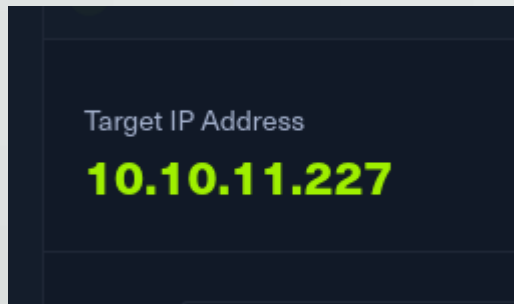




# HTB machines - Keeper

Write up by Chanan shenker

- Start:
- I connected to the VPN, turned on the machine and got an IP address to start.



- Scanning:

```
(root@kali)~[~/Desktop/lab]
# nmap 10.10.11.227 -sV -sC -oN ./scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:10 IDT
```

- I ran the command above and found two ports open on the target. Port 22 and 80.
- Port 80 tells me that this is hosting a website, so let's go.

```
(root@kali)~[~/Desktop/lab]
# nmap 10.10.11.227 -sV -sC -oN ./scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:10 IDT
Nmap scan report for 10.10.11.227
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_ 256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

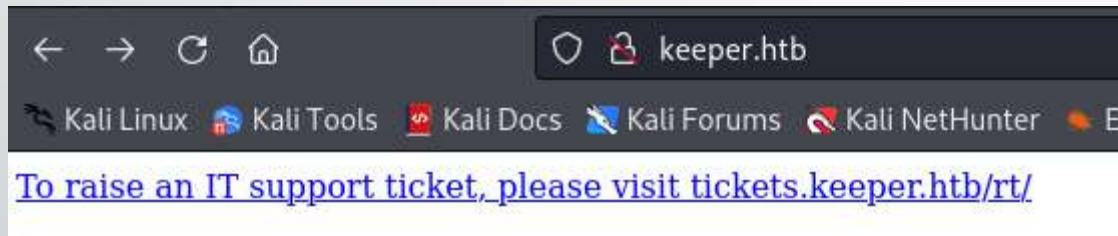
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

- I added the machine to /etc/hosts.

