Experiment 03

Learning Objective:

Google Dorks is a search technique that uses advanced operators to search for information that is not typically indexed by search engines.

Tools: Google

Theory:

What is Google dorking?

Google dorking, also called Google hacking, is a search-hacking technique that uses advanced search queries to uncover hidden information in Google. Google dorks, or Google hacks, refer to the specific search commands (including special parameters and search operators) that when entered into the Google search bar reveal hidden parts of websites.

When Google crawls the web to index pages for its search engine, it can see parts of websites that normal internet users can't. Google dorks and Google hacks uncover some of that hidden data, letting you see information that organizations, companies, and website owners may not want you to see.

A simple example of an advanced search query is the use of quotation marks. Using quotation marks in searches gives you a list of results that includes web pages where the complete phrase is used, rather than some combination (complete or incomplete) of the individual words you entered into the search field.

There are many more types of Google hacks using advanced search queries, but their technical explanations don't actually get much more complicated than that. Their power lies in the ability to use them creatively.

What is Google dorking used for?

Google dorking is used to find hidden information that is otherwise inaccessible through a normal Google search. Google dorks can reveal sensitive or private information about websites and the companies, organizations, and individuals that own and operate them.

In preparing for an attack, malicious hackers might use Google dorks to gather data on their targets. Google dorks are also used to find websites that have certain flaws, vulnerabilities, and sensitive information that can be exploited.

Security companies try dorking to better understand how someone might approach hacking into systems. Or, companies might use Google dorks to find information that can be leveraged in SEO and performance marketing strategies. Using Google hacks helps companies see exactly what kind of information others can find about them.

Along with information-gathering, dorking may grant access to servers, cameras, and files.

Google dorks can be used to access all the webcams in a given area, they have even been used to access phone apps. Some dorking techniques have uncovered files of failed login attempts, including usernames and passwords. Other dorks have even let hackers bypass login portals.

Is Google dorking illegal?

Google dorking is completely legal — it's just another form of searching after all. Google was built to handle advanced searches, and banning this functionality would limit information access.

But Google hacks can quickly become illegal if they're used to surreptitiously access someone else's device, log in to someone else's account, or access or download protected files or documents. Searching for information may not be illegal, but using it for unauthorized purposes almost certainly is.

Google dorks: a historical background

Google dorks began in 2002 when the computer-security expert Johnny Long started using custom queries to search for elements of websites that he could leverage in cyberattacks. A form of penetration testing, Long called the custom search commands he used Google dorks, and the list of these queries grew into the Google Hacking Database. There, you can find all sorts of advanced queries that can be used to uncover various kinds of hidden information.

Though his tools have been used for unethical purposes, Johnny Long has devoted his infosec expertise to charity and international development, building infrastructure and technology training programs in underdeveloped countries.

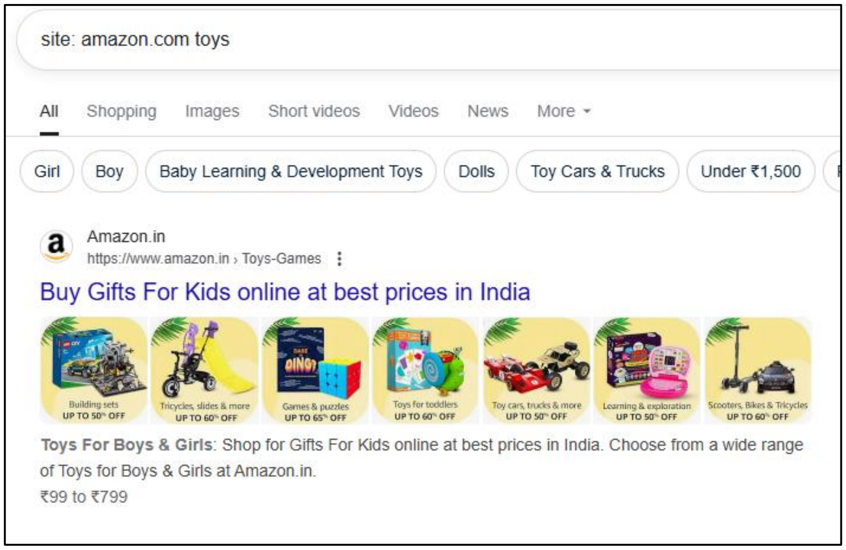
Common Google dork operators and commands:

For a better idea of how Google dorks work, here's a list of some of the most common Google dorking commands. You may even find some of these useful in your daily search engine life.

