WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

VULNERABILITY NETWORK SCANNER

Manoj kumar. S

DR.MGR Educational and research institute, Maduravoyal, Chennai-600095

ABSTRACT

Network scanning is considered to be the first step taken by attackers trying to gain access to the targeted network. Therefore, it is useful for computer and network administrators to quickly locate scanned targets by network attackers. Resources and services can be further secured by tapping or installing security measures such as a firewall, infiltration detection system (IDS) or some alternative computer system. This article presents an investigative study of network scanning techniques. This study will identify the existing scanning methods. It also discusses how malicious code scanning methods can be used to detect vulnerable hosts and services. In addition, this article explores current approaches to detecting scanning on the network Network scanning is the process of detecting active devices on the network, signaling devices using a feature or feature of the network protocol, and waiting for a response. Today most network scanning is used in monitoring and administration, but scanning is also used to identify users for network components or attacks. The specific protocol features used in scanning depend on the network, but scanning for IP networks usually sends a simple message (for example a ping) to every possible IP address within a certain range, and then uses another protocol to recover data on Pink devices. Received.

1. INTRODUCTION

Network scanning is network port scanning and vulnerability scanning. Network port scanning Is the process of sending data packets over a network to specific service port numbers within a computer system (for example, port 23 for telnet, port 80 for HTTP, and so on). It identifies the network services available on a particular computer. This process can be useful for troubleshooting system problems or for tightening the security of the system

Network scanning Consists of three important methods used by an attacker to gather information. At footprint stage, the attacker makes a profile to the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. At the scanning stage, Attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer

At the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on. Network scanning refers to the use of a computer network to gather information of the computing systems. Network scanning is also mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

Scanning the network allows you to monitor the devices on your network, see how they work, diagnose vulnerabilities, and understand the traffic between connected devices and applications. Network scanning is the process of helping administrators collects information from all devices or endpoints on a network. During the scan, all active devices in the network send signals to the network and once the response is received, the scanner evaluates the results and checks for inconsistencies.

PROPOSED SYSTEM:

Combining this 4 tools into single application using python

1. PORT Scanner
    a) Port Scanner using Socket
    b) Port Scanner using ICMP (Live hosts in a network
    c) Port Scanner using TCP scan
    d) Threaded Port Scanner for increasing efficiency
2. IP Scanner

3. Send Ping
4. Packet Sniffer

Module Description:

1. PORT SCANNER:

A port scanner is to search a network host for open ports. It is often used by administrators to check the security of their networks and compromise by hackers. port scanner search for a open ports on your computer. Programs use ports to view and communicate with the outside world (the Net) (we use doors). Viruses are now built into port scanners that search unsuspecting computers on the Internet with open ports; If they detect them, they will disable or worsen your software and may report your personal activity and other information to another company. Port scanning is the process of scanning of multiple ports on the target host.

This program is based on how to scan the local database of remote system services connected to the server with the help of the IP / DCP address of the computer connected to the server. The scanner is used for checking links and allowing you to manipulate the local database of services . Once a hacker has installed the port scanner on your computer, they will know which services you accept. using this types of scanner we can gain unauthorized access to your computer.

DIFFERENT TYPES OF PORT SCANNER:

1. Port Scanner using Socket
2. Port Scanner using ICMP (Live hosts in a network
3. Port Scanner using TCP scan
4. hreaded Port Scanner for increasing efficiency

2. IP SCANNER:

The iP scanner tool most used in the line of field of networking. An IP scanner, as its name implies, is a scanner that scans various information on IP addresses and devices on your network. So, in a nutshell, an IP scanner scans all your network devices and the and gain information associated with them.

USES OF IP SCANNER

Security: The most important reason thing why we uses the IP scanner is for security purposes. we can also check the devices that are connected to your network. we also get detailed information about the devices that are connected to the network. It will allow to track the devices and detect unknown or suspicious devices on the network.

Network Scan: IP scanner is used to get the devices and their relevant information within a short amount of time. we can use IP scanner to get the devices information of the network. Information is useful for security purpose to mapping the network.

The IP Scanner scans the devices to the selected IP address range. we can set the range of the IP address that we want to scan on the network and get a list back the information from the IP scanner. The IP will contain all the information related to the devices on the network.

