PREVENTION OF PORT FORWARDING AND PRIVILEGE ESCALATION

Mrs. J.Mythili M.E.,K.Arun Prasanth , R.J Dharsun,

R.Dhinakaran, N.Gowtham

Assistant Professor/CSE, Dept.of.CSE,

Department of Computer Science and Engineering, Sengunthar Engineering College (AUTONOMOUS).

ABSTRACT

A privilege escalation in the Linux system can be defined as a method of gaining access to the kernel system and allowing the user to have an administrative access to the local admin account system on the computer. This problem describes the of concept attack scheme using Dynamic port forwarding. The attack scheme, the same interaction on the physical access to the computer system could be accomplished by the attacker using a little effort specialized Port vulnerability to take over the computer system in full where it will collect valuable information,to avoid that through IP block and Preventing Port vulnerability.To preventing like user-friendly python programming language to run check and resolve the problem.

Privileges describe what a user is permitted to do such as viewing files, modifying or deleting data. Privilege escalation takes place when a user gets access to more resources or services than they are normally allowed to perform unauthorized actions. It attacks the main kernal OS of the Computer system like as a user to escalate the admin permission.

Keywords: **Privilege escalation, Port ,vulnerability**

1. INTRODUCTION

Port vulnerability mechanims to scanning 65,565 ports then to block backdoor operation running on that port,In case the system Port forwarded to prevent that process.A privilege escalation in a way to obtain the permission form unprivileged access to the higher level of administrator privilege. In Linux system that is being access into guest account have a restricted features and limitation to certain function. A privilege escalation in a way to obtain the permission form unprivileged access to the higher level of administrator privilege. In Linux system that is being access into guest account have a restricted features and limitation to certain function. It is include to limit the activity of the guest user to change or going into the system's programs. Whereby User Account Control (UAC) is a Linux program that has a concept of privilege escalation by means if the guest user is performing a task under administrative level of permission.The existing Kernels of operating systems are written in low-level unsafe languages inevitably vulnerable to memory corruption attacks.

User Account Control or UAC in Linux is a security feature which helps to prevent an unauthorized changes to the Linux operating system that can be initiated by applications, users or malware. This feature will ensure only certain changes will be executed under normal guest account which required approval from the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

administrator account.

2. LITERATURESURVEY

Scanning of ports on a computer occurs frequently on the Internet. An attacker performs port scans of Internet protocol addresses to find vulnerable hosts to compromise. However, it is also useful for system administrators and other network defenders to detect port scans as possible preliminaries to more serious attacks. It is a very difficult task to recognize instances of malicious port scanning. In general, a port scan may be an instance of a scan by attackers or an instance of a scan by network defenders. In this survey, we present research and development trends in this area. Our presentation includes a discussion of common port scan attacks. We provide a comparison of port scan methods based on type, mode of detection, mechanism used for detection and other characteristics. This survey also reports on the available data sets and evaluation criteria for port scan detection approaches.

In Paper[1]the authors designed Scanning of ports on a computer occurs frequently on the Internet. An attacker performs port scans of IP addresses to find vulnerable hosts to compromise.

However, it is also useful for system administrators and other network defenders to detect port scans as possible preliminaries to more serious attacks. It is a very difficult task to recognize instances of malicious port scanning. In general, a port scan may be an instance of a scan by attackers or an instance of a scan by network defenders.

Port scanning is designed to probe a network host for open ports and other services available. It is useful for system administrators and other network defenders to detect port scans as a useful technique for recognizing precursors to serious attacks. From the attacker's viewpoint, a port scan is useful forgathering relevant information for launching a successful attack. Thus it is of considerable interest to attackers to determine whether or not the defenders of a network are scanning ports regularly.

In the transmission layer, there has two important transmission protocol transmission control protocol (TCP) and the user data report protocol (UDP). The so called port scanning has the very simple principle. It uses the socket import API that provided by the operation system and does the connection with TCP or UDP. Moreover, utilizes the protocol character to connect each port of the network target host, based on the backward result and connection to judge the port open. [3] The port scanning will try to connect the various services of the different ports by the long distance TCP/IP protocol.

