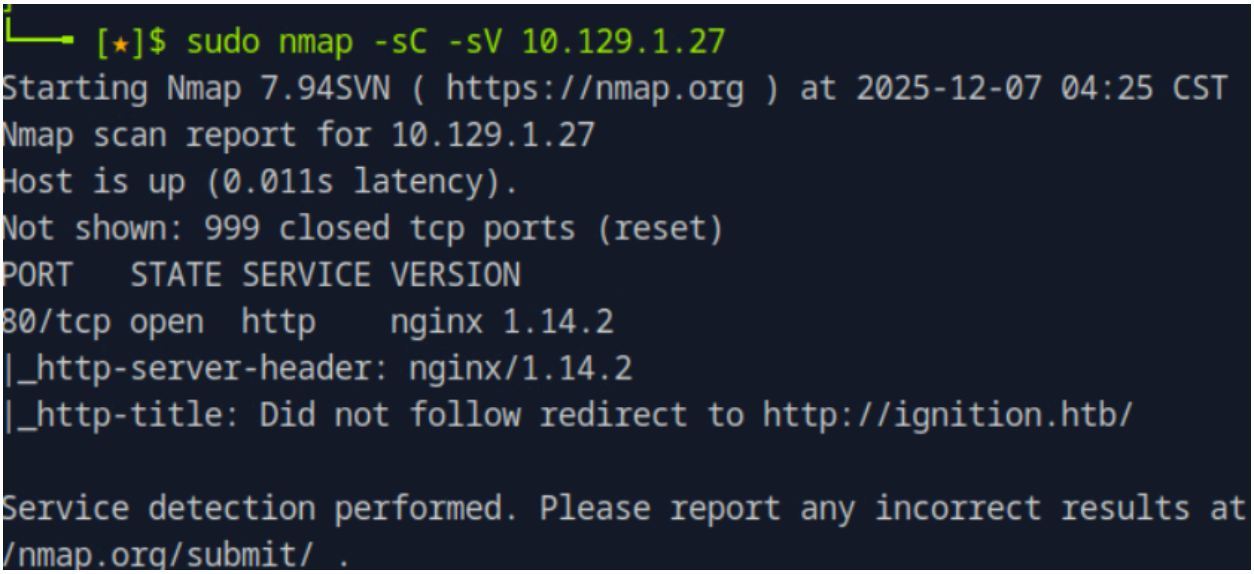
Ignition Writeup

Created @December 7, 2025 11:26 PM

Introduction

Networking knowledge plays a tremendous part for your overall readiness as an upcoming cybersecurity engineer. Features such as Active Directory, Kerberos Authentication, Server Message Block, Hypertext Transfer Protocol, Secure Shell can all be dissected into their (almost) simplest form if enough networking knowledge is applied. However broad, we will be exploring only a part of the whole networking subject, specifically HTTP, VHosts and DNS, with this target.

Before you get started with this target, we strongly recommend you brush up on your Networking knowledge by reading our Introduction to Networking on HTB Academy!



