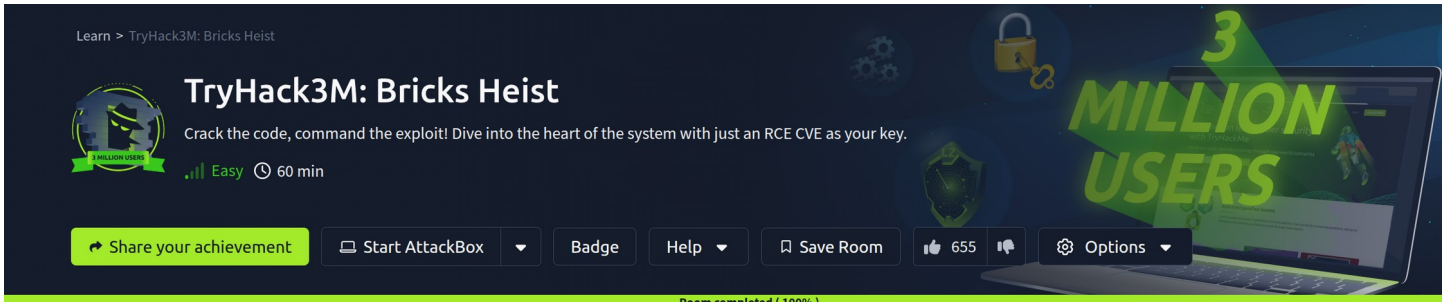
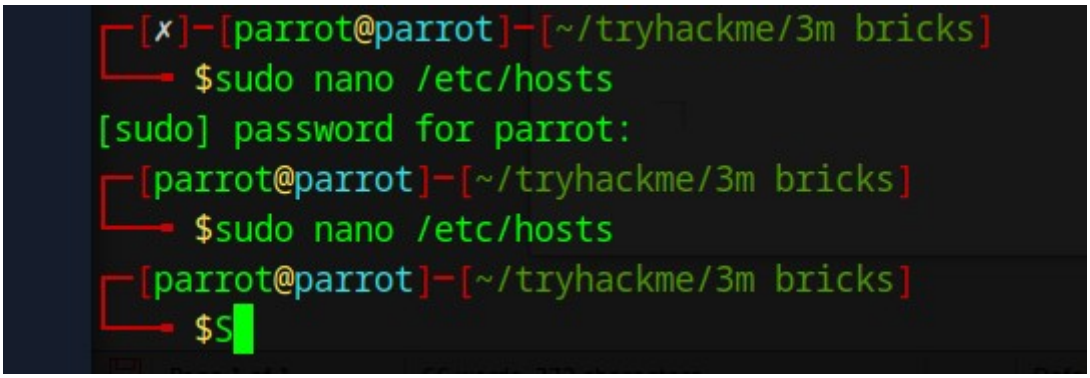
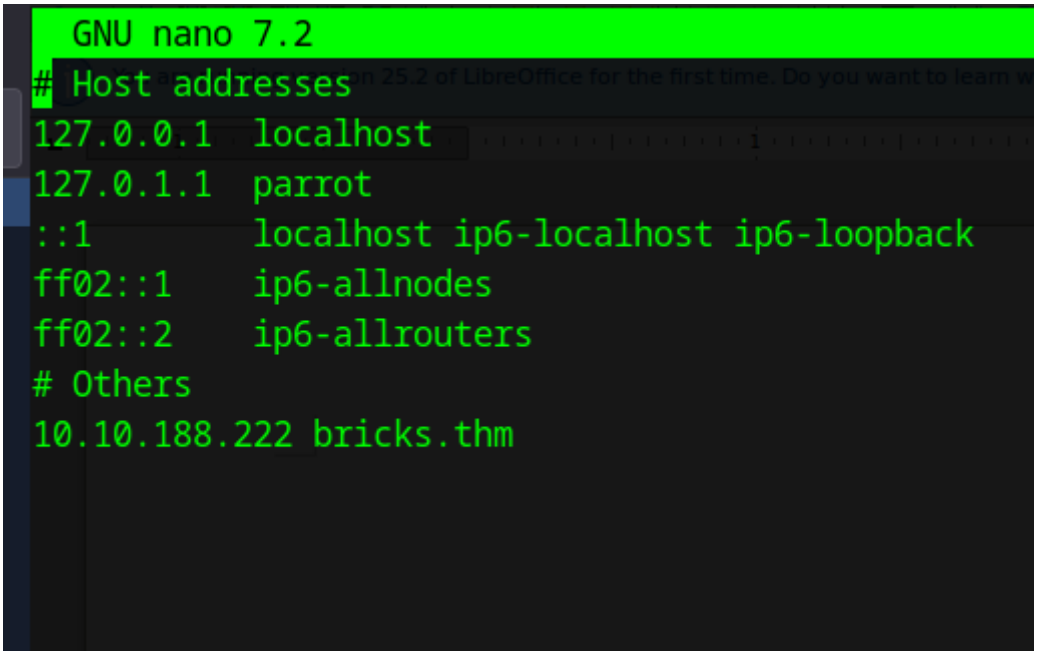
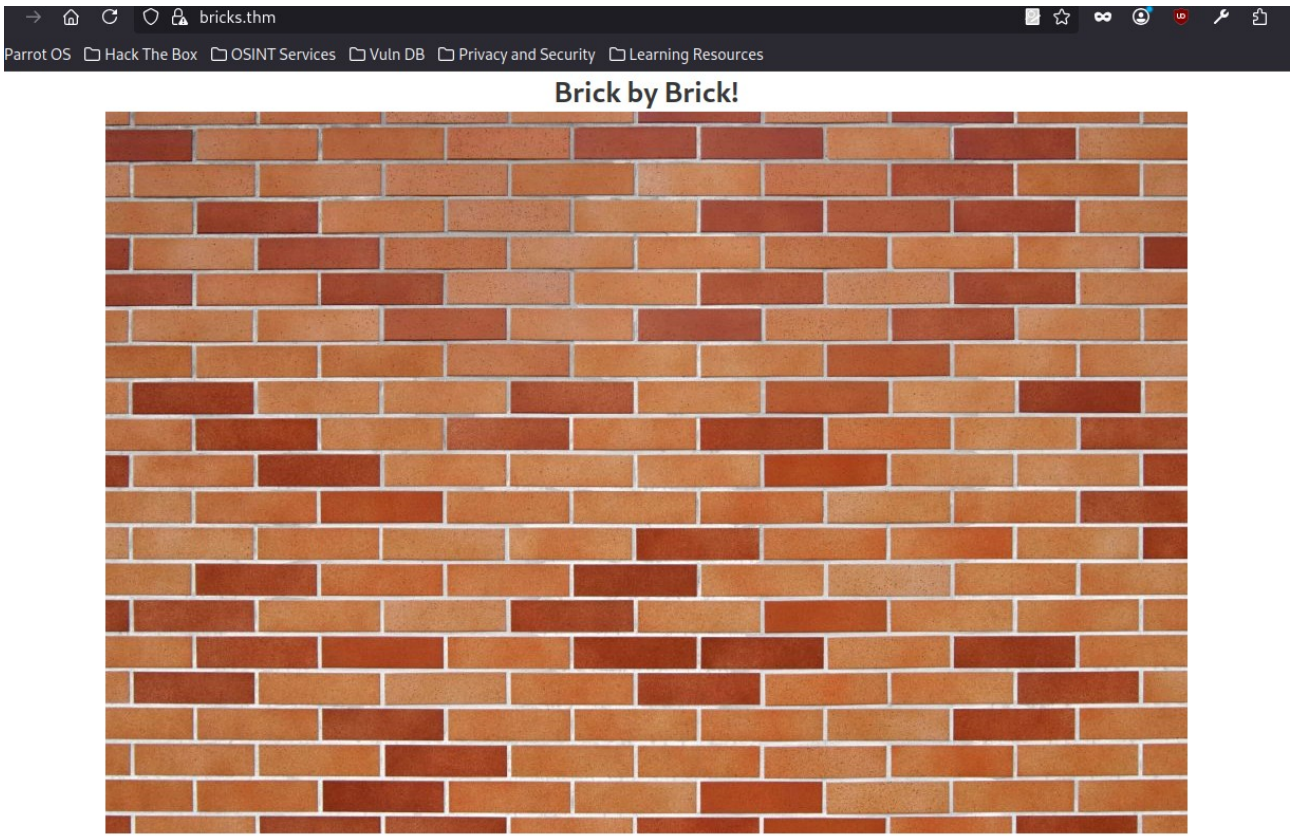


We start by adding the ip and host name to our hosts file





Next we navigate to the site:



The Site indicates that is it a wordpress site so we start with wpscan. We discover that it is running bricks 1.9.5 which is a vulnerable version. Searching in msfconsole for brick 1.9 yields an exploit. We run said exploit and get a meterpreter shell :).

What is the content of the hidden .txt file in the web folder?
THM{fl46_650c844110baced87e1606453b93f22a}

To find the suspicious process I listed out all running processes using systemctl | grep running.

Find a service called ubuntu.service that's description is TRYHACKM3
What is the name of the suspicious process?

nm-inet-dialog

What is the service name affiliated with the suspicious process?

Ubuntu.service

What is the log file name of the miner instance?
Inet.conf

What is the wallet address of the miner instance?

bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa

The wallet address used has been involved in transactions between wallets belonging to which threat group?

LOCKBIT