

COMPARATIVE ANALYSIS OF DIFFERENT SECURITY TOOLS TO DETECT NETWORK RISKS

Juita Tushar Raut

Research Scholar, Computer Science & Applications, JJT University, Rajasthan, India

Dr. Yogesh Kumar Sharma

Research Guide, Computer Science & Applications, JJT University, Rajasthan, & Associate Professor (HOD/ Research Co-ordinator) Department of Computer Science, SJJT University, Rajasthan, India

Dr. Vikram Patil

Research Co-Guide, Computer Science & Applications, JJT University, Rajasthan & Director ADCET, Ashta, Dist-Sangali, Maharashtra, , India

Abstract: Now a day's providing security to the network is becoming a major challenge. Data is not considered as safe which travelled across to network. Various threats like hacking, spyware, phishing, spoofing, and sniffing exist. This paper discussed various network threats. Various open-source tools those are available to protect such types of attack. Tools like Acunetix, Intrusion prevention system (IPS) have been discussed in this paper.

Keywords: Spyware, Phishing, Spoofing, Snipping, IPS.

I. INTRODUCTION

Network Security is a set of rules and configuration which is designed to protect Confidentiality, Integrity, and Availability of the computer network. It is a protection of access to the files and directories in a computer network against hackers or intruders to misused the data and also changed the data. The aim of network security is to provide authentication to users. It provides protection against confidential data, ensuring data integrity, and continuous service of data. There is another way to protect the data using the Intrusion Prevention System (IPS). These systems continuously monitor the network, looking for malicious incidents, and capturing the information.

II. RELATED WORK

There are currently numerous of free tools available to conflict phishing and other web-predicted cheats, detective tools, etc.

Nabanita Mandal and Sonali Jadhav [2], in recent years providing severity to the network in an open-source has become a major challenge. Because information passing through the network is not safe. Already various types of extortions have existed in the system like sniffing, hoaxing, and phishing.

In this paper, the authors presented some threats which are attacks on the network. Also, there are some preventive techniques against such kind of issues. The author discussed various types of reconnaissance commands, also security scanner, and preventive techniques in this article. All these commands run on the Ubuntu operating system. In short, this article mainly focussed on such kind of commands, sniffing tools, and firewalls to better understand the numerous threats, attacks, and susceptibilities within the network.

Himani Sharma, et al [7], described phishing is a kind attack in which phishers use spoofed emails and malicious websites to thieves sensitive data of people. Now a day's various types of security tools are available to detect phishing, scams. This article, choose a total of eight detective tools for this study and figure out which tool is better. For this scanning, the author uses a dataset to find the results. Each tool was tested against the dataset that contains phishing and authenticates websites. The author conducted

surveys among fifty students and concluded that most of the internet users are unaware of such kinds of attacks.

Inderjit Kaur, et al [9], nowadays the expansion of the network is growing fast with its acceptance. But it is necessary to protect the network from the outside an attack. There is one of the techniques to observe the online data known as packet sniffing. There are numerous sniffing tools are available to monitor the information like Wireshark, Tcpdump, Nmap, Zenmap, Capsa, and many more.

