Cyber Kill Chain Analysis Report

Scenario Overview

In this attack, write a backdoor code in python, make for executable to convert into .exe file, and distribute it via phishing email to the target user. Target user is open the email and execution the .exe file, and establishes the reverse shell, gaining access to the IT workstation system. Subsequent reconnaissance using the Nmap to identify the vulnerability are information and network information after reconnaissance find active directory and find any other network. More reconnaissance to other network finds different service are run in machine and remote desktop application are run in machine 3389 port are open, to take access through the RDP find the vulnerability then apply brute force attack using the hydra tool and successfully obtains the username and password, gaining the remote access in machine.

Cyber Kill Chain Stages

1.Reconnaissance

- **Objective**: Gather information about the target.
- **Actions**: Research the target organization and its employees to identify a suitable target for the phishing attack.
- **Tools Used**: Open-source intelligence (OSINT) tools, social media platforms, company websites.

2.Weaponization

- **Objective**: Create a malicious payload.
- **Actions:** Develop a backdoor in Python, then convert the script into an executable file (.exe) using a tool like PyInstaller.
- **Tools Used**: Python, PyInstaller.

3.Delivery

- **Objective**: Deliver the malicious payload to the target.
- **Actions**: Craft a phishing email with a compelling subject line and body, attach the malicious .exe file, and send it to the target user.
- **Tools Used**: Email services, social engineering techniques.

4.Exploitation

- **Objective:** Exploit vulnerabilities to execute the payload.
- **Actions**: The objective client opens the phishing email and runs the joined .exe document, unconsciously executing the secondary passage code.
- **Tools Used**: Phishing email with a malicious attachment.

5.Installation

- **Objective**: Install a backdoor on the target system.
- **Actions**: The backdoor code installs itself on the target IT workstation, establishing a connection to the attacker's machine via reverse shell.
- **Tools Used**: Custom secondary passage code, switch shell script.

6. Command and Control (C2)

- **Objective**: Maintain remote control over the compromised system.
- **Actions**: The attacker uses the reverse shell to communicate with the compromised IT workstation, directing the system and issuing commands.
- **Tools Used**: Invert shell devices, order line interface.

7.Actions on Objectives

Objective: Achieve the attacker's ultimate goals.

Actions:

1. **Initial Actions**: Utilizing Nmap, carry out reconnaissance on the compromised network to gather data about other systems and users.
2. **Identify Secondary Targets**: Distinguish one more organization and track down two clients, with one client's remote access port open.
3. **Brute Force Attack**: Crack the remote access port's username and password using brute force methods.
4. **Gain Access**: Sign in to the subsequent machine utilizing the qualifications, laying out remote access.

Tools Used: Nmap for network examining, animal power instruments like Hydra or Medusa

Detailed Report

1.Reconnaissance:

The assailant does an intensive examination of the objective organization, gathering data on the two clients and organization foundation. The aggressor then utilizes this information to distinguish an objective for the phishing email.

2. Weaponization:

The aggressor has made a Python script fully intent on involving it as a secondary passage. They can execute the content on Windows machines by utilizing PyInstaller to change over the content into an executable.exe document. The Python interpreter and the necessary components are combined into a single executable file during the conversion process.

3. Delivery:

A phishing email is a malicious message sent with the intention of tricking the recipient into opening the file that is attached. The malicious message appears to be genuine, possibly posing as a trustworthy individual.

4. Exploitation:

The backdoor malware is activated when the recipient clicks on the.exe file in the phishing email. This malicious code exploits the recipient's trust and their decision to execute the.exe file on their computer.

5. Installation:

The target IT workstation has the backdoor code installed, which creates a persistent backdoor shell connection to the attacker machine. This connection enables an attacker to run arbitrary code on the system.

6. Command and Control (C2):

The reverse shell enables the attacker to continue monitoring and executing commands on the compromised system, allowing them to move around the network, increase privileges, and eventually crash the network.

7. Actions on Objectives:

I utilized Nmap to conduct a network scan, identifying new computers and users and uncovering an additional network segment. During this phase, we find that one of them has an open remote access port and then executes a brute-force attack, utilizing tools like Hydra, to breach the remote access port and find the login credentials. After finding the credentials, through attacker machine logs into the other machine and gains complete control over the system.