```
..1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

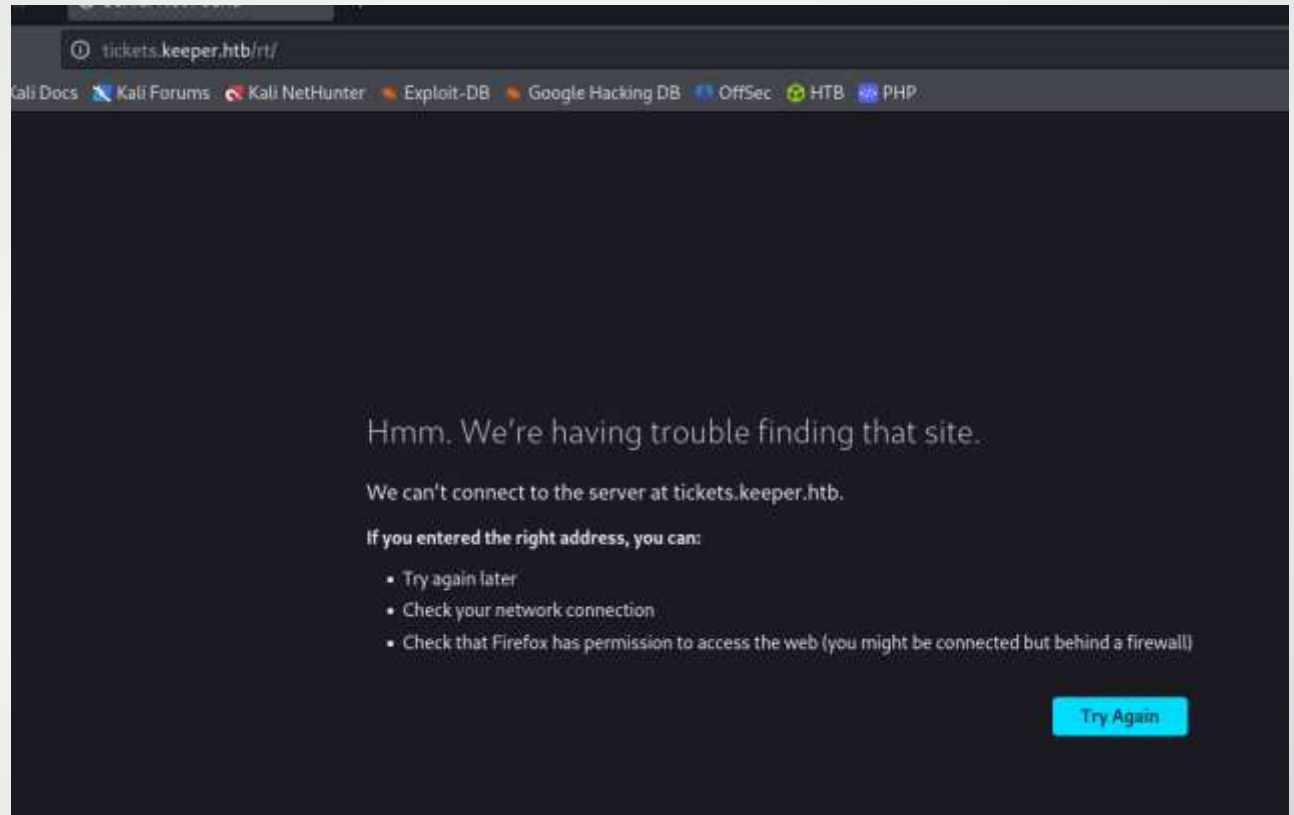
10.10.11.227 keeper.htb
```

- And tried to access the webpage.

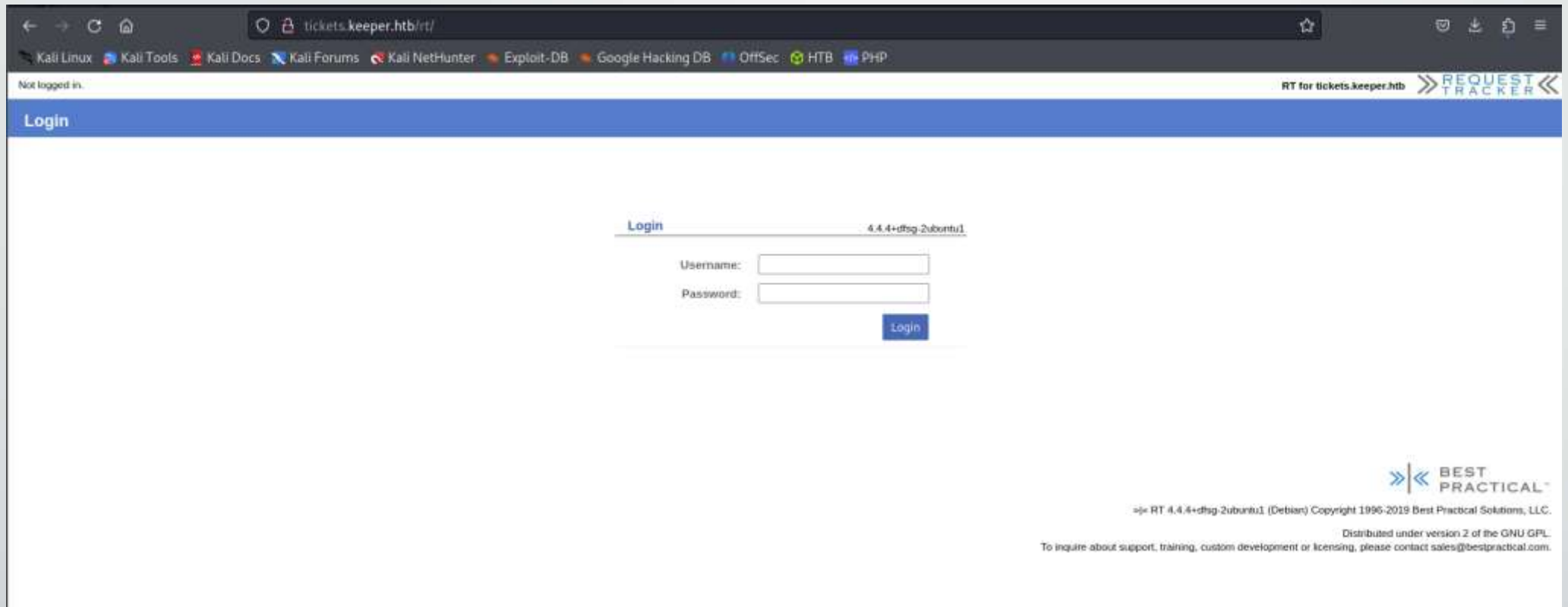


- I clicked on the link and it redirected me to another page that is a subdomain of keeper.htb.

- So i added the subdomain to /etc/hosts file and accessed it again.



