Lots of Fun Ideas Writeup

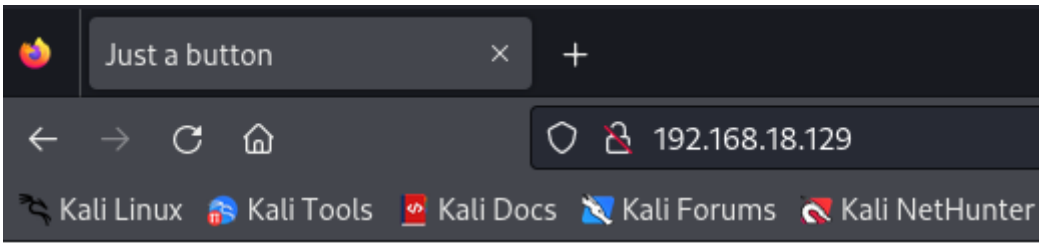
Lots of Fun Ideas (LoFI) is an easy machine aimed at covering an LFI vulnerability, with a filter to stop a common payload "../". After bypassing this filter the user can find the SSH key for a user on the system and then log in as that user. Following this, the user then must take advantage of a binary that they have sudo privileges for to get root access, and the flag.

Enumeration

We can start by running a basic nmap scan which searches for services on an IP address and uses default scripts and default host enumeration.

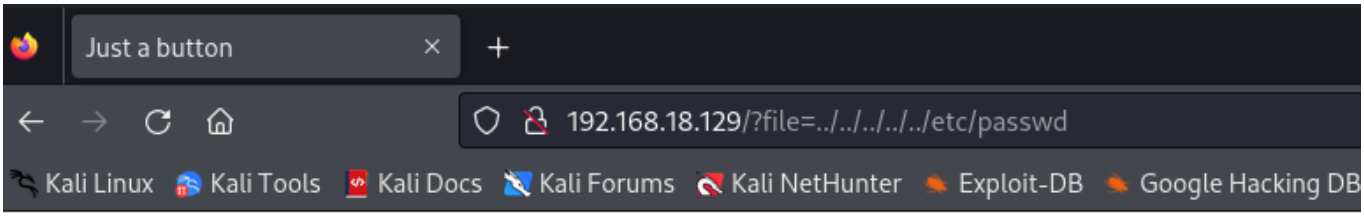
```
# Nmap 7.93 scan initiated Wed Feb 21 10:34:44 2024 as: nmap -sCV -oN nmap/output
192.168.18.129
Nmap scan report for 192.168.18.129
Host is up (0.00069s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4c683bb309ca1361f134e03967e5c36d (ECDSA)
|_  256 1ca902a7f33126e336c36439e5d262e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Just a button
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Feb 21 10:35:07 2024 -- 1 IP address (1 host up) scanned in
22.82 seconds
```

From the output of this nmap scan we can identify a website running on port 80 and an SSH server open on port 22. Upon opening the website the user sees a piece of text.



What is CTF?

Clicking the hyperlinked text displays an additional line of text that says "This is a text file" and adds a PHP argument called "file" with reference to a file called "file.txt". To people aware of what Local File Inclusion is, one of the most common payloads for abusing this vulnerability is to use "../" to search for files out of the current directory. Taking this information and replacing the value given to the file argument with a payload to try and load the "/etc/passwd" will be unsuccessful how ever, due to the filter that is in place.



What is CTF?

