Lab – Using Shodan to Search for Vulnerable Databases

Disclaimer: Please use this lab responsibly. Attempting to access any system you do not own or have permission to access is illegal. This lab is meant to be used for educational and research purposes only.

Overview

In this lab, you will learn how to conduct a passive reconnaissance scan while looking for well-known database applications that require little or no authentication. Two such database types are MongoDB and Elastic.

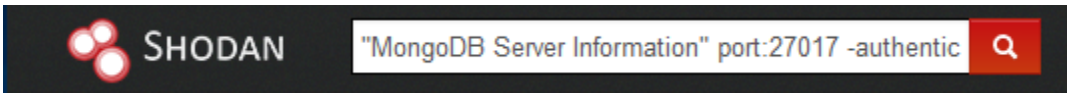
Search for Unsecured Vulnerable MongoDB Databases

Some databases by design do not use authentication by default. Two such databases are MongoDB and Elasticsearch

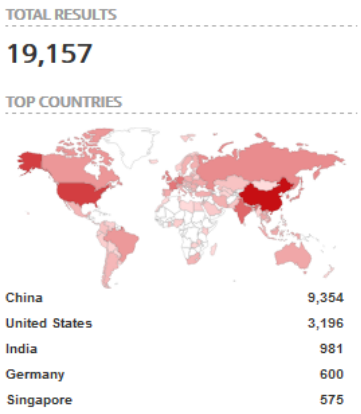
In the search bar, if we type,

```
“MongoDB Server Information” port:27017 -authentication
```

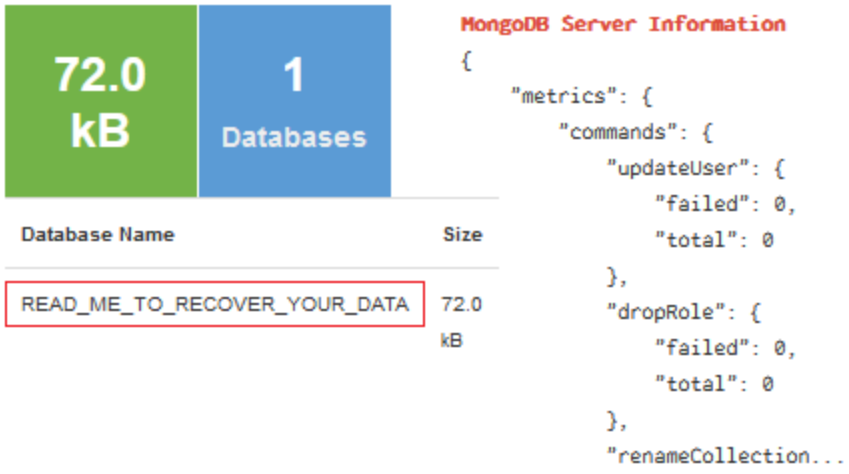
will retrieve MongoDB servers from Shodan, showing us how many MongoDB databases are running on port number 27017.



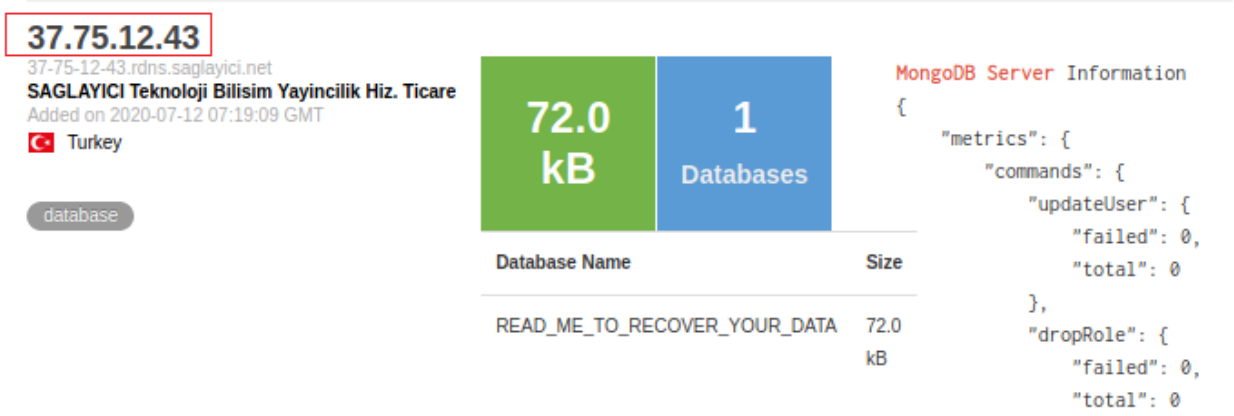
The search returns the results for nearly 20,000 MongoDB servers.



