use it to audit my own firewall, just to ensure the correct ports are opened and closed.

Powerful for such a small application. Easy to install on Linux, if not a default app that's already installed. If you need a quick scan of a network for up/down hosts and their IP address/name it's great. If you get into OS detection and mass port scanning of a large network, it does slow down a far bit.

3.7.Alternatives Considered:

While mainly a CLI tool, there is an unofficial GUI. This can help the learning curve but unlike **Nessus** and **Nexpose** where there is a well-made user interface, with NMAP you need to really leverage the CLI for the power behind it. When it comes to modules being community-driven however; NMAP normally has the latest exploits before commercial products receive them.

We have used these:

Angry IP Scanner, Advanced IP Scanner, Fing and Masscan.

These apps are all Windows-based other than Masscan but they all work the same other than some of them are a paid product.

Nessus is also a network scanner, but compared to Nmap, it's a bulky, juggernaut. Using Nessus to enumerate a network is like using a machine gun to cut a loaf of bread. If you are trying to be "quiet", you're not going to achieve that with Nessus. With Nmap however you can specify how loud you'd like to be and what kind of packets you want to send.

IV. HISTORY OF SOLAR WINDS:

Solar Winds was officially founded in 1999 in Tulsa, Oklahoma, and (as of 2009) had maintained profitability since its founding.

The company was co-founded by Donald Yonce (a former executive at Walmart) and his brother David Yonce. Solar Winds released its first products, Trace Route and Ping Sweep, earlier in March 1998 and released its first web-based network performance monitoring application in November 2001.

According to Michael Bennett, who became the chief executive officer in 2006, the name Solar Winds was chosen by an early employee and that the company has nothing to do with solar or wind power.

In 2006, the company moved its headquarters to Austin, Texas, where about 300 of the company's total 450 employees were based as of 2011. Solar Winds was officially founded in 1999 in Tulsa, Oklahoma, and (as of 2009) had maintained profitability since its founding.

The company was co-founded by Donald Yonce (a former executive at Walmart) and his brother David Yonce. Solar Winds released its first products, Trace Route and Ping Sweep, earlier in March 1998 and released its first web-based network performance monitoring application in November 2001.

According to Michael Bennett, who became the chief executive officer in 2006, the name Solar Winds was chosen by an early employee and that the company has nothing to do with solar or wind power.

In 2006, the company moved its headquarters to Austin, Texas, where about 300 of the company's total 450 employees were based as of 2011.

4.1. Features of Solar Winds:

Customers today shouldn't have to deal with a collection of spreadsheets, incompatible tools, swivel-chair management, and overpriced products and deployment services. The Solar Winds Orion Platform can help conquer your infrastructure monitoring and management by offering superior tool consolidation for your environment while providing unique integrated functionalities, allowing customers to join the dots and solve problems with accuracy and speed at an affordable price.

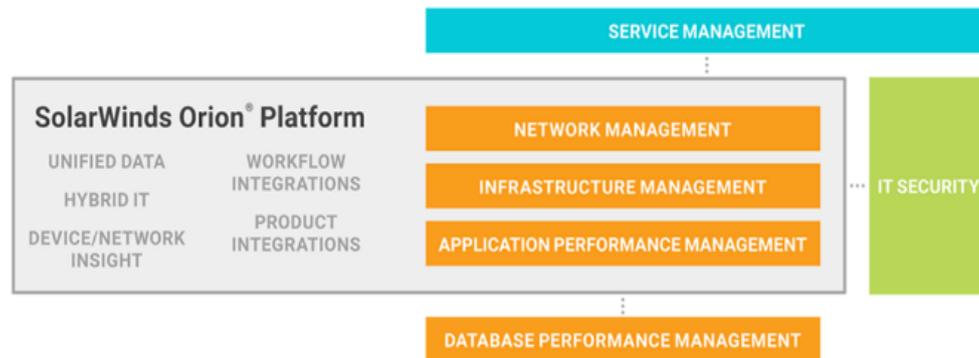


Fig: - Features of solar Winds

4.2. Solar Winds user interface:

- Detect, diagnose, and resolve network performance issues
- Track response time, availability, and uptime of routers, switches, and other SNMP-enabled devices
- Monitor and analyze network bandwidth performance and traffic patterns
- Find bandwidth hogs on a network and see which applications are using the most bandwidth
- View visual hop-by-hop analysis for devices along the delivery path with Net Path
- Enterprise Command Center.

4.3. Use Cases and Deployment Scope:

Solar Winds NPM was introduced into my environment recently and exclusively for virtual machines, especially our two data centers located in different states with domains to troubleshoot network slowness, major bottlenecks, the average response time, and latency between the data access between two data centers.

Currently, it is implemented in some of the data centers in the network which are critical to day to day life.

It addresses the network latency, the response time between the data centers, memory usage, and the bandwidth. Our team generates reports based on data collected from the logs.

We use Solar Winds NPM to monitor a relatively small airborne platform to ground network with routers, WAPs, firewalls, encryption devices (TACLANES), and servers. It addresses management of network nodes and mapping of the network.

