

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.

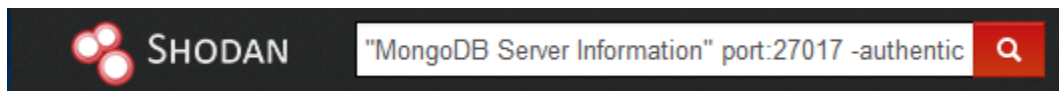
Search for Unsecured Vulnerable MongoDB Databases

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,

```
{
  "contact": "kirowgroup@cock.li",
  "bitcoin_address": "17U1FSe4vThE9K7J9bqt9mJBghq4Kkqgfw",
  "message": "ALL YOUR INDEX AND ELASTICSEARCH DATA HAVE BEEN BACKED UP AT OUR SERVERS. TO RESTORE SEND 0.05 BTC TO THIS BITCOIN ADDRESS 17U1FSe4vThE9K7J9bqt9mJBghq4Kkqgfw THEN SEND AN EMAIL WITH YOUR SERVER IP 1"
}
```

72.0
kB

1
Databases

Database Name	Size
READ_ME_TO_RECOVER_YOUR_DATA	72.0 kB

MongoDB Server Information

```

{
  "metrics": {
    "commands": {
      "updateUser": {
        "failed": 0,
        "total": 0
      },
      "dropRole": {
        "failed": 0,
        "total": 0
      },
      "renameCollection..."
    }
  }
}

```

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

37.75.12.43

37-75-12-43.rdns.saglayici.net

SAGLAYICI Teknoloji Bilisim Yayıncılık Hiz. Ticare

Added on 2020-07-12 07:19:09 GMT

Turkey

database

72.0
kB

1
Databases

Database Name	Size
READ_ME_TO_RECOVER_YOUR_DATA	72.0 kB

MongoDB Server Information

```

{
  "metrics": {
    "commands": {
      "updateUser": {
        "failed": 0,
        "total": 0
      },
      "dropRole": {
        "failed": 0,
        "total": 0
      }
    }
  }
}

```

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

Ports

21	25	53	80	110	137	139	143	443	587
1433	3306	3389	5985	8080	8787	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"

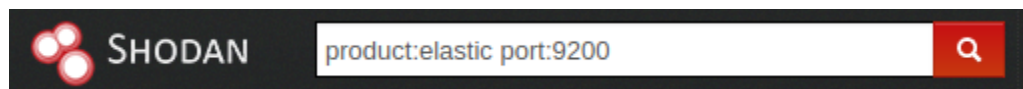
What this search filter does

“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.

**52.73.39.182** 
ec2-52-73-39-182.compute-1.amazonaws.com
Amazon.com
Added on 2020-07-12 07:56:48 GMT
 **United States, Ashburn**

cloud database

7.0 MB

1 Nodes

Cluster Name	elasticsearch
Status	yellow
Number of Indices	6

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.



Services



Elastic Version: 2.2.0

HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 317

```
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
```

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.