Consider this a Google dorking cheat sheet:

- **Site**

  Using "site:" in a search command will provide results only from the specific website mentioned.



site: amazon.com toys

All
Shopping
Images
Short videos
Videos
News
More
Girl
Boy
Baby Learning & Development Toys
Dolls
Toy Cars & Trucks
Under ₹1,500
Building sets UP TO 50% OFF
Tricycles, slides & more UP TO 60% OFF
Games & puzzles UP TO 65% OFF
Toys for toddlers UP TO 60% OFF
Toy cars, trucks & more UP TO 50% OFF
Learning & exploration UP TO 50% OFF
Scooters, Bikes & Tricycles UP TO 60% OFF

Amazon.in
https://www.amazon.in › Toys-Games

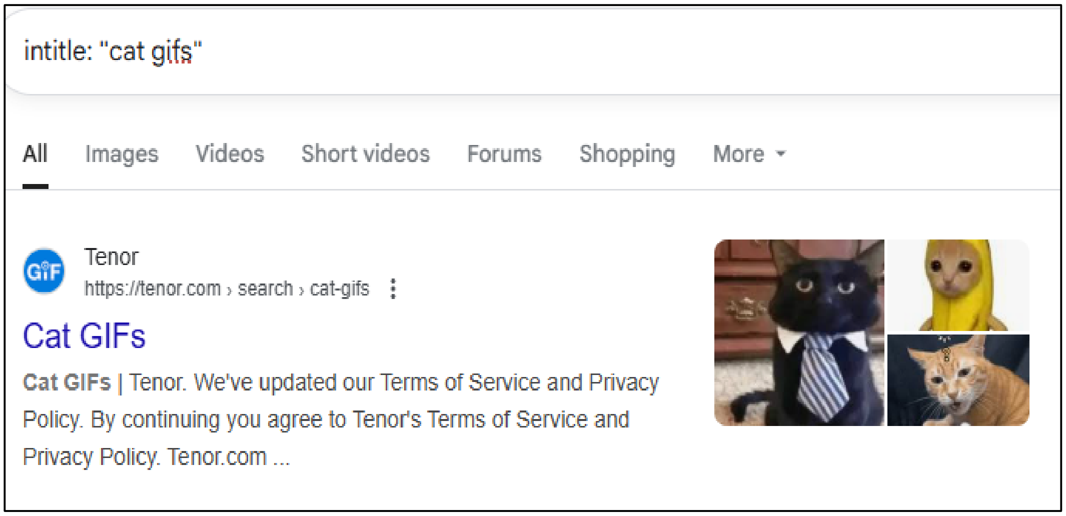
Buy Gifts For Kids online at best prices in India

Toys For Boys & Girls: Shop for Gifts For Kids online at best prices in India. Choose from a wide range of Toys for Boys & Girls at Amazon.in.

₹99 to ₹799

- **Intitle**

Using "intitle:" asks Google to search only for pages with that specific text in their HTML pages titles.



intitle: "cat gifs"

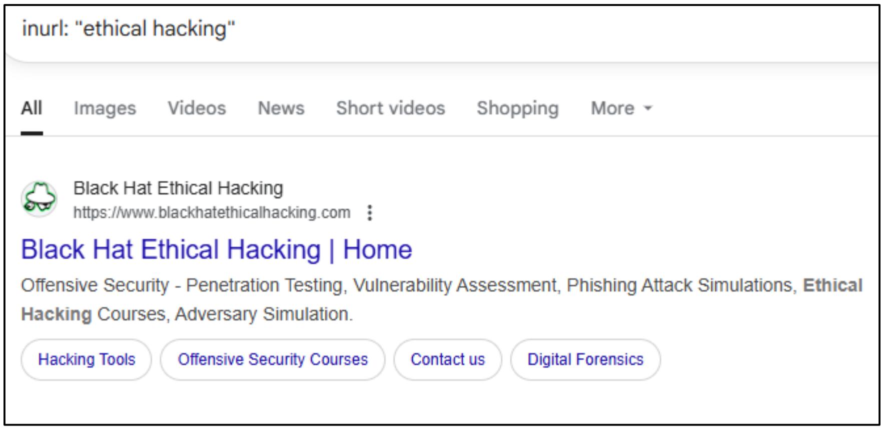
Tenor
https://tenor.com › search › cat-gifs

Cat GIFs

Cat GIFs | Tenor. We've updated our Terms of Service and Privacy Policy. By continuing you agree to Tenor's Terms of Service and Privacy Policy. Tenor.com ...

