

Preignition

Enumeration

nmap scan.

```
(funa@kali)-[~/l3ickey/htb/Preignition]
└─$ sudo nmap -sV $target_IP
[sudo] funa のパスワード:
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-27 16:10 JST
Nmap scan report for 10.129.245.187
Host is up (0.25s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

From the scan result, a single entry is shown and catches our attention. It is an http service running on port 80, signaling that this target might be hosting some explorable web content. To look at the contents ourselves, we can open a web browser of our choice and navigate to the target's IP address in the URL bar at the top of the window.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

gobuster in directory enumeration mode.

```

(funa@kali)-[~/l3ickey/htb/Preignition]
$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u $target_IP
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.129.245.187
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.1.0
[+] Timeout:            10s
=====
2021/12/27 16:23:06 Starting gobuster in directory enumeration mode
=====
/admin.php              (Status: 200) [Size: 999]
=====
2021/12/27 16:25:00 Finished
=====

```

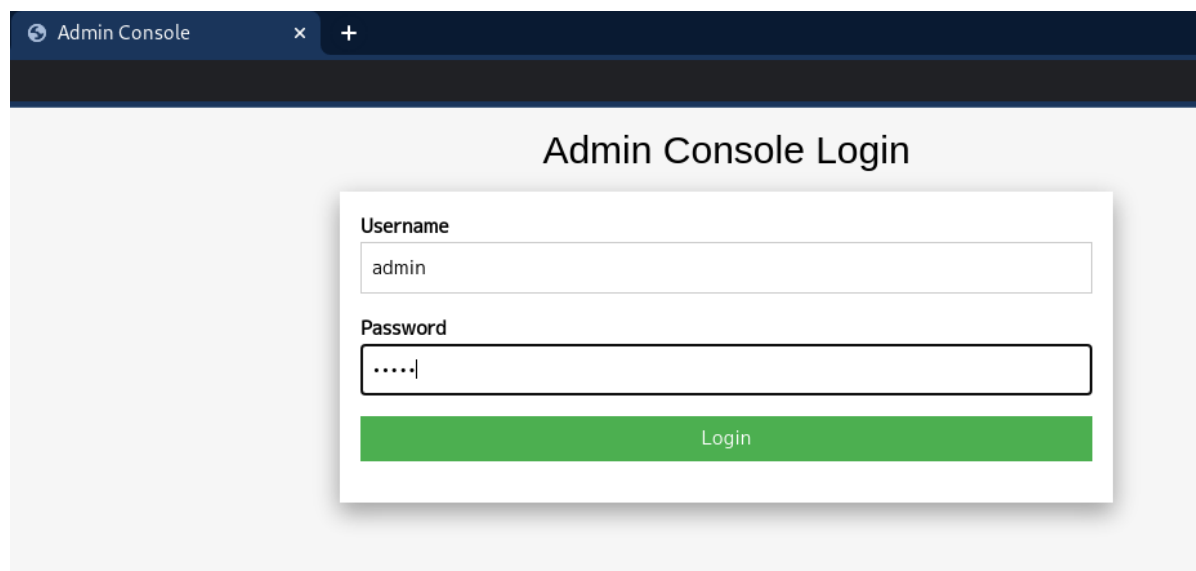
Foothold

open `admin.php` in your web browser. We can try our luck with some default credentials since this is a fresh nginx installation.

```

Username: admin
Password: admin

```



Admin Console Login

Username
admin

Password
.....

Login

Congratulations!