Flag4 CTF

Dr. C. Umarani[1], R P Shruti[2]

[1]Assistance Professor, [2]Student,
[1,2]Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

In today's world a place where there is a large scope for Security, many people are busy building applications, web pages and many more but no one actually concentrates on security aspect of it. As the technology increases, the flaws in the security system also increases. The CTF machine is one such solution for this problem, where the person who is learning hacking can use these kind of machines and learn security in a much deeper way.

Capture The Flag are games where the hackers have to solve puzzles and find bugs so that they can get through system flaws and find flag, which is the main goal. Typical CTFs offer many challenges, most commonly the hackers have to exploit some kind of service so that you can get remote access to the server and read the content of the file that contains a special string called "flag", which is a proof that he/she has hacked the system.

KEYWORDS: *CTF, vulnerability, flag, security, capture the flag, remote desktop service, tftpd, tftpd32/64, mssql server*

How to cite this paper: Dr. C. Umarani | R P Shruti "Flag4 CTF" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1643-1644, URL: www.ijtsrd.com/papers/ijtsrd35734.pdf

IJTSRD35734

I. INTRODUCTION

There can be many ways to learn hacking and CTF machines are one among the most effective ways. The Main goal of CTF is to find the flags hidden in the machine by remotely getting access through the vulnerabilities set up. The concept CTFs came from the traditional outdoor game where two teams each have few flags and their objective is to capture other team's flags from the base and bring it back to their base which would end the game.

Finding out the vulnerabilities using some tools or techniques like nmap, sql-injection, etc. is the toughest job. But once the vulnerability has been found, the hacker can get into the machine using some other tools like metasploit.

Vulnerability: It is the weakness in system which can be exploited by the attacker to gain unauthorized access. These vulnerabilities can allow attackers to run code, access system's memory, install malware through which he/she can steal, destroy or modify sensitive data which may affect the company's status, fame and trust.

Flag: Flags are secrets hidden in purposefully vulnerable programs or websites. There are two type of CTFs based on the flags. An attacker steals flag from his competitor, this is known as attacker/defence style CTF. The other is where the flags are obtained from organizations, which is known as jeopardy-style.

II. Existing System

The aim of this paper is to help hackers learn break into vulnerabilities. In the existing system there are many combinations of vulnerabilities set up to help hackers. Setting up vulnerabilities can be in many ways like web vulnerability, database vulnerability, weak password vulnerability and many more. There are many new CTFs everyday with every vulnerability glooming. CTFs are a way to practice hacking.

III. Proposed System

The combination of different vulnerabilities included makes every CTF different. In the proposed system, combination of few vulnerabilities have been used. RDS (Remote Desktop service) is one of the vulnerability through which the hacker gets remote access. Another vulnerability is through MSSql which has code execution vulnerability. Another vulnerability is tftpd32 which has buffer overflow vulnerability which can cause denial of service. These vulnerabilities combined causes the creation of the flag4 CTF machine. Any hacker can use these CTFs and get to know vulnerabilities in real time machines.

A. Securing a machine

It is really important to secure a machine in the organization point of view because data is everything they have and that is what they have to secure. This is when CTF comes into picture. The hackers are rewarded as per the level of difficulty for finding the vulnerabilities and bugs.

But when it comes to CTF's, more the vulnerability much easier to get through. Therefore based of the level of difficulty required, the difficulty is setup. In the flag4 CTF, I have set the difficulty to medium as I have configured three vulnerabilities which will be discussed further in the paper.

B. Setting up the vulnerabilities

Vulnerabilities can be setup in many ways and in many levels. There are three levels of difficulty, they are:

Simple: This level of difficulty will require installation of some affected software.

Moderate: This level of difficulty will require installation of some affected software on a specific operating system.

Complex: This level of difficulty will require installation and configuration of some affected software on a specific operating system.

In the flag4 CTF, we are using windows operating system. Since windows has GUI and many of the users are familiar with the architecture of windows, it becomes easy for the attackers to guess where the flag can be placed. As most of the real world systems in our country are installed with windows OS, this can be a really practical thing to hack into. In this flag4 CTF, I have installed three software's and configured them according to my needs. These software's include Adobe ColdFusion, MSSQL, and TFTP.