DETAILS PROVIDED BY IP SCANNER:

- IP Addresses
- Mac Addresses
- Vendor
- Operating System
- Number of Open Ports
- Status of Ports

3. SEND PING:

A ping (Pocket Internet or Internet-Network Cropper) is a basic web program that allows the user to verify the presence of a specific target IP address and accept requests from the computer network administration. The abstract is designed to match the sound of the submarine's words returning sonar pulse send Ping sends an Internet Control Message Protocol (ICMP) echo request to the specific interface on the device network. When the ping command is selected , the ping signal is sent to targeted address. When the target host receives the request, and it responds by sending an echo response packet is activate.

It has serves two specific purposes one is verifying the target host is available and determining round-trip time (RTT) and latency.

RTT is used to Check the time how long it taken to receive a response. Measured in milliseconds in the process starts when a browser sends a request to a server ad response from the server is received. RTT performance metric of web applications. Ping commands send multiple requests usually four or three and display results. The echo ping results show whether a particular request send and received a successful response. It includes all the number of bytes received and the time to took to receive a reply or server

4. PACKET SNIFFER:

If any data is to be sent over the computer network, it will be split into smaller units called data packets at the sender's terminal and reconnected to the sender's terminal in its original form. It is the unit of communication through in a computer network. The process of capturing data packets across a computer network is called pocket sniffing. It's like tapping a wire on a telephone network. It is often used by crackers and hackers to illegally gather information about the network. It is used by ISPs, advertisers and governments

- sniffing to track all your activities such as:
- who is receiver of your email
- content of that email
- what we download
- sites we visit
- what we looked on that website
- downloads from a site
- events like video, audio

Pocket sniping is done using a tool collect all the data into package. It may or may not be filtered. Some data packets are filtered only when they need to be captured and not at all when all packets need to be captured. WireShark and SmartSniff used for pocket sniffing tools.

HOW TO PREVENT FROM PACKET SNIFFING

1. Encrypting data we receive or send
2. Use only trusted Wi-Fi networks
3. Scanning your network regularly

PROPOSED SYSTEM ADVANTAGES:

- we can handle a large commercial size data of bases
- Simple and easy to implement
- Higher accuracy for scanning multiple
- Easy to use - Even an unexperienced user will be able to scan the network with just a few clicks by using this scanner.
- Good performance - The program uses multi-threaded scanning. The network scan rate achieves thousands of computers per minute Higher detection rate
- Available to all users -No administrator privileges are required for scanning.

PROBLEM STATEMENT

The only way to track all ports is by using a port scanner, and the gives very accurate port scanner will be an online port scan. Scanning your ports using software like nmap will work good, but it will not test your firewall's ability to block port activity. And Our free programming PORT SCANNER will help you us to do just that the perfect result and accurate in short period of time.

2. CONCLUSION

In today's world, every company, strives hard to safeguard its devices and systems from unauthorized access. The every company must have be have a prevention plan in hand to avoid future attacks on the network.

Every company need to invest in the robust network scanning tools to secure the system against potential cyberattacks without compromising with the performance. Before choosing a tool, they need to understand which type of scanning tool is a perfect useful and fit for their company network. The admins need to implement the right tools to protect the systems from being hacked along with a robust scanner to translate packet data into easily readable information.

REFERENCE

[1] L. Granquist, Port 0 Scanning,Bugtraq mailing list archives, D. Comer, Internetworking with TCP/IPVol. 3, Second Edition. Prentice Hall, 2000

[2] Ryan Spangler, "Packet Sniffer Detection with AntiSniff". University of Wisconsin, Department ofComputer and Network Administration, May 201 1.

[3] Miller, R. (2019). The OSI Model: An Overview. SANS Institute., Page(s):5-12

[4] Nimisha P, R. G. (2014). Packet Sniffing: Network Wiretapping. IEEE International Advance Computing Conference.

[5] Pallavi Asrodia, H. (2012). Network Traffic Analysis Using Packet Sniffer . International Journal of Engineering Research and Applications

[6] M. de Vivo, G. de Vivo, G. Isern, Internet S e c u r i t y A t t a c k s a t t h e B a si c L e v e ls . Operating Systems Review, Vol. 32, No. 2. SIGOPS, ACM, April 1998.

[7] Kocher, Joshua E., and David P. Gilliam. "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning." 14th IEEE International Workshops on Enabling Technologies:

[8] Chris Senders, Practical Packet Analysis, using Wireshark to solve real-world network problems, No Starch Press Inc, San Francisco, 2007