ORIGINAL RESEARCH PAPER | Engineering

APPLICATION ON DETECTION OF SYSTEM PORTS

KEY WORDS: PORT, WHOIS, CVE, SNIFFER

Ms.Warsha M.Choudhari	Professor,Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
Ankita Lohkare	Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
Ruchika Bangade	Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
Aditya Khante	Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
Abhishek Shukla	Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
Vaishanvi Rokade	Information Technology, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India

ABSTRACT

Application on detection of system ports determines what host are available on the network. Devices get hacked in the network, if they have open ports. Basically, majority of attacks performed on system is performed by scanning ports. Application on detection of system ports which scan for ports and tell user that which port is open. With the help of NMAP and NSE (Nmap Script Engine) whether the device is vulnerable or not can be determined based on CVE (Common Vulnerable Exposers). Due to vulnerable service running on port device connected in network get hacked. Traffic generated on system can be monitored on the host system. So that any kind of DDOS attack can be avoided. Also, the information about the IP address can be fetched from WHOIS sever.

1. INTRODUCTION

Network scanning refers to a set of procedures for identifying host, ports and services on a device in a network. Network scanning is one of the components of intelligence gathering, an attacker uses to create a profile of the target organization Application on detection of system ports determine what host are available on the network, the services that are enabled. With an increase in computer literacy people are becoming aware about the loopholes present in the Operating Systems, networking protocols, software applications which are used on a daily basis. To further complicate the things most of us do not follow good security practices, making the job of computer criminals even easier. Computer crimes have increased over the years.

One critical piece of information is the list of open ports of the system. Open ports of a system can be exploited in a number of ways. Having a system which predicts occurrence of attacks in the near future is advantageous. As port scans are usually performed before an actual attack, identification of port scan attempts gives precautionary indication that attacks might follow in the near future. This would make it possible to take precautionary steps to strengthen the defenses of the system. Information such as the open port information, the possible location from where the scan came, information from WHOIS database would help in providing clues about the scanner. This information can be used against attacker if an attack takes place in future.

A port scanner is an application designed to a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities. Sniffer shows information of traffic generated over a system and by that DDOS attack can be avoided.

After scanning the ports Nmap, Kali Linux can be used to exploit the vulnerabilities and system can be made secured by taking proper measures.

2. SYSTEM ARCHITECTURE

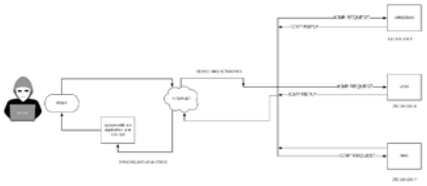


Fig. 2.1 Architecture Diagram

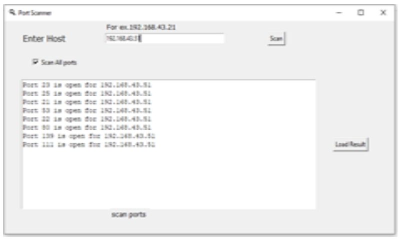
There are different devices with different operating system connected to the internet within same network with Application on Detection of System Port. This application devices connected to the internet can communicate with each other using ICMP request and ICMP reply protocol.

If the devices are connected to the internet, connection is established between the port. Sometimes user fail to secure the port and it may remain open. By scanning the other devices with different operating system with this application user can see open and close ports.

After getting port information, vulnerabilities can be exploited with the help of NMAP and KALI LINUX and CVE info and precautions can be taken.

Also, network traffic can be monitored using sniffer DDOS can be prevented

3. RESULT



Enter Host: 192.168.43.51

For ex.192.168.43.21

☑ Scan All ports

```
Port 23 is open for 192.168.43.51
Port 25 is open for 192.168.43.51
Port 21 is open for 192.168.43.51
Port 53 is open for 192.168.43.51
Port 22 is open for 192.168.43.51
Port 80 is open for 192.168.43.51
Port 139 is open for 192.168.43.51
Port 111 is open for 192.168.43.51
```

Fig. 3.1 Result of Port Scanner

This the output of the port scanner after entering the ip address showing which ports are open.

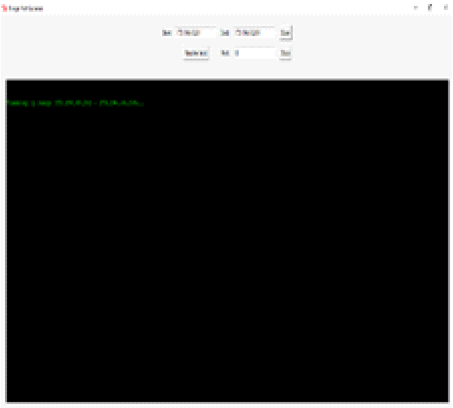


Fig.3.2 Result of Port Scanner

This the output of our Range port scanner after entering the ip range Showing the scanning process.

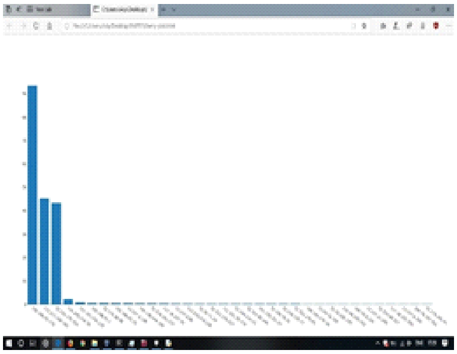


Fig.3.3 Result of Sniffer

This the output of Sniffer module showing of how much traffic generated from which ip using pacp file which is generated by wireshark

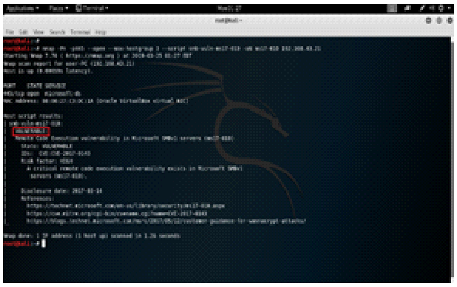


Fig.3.4 Result of CVE

Result of CVE using nmap search engine scripts to find the vulnear abilities in the system.

WHOIS

Enter a domain:

Fig 3.5 Result of WHOIS

4. CONCLUSION

Application on detection of system ports information obtained by scanning the device in network having IP address can be used both proactively to identify and notify while its open & close and by attackers to perform observation about the types and quantities of targets available and what weakness exist. The computers or devices connected in a network can be secured by scanning for open ports.

CVE using nmap search engine scripts to find the vulnearabilities in the system.

Sniffer shows information of traffic generated over a system and by that DDOS attack can be avoided.Fake Traffic generated can be easily monitored and precautions can be taken using this application

In WHOIS module by entering the domain name it shows the whole detail of domain like the date of creation ,date of expiry etc.

5. REFERENCES

[1]. Jayant Gadge and Anish Anand Patil, "Port Scan Detection.",October 8,2001.

[2]. Monowar H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita," Surveying Port Scans and Their Detection Methodologies.",2013