- **Inurl**

Using “inurl:” will search only for pages with that specific text in their URL.



inurl: "ethical hacking"

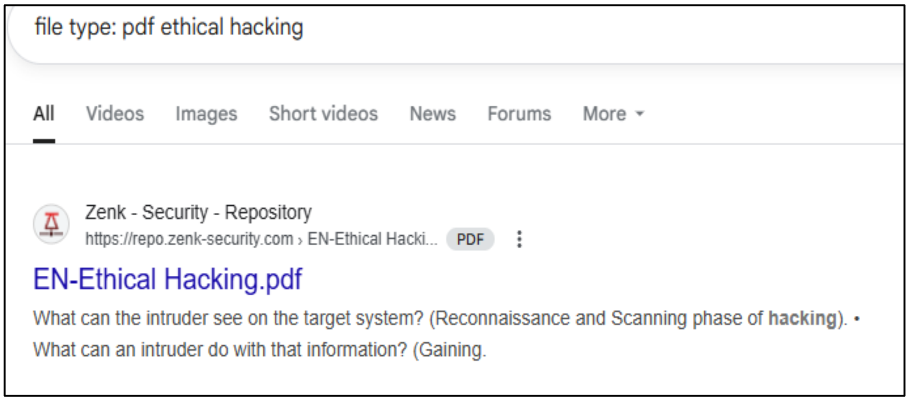
Black Hat Ethical Hacking
https://www.blackhatethicalhacking.com

Black Hat Ethical Hacking | Home

Offensive Security - Penetration Testing, Vulnerability Assessment, Phishing Attack Simulations, **Ethical Hacking** Courses, Adversary Simulation.

- **Filetype** or **ext**

Using “filetype:” or “ext:” will narrow your search to the specific file type mentioned.



file type: pdf ethical hacking

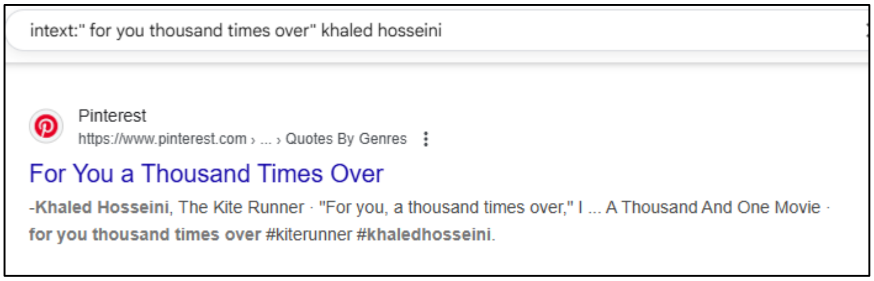
Zenk - Security - Repository
https://repo.zenk-security.com › EN-Ethical Hacki... PDF

EN-Ethical Hacking.pdf

What can the intruder see on the target system? (Reconnaissance and Scanning phase of **hacking**). • What can an intruder do with that information? (Gaining.

- **Intext**

Using “intext:” in a search query will search only for the supplied keywords. In the example below, all results listed will have the quoted text somewhere on the page.



intext:" for you thousand times over" khaled hosseini

Pinterest
https://www.pinterest.com › ... › Quotes By Genres

For You a Thousand Times Over

-**Khaled Hosseini**, The Kite Runner · "For you, a thousand times over," I ... A Thousand And One Movie · **for you thousand times over** #kiterunner #**khaledhosseini**.

As shown in the example for "filetype" above, you can mix and match these Google dork commands depending on information you want to find. Make sure to use a colon after the type of dork you enter.

Advanced Google dork operators and commands:

Now let's examine more advanced Google hacking commands. Advanced Google hacks let you look up the archives of files, read recently-deleted content, and access CCTV webcams of certain areas like a parking lot or the grounds of a college campus.

Here are some examples of the more advanced ways to use Google

dorking: • **Cache**

Using "cache" in your search can let you see older versions of a website or access files that have recently been removed. Try entering something like "cache:twitter.com/madonna" to see a history of the artist's posts, including recently-deleted tweets.

