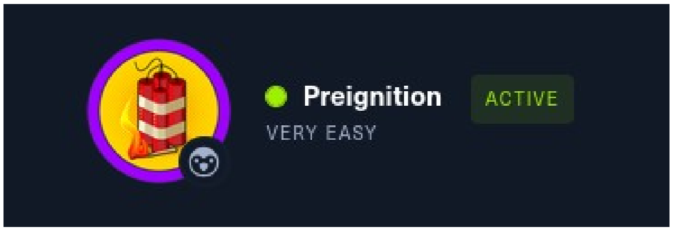


TARGET MACHINE IP ADDRESS

10.129.126.105

1. Directory Brute-forcing is a technique used to check a lot of paths on a web server to find hidden pages. Which is another name for this? (i) Local File Inclusion, (ii) dir busting, (iii) hash cracking?

   Answer: dir busting

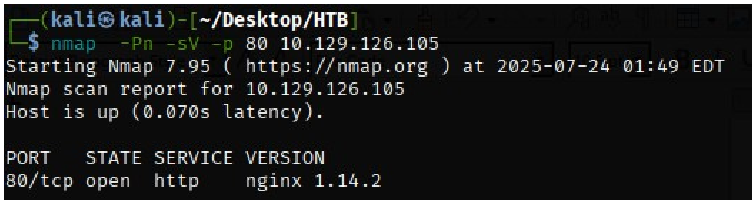
2. What switch do we use for nmap's scan to specify that we want to perform? version detection

   Answer: -sV

3. What does Nmap report is the service identified as running on port 80/tcp?

   Answer: http

4. What server name and version of service is running on port 80/tcp?



```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ nmap  -Pn -sV -p 80 10.129.126.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 01:49 EDT
Nmap scan report for 10.129.126.105
Host is up (0.070s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
```

   Answer: nginx 1.14.2

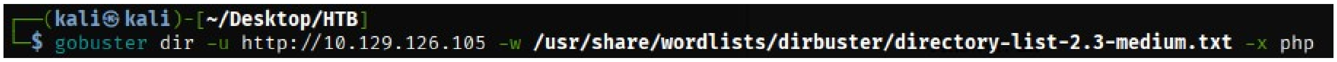
5. What switch do we use to specify to Gobuster we want to perform dir busting specifically?

   Answer: dir

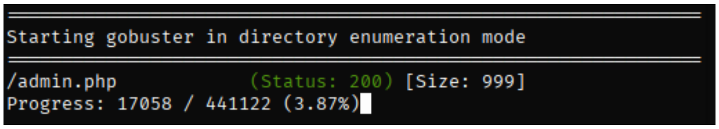
6. When using gobuster to dir bust, what switch do we add to make sure it finds PHP pages?

   Answer: -x php

7. What page is found during our dir busting activities?



```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ gobuster dir -u http://10.129.126.105 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
```



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 200) [Size: 999]
Progress: 17058 / 441122 (3.87%)
```

   Answer: admin.php

8. What is the HTTP status code reported by Gobuster for the discovered page

   Answer: 200

9. Submit root flag

   Answer: 6483bee07c1c1d57f14e5b0717503c73