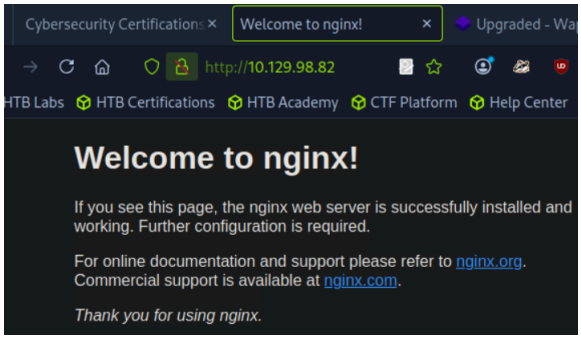
Preignition Write-up

Created @November 24, 2025 1:23 AM

Introduction
In most environments, web servers play a big part in the infrastructure and in the daily processes of many
departments. Web servers can sometimes be used strictly internally by employees, but most of the time can be found to be public-facing, meaning anyone from the Internet can access them to retrieve information
and files from their hosted web pages. For the most part, the web pages hosted on the web servers are managed through their administrative panels, locked behind a log-in page. Let us think of an example: You have decided to start your own blog and use WordPress to achieve this. If you are unfamiliar with WordPress, you can read more about it here, but it is essentially a popular web application that allows you
to easily manage the content you want to post for the rest of the world to read. Once installed, your WordPress website will have a public-facing side and a private-facing one, the latter being your administrative panel hosted at www.yourwebsite.com/wp-admin . This page is locked behind a log-in screen.
A quick note: you can learn more about hacking WordPress websites by checking out the Hacking

Once you, as an administrator of the WordPress site, log into its' admin panel, you will have access to a myriad of controls, ranging from content uploading mechanisms, to theme selection, custom script editing
for specific pages, and more. The more you learn about WordPress, the more you will see how this is a vital
part of a successful pentest, as some of these mechanisms could be outdated and come with critical flaws that would allow an attacker to gain a foothold and subsequently pivot through the network with ease.
Thus, we conclude that Web enumeration, specifically directory busting (dir busting), is one of the most
essential skills any Penetration Tester must possess. While manually navigating websites and clicking all the
available links may reveal some data, most of the links and pages may not be published to the public and,
hence, are less secure. Suppose we did not know the wp-admin page is the administrative section of the
WordPress site we exemplified above. How else would we have found it out if not for web enumeration and
directory busting?

```
[★]$ sudo nmap -sV 10.129.98.82
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-23 06:25 CST
Nmap scan report for 10.129.98.82
Host is up (0.078s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
```



At the top of the page, we observe the mention of the nginx service. After researching basic information
about nginx and its purpose, we conclude that our target is a web server. Web servers are hosts on the target network which have the sole purpose of serving web content internal or external users, such as web
pages, images, videos, audio files, and other types. Typically, a web server is accessible from the Internet to
allow for the stored content to be explored by the online public for many reasons: shopping, providing and
requesting services, banking, reading the news, and more.
What we are looking at on our browser screen is the default post-installation page for the nginx service,
meaning that there is the possibility that this web application might not be adequately configured yet, or
that default credentials are used to facilitate faster configuration up to the point of live deployment. This,
however, also means that there are no buttons or links on the web page to assist us with navigation between web directories or other content.
When browsing a regular web page, we use these elements to move around on the website. However, these elements are only links to other directories containing other web pages, which get loaded in our browser as if we manually navigated to them using the URL search bar at the top of the browser screen. Knowing this,
could we attempt to find any "hidden" content hosted on this webserver?
The short answer is yes, but to avoid guessing URLs manually through the browser's search bar, we can find
a better solution. This method is called dir busting, short for directory busting. For this purpose, we will be
using the tool called gobuster , which is written in Go. If you do not have gobuster installed on your machine yet, you can follow the instructions below to install it successfully. Pwnbox already comes pre equipped with gobuster and all the necessary tools to finish any lab on Hack The Box.

Installing gobuster

First, you need to make sure you have Go installed on your Linux distribution, which is the pr