• **:ftp**

This advanced Google hack can be used at the end of a combined query to find FTP servers. FTP servers often hold large amounts of files.

Search **shakespeare:ftp** to find a massive archive of all his texts.

• **Filetype:log**

Using this Google dork will search for log files.

All of these can be combined with other keywords and operators for more precise searches. You can hone your search by adding additional parameters or commands and tightening the syntax you use. Dorks can also be automated to regularly scan for vulnerabilities and other information.

What Is Shodan?

Shodan is a search engine that focuses on internet-connected devices and services. It is designed to discover and provide information about various devices, systems, and services that are accessible over the internet. Shodan is often referred to as the "search engine for hackers" due to its ability to identify vulnerable or misconfigured devices.

Shodan works by constantly scanning the internet and collecting information about devices and services, including servers, routers, webcams, industrial control systems, and more. It goes beyond traditional search engines by indexing information specific to these devices, such as open ports, banners, protocols, and vulnerabilities.

The key features and capabilities of Shodan include:

1. **Device Discovery:** Shodan scans IP addresses and collects data about devices and services connected to the internet. It provides information on the device type, open ports, services running on those ports, and other details.

2. **Search Functionality:** Shodan offers a powerful search interface that allows users to find specific devices or services based on various criteria. Users can search by device type, location, operating system, port, and even specific keywords or banners.

3. **Vulnerability Detection:** Shodan can identify devices with known vulnerabilities by matching the collected information with vulnerability databases. This feature helps security professionals and researchers identify potential targets for further investigation or alert device owners about the risks.

4. **Exploit Integration:** Shodan integrates with exploit databases, such as ExploitDB, to provide information on known exploits for specific devices or services. This allows users to assess the potential risks associated with vulnerable devices.

5. **Geolocation:** Shodan can determine the approximate physical location of devices based on their IP addresses. This feature enables users to search for devices in specific geographical areas or analyze the distribution of devices globally.

6. **IoT Device Monitoring:** Shodan has a specialized focus on Internet of Things (IoT) devices. It helps identify vulnerable IoT devices that may be susceptible to attacks, raising awareness about security risks in the IoT landscape.

How does Shodan work?

Shodan works by crawling the internet constantly 24 hours a day, seven days a week. The crawling, however, does not sweep through IP address ranges like a network scanner such as Nmap or MassCAN would. The Shodan crawlers attempt to perform a full protocol-specific handshake to determine whether a port is open or closed. Since there are numerous measures to spoof ports, Shodan implements several measures to ensure that the port that it is reporting is indeed open.

For example, in the case of RDP, Shodan takes a screenshot of the discovered open RDP port, performs optical character recognition on the captured screenshot and performs various security checks to determine whether you can hack into RDP.

What is Remote Desktop Protocol, and what is it used for?

The Remote Desktop Protocol (RDP) is a protocol used by system administrators to remotely administer their Windows servers or workstations. This requires an RDP client that remotely connects to the RDP server, the Windows machine.

Discovering open RDP ports using Shodan

Before we can begin searching for open RDP ports, we need to familiarise ourselves with two significant features of Shodan, namely facets and filters.

Facets display a detailed view of the most frequent global information. It would help if you remembered that these usually change depending on the search applied. These will appear on the left side of the screen and will include:

• Total results. This displays the total number of hits from the search that has been executed. •

Top countries. This displays the countries in which the search returns hits.

• Top organizations. This displays the organizations that are affected by the hits from the search.

• Top products. This displays the products related to the hits from the conducted search.

• Top operating systems. This displays the operating systems affected by the search that is conducted.

On the other hand, filters help you drill down to a more granular view of the hosts you would like to inspect. The following are some of the filters that you can use:

• City – this is how you specify the name of the city.

• Country – this is a two-letter code, and it is how you specify the country. •

Has_screenshot – with this, you can specify the screen image.

• OS – this is how you specify the operating system.