The port scanning technology can through one exploring method and technology to detect the hidden trouble of the system or the network. Compare with other host in the network, each computer is the closed space. Moreover, the channel to communicate with the outside world is the port. In the OSI model, the port belongs to the transmission layer. The transmission layer will identify each service through one port number.

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services associated with that port. Port scanning is a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Nmap is a free, open source tool that is available under the GNU General Public License as published by the Free Software Foundation. It is most often used by network administrators and IT security professionals or Hackers to scan enterprise networks, looking for live hosts, specific services, or specific operating systems.

Ports are an integral part of the Internet's communication model. All communication over

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the Internet is exchanged via ports. Every IP address contains two kinds of ports, UDP and TCP ports, and there are up to 65,535 of each for any given IP address.

Services that rely on the Internet (like web browsers, web pages, and file transfer services) rely on specific ports to receive and transmit information. Developers use file transfer protocols (FTPs) or SSH to run encrypted tunnels across computers to share information between hosts.

Once a service is running on a certain port, you can't run other services on it. For example, starting Apache after you've already started Nginx on port 80 will lead to a failed operation because the port is already in use.

Open ports become dangerous when legitimate services from ports are exploited through security vulnerabilities or malicious services are introduced to a system via malware or social engineering, cybercriminals can use these services in conjunction with open ports to gain unauthorized access to sensitive data.

Closing unused ports reduces your security risk by reducing the number of attack vectors your organization is exposed to ports.

3. WORKING AND METHODOLOGY

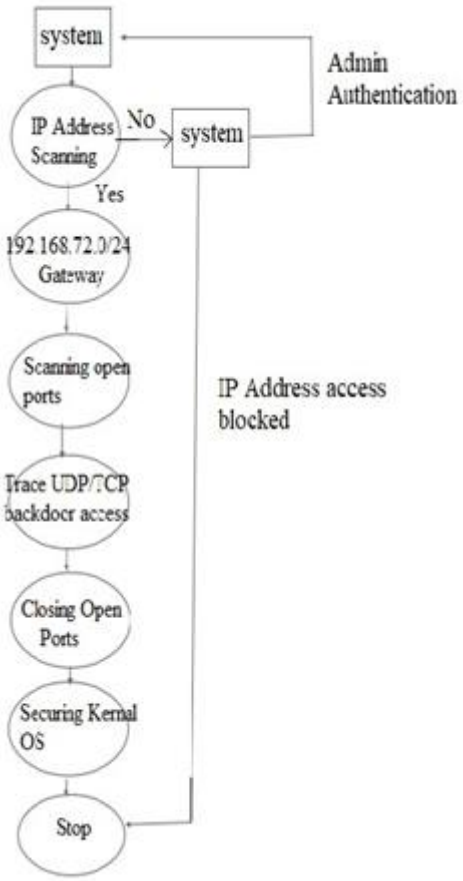
The key features of the port vulnerability major attacker will concentrated on the system vulnerability to bypass the firewall system through the client accessing control methodology that can break through the firewall first to port vulnerability the type of vulnerable for the system hijacking,

This is the mechanism to access the client data and information theft,bank account details then all over system control comes under the attacker.The client used atleast one or two ports like port 80 http for internet access,port 21 ftp for file transfer one communication to another communication system.

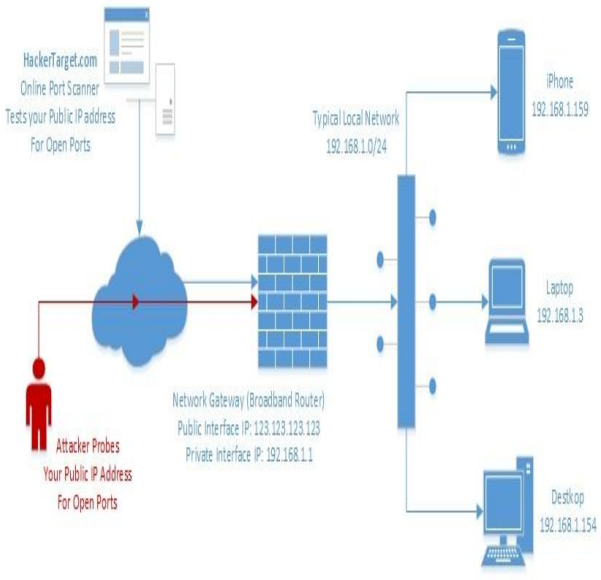
- **HTTPS (443):** Allows you to connect to the Internet by establishing a secure connection between web pages and the browser
- **SSH (22):** SSH or Secure Shell carries out the task of remotely connecting to a server or host, allowing you to execute a number of commands and move files.
- **Telnet (23):** Telnet establishes a connection between a server and a remote computer.
- **SMTP (25):** SMTP or Simple Mail Transfer Protocol ensures email messages are communicated over the network securely.