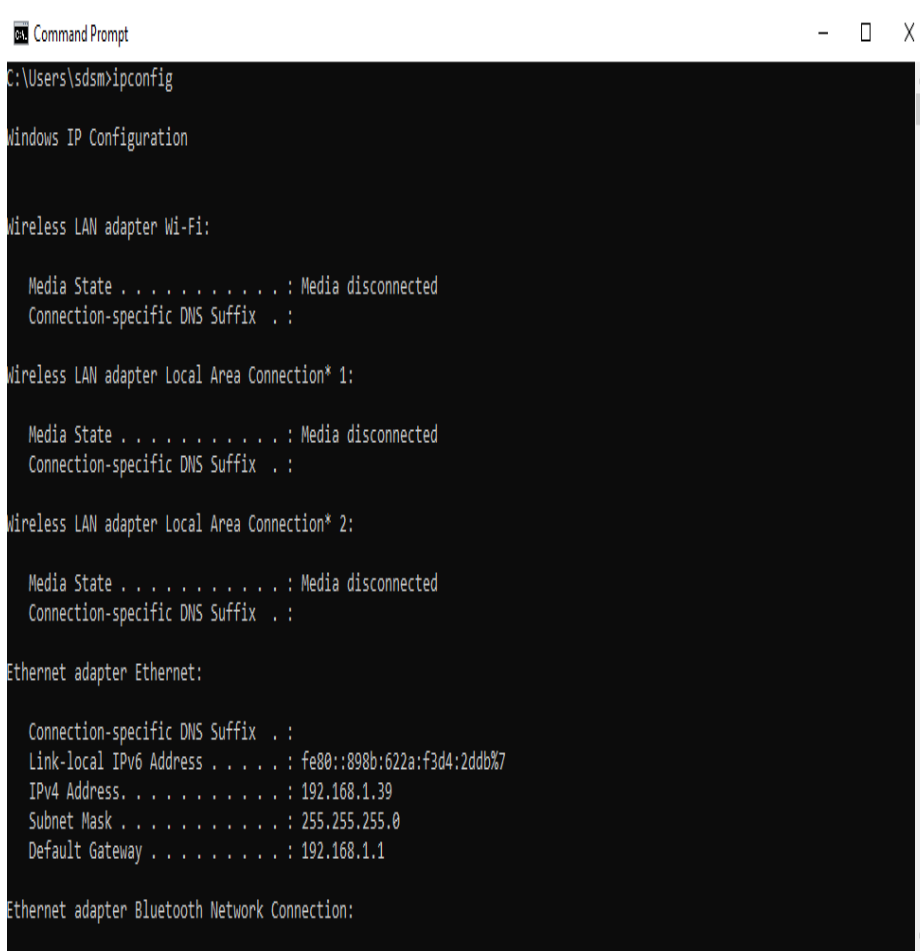
In this article, authors mainly focussed on various sniffing tools with their analysing capacity to capture the network traffic within a network. Few of them are used only for capturing the information without investigating the traffic. So, authors finally conclude that some tools are used for intrusion detection and few are used for pen-testing.

III. NETWORK ACCOUNTABILITY

It is a weakness which can be exploited by an intruder to perform malicious actions within a computer system. It can be any type like Bugs, weak passwords, missing data encryption, missing authorization.

To attack a particular machine, the first step is Reconnaissance. It means observation about the victim. It can be active or passive. In active type attacker engages with the targeted system to collect information about vulnerabilities. In passive type attacker to gain information about the targeted system without actively engaging with the systems. The commands are mainly ipconfig, netstat, netsh, and snort.

Fig.1 shows ipconfig command which is used for reconnaissance.



```
Command Prompt
C:\Users\sdsd>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

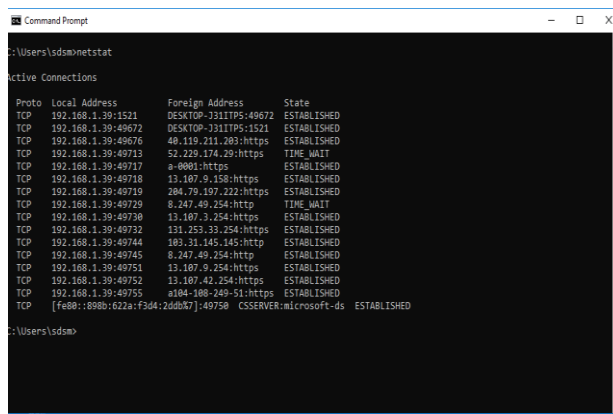
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::898b:622a:f3d4:2ddb%7
    IPv4 Address. . . . . : 192.168.1.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:
```

