**BOLT – TryHackMe Writeup**

[*https://tryhackme.com/room/bolt*](https://tryhackme.com/room/bolt)

This room is a Easy level room that tests some basic enumeration, exploitation and file system traversing skills.

-------------------------------------

After having obtained the IP address, we can use AutoRecon [ a tool that automates the reconnaissance phase of CTF and other tests ].

At its most basic,

sudo autorecon bolt.thm

The results show that we have 3 ports open.

22 – SSH

80 – HTTP, most likely a web application

8000 – HTTP, most likely a web application

Using the browser to visit Port 80, we find the default landing page for Apache. We can try a directory brute force using ffuf but we do not find anything useful.

*ffuf -u http://bolt.thm:8000/FUZZ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o Bolt:8000\_ffuf -c*

We try to access the Port 8000 over the browser and we find Bolt CMS. Looking over the page we find a large hint on the user name and the password associated with it. That was easy …

The login page for Bolt CMS is located at “<http://bolt.thm/bolt/login>” . The login credentials work and we are met with the dashboard. We find the version of the Bolt CMS running and we find there is a Authenticated RCE exploit available on Exploit-DB and Metasploit. (If not in the Metasploit database, update the framework).

The required options are entered; its not advised to disable the AutoCheck as for some reason it doesn’t work. Once the correct options are set the exploit can be run. We get a shell back and we enumerate the machine to look for flag.txt. The find utility can be used:

*find / -name “flag.txt” -type f 2>/dev/null*

Room completed.

\*Note: This lab was completed using Metasploit.