Cybersecurity

Activity File

Activity File: Shodan

- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- You are now tasked with performing OSINT by using Shodan.io.
- You will use Shodan.io to look at previously completed port scans on several targets, without using Nmap to provide additional insight into the target.
- Additionally, you will need to create a Shodan.io account to gather information on megacorpone.com.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your report on Day 4!

Instructions

1. Navigate to https://account.shodan.io/register, and create a free account on Shodan.io.

2. After registering, log in and navigate to https://shodan.io.

3. In a terminal session, perform an nslookup on www.megacorpone.com.

4. In Shodan, search the IP address that was returned from the nslookup query.

5. Answer the following questions:

    - What ports are open? 22, 80, 443

    - What version of SSH is the server running? OpenSSH

    - What OS is the server? Debian

    - What is the version of the web server running? Apache httpd

    - Which vulnerabilities may be present on the server? (CVE numbers are fine.) 2020-11023, 2020-11022, 2019-11358, 2015-9251, 2013-4365, etc..

    - Where is this server located? Monreal QC, Canada