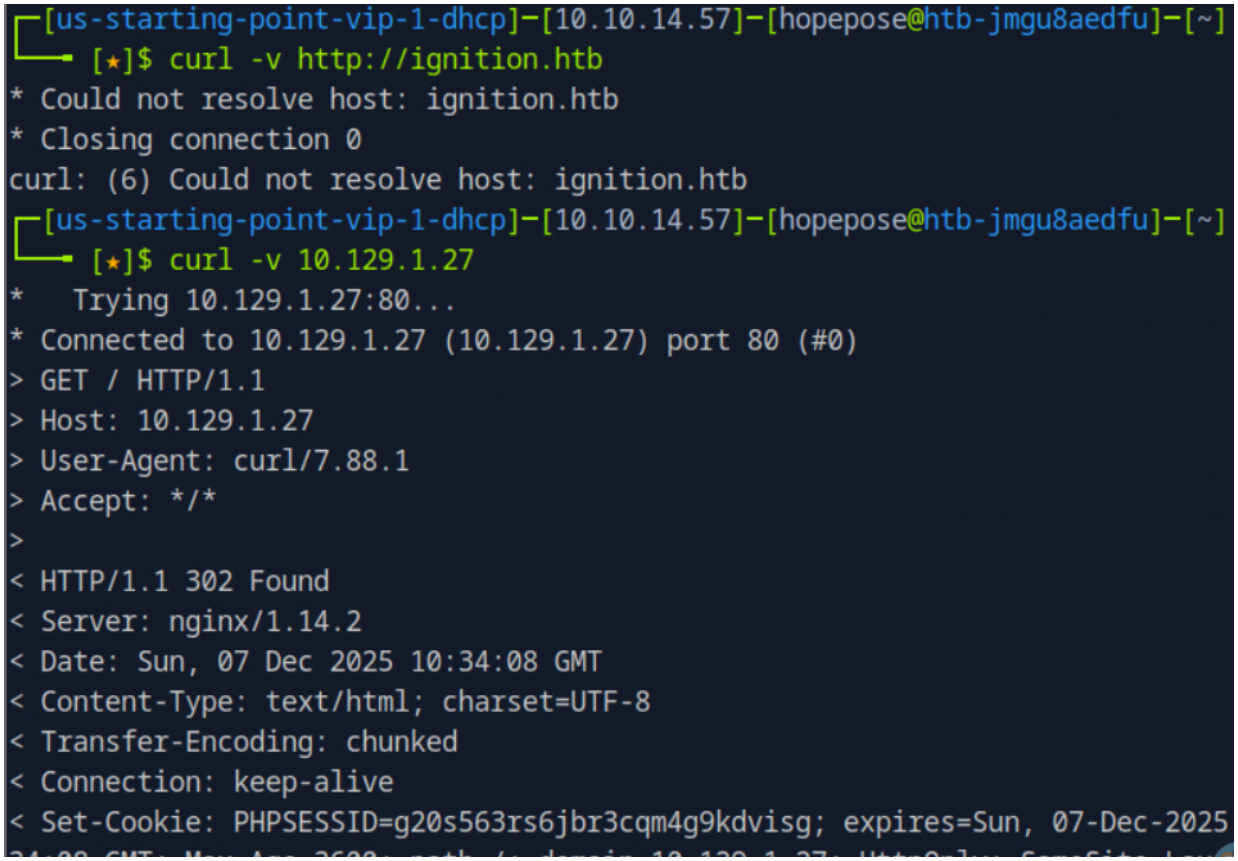
Enumeration

Starting off with an nmap scan, we select the -sC and -sV switches to trigger default script scanning and version detection. This yields us a singular result, port 80 open and running nginx 1.14.2. So far, this seems straight forward. However, from the output right below that, we notice that http-title returns Did not follow redirect to http://ignition.htb . Keep this URL in mind for now.

Upon attempting to access the webpage through a browser window, we are presented with the following error. The Check if there is a typo in ignition.htb references the same URL we found during our nmap scan, but without further details as to what might cause this error to pop up when simply attempting to access the website. Below, a more detailed error code is displayed: DNS_PROBE_FINISHED_NXDOMAIN

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers).[1] This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The term virtual hosting is usually used in reference to web servers but the principles do carry over to other

Internet services.
A technical prerequisite needed for name-based virtual hosts is a web browser with HTTP/1.1 support (commonplace today) to include the target hostname in the request. This allows a server hosting multiple sites behind one IP address to deliver the correct site's content. More specifically it means setting the Host HTTP header, which is mandatory in HTTP/1.1.[2]
Furthermore, if the Domain Name System (DNS) is not properly functioning, it is difficult to access a virtually-hosted website even if the IP address is known. If the user tries to fall back to using the IP address to contact the system, as in http://10.23.45.67/, the web browser will send the IP address as the host name. Since the web server relies on the web browser client telling it what server name (vhost) to use, the server will respond with a default website—often not the site the user expects.
A workaround in this case is to add the IP address and host name to the client system's hosts file. Accessing the server with the domain name should work again.[..]In short, multiple websites can share the same IP address, allowing users to access them separately by visiting the specific hostnames of each website instead of the hosting server's IP address. The webserver we are making requests to is throwing us an error because we haven't specified a certain hostname out of the ones that could be hosted on that same target IP address. From here, we'd think that simply inputting ignition.htb instead of the target IP address into the search bar would solve our issue, but unfortunately, this is not the case. When entering a hostname instead of an IP address as the request's destination, there is a middleman involved that you might not know about. Because DNS is involved when translating the hostnames to the one IP address available on the server's side, this will prove to be an issue once the target is isolated, such as in our case. In order to solve this, we can edit our own local hosts file which includes correlations between hostnames and IP addresses to accomodate for the lack of a DNS server doing it on our behalf. Until then, we must first confirm that we are correct. In order to get a better view of the exact requests and responses being made and to confirm our suspicion, we will need to make use of a popular and easy to use tool called cURL . This tool will allow us to manipulate HTTP requests made to a server and receive the responses directly in the terminal, without the latter being interpreted by our browser as generic error messages such as in the example above.
cURL is pre-installed with almost every Linux operating system. To see its' capabilities, type curl -h in your terminal



As observed from the screenshot above, our request contains a Host field which is home to the target's IP address instead of the hostname. The 302 Found response, together with the Location header, indicates that the resource we requested (/) has been (temporarily) moved to http://ignition.htb/ . This means that our assumptions were true.

