Recon for Ethical Hacking / Penetration Testing & Bug Bounty

Navigating the Art of Reconnaissance in Ethical Hacking, Penetration Testing & Bug Bounty Hunting

❖ Introduction

In the ever-evolving cybersecurity landscape, one truth remains constant: knowledge is power. Ethical hackers, penetration testers, and bug bounty hunters are driven by an insatiable curiosity to uncover vulnerabilities, safeguard systems, and contribute to a safer digital realm. Welcome to the enlightening Udemy course "Recon for Ethical Hacking / Penetration Testing & Bug Bounty." In this article, we invite you to embark on a journey of discovery through the intricacies of the reconnaissance foundation upon which effective cybersecurity strategies are built.

❖ Introduction to Shodan

Shodan is a powerful tool used for online reconnaissance, like a search engine for internet-connected devices. It scans the web to find and index various devices, such as webcams, routers, servers, and more. Shodan reveals information about these devices, like open ports, vulnerabilities, and even the data they expose. It's often used by security professionals to identify potential weaknesses in a network's security. Shodan can be a valuable asset for assessing the security of your own systems or discovering vulnerabilities in other online devices, making it a key tool in the world of digital reconnaissance and cybersecurity.

❖ Mastering Shodan Filters

Mastering Shodan filters involves refining your search queries to pinpoint specific devices or services. You can filter by criteria like location, port number, or even specific software versions to find vulnerable systems. Learning to use filters effectively allows you to uncover precise information about the devices and services you're interested in while minimizing noise in your search results. This skill is essential for targeted reconnaissance and security assessments.

- **Country Filter:** This filter allows you to narrow down Shodan search results to devices or services located within a specific country, helping you focus on a particular geographic area for reconnaissance.

Filter: country:"Country Code"
Example: To find open webcams in the United States, use country:"US" port:80 webcam.

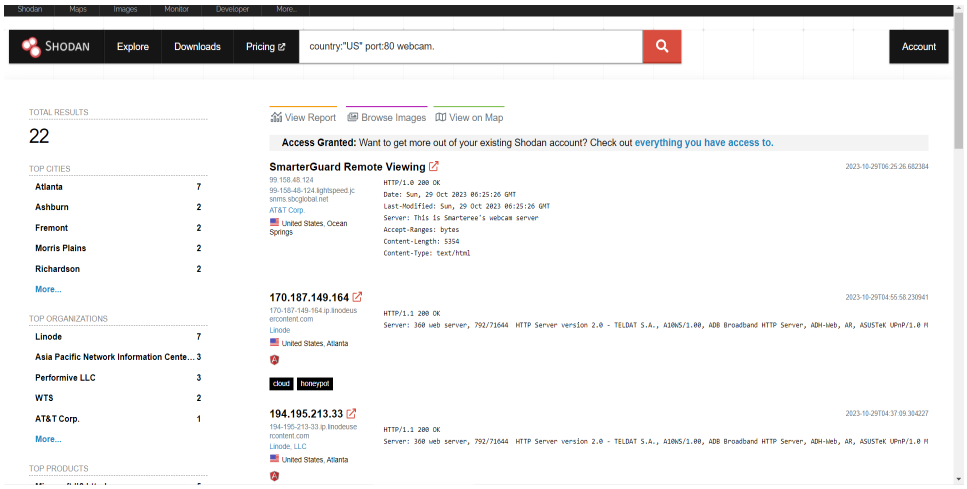

Figure:- The above figure shows how we can get open ports of a particular country.

- **Port Filter:** The port filter helps you find devices or services running on a specific port number, making it useful for identifying open ports and services on target systems.

Filter: port:Port Number
Example: To find MongoDB databases, use port:27017.