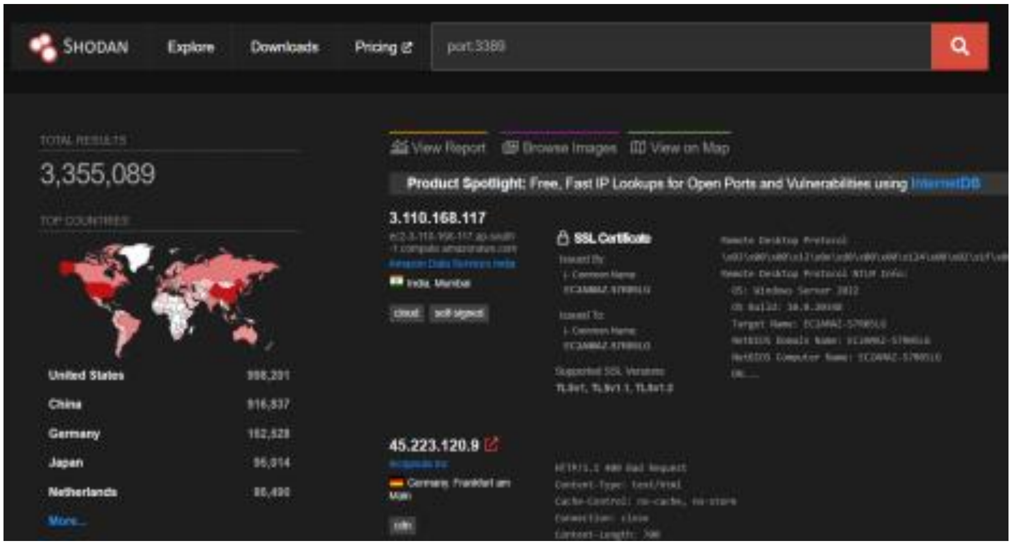
• Port – this is how you specify the port.

• Product – this is how you specify the product.

• State – you can specify the state in which you want to search for devices.

• Version – this is how you specify the version of the service you are interested in. You should note that the search results might vary greatly depending on the filter that has been used. To begin searching for open RDP ports, you can input the following into the search bar: port:3389.

The filter above returns all of the hits discovered by Shodan as having the default RDP port 3389 open. As we can see below, there are a total of 3,355,089 results.



TOTAL RESULTS
3,355,089

TOP COUNTRIES

United States	998,201
China	916,837
Germany	162,528
Japan	96,014
Netherlands	86,490

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

3.110.168.117
ec2-3-110-168-117.ap-south-1.compute.amazonaws.com
Amazon Data Services India
India, Mumbai
cloud self-signed

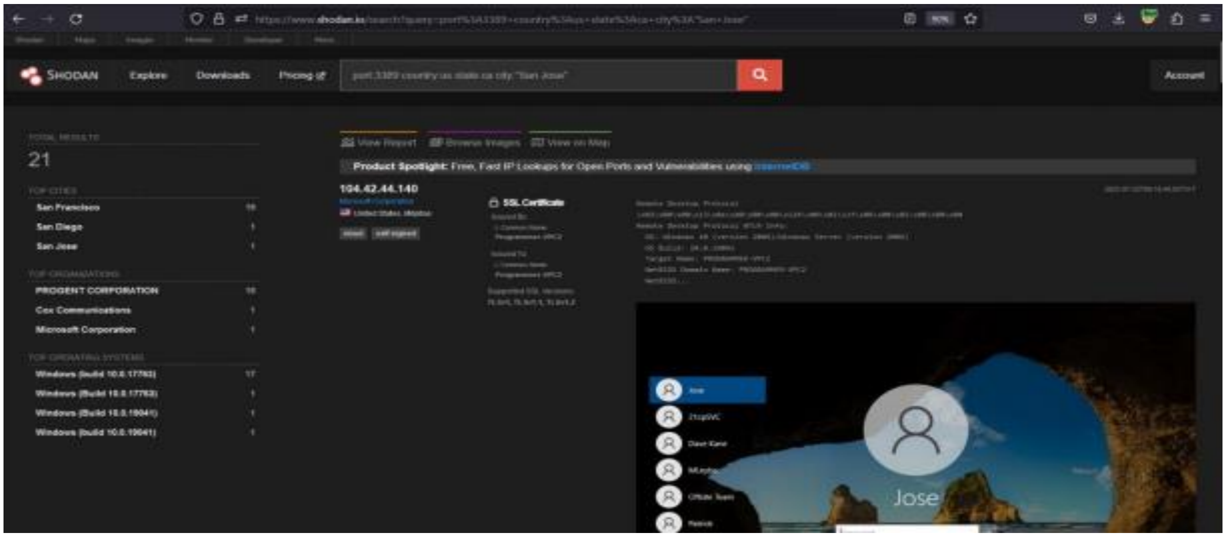
SSL Certificate
Issued By:
|- Common Name:
EC2AMAZ-5780510
Issued To:
|- Common Name:
EC2AMAZ-5780510
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
[illegible]
Remote Desktop Protocol NTLM Info:
  OS: Windows Server 2012
  OS Build: 10.0.20348
  Target Name: EC2AMAZ-5780510
  NetBIOS Domain Name: EC2AMAZ-5780510
  NetBIOS Computer Name: EC2AMAZ-5780510
  DN...
```

45.223.120.9
[illegible]
Germany, Frankfurt am Main
cdn