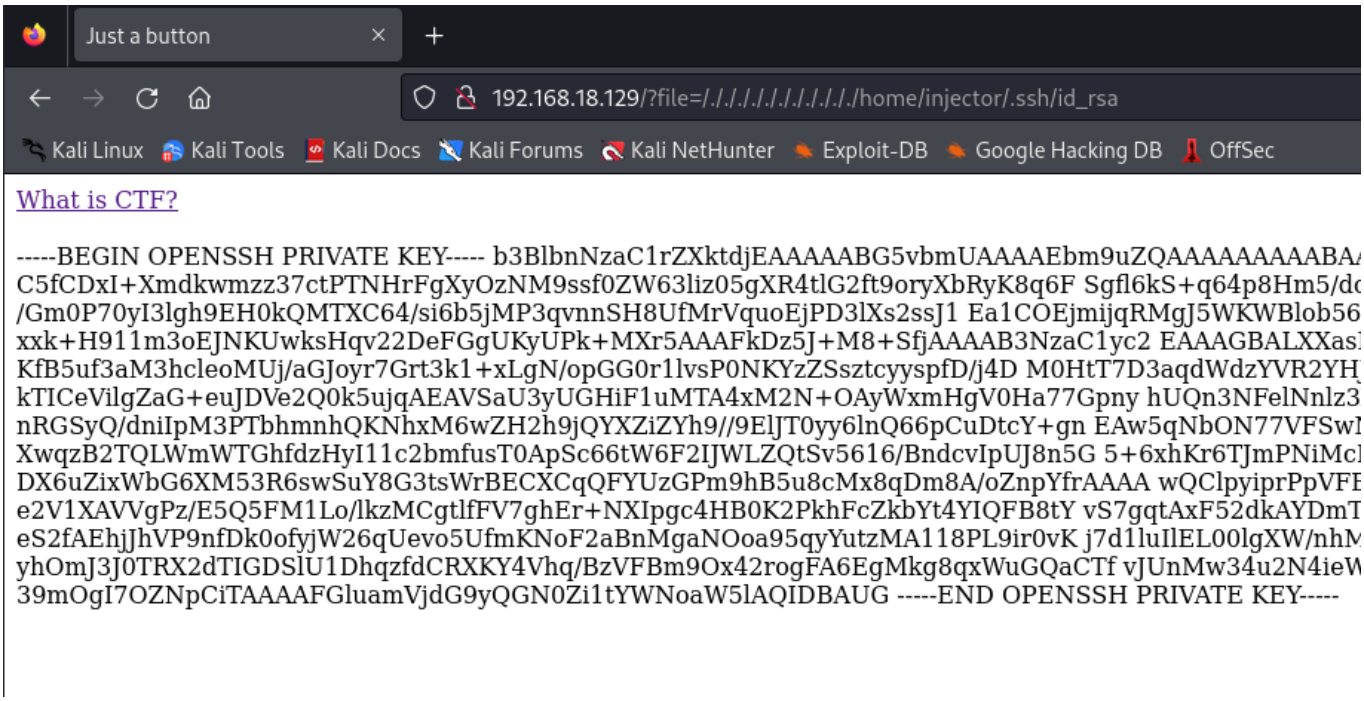
Exploitation

There are countless payloads that the user could try at this point, such as replacing "../" with "..../" although this would still be unsuccessful due to how the filter works. Instead, the user must find a payload that does not utilise "../". Although there are numerous payloads that will work, a few examples are:

```
http://192.168.18.129/?file=///////../../../etc/passwd

http://192.168.18.129/?
file=....//....//....//....//....//....//....//....//....//....//....//....//
....//....//....//....//....//....//....//....//....//etc/passwd

http://192.168.18.129/?file=/etc/passwd
```

```
http://192.168.18.129/?file=/./../../../../../../../../../../etc/passwd
```

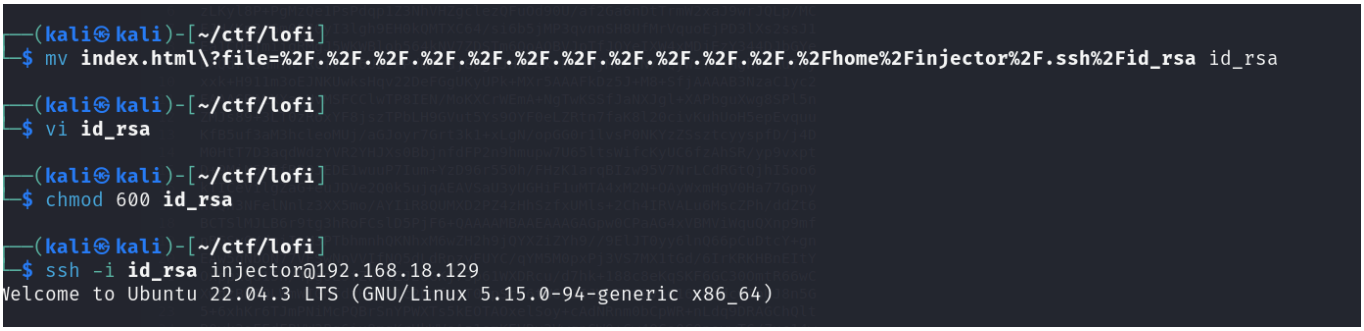
By submitting a successful payload the user will notice the presence of one user out of the ordinary, "Injector". By using the LFI vulnerability and this information the tester can then make assumptions and find an SSH key.



The user could then attempt to copy the SSH key and manually format it, or perform a request to retrieve the information from the website and then format the file manually. Attempting to copy the information straight from the website is painstakingly tedious, and retrieving the information from the website has its own problems, but is definitely the easier solution.

Once downloaded, the original file will contain some HTML code which must be removed, and if you are using an editor such as Sublime, you may need to add a new line to the file after editing it, otherwise the file will not work as needed. This can be done by opening the editor in a

command-line text editor such as vi and exiting the file with "wq!".



Completing this process and using the id_rsa key will give the user an SSH connection to the box.

Privilege Escalation

The user could then perform some basic enumeration on the machine through the use of LINPEAS to find the path to root, or by simply typing "sudo -l" which is a command used to show what commands the current user can invoke as other users.

The user can then check a website such as GTFOBins, which is a useful website for bypassing local security restrictions on Unix machines and search for "ltrace". Viewing the sudo capabilities of this binary reveals a way for the user to get root. By copying this command running it in the SSH shell, the user is greeted with a root shell, and when visiting the root folder, will find the flag file.