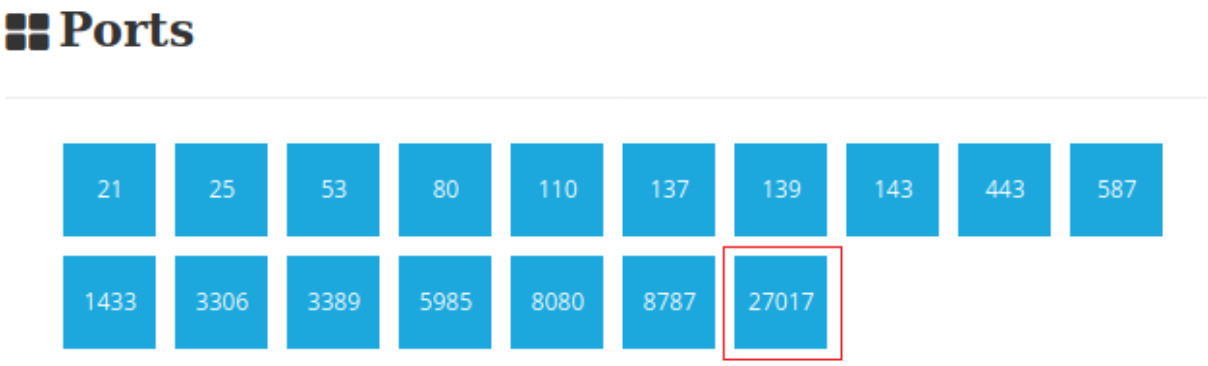
If you examine the search results, you’ll note that nearly all the servers have already been hacked into and left with a message that states,



To gain access to the unsecured data, we click on the IP address.



On the next page, under ports, find the port the MongoDB is using port 27017.



Clicking on the port number will take you directly into the unsecured database without being prompted for any user name or password.

I did not attempt to exploit any vulnerable database, and neither should you as this would be illegal!

To search for Mongo Express, the web GUI for MongoDB, use the following query:

Search term: `"Set-Cookie: mongo-express=" "200 OK"`

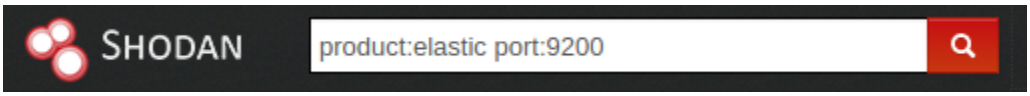
What this search filter does

"Set-Cookie: mongo-express=" "200 OK' retrieves MongoDB express database from Shodan that outputs 200 HTTP code that is 'OK' code (request successful). Hence, it gives us the Mongo Express open databases in the search results output.

There are additional database types that can be found using this search query to include **CouchDB, RethinkDB, and Cassandra**. Just replace the name Mongo-Express with the name of the chosen database.

Search for Unsecured Vulnerable Elastic Databases

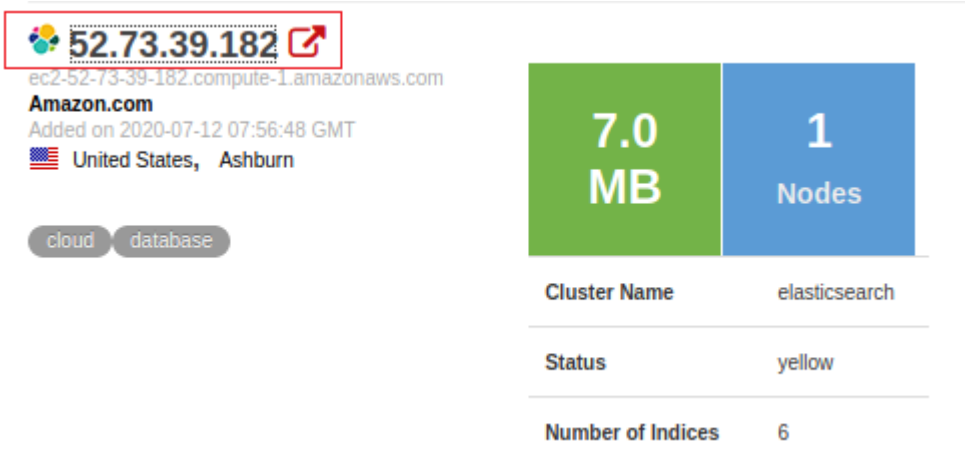
For this search query, we will be using the following search filter, **product:elastic port:9200**



You'll notice in your results that many of the Elastic databases have been compromised and left with a banner message stating:

```
Elastic Indices:
    you_base_was_hacked_and_dumped
    79128
    wegeturdb@criptext.com
    you_have_7days_to_contact_us
    wegetyourdb@protonmail.ch
    contact_us_or_your_data_will_be_leaked
```

You can click on the IP address assigned to the database server.



On the next page, if you click on the port number 9200, you are given full access to the database with the above message in the banner.

Summary –

In this short lab, you learned how to use the Shodan search engine to find well known vulnerable database applications. You can imagine yourself as a pentester or a digital forensics investigator looking into an attack on your client's database server. Imagine your surprise when you find your client's database in your Shodan search results. This type of passive reconnaissance scan is no different than looking for vulnerable ports using NMAP.