```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 700
```

We can drill down further by applying more filters. We can add the following: country:us state:ca city:"San Jose."



SHODAN Explore Downloads Pricing

port:3389 country:us state:ca city:"San Jose"

TOTAL RESULTS
21

TOP CITIES

San Francisco	19
San Diego	1
San Jose	1

TOP ORGANIZATIONS

PROGENT CORPORATION	19
Cox Communications	1
Microsoft Corporation	1

TOP OPERATING SYSTEMS

Windows (build 10.0.17763)	17
Windows (Build 10.0.17763)	1
Windows (Build 10.0.19041)	1
Windows (build 10.0.19041)	1

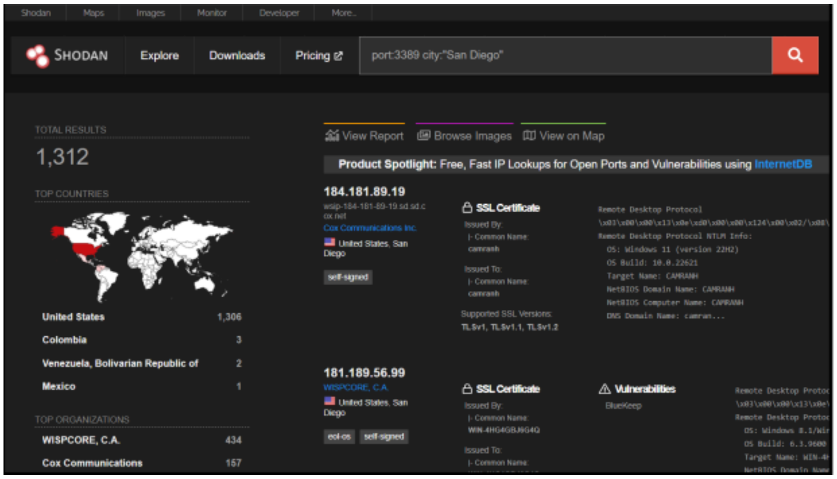
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

104.42.44.140

SSL Certificate

This specifies the country as the United States of America, state as California and city as San Jose. See the screenshot below. Note that the double quotes are used since the value we are specifying has a space character.

Doing this greatly reduces the total results to 21. You can drill down further by issuing an area code or postal code if you have one. However, sometimes you could search for a city and receive more than one location, say for instance, we search for RDP ports in the city of "San Diego." This is shown below:



SHODAN Explore Downloads Pricing

port:3389 city:"San Diego"

TOTAL RESULTS
1,312

TOP COUNTRIES

United States	1,306
Colombia	3
Venezuela, Bolivarian Republic of	2
Mexico	1

TOP ORGANIZATIONS

WISPCORE, C.A.	434
Cox Communications	157

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

184.181.89.19
wsip-184-181-89-19.sd.sd.cox.net
Cox Communications Inc.
United States, San Diego
self-signed

SSL Certificate
Issued By:
|- Common Name:
camranh
Issued To:
|- Common Name:
camranh
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x00\x124\x00\x02/\x08\
Remote Desktop Protocol NTLM Info:
  OS: Windows 11 (version 22H2)
  OS Build: 10.0.22621
  Target Name: CAMRANH
  NetBIOS Domain Name: CAMRANH
  NetBIOS Computer Name: CAMRANH
  DNS Domain Name: camran...
```

