Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

BACKDOOR ENTRANCE TO A WINDOWS SYSTEM

[1] Amandeep Kaur,[2] V. Vishal, [3] Amjan Shaik, [4]J. Ramesh Babu
[1] Assistant Professor, [3]Professor, [4]Associate Professor
Department of Computer Science and Engineering, St. Peter's Engineering College, Medchal,Hyderabad,TS,India.

Abstract:

In any computer, there are two points of entry to gain remote access. One requires user credentials to log in while another entry point is also known as a backdoor entry point. The backdoor is a simple executable file that is installed on the target computer to gain a reverse shell whenever necessary. There are many ways that we can use to create backdoors to computers. An attacker with good knowledge can easily create a custom backdoor. Most of these custom backdoors are easily identified as malicious files by windows security systems. To address this issue, we developed an advanced backdoor that acts as a normal file but works as a backdoor. Once the backdoor is installed it allows an attacker to sustain access to the computer and can make changes to the computer. At first, the reverse shell access which is gained through the backdoor will have user permissions and privilege escalation methods are used to gain access to an administrator-privileged shell. It is used to gain remote access to a computer with the help of RCE(remote code execution) vulnerability.

Keywords: Privileges, Access, Intruder, Remote Code, Execution, Vulnerability

I.INTRODUCTION

A backdoor refers to a method utilized by individuals like hackers, governments, or IT professionals to gain unauthorized and remote access to a computer or device. It allows them to bypass your permission and knowledge. Hackers can implant a backdoor through various means, including malware, exploiting software vulnerabilities, or directly installing it within the hardware or firmware of your device. Once unauthorized access is achieved, backdoors can be utilized by hackers for different purposes, such as surveillance, data theft, crypto jacking, sabotage, or launching malware attacks. Backdoor hacking affects everyone, as hackers continuously develop new techniques and malware to gain access to user devices.

BACKDOOR

A backdoor attack is a technique used to gain unauthorized access to a computer system or encrypted information by bypassing the system's standard security protocols. Developers may create backdoors to enable troubleshooting or other legitimate purposes by providing access to applications, operating systems (OS), or data. Regardless of the intention behind their installation, whether as an administrative tool, an attack vector, or a mechanism for governmental access to encrypted data, all backdoor installations pose a security risk. Threat actors constantly search for such vulnerabilities to exploit.

A backdoor attack occurs when threat actors create or utilize a backdoor to gain remote access to a system. These attacks enable them to take control of system resources, conduct network reconnaissance, and install various types of malware.In certain scenarios, malicious actors create worms or viruses with the intention of leveraging pre-existing backdoors that were either developed by the original software creators or were a result of previous attacks.To portray the detrimental effects of backdoors on security systems, let's imagine a highly fortified bank vault that incorporates multiple layers of robust security measures.

It has armed guards stationed at the front door, advanced locking mechanisms, and biometric access controls that make unauthorized access virtually impossible. However, the presence of a backdoor, such as a large ventilation shaft, renders the vault vulnerable to attack by bypassing these measures.

Once access is obtained, threat actors engage in malicious activities, including:

i. Stealing sensitive information
ii. Performing fraudulent transactions
iii. Installing spyware, keyloggers, and Trojan horses
iv. Utilizing rootkits

II.RELATED WORK

In this project, the primary method employed is the Reverse TCP connection.

What is a Reverse TCP Connection?

TCP/IP, or Transmission Control Protocol/Internet Protocol, serves as the communication language of the Internet. It allows computers to communicate with each other by packaging data into packets and sending them to the intended destination. A basic firewall typically blocks incoming connections. However, in a reverse TCP connection, the attacker manipulates the host to initiate a connection to the attacker's machine. This is the fundamental concept behind a reverse TCP connection.

TCP:

TCP/IP operates through two layers. TCP (Transmission Control Protocol) is responsible for breaking down large data into network packets, sending them, and having another TCP layer on the receiving end decode the packets and transform them into usable information.

IP:

IP (Internet Protocol) is responsible for routing the compiled network packets to their intended destinations. The IP layer functions like a GPS for the packets.

This attack involves two basic concepts:

Bind Shell: It refers to a type of shell where the target machine opens a communication port or listener, waiting for an incoming connection. The attacker then connects to the victim machine's listener and issues commands.

Reverse Shell: This type of shell involves the target machine initiating a connection to the attacking machine. The machine carrying out the attack has a designated listener port that enables the reception of the connection, facilitating the execution of code or commands.

TCP/IP incorporates four abstraction layers:

Link Layer: This layer involves the physical equipment used to connect nodes and servers.

Internet Layer: It facilitates connections between hosts across networks.

Transport Layer: This layer handles host-to-host connections.

Application Layer: This layer ensures communication between applications on the network.

When the host initiates a connection, it is known as a forward connection. However, when the server initiates a connection to the host, it is called a reverse connection (a less common scenario). Firewalls typically block all incoming connections, including reverse connections. However, if a host initiates a connection (forward connection), it is allowed, and the corresponding return connection is permitted by the firewall.

In a reverse_tcp scenario, instead of the attacker initiating the connection (which would be blocked by the firewall), the compromised device itself establishes a connection to the attacker. This connection is permitted by the firewall, allowing the attacker to take control of the device and issue commands. It essentially represents a type of reverse shell.

