SSBCute Proving Grounds

Penetration Test Report

Table of Contents

1. – High-level Summary……………………………………………………………………………………………………………………….3
   1. - Recommendations…………………………………………………………………………………………………………….3
2. - Methodologies……………………………………………………………………………………………………………………………….4
   1. - Information Gathering……………………………………………………………………………………………………….4
   2. - Service Enumeration………………………………………………………………………………………………………….4
   3. – Penetration………………………………………………………………………………………………………………………..4

**System Vulnerable**……………………………………………………………………………………………………………….9

* 1. – Report……………………………………………………………………………………………………………………………….9

1.0– High-level Summary

An internal penetration test was performed on the SSBCUTE network in the Offensive Security Proving Ground Labs. An internal test simulates an attacker that is directly connected into the network, in this case through a VPN tunnel.

The purpose of this test was to simulate an attack where the attacker had access to the network, with attempts made to break into a system and then elevate privileges on the machine. Over-all, the intent was to enumerate the services on the exposed network, determine an attack vector to get access, and then exploit any flaw found within the system.

During the test it was found that the cutenews CMS was a version that was vulnerable to an exploit that creates a shell into the system, and then privilege escalation was performed through a command given SUID privilege. This allowed for root access to the device.

1.1– Recommendations

At this point in time, there is no fix for the cutenews CMS, as the website shows the current version is 2.1.2. While it would be possible to change the directories around, a hacker would be able to customize the code to match the new directory scheme on the exploit. It may be possible to have a validation process for users to register, as currently the exploit creates a random user in order to get its shell code to work.

Outside of that, migrating to a more secure CMS platform may be in order to fully protect against the vulnerability in the Cute News CMS framework.

After getting access to the device, it was possible to root the shell due to SUID permissions allowing for exploiting the hping3 file to spawn a shell with root privileges. I would recommend removing the SUID setting on that file to prevent it from being exploited later on.

2.0-Methodologies

Below is the methods that were undertaken to break into the device, and ultimately achieve root access on the device.

2.1-Information Gathering

The information gathering portion was mostly null, as the network address of 192.168.191.128 was provided ahead of the pentest commencing.

2.2-Service Enumeration

Checking for TCP connections on the device, found that the following services were open:

22 Secure Shell Remote access

80 HTTP Website

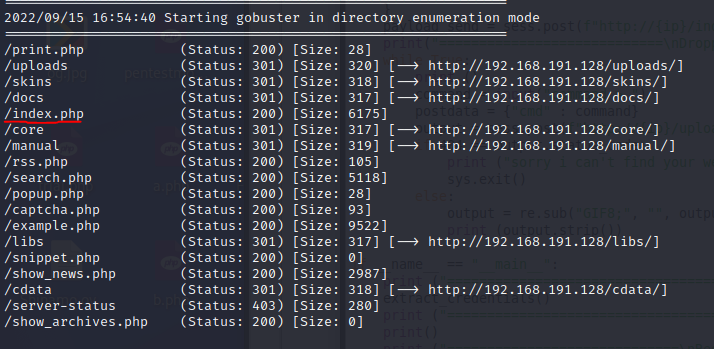
110 Pop3 Courier Pop3

995 Pop3 Courier Pop3

Also found on the UDP side was the BackOrifice management port open. Please verify if this is intentional and in active use. Otherwise it would be beneficial to turn that port down.

2.3-Penetration Testing

During the testing, ran a gobuster to check for .php and .sh files, and found index.php.



This turned out to be a log on page, that also showed the version number for the CMS.

Graphical user interface, application, website

Description automatically generated

Checking for the version of CuteNews showed that there was a python exploit available under 48800.py. Modifying this code for the directory structure of this website allowed for a shell to be spawned under the website authority.

Text

Description automatically generated

With this base shell, it was possible to move to the /tmp folder, and upload a stronger shell to get a fuller range of commands allowed on the device.

Text

Description automatically generated

By navigating to the directory hosting the shell within the browser, it was possible to spawn a reverse shell, and from there to upgrade it to a bash shell utilizing the python on the system.

Graphical user interface

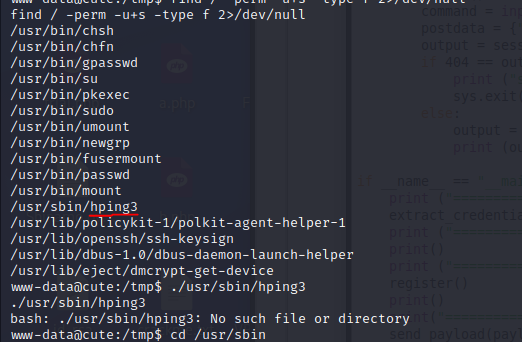
Description automatically generated with low confidence

With this authority, it was possible to locate the local.txt flag and get the contents of it.

Text

Description automatically generated

Checking the SUID enabled files on the system, it was found that hping3 was one of the files given the permissions. This is one of the files that can be abused for a root privilege exploitation when SUID-enabled.



Applying the exploit applied root privileges in the new shell immediately.

Graphical user interface, text, application

Description automatically generated

And from there, getting the proof.txt file contents was possible.

Text

Description automatically generated

**System Vulnerable 192.168.191.128:**

**Vulnerabilities Exploited:**

CVE-2019-11447 was exploitable due to the 2.1.2 version of CuteNews that allowed shell access

SUID enabled hping3 was able to be exploited by spawning a root shell within the process

**Vulnerability Fixes:**

Do not allow automatic registration for new users on the CuteNews website

Migrate to a less vulnerable CMS when able to do so

Remove the SUID set permission on the hping3 file so it does not run as root

**Severity: Critical**

**Proof of Privilege Escalation:**

Local.txt: 68353e79634737f19bc367fa15e54d75

Proof.txt: b2a9de4680a5984bbcf159d5e5e1af60

2.4-Report: Clean-up

The shell.php file was removed from the /tmp directory. Linpeas.sh was uploaded to /tmp to scan for vulnerabilities, and then removed as well. These were the only files added to the system, and both have been removed. The only thing remaining is a random user created on the website that was created while using the python exploit. There is no method to remove that without admin privileges to remove the user from the database.