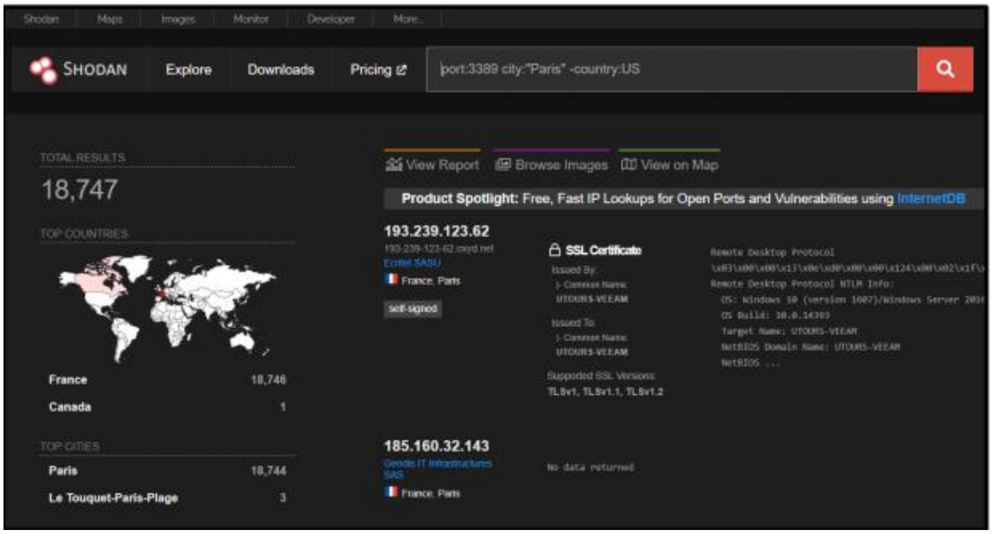
181.189.56.99
WISPCORE, C.A.
United States, San Diego
eol-os self-signed

SSL Certificate
Issued By:
|- Common Name:
WIN-4HG4GBJ6G4Q
Issued To:
|- Common Name:

Vulnerabilities
BlueKeep

```
Remote Desktop Protoc
\x03\x00\x00\x13\x0e\
Remote Desktop Protoc
  OS: Windows 8.1/Win
  OS Build: 6.3.9600
  Target Name: WIN-4H
  NetBIOS Domain Name
```

We quickly realize that there are two countries with the city Paris. To remove the USA from the facets, we use "-country:us". That is, we include a minus sign in front of the country filter as shown below:



port:3389 city:"Paris" -country:US

TOTAL RESULTS
18,747

TOP COUNTRIES

France	18,746
Canada	1

TOP CITIES

Paris	18,744
Le Touquet-Paris-Plage	3

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

193.239.123.62
193-239-123-62.rxyd.net
Ecritel SASU
France, Paris
self-signed

SSL Certificate
Issued By:
|- Common Name:
UTOURS-VEEAM
Issued To:
|- Common Name:
UTOURS-VEEAM
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

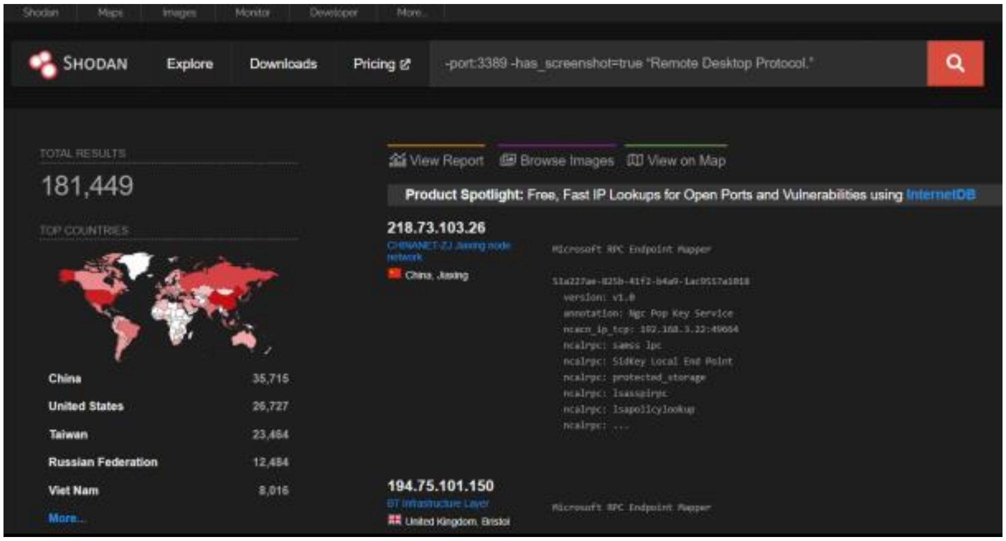
```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 201
  OS Build: 10.0.14393
  Target Name: UTOURS-VEEAM
  NetBIOS Domain Name: UTOURS-VEEAM
  NetBIOS ...
```