A. Adobe ColdFusion:

In flag4 CTF I have installed Adobe ColdFusion 9. There are newer versions of adobe available, but having some vulnerabilities is good for us.

By setting this up, RDS login method can be attacked through a metasploit module and can gain administrative login, this can further be used to gain shell access.

Another method is default credentials can be set up as a vulnerability, and directory traversal can be used to gain the flag.

B. MSSQL:

In most of the systems MSSQL is run almost all the time. This can be used as a vulnerability. Here, in flag4 CTF machine we are using MSSQL 2005 and MSSQL management suite to set up the vulnerabilities. Since this is the vulnerability, we get access to the database directly with least effort.

C. TFTP:

Which can be abbreviated as Trivial File Transfer Protocol, is an old service which provides FTP services to unauthenticated users. Here, we are using Tftpd32 instead of Tftpd64, again for the same reason of vulnerability. Tftpd32 is also vulnerable to buffer overflow. And there is also a metasploit module associated with Tftpd32 which can be really easy to begin with.

C. Flag Placement

In the flag4 CTF machine, the flag is hidden in the form of string and also in the steno graphed image which can be retained using some stenographic tools. This is just to make sure that the attacker thinks in many ways while trying to crack a real world machines.

Placing a flag is completely the creator's idea. The file which contains flag can be simply named as flag.txt if the creator wants it to be too simple. But it can also be named something else and also the file containing flag can be placed with different extension just to make it a bit tricky. Even the credentials can be placed as flags.

In flag4, the flags are placed in different folders and also few of them are placed within an image just to trick the attacker.

D. Flowchart

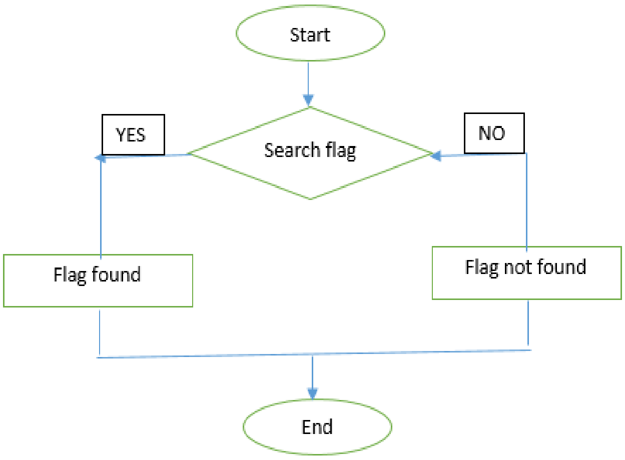

Fig: Flowchart of CTF

IV. Conclusion

As we are getting advanced in technology, we are also calling threat by our self. That is why every person who uses technology should have basic awareness about how to safeguard his/her device. This is only possible when they know about the flaws and vulnerabilities in system. This paper helps to know how the everyday simple mistakes of us can cause serious damage to the data. The flag4 CTF is very useful to the beginners who have not cracked any CTF's as it is of moderate difficulty.

References

[1] https://ieeexplore.ieee.org/abstract/document/7427865

[2] https://ieeexplore.ieee.org/Xplore/home.jsp

[3] https://www.usenix.org/conference/3gse15/summit-program/presentation/chothia

[4] https://ieeexplore.ieee.org/abstract/document/7092098

[5] https://www.usenix.org/conference/3gse14/summit-program/presentation/chung

[6] https://dl.acm.org/doi/abs/10.1145/3017680.3017783

[7] https://ieeexplore.ieee.org/abstract/document/8614801

[8] https://ieeexplore.ieee.org/abstract/document/7911890

[9] https://www.sciencedirect.com/science/article/pii/B9781931836692500389

[10] https://patents.google.com/patent/US7293282B2/en

[11] https://patents.google.com/patent/US7246171B1/en

[12] https://www.hjp.at/doc/rfc/rfc1350.html

[13] https://owasp.org/www-project-top-ten/