We are using Solar Winds for all our networks as well as all client network infrastructures in the organization.

This will help us to provide real-time monitoring and IP flow top talkers instantly in a live scenario.

4.4. Pros and Cons

- + In the organization, our team basically monitors the data centers response time, the nodes in the cluster environment, and how they are performing from time to time.
- + These are production environments and very critical about data flow across the network and we also collect performance statistics from time to time and the data latency between two data centers and create reports.
- + Effective analysis of nodes
- + Comprehensive dashboard that is easy to tailor
- + Map editor is relatively easy to use
- + The other BIG deal is anticipating disk capacity - when volumes get to full, servers crash. With NPM, we can and create set thresholds for warning us before we run into issues, and then we can add storage, memory, and CPU, (especially on our Virtual environment.)

We also like the alerts that let us know when there are upgrades available.

- Sometimes it gives more verbose information if some of the VM cluster's installed SQL server has performance bottlenecks and it is hard to troubleshoot of them.
- We have issues in terms of data latency especially on SQL installed VM ware across data-centers which are working on dynamics which are hard to point exact hardware or SQL issues with the performance tool.
- The map editor select rectangle needs to be improved on as when you drag it it can get out of control.
- Need a more intuitive way to configure interfaces between nodes in map editor.

- Acknowledging and erasing node warnings should be more intuitive.
- It would be nice to be able to set up SNMP3 for some of our systems in an easier fashion. But it is not a show stopper
- Email alerts sometimes go wonky after an upgrade.

4.5. Alternatives Considered

- Nagios

Every monitoring tool has its merits and demerits. This is the competitive world and every organization will find an outstanding tool with a reasonable budget. There are so many monitoring tools available in the outside market and SolarWinds NPM is one among them. This outweighed because it has an efficient troubleshoot mechanism, gives accurate results, can go to history and find details. It communicates between the data centers effectively while others on the market are not good when it comes to a clustered environment. The cost competes with other products

- PRTG Network Monitor, Nagios Network Analyzer, IpswichWhat sup Gold and OpenVMS

Solar Winds is an all in one solution. We don't need to install different servers for different packages. It provides easy installation, easy maintenance, easy monitoring by NOC and end-users of NOC. Solar Winds tools have more features than other tools. We have done POC for many and we are satisfied with Solar Winds performance.

4.6. Likelihood to Recommend:

My only major complaint is that it seems to be too comprehensive for our applications. We have a relatively small network that we are monitoring and the features of NPM are not fully utilized in the application.

If you have a decent sized server farm, you will want to monitor it. If you spend time arguing with ISPs about whether they are at fault, you need Net Path to clarify.

If you are a very small business, you may get by without it, but it can really save your team time and effort when you deal with multiple servers.

We don't monitor EVERY node on our network - just the high level points - all servers, all network egress/ingress points, keeping ahead of storage space issues, and getting an email if something is happening you would otherwise be unable to check on a regular basis.

We spent a lot on the solution because we got it with our new switching equipment and were told it

was the best way to manage and monitor our switches.

V. HISTORY OF WIRESHARK:

In late 1997 Gerald Combs needed a tool for tracking down network problems and wanted to learn more about networking so he started writing Ethereal (the original name of the Wireshark project) as a way to solve both problems.

Ethereal was initially released after several pauses in development in July 1998 as version 0.2.0. Within days' patches, bug reports, and words of encouragement started arriving and Ethereal was on its way to success.

In 2006 the project moved house and re-emerged under a new name: Wireshark.

In 2015 Wireshark 2.0 was released, which featured a new user interface.

- Deep inspection of hundreds of protocols, with more being added all the time Live capture and offline analysis.
- Multi-platform: Runs on Windows, Linux, OS X, FreeBSD, Nets, and many others.
- The most powerful display filters in the industry.
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual Uptime and many others.
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

5.1. User interface of Wireshark:

When you open Wireshark without starting a capture or opening a capture file it will display the "Welcome Screen," which lists any recently opened capture files and available capture interfaces. It is possible to select more than one interface and capture from them simultaneously.

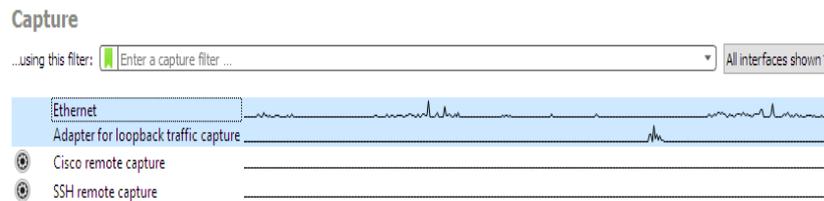


Fig: - User interface of Wireshark

Hovering over an interface will show any associated IPv4 and IPv6 addresses and its capture filter. Wireshark isn't limited to just network interfaces — on most systems you can also capture USB, Bluetooth, and other types of packets.