Fig.1 ipconfig command

Fig.2 shows netstat command which is used for detailed information about system and also with other computer which is connected via network.



```
Command Prompt
C:\Users\sdsdm>netstat

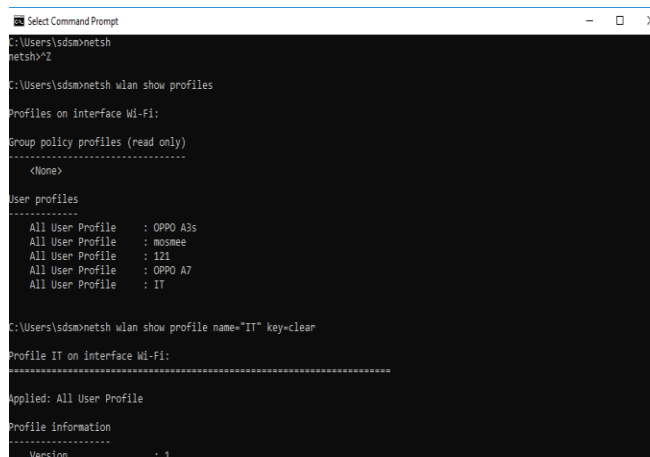
Active Connections

Proto Local Address           Foreign Address         State
TCP    192.168.1.39:1521       DESKTOP-3311TPS:49672  ESTABLISHED
TCP    192.168.1.39:49672     DESKTOP-3311TPS:1521  ESTABLISHED
TCP    192.168.1.39:49676     40.119.211.203:https   ESTABLISHED
TCP    192.168.1.39:49713     52.229.174.29:https    ESTABLISHED
TCP    192.168.1.39:49717     a-0001:https          ESTABLISHED
TCP    192.168.1.39:49718     13.107.9.158:https     ESTABLISHED
TCP    192.168.1.39:49719     204.79.197.222:https   ESTABLISHED
TCP    192.168.1.39:49729     8.247.49.254:http      TIME_WAIT
TCP    192.168.1.39:49730     13.107.9.254:https     ESTABLISHED
TCP    192.168.1.39:49732     131.253.33.254:https   ESTABLISHED
TCP    192.168.1.39:49744     103.31.145.145:http    ESTABLISHED
TCP    192.168.1.39:49745     8.247.49.254:http      ESTABLISHED
TCP    192.168.1.39:49751     13.107.9.254:https     ESTABLISHED
TCP    192.168.1.39:49752     13.107.42.254:https    ESTABLISHED
TCP    192.168.1.39:49755     a104-160-249-51:https  ESTABLISHED
TCP    [Fe80::898b:622a:F3d4:2ddbK7]:49750  CSERVER:microsoft-ds  ESTABLISHED

C:\Users\sdsdm>
```

Fig. 2 netstat command

Fig. 3 shows netsh command which is used to display or modify the network configuration of a computer that is currently running.



```
Select Command Prompt
C:\Users\sdsdm>netsh
netsh>?

C:\Users\sdsdm>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
-----
<None>

User profiles
-----
All User Profile : OPPO A3s
All User Profile : mosmee
All User Profile : 121
All User Profile : OPPO A7
All User Profile : IT

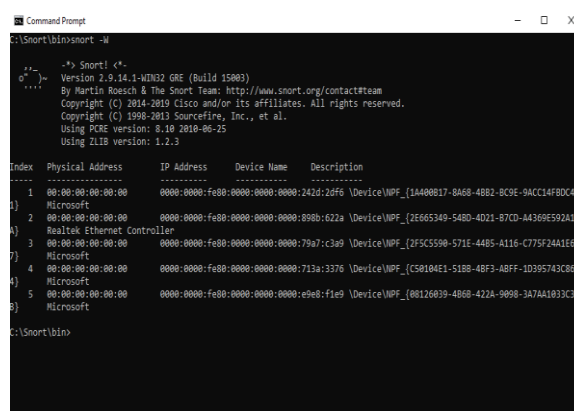
C:\Users\sdsdm>netsh wlan show profile name="IT" key=clear

Profile IT on interface Wi-Fi:
-----
Applied: All User Profile

Profile information
-----
Version : 1
```

Fig.3 netsh command

Fig.4 shows snort command. Snort is used to read IP packets , logs th IP packets and also used as Intrusion Prevention System.



```
Command Prompt
C:\Snort\bin>snort -w

Snort!
Version 2.9.14.1-UM32 GRE (Build 15903)
By Martin Roesch & The Snort Team: http://www.snort.org/contactteam
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.19 2018-06-25
Using ZLIB version: 1.2.3

Index Physical Address IP Address Device Name Description
-----
1 00:00:00:00:00:00 0000:0000:fe80:0000:0000:2426:2dfe \Device\NPF_{1A400B17-8A68-48B2-BC9E-9ACC14F80C...
Microsoft
2 00:00:00:00:00:00 0000:0000:fe80:0000:0000:898b:622a \Device\NPF_{2E665349-548D-4D21-87CD-AA369E592A1...
Realtek Ethernet Controller
3 00:00:00:00:00:00 0000:0000:fe80:0000:0000:79a7:c3a9 \Device\NPF_{2F5C5590-571E-4485-A116-C775F24A1E8...
Microsoft
4 00:00:00:00:00:00 0000:0000:fe80:0000:0000:713a:3376 \Device\NPF_{C58104E1-51B8-48F3-ABFF-1D395743C8...
Microsoft
5 00:00:00:00:00:00 0000:0000:fe80:0000:0000:e6e8:1fe9 \Device\NPF_{08126039-4868-422A-9098-3A7AA1833C...
Microsoft

C:\Snort\bin>
```