Then main disadvantage is enter external IP address to the admin that access into company or campus network that is to track the particular system to scan open ports by the attacker.To block external IP address system into the network. Then such system admin to scan individual opening ports and trace that port acts as a another illegal usage were running backdoor access undertake by the attacker by send shortcut TCP/UDP/UNIUX packets. They were attacker to enter in port 80 then port forwarded to port 50.We to find the open ports that to disconnect to block that will disconnect connection the to attacker that port default closed that cannot be opened again. Then next step suppose attacker will port forwarded to sending any payload, trojan files acts as a background processes, attacker try to reach kernal system to access all permission this step called as privilege Escalation process. To prevent that step payload misconfiguration were bash coding block escalating the system permission to gaining access file will be prevented.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731



- nmap-sT, which scans TCP ports,
- nmap-sU, which scans UDP ports,
- nmap-sV, which probes for the services being used on certain ports;
- nmap followed by an Internet Protocol address scans ports on that IP address
- nmap followed by an IP address with a slash after the last digit (e.g., 192.168.1.0/23) scans a subnet.



4. CONCLUSION

Port forwarding is a very useful method for connecting to machines on an internal network guarded by a firewall. It allows you to put mail servers, FTP servers, web servers, or Telnet hosts behind a firewall, where they can enjoy many of its protections. However, it also opens some security holes, which demand stricter attention to your security procedures and log files. It's easy to configure, but should be used with caution.As we perform port scan using nmap it will give us information about all port state and services running on that port by using various techniques. It will help us to narrow our choice to whether to attack on that host or not. But here we should keep in are mind that it is the first step to hack or protect any network after that there is lot more things remaining to do further. It will just give as an idea about which type of network is there.Privilege escalation attacks, irrespective of operating systems and environment, are still a major issue in the cyber-security spectrum. And the problem can't be curbed unless the rules are strengthened, but then again compromises in performance and efficiency are unavoidable since humans are involved. A perfect balance, a sweet spot has to be found and the most important part is that system admins need to be aware and ditch the mentality "this cannot happen to my system". The enforcement will take time, but it is, indeed, possible to render the ever persistence privilege escalation attacks, avoid.

5. FUTURE ENHANCEMENT

The Privilege Escalation review monitoring unknow background payload usage,opening unknow links can be used in any of the real

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

application in order to prevent unauthorized reviews.

Also to recommendation to admin to monitor the particular system usage that means legal value to prevent entire campus or college networks.

Preventing Port can be enhanced better in other field also.

REFERENCE

[1] 2014Tariq Ahamad Ahanger, Port Scan – A Security Concern, International Journal of Engineering and Innovative Technology(IJEIT),ISSN-2277-3754, Volume 3 Issue 10 April.

[2] Nmap Network Scanning Guide – Gordon Lyon.

[3] Zhang, J., et al.: Network program design. Wuhan University Press (2004).

[4] The vague detection strategy based on the port scanning. Journal of Computer Applications 23(10), 87–92 (2003).

[5] Wang, L., Wang, J.: The computer application of the vulnerability scanning system based on the network, vol. 23(98-99), p. 102 (2003).

[6] The information network security of vulnerability scanning based on plugni, vol. (12), pp. 4–50 (2003).

[7] The research of TCPSYN port scanning. Journal of Guangxi University of Technology 13(1), 25–27 (2002).

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731