By following these steps, you can establish a reverse TCP connection for your project.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

III.EXISTING SYSTEM

"Backdoor entry refers to the act of obtaining unauthorized access to a specific system, allowing the user to have complete control over its operations using the command prompt. However, in the current backdoor system, users can only view or read the contents ofspecific files without theability to modify them. Additionally, networking commands such as ipconfig or netsh are not accessible in the existing system. Consequently, the current system fails to fulfill all the necessary requirements for a hacker or administrator."

IV.PROPOSED SYSTEM

In the proposed system, various modules such as OS, subprocess, and socket are utilized to address the limitations of the existing system. Through these modules, we can overcome the drawbacks and enhance the system functionalities. Notably, the proposed system introduces the ability to modify file contents, and it also provides disclosure of user/hacker information. This aspect makes it challenging to identify the hacker's identity. Additionally, network commands like ipconfig and netsh are functional within the proposed system, further expanding its capabilities.

Requirements for Reverse TCP:

Setting up a reverse TCP connection can be easily accomplished with the following requirements:

i. Linux machine (recommended and preferred)
ii. Metasploit (easiest way)

Setting up Reverse TCP:

To set up a reverse TCP connection, follow these steps:

Launch a terminal on your Linux machine.

Generate a payload using msfvenom, ensuring configuration of the following parameters:

a. LHOST: The IP address of the target machine you wish to attack.

b. LPORT: The port on LHOST to which the target machine will connect.

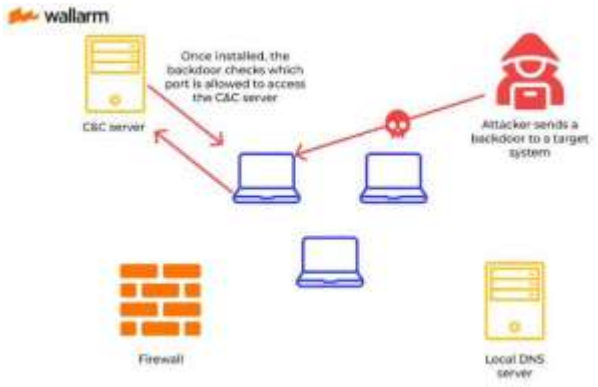

Fig IV.I System Architecture

ALGORITHM

1. Define the objective: Gain unauthorized access to a target Windows system.
2. Identify vulnerabilities: Research and analyse potential vulnerabilities in the target system, such as outdated software, weak passwords, or unpatched security flaws.
3. Select an attack vector: Choose a method to exploit the identified vulnerabilities, such as exploiting software vulnerabilities, social engineering, or phishing attacks.
4. Reconnaissance: Gather information about the target system, including IP addresses, network architecture, and user accounts.
5. Exploit vulnerabilities: Utilize the chosen attack vector to exploit the vulnerabilities discovered in the target system. This may involve running malicious code, executing a remote exploit, or using a known security flaw.
6. Gain access: Once the vulnerabilities are successfully exploited, gain unauthorized access to the target system. This can be achieved by bypassing login credentials, escalating privileges, or compromising administrator accounts.

7. Establish persistence: Implement techniques to maintain access to the compromised system, such as creating a backdoor or modifying system configurations to ensure continuous access.

8. Execute desired actions: Once inside the system, perform desired actions based on the objective, such as retrieving sensitive data, installing additional malware, or monitoring user activities.

9. Cover tracks: Minimize evidence of unauthorized access by erasing logs, modifying timestamps, or using anti-forensic techniques to hinder detection and investigation.

It's important to note that developing or engaging in any activities related to unauthorized access, including creating or using backdoors, is illegal and unethical. This algorithm is provided for educational purposes only to raise awareness about potential security risks.

V.SCREEN SHOTS:

Fig V.INC Command in Linux Terminal

Fig V.IIConnecting to the windows system

VI.CONCLUSIONS:

The utilization of a backdoor offers technological advantages in terms of remote system monitoring. It finds practical applications, particularly in software companies where monitoring employee computers helps gauge work efficiency. Additionally, it enables parental monitoring, serving as a tool for responsible oversight. One noteworthy characteristic of this backdoor software is its ability to evade detection by firewalls. Consequently, Windows computers protected by firewalls become highly vulnerable to exploitation, granting unauthorized remote access. It is important to acknowledge that backdoors can be used both positively and negatively. On the negative side, they can be misused to establish connections with computers without proper authorization. However, the backdoor developed in this context is solely intended for educational purposes and not for illegal activities.In addition to creating a read-only backdoor, our project extends its capabilities to include file copying from the reverse shell to the Linux computer and replacing existing files with modified versions, effectively granting write permissions. This addresses a significant drawback of the existing backdoor system, which lacks admin rights to make changes to the Windows computer.

REFERENCES:

[1] EmanEsmaeel Hamed and Muna Majeed Lafta. "Intrusion Windows XP by Backdoor Tool." Journal of AlNahrain University, Vol.11(3), December 2008.

[2] M. Young. The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[3] Chris Wysopal and Chris Eng. "Static Detection of Application Backdoors." Veracode Inc.

[4] "Exploring Windows Backdoor – Bypassing Firewall on Webhosting Providers." Retrieved from https://dl.packetstormsecurity.net/papers/general/my_research1.pdf