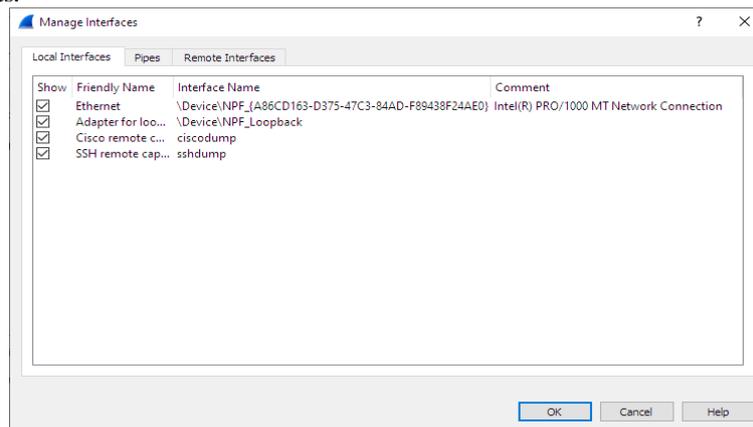


Fig: -“The Manage Interfaces Dialog Box.

5.2. Use Cases and Deployment Scope

Wireshark was my go-to tool for capturing and analyzing network traffic while building automation technologies (web bots) for years. It allowed me to quickly see what headers, cookies, and data were being sent during web requests and responses. So I could quickly and accurately mimic the data for automation, and it made life so much easier to have all that data collected and presented in one decent interface.

Wireshark is highly used in the troubleshooting side though, it is used by any of the computer networking enthusiast.

Furthermore, this software is nearly used by all the developers which are directly or indirectly involved in the development/ testing of the applications.

5.3. Pros and Cons

- + Captures all kinds of packet data in network traffic.
- + Save & restore captured packed data.
- + Show errors and issues in levels below the HTTP protocol.
- + Thi5s software dissects the packets to the maximum limit possible. It shows you everything

passing by in the packet including all the headers. It is amazing to see, without fail, how computers are actually interacting

- + This software can be downloaded and installed on any OS (Windows, Mac or Linux). It never limits you to one OS
- Can't modify or manipulate things/data on the network (only records data).
- A better interface would be nice - it's functional as-is, but it could use some polish.
- The way the software presents the information is sometimes cloggy. It can be well presented in some ways which will let the users understand the data in a much better format.

5.4. Alternatives Considered

I believe Fiddler is a slightly better choice, as it is more explicitly geared towards the HTTP protocol.

Because I'm building automation software, this feature is invaluable to me

Otherwise, Wireshark is the better choice because it can capture ANY type of network traffic, which is crucial for network admins (along with people in other professions).

As of now, we have used on Wireshark and what I have heard so far, this software is the best in its league.

It is free compared to solarwinds deep packet software. It is easier to use than tcpdump or Ettercap, and it has a much better presentation of the data. It's not as in depth as PRTG Network Monitor, but for an on the spot analysis, it is better for resource management and much quicker to set up and configure.

5.5.Likelihood to Recommend

If you need to analyze packet data across your network and want the low-level details, Wireshark is perfect for the job. It records the necessary data and presents it in a way that's relatively easy to read, analyze, and understand.

I believe Fiddler is a slightly better choice, as it is more explicitly geared towards the HTTP protocol. Wireshark is used for all the network related tasks. In cases where you think the application is not interacting well or if there is some network issue.

It needs a good knowledge of networking so as to operate and understand the data provided by the software

it is invaluable for capturing and analyzing network traffic and identifying issues with devices that are either malfunctioning, or possibly even set up as rogue devices on a network.

It's not a "set it and forget it" application, but it is well suited for on-the-spot analysis.

VI. CONCLUSION:

In the last 10 years, Cyber Security became an important area of research due to the exponential growth in the number of attacks on computers and networks. Usually, the existing commercial Cyber Security products are based on blacklisting and heuristic methods which completely fail to detect new types of attacks to the computers and networks. There are so many tools in network scanning, out of which my most favorite tools are NMAP, SOLAR WINDS AND WIRESHARK. In this paper the major concept is to assess the best tool but all three are my favorite since the uses of the tools varies on the performance and interface of the platform. All the tools are used in port scanning and each results are perfect but differs in the output format. Therefore, EVERYTHING DEPENDS ON THE USER. But every tool has its own drawbacks so you can refer some review websites like **GitHub** to know the usages. Most users and websites never visit the review websites. Thus I conclude that the tools must depend on the reviews of the users, thus resulting in EFFICIENT TOOLS.

REFERENCE:

- [1]. Angela Orebaugh, Becky Pinkard: Nmap enterprise your guide to network Scanning (2008).
- [2]. Joe Dissmeyer: Solar Winds Orion Network Performance Monitor (2013).
- [3]. Solar Winds IT monitoring and management tools are built for SysAdmins and network engineers who need powerful and affordable tools.<https://www.solarwinds.com/>.
- [4]. Wireshark is the world's foremost and widely-used network protocol analyzer.<https://www.wireshark.org/>.
- [5]. Trust Radius is the most trusted review site for business technology <https://www.trustradius.com/>.