React(10.12.1.188)-GhostIA

Sarah Ferenczi

Enumeration

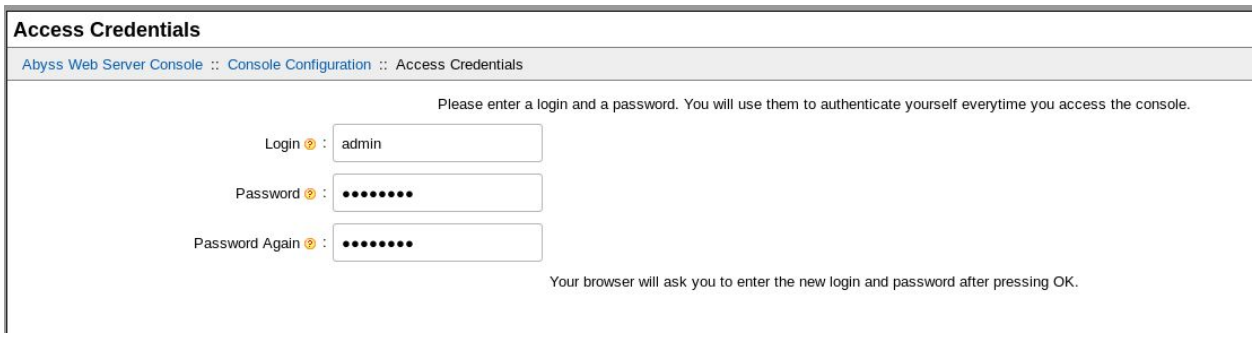
```
root@kali:~# nmap -sC -sV 10.13.1.188 --min-rate 4000
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-14 15:54 EDT
Nmap scan report for 10.13.1.188
Host is up (1.6s latency).
Not shown: 684 closed ports, 313 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Abyss httpd 2.11.1-X1 (AbyssLib/2.11)
|_http-server-header: Abyss/2.11.1-X1-Win32 AbyssLib/2.11
5800/tcp open  http-proxy sslstrip
|_http-title: TightVNC desktop [react]
5900/tcp open  vnc        VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|_    STDV VNCAUTH_ (2)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.56 seconds
```

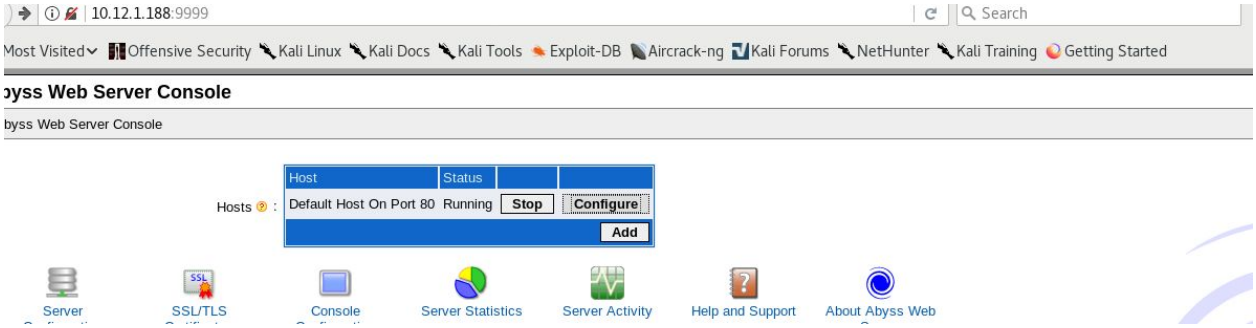
First we run an nmap scan, we can see port 80 is open.

On the page, we do not find much, however, if we look back to the nmap scan, we can see a high port that is open named filtered_abyss, so let's go ahead and check out that port.

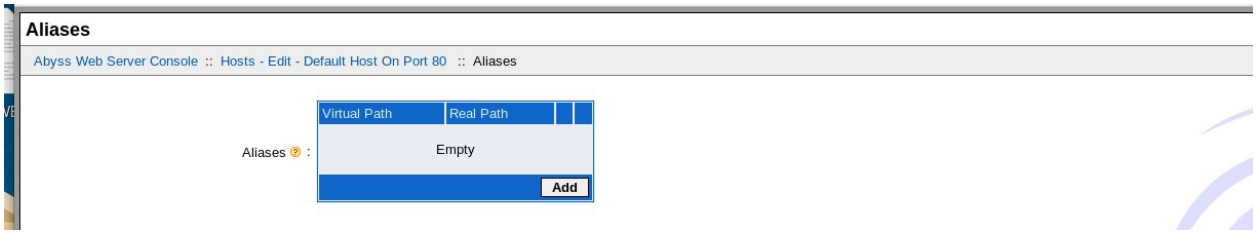
Exploitation



If we use the credentials admin/password, we can go ahead and access the console.

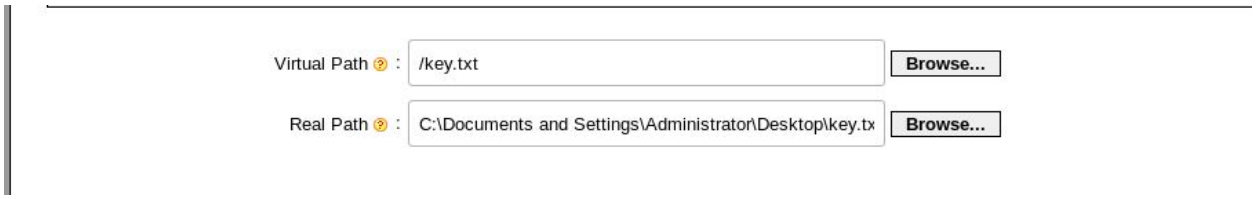


Then if we click on configure, we will be redirected to another page with more settings.



From there, we can click on Aliases and we are greeted with this page.

If we add the real path, we can access the key for the box.



Then we can go ahead and make the directory on the web.

Once we navigate back to port 80, we can go ahead and grab the key.