Fig.4 snort command

To prevent active reconnaissance, an intrusion prevention system along with a firewall is used. This combination helps to detect this type of attack. In passive reconnaissance there is no direct communication with client. It just gathered information without knowing to clients.

IV. SCANNING THE NETWORK

Network scanning is used to gather information of the computer system. It is mainly used for security evaluation, maintenance of system, and also performing attacks by an intruder. It evaluated the target host's also filtering system between user and targeted hosts. It scans port as well as the vulnerability of the computing system.

In this paper, we were used Acunetix as a vulnerable scanning tool. It is used to scan web applications. This tool is available on Windows, Linux operating system as well as online service. Fig.5 shows scanning windows of acunetix tool.

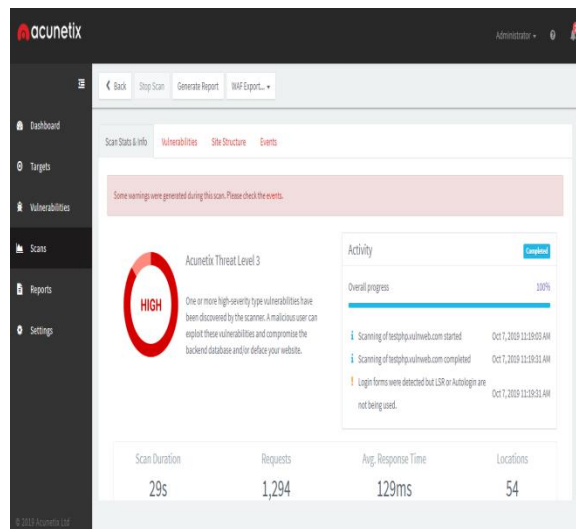


Fig. 5 scanning progress

Fig . 6 shows the vulnerability report. In this scanning, we used a sample website to test the data. In that, we found total 20 of vulnerabilities in which 17 are high severity vulnerabilities found and 3 are medium vulnerabilities.

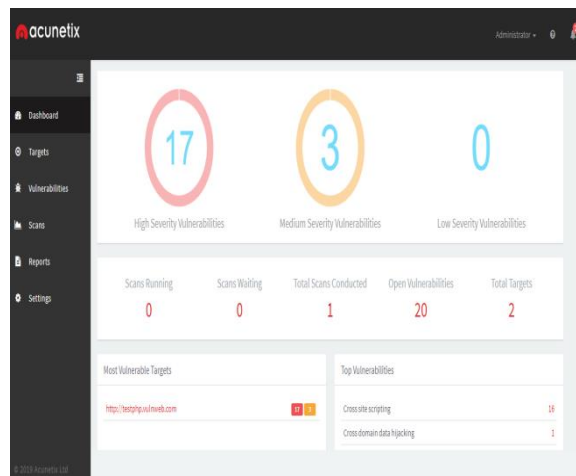


Fig.6 vulnerability report

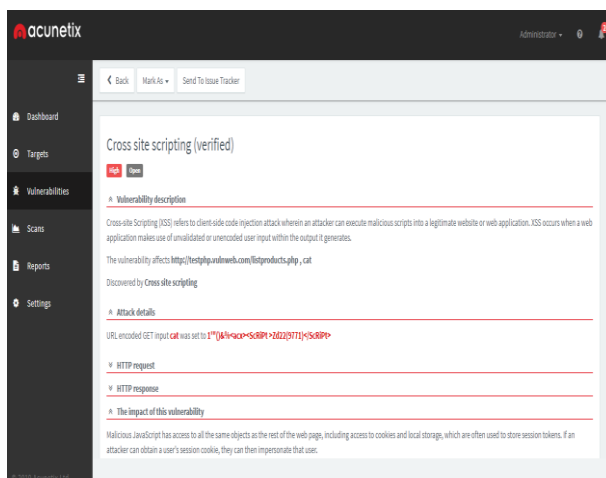


Fig.7 Report of a single vulnerability

V. INTRUSION PREVENTION SYSTEM

Intrusion Prevention System (IPS) is a software or device to detect or prevent malicious threats. It continuously observed your network, looking for possible malicious activity and collect their information. IPS directly sits behind the firewall and communication path between source and destination. It analyzes the traffic and takes actions on all traffic flows that enter into the network. It is also called a Intrusion detection prevention system.