To solve the issue we are currently facing here, we will modify our local DNS file named hosts located in the /etc directory. The first command illustrated below has the purpose of inputting the target's IP address with its' associated hostname in the hosts table, which would in turn allow your web client to visit the website which was previously reporting an error. Make sure to replace the {target_IP} part on the first line with the actual IP address for your own target instance, and the {your_password} part on the second line with your VM's user account password, since this action requires superuser privileges. The second command has the role of verifying your previous input. Reading the /etc/hosts file of your Linux system should return an entry for ignition.htb with the associated target IP address.

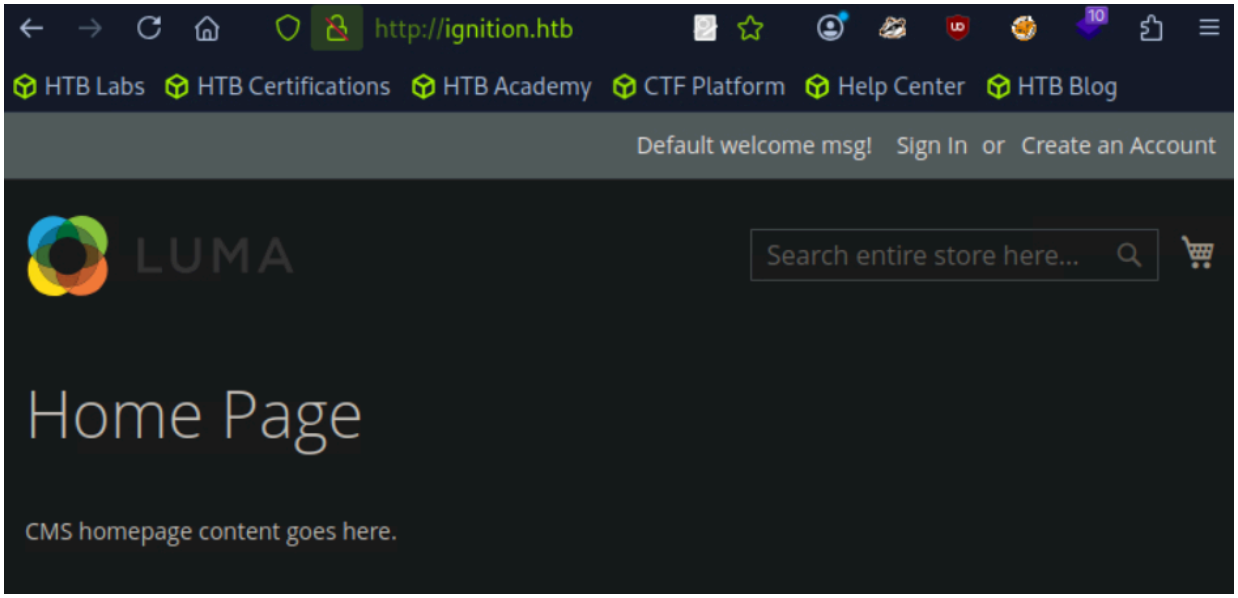
```
┌─[us-starting-point-vip-1-dhcp]─[10.10.14.57]─[hopepose@htb-jmgu8aedfu]─[~]
└──╼ [★]$ echo "10.129.1.27 ignition.htb" | sudo tee -a /etc/hosts
10.129.1.27 ignition.htb
┌─[us-starting-point-vip-1-dhcp]─[10.10.14.57]─[hopepose@htb-jmgu8aedfu]─[~]
└──╼ [★]$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       debian12-parrot

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 localhost
127.0.1.1 htb-jmgu8aedfu htb-jmgu8aedfu.htb-cloud.com
10.129.1.27 ignition.htb
```

Once this configuration is complete, we can proceed to reload the target's webpage and verify if it loads successfully. Since the requested hostname now has an association in your hosts file, the website can load without issue. From here, we can start working towards gaining a foothold.

Foothold

After exploring the landing page for a short period of time, we can deduce that nothing helpful can be leveraged here. The only option of exploring the website further is using gobuster.