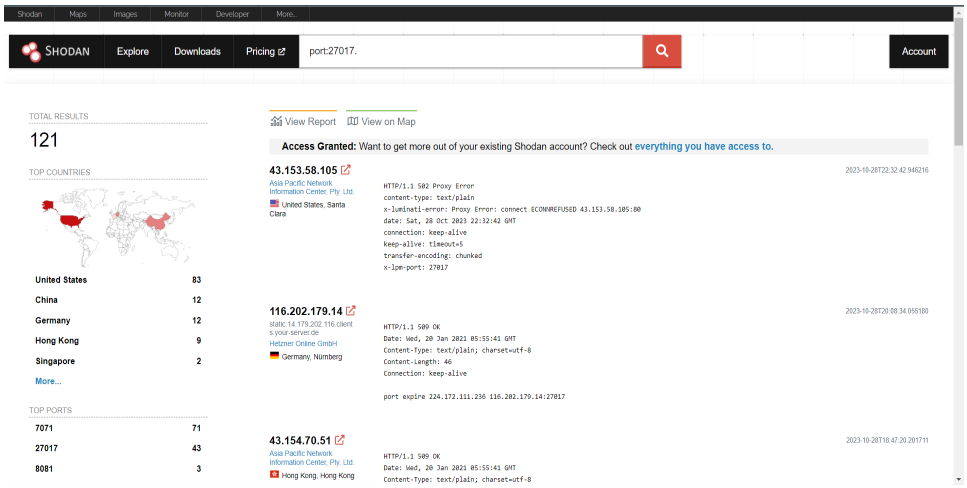

Figure:- The above figure shows the result of port 27017.

- **Product Filter**: This filter lets you search for devices or services based on the software or product they use, enabling you to discover systems running specific applications or versions.

Filter: product:"Product Name"
Example: To find Apache web servers, use the product:"Apache".

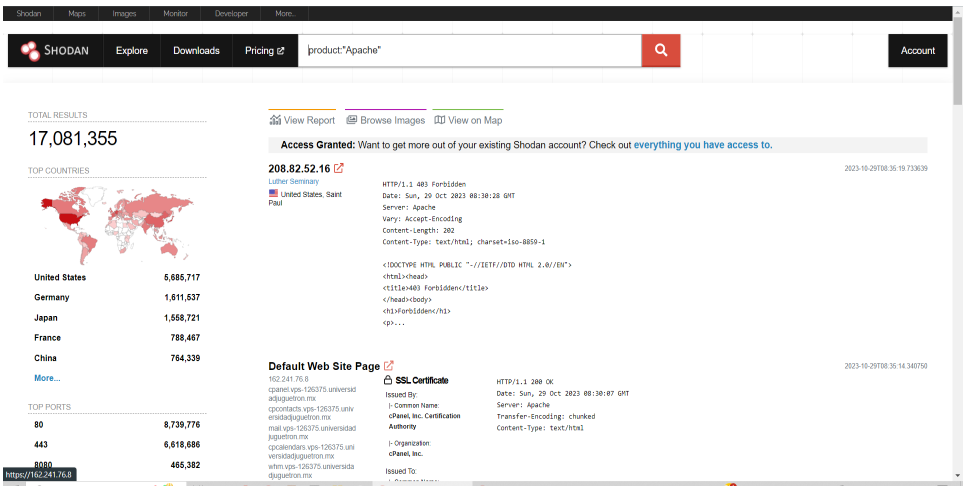

Figure:- The above figure shows the result of ip address of Apache web sever

- **SSL Filter**: With the SSL filter, you can locate devices or services that use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption, useful for identifying secure communication services.

Filter: ssl:"SSL Version"
Example: To find servers supporting SSLv2, use ssl:"SSLv2".

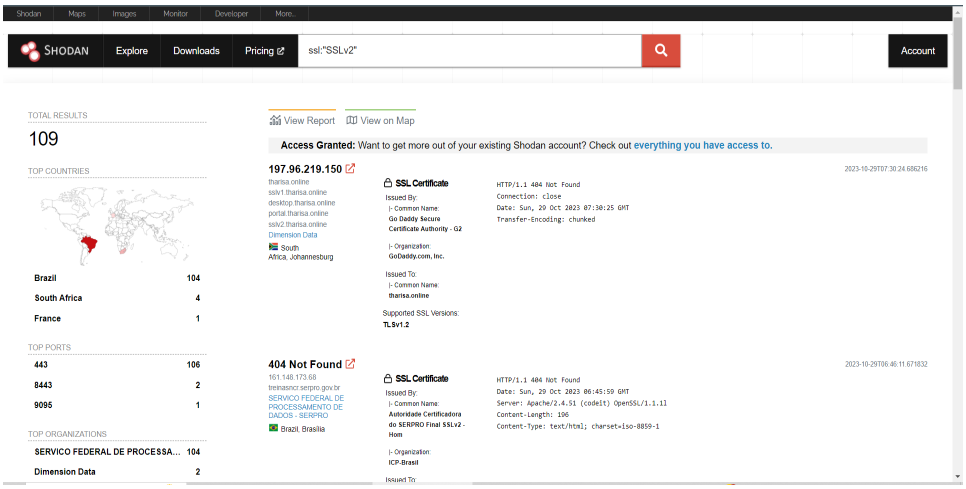

Figure:- The above figure shows the results server supporting SSL v2

- **Organization Filter:** This filter allows you to search for devices associated with a specific organization or company, helping you find systems linked to a particular entity.