It sending an alarm to the administrator, dropping the malicious packets, block the traffic, and also reset the connection. Intrusion Prevention system is found in four different ways.

- 1) Network-based: This is used to protect our computer network. It reads all incoming packets and finds suspicious patterns and notifying administrators. It detects suspicious activity such as a denial of service attack, port scan, etc.
- 2) Wireless: Which protect the wireless network. It monitors network performance and also discovers access points with its configuration.
- 3) Network behaviour: It analyses and monitors the network system and generates alerts.
- 4) Host-based: It comes as installed software to protect a single computer. For example snort, Suricata, malware defender.

VI. Comparison

Command /Tool	Purpose
Ipconfig	reconnaissance
Netstat	reconnaissance
Netsh	reconnaissance
Snort	Packet sniffer
Acunetix	Web scanning

Table I. Security tools and their purpose

The table I shows the tools with respect to their purpose that is used in this research.

It can be observed that all the commands like ipconfig, netstat netsh acts as a reconnaissance. It means information- gathering tools. The command like snort is used as a packet sniffer. This is also used as intrusion prevention system. Tools like Acunetix work as web scanning.

VII. CONCLUSION

Now a day's security in the network is a major Issue. In the market many security tools are available to protect the data but still, data transmitted over the network is not safe. In this paper section III and IV gives the details of commands and security tool that provides scanning and reconnaissance of the system. Section V gives the details of the intrusion prevention system to understand the risk, attacks, and accountability of the network.

REFERENCES

- [1] Ms. Shweta Thakre (2018),” Studying the Effectiveness of Various Tools in Detecting the Protecting Mechanisms Implemented in Web-Applications”, ISBN: 978-1-5386-2456-2, Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA 2018).
- [2] Nabanita Mandal, Sonali Jadhav (2016),” A Survey on Network Security Tools for Open Source”, 978-1-5090-1936-6.
- [3] S. Mishra, L. Jena, and A. Pradhan,” Networking Devices and Topologies: A succinct study”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No.11, pp. 347-357, November 2012.
- [4] Kurundkar G.D, Naik N.A, Dr.Khamitkar S.D ,“Network Intrusion Detection using SNORT”, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 2, Issue2,Mar-Apr 2012,pp.1288-1296.
- [5] Fakhreldeen Abbas Saeed, Eltyeb E. Abed Elgabar (2014),” Assessment of Open Source Web Application Security Scanners”, ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology, Vol. 61 No.2.
- [6] Dr. Yogesh Kumar Sharma, “Deep and machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic”, IOSR Journal of Engineering (IOSR JEN), ISSN (E):2250-3021, ISSN (P):2278-8719, PP 63-67.
- [7] Himani Sharma, Er. Meenakshi, Dr. Sandeep Kaur Bhatia (2017),” A COMPARATIVE ANALYSIS AND AWARENESS SURVEY OF PHISHING DETECTION TOOLS”, 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT).
- [8] Pallavi Asrodia, Hemlata Patel (2012),” Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis”, ISSN No. (Online): 2277-2626, International Journal of Electrical, Electronics and Computer Engineering, ISSN No. (Online): 2277-2626.
- [9] Inderjit Kaur, Harkarandeep Kaur, Er. Gurjot Singh (2014), “Analysing Various Packet Sniffing Tools”, International Journal of Electrical Electronics & Computer Science Engineering Volume 1, Issue 5 (October 2014), ISSN: 2348 2273.
- [10] Sunita Saini and Dr. Yogesh Kumar Sharma, “A research study of wireless network security: A Case study”, International Journal of Advanced Research in Computer Science and Software Engineering, volume 6 issue 3, March 2016,ISSN 2277 128X.