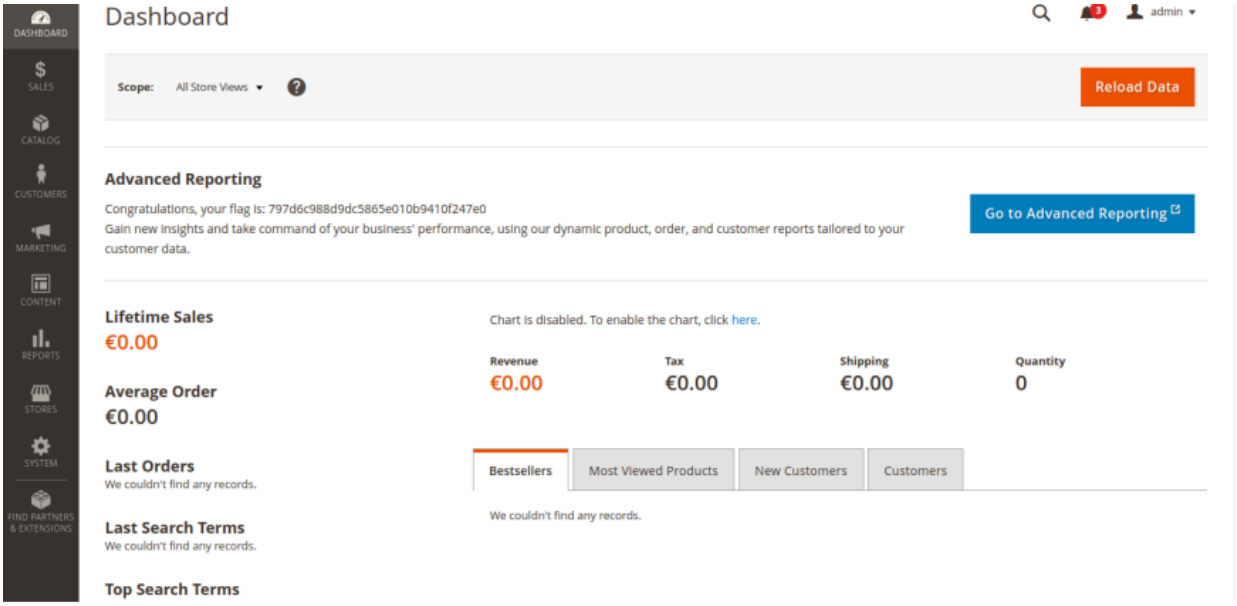
```
┌─[us-starting-point-vip-1-dhcp]─[10.10.14.57]─[hopepose@htb-jmgu8aedfu]─[~]
└──╼ [★]$ gobuster dir --url http://ignition.htb/ --wordlist /usr/share/wordlis
s/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ignition.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
mall.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
```

```
Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 200) [Size: 28673]
/home                 (Status: 200) [Size: 25802]
/media                (Status: 301) [Size: 185] [--> http://ignition.htb/media/]
/0                    (Status: 200) [Size: 25803]
/catalog              (Status: 302) [Size: 0] [--> http://ignition.htb/]
/static               (Status: 301) [Size: 185] [--> http://ignition.htb/static/]
/admin                (Status: 200) [Size: 7092]
/Home                 (Status: 301) [Size: 0] [--> http://ignition.htb/home]
/cms                  (Status: 200) [Size: 25817]
/checkout             (Status: 302) [Size: 0] [--> http://ignition.htb/checkout/cart/]
/robots               (Status: 200) [Size: 1]
/setup                (Status: 301) [Size: 185] [--> http://ignition.htb/setup/]
/wishlist             (Status: 302) [Size: 0] [--> http://ignition.htb/customer/account/login/ref
erer/aHR0cDovL2lnbml0aW9uLmh0Yi93aXNobGlzdA%2C%2C/]
/soap                 (Status: 200) [Size: 391]
/rest                 (Status: 400) [Size: 52]
/errors               (Status: 301) [Size: 185] [--> http://ignition.htb/errors/]
Progress: 6231 / 87665 (7.11%)[ERROR] Get "http://ignition.htb/suzuki": context deadline exceeded
```

From the output of our gobuster script, we find our target. The /admin page returns a 200 response code, signalling its' availability. We can navigate to it by appending it to the end of the URL:http://ignition.htb/admin .

A login screen is presented to us, with a logo for Magento boasting in the middle of the page. A username and password are being requested. Normally, we would go off credentials we extracted through other means, such as an FTP server left unsecured, as seen before. This time, however, we will attempt some default credentials for the Magento service, since there is no other basis upon which we can rely

According to the documentation, we should not attempt to brute force this login form because it has antibruteforce measures implemented, we will need to guess the password. Since the password must be seven or more characters long & to include both letters and numbers, we can attempt to use the most common passwords of the year 2021 as well as a common username, such as admin . From the list, only the following password fulfils the requirements.


DASHBOARD
SALES
CATALOG
CUSTOMERS
MARKETING
CONTENT
REPORTS
STORES
SYSTEM
FIND PARTNERS & EXTENSIONS
Dashboard
admin
Scope: All Store Views
Reload Data
Advanced Reporting
Congratulations, your flag is: 797d6c988d9dc5865e010b9410f247e0
Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data.
Go to Advanced Reporting
Lifetime Sales
€0.00
Average Order
€0.00
Last Orders
We couldn't find any records.
Last Search Terms
We couldn't find any records.
Top Search Terms
Chart is disabled. To enable the chart, click here.
Revenue
€0.00
Tax
€0.00
Shipping
€0.00
Quantity
0
Bestsellers
Most Viewed Products
New Customers
Customers
We couldn't find any records.