Filter: org:"Organization Name"
Example: To find devices belonging to a specific company, use org:"Example Company".

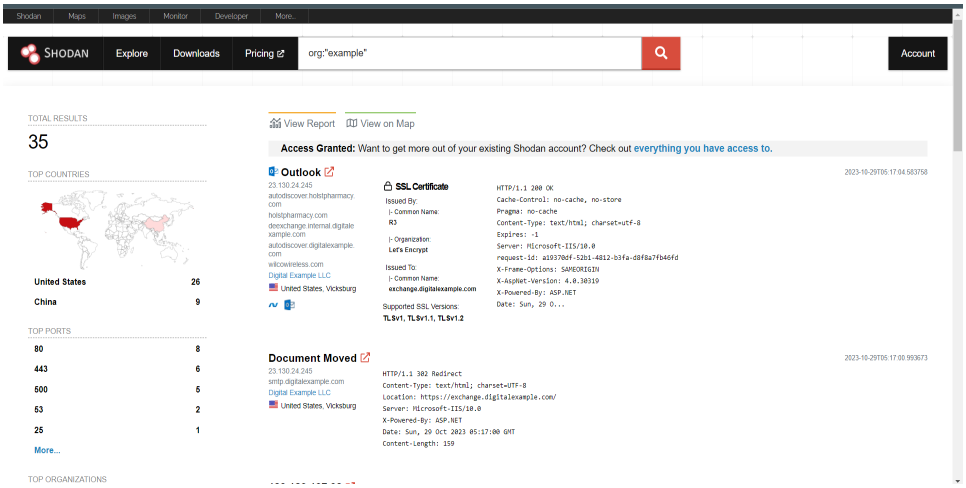

Figure:- The above figure shows the results of a specific organization.

- **<u>Host Name Filter:</u>** This filter enables you to search for devices by their hostname, making it easier to identify specific servers or domains within Shodan's database.

Filter: hostname:"Domain Name"
Example: To find devices associated with a specific domain, use hostname:"example.com".

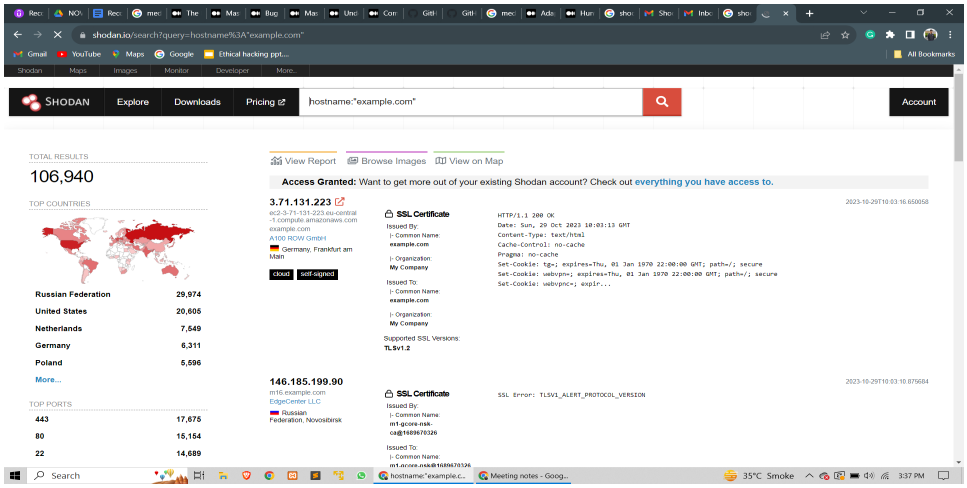

Figure:- The above figure shows the output of a specific domain using Hostname filter.

References:-

1. Shodan:- https://www.shodan.io/
2. Medium :- https://medium.com/@hexadefend/the-hackers-search-engine-shodan-part-2-6cf5c9b77ae7