```
10.10.11.227 keeper.htb tickets.keeper.htb
```



- Viola, a login page for 'best practical solutions ', a ticket management system.
- I couldn't find anything juicy about the software (like exploit, CVEs etc.) so I decided to try and crack the password. So I fire up burp suite.
- Burp suite is a very popular tool used by penetration testers and has a wide variety of features to exploit web applications

- The tool I use is called intruder. It works by capturing a request that I send out through the burp suite proxy and send it to the intruder so I can make it send the request over and over with different values each time. Obviously the value I would like to change is the password.
- This is the captured request. Note the part at the bottom where it says user=<>&pass=<>.
- So that the part I want to change every request.
- the username 'root' I found out by a quick google search about default users for 'Best practical solutions'.

```

1 POST /rt/NoAuth/Login.html HTTP/1.1
2 Host: tickets.keeper.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 56
9 Origin: http://tickets.keeper.htb
10 Connection: close
11 Referer: http://tickets.keeper.htb/rt/NoAuth/Login.html
12 Cookie: RT_SID_tickets.keeper.htb.80=ffdddle0ccabc228f02023a7f0bfd5d3
13 Upgrade-Insecure-Requests: 1
14
15 user=root&pass=123&next=7de87a83e5fd1ea677e65180352b6b4f

```

```

11 Referer: http://tickets.keeper.htb/rt/NoAuth/Login.html
12 Cookie: RT_SID_tickets.keeper.htb.80=ffdddle0ccabc228f02023a7f0bfd5
13 Upgrade-Insecure-Requests: 1
14
15 user=root&pass=123&next=7de87a83e5fd1ea677e65180352b6b4f

```

- So I start the brute force attack.

The screenshot displays the Burp Suite Intruder interface. The main window is titled '3. Intruder attack of http://tickets.keeper.htb - Temporary attack - Not saved to project file'. It features a 'Results' tab with a table showing the progress of the brute force attack. The table has columns for Request, Payload, Status, Error, Timeout, Length, and Comment. The 'Status' column shows '200' for all requests, indicating successful connections. The 'Payload' column lists various strings being tested, including 'Password', 'http', 'factory', 'RIP000', '12345', '1234admin', 'ANYCOM', and 'IL MI'. The 'Length' column shows a consistent value of 5046 for all requests. The 'Error' and 'Timeout' columns are empty, suggesting no errors or timeouts occurred. The 'Comment' column is also empty. The 'Request' column shows indices from 0 to 9. The 'Payload' column shows the strings being tested. The 'Status' column shows '200' for all requests. The 'Error' column shows empty checkboxes. The 'Timeout' column shows empty checkboxes. The 'Length' column shows '5046' for all requests. The 'Comment' column is empty. The 'Request' column shows indices from 0 to 9. The 'Payload' column shows the strings being tested. The 'Status' column shows '200' for all requests. The 'Error' column shows empty checkboxes. The 'Timeout' column shows empty checkboxes. The 'Length' column shows '5046' for all requests. The 'Comment' column is empty.

The background window shows the 'Payload sets' section with 'Payload set: 1' and 'Payload count: 1,315'. The 'Payload type' is set to 'Simple list'. The 'Payload settings [Simple list]' section shows a list of payloads: '1234admin', 'ANYCOM', 'ILMI', 'PASSWORD', 'admin', 'comcomcom', 'Admin', 'password', and 'synnet'. The 'Payload processing' section is also visible.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
1	Password	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
2	http	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
3	factory	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
4	RIP000	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
5	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
6	1234admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
7		200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
8	ANYCOM	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
9	IL MI	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	

- Now, the way we can figure out what password was successful we have to look at the content length of the response it got.
- Next to 'password' we get a much smaller content length in the response. Lets check if it's the one.
- And were in :)

Request ^	Payload	Status	Error	Timeout	Length	Co
10	PASSWORD	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
11	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
12	comcomcom	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
13	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
14	password	302	<input type="checkbox"/>	<input type="checkbox"/>	327	
15	synnet	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
16	adminttd	200	<input type="checkbox"/>	<input type="checkbox"/>	5045	
17	manager	200	<input type="checkbox"/>	<input type="checkbox"/>	5045	
18	monitor	200	<input type="checkbox"/>	<input type="checkbox"/>	5046	
19	recover	200	<input type="checkbox"/>	<input type="checkbox"/>	5045	

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec HTB PHP

Home Search Reports Articles Assets Tools Admin Logged in as root

RT for tickets.keeper.htb REQUEST TRACKER

RT at a glance [View ticket list](#) [General](#) [Search...](#)

10 highest priority tickets I own [Edit](#)

10 newest unowned tickets [Edit](#)

Bookmarked Tickets [Edit](#)

Quick ticket creation

Subject:

Queue: [General](#) Owner: [Me](#)

Requesters: [root@localhost](#)

Content:

[Create](#)

My reminders [Edit](#)

Queue list [Edit](#)

Queue	new	open	stalled
General	1	-	-

Dashboards [Edit](#)

Refresh

Don't refresh this page [Set](#)



- To my annoyance I discovered that those are the default credentials and could have save my self a lot of time if id just looked online, but hey we learned something.
- Now lets dig. I couldn't find anything interesting in the page but a little look around and I found under the admin > users tab this.

The screenshot shows the 'Admin' section of the Request Tracker interface, specifically the 'Privileged users' page. The page has a navigation bar at the top with links like Home, Search, Reports, Articles, Assets, Tools, and Admin. The 'Admin' link is active, and the user is logged in as 'root'. The page title is 'Select a user'. Below the title, there are search filters for finding users by name, email, or other criteria. A table lists the privileged users, showing their ID, Name, Real Name, Email Address, and Status.

#	Name	Real Name	Email Address	Status
27	Inorgaard	Lise Nørgaard	lnorgaard@keeper.htb	Enabled
14	root	Enoch Root	root@localhost	Enabled

- A tab with two users. One is root and had nothing interesting in it. And the other is Inoogaard.

- As we can see in his tab is a username and at the bottom a default password.
- Remember on the nmap scan we found port 22/SSH open. So let try and login with Inorgaard's credentials.

^ Identity

Username: Inorgaard (required)

Email: Inorgaard@keeper.htb

Real Name: Lise Nørgaard

Nickname: Lise

Unix login: Inorgaard

Language: Danish

Timezone: System Default (Europe/Berlin)

Extra info: Helpdesk Agent from Korsbæk

^ Access control

☒ Let this user access RT

☒ Let this user be granted rights (Privileged)

root's current password:

New password:

Retype Password:

^ Comments about this user

New user. Initial password set to Welcome2023!

- And boom we are in. a quick look in the users directory we find the flag and we can submit it.

```
(root@kali) - [~/Desktop/lab]
# ssh lnorgaard@10.10.11.227
lnorgaard@10.10.11.227's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$
```

```
Last login: Tue Aug  8 11:31:22 2023
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
lnorgaard@keeper:~$ cat user.txt
b655 [REDACTED] abd7
lnorgaard@keeper:~$
```