185.160.32.143
Geodis IT Infrastructures SAS
France, Paris

```
No data returned
```

We can use a trick to identify RDP servers that are running on elevated ports. To do this, we would need to use the following filter: -port:3389 -has_screenshot=true "Remote Desktop Protocol."

This simply tells Shodan to ignore everything on port 3389, which is the default RDP port, ignore any screenshots, but then look for the text string "Remote Desktop Protocol". This results in results similar to the following:



-port:3389 -has_screenshot=true "Remote Desktop Protocol."

TOTAL RESULTS
181,449

TOP COUNTRIES

China	35,715
United States	26,727
Taiwan	23,464
Russian Federation	12,484
Viet Nam	8,016

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

218.73.103.26
CHINANET-ZJ Jiaxing node network
China, Jiaxing

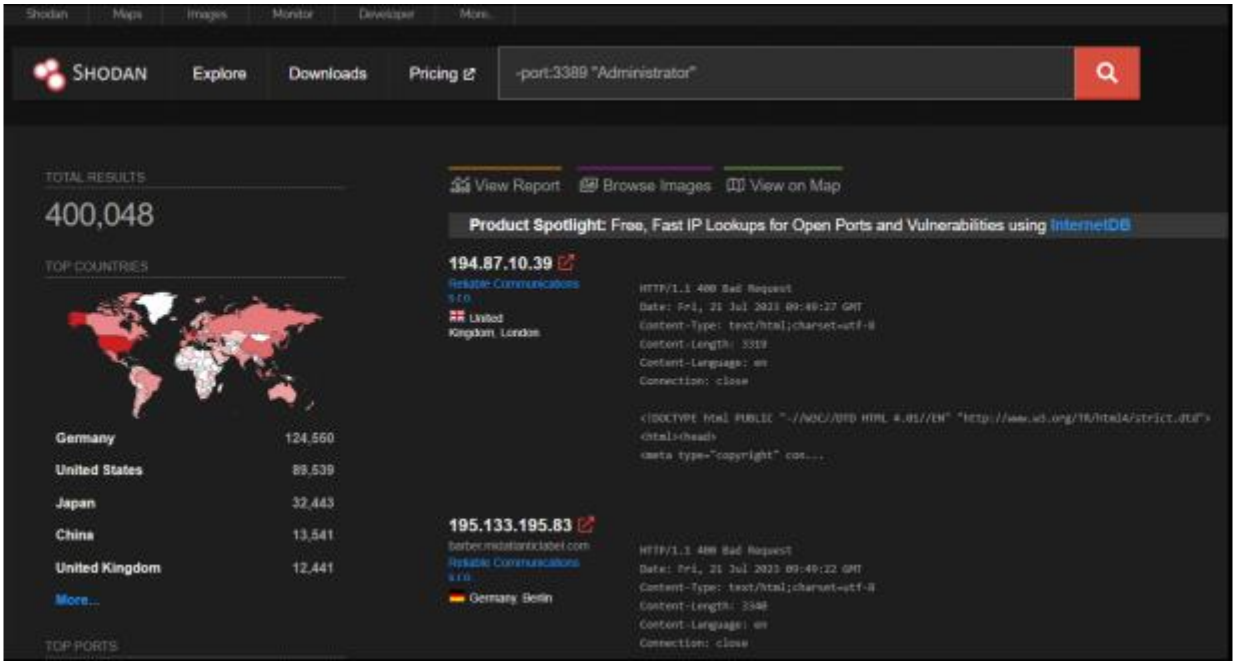
```
Microsoft RPC Endpoint Mapper

51a227ae-825b-41f2-b4a9-1ac9557a1018
  version: v1.0
  annotation: Ngc Pop Key Service
  ncacn_ip_tcp: 192.168.3.22:49664
  ncalrpc: samss lpc
  ncalrpc: SidKey Local End Point
  ncalrpc: protected_storage
  ncalrpc: lsasspirpc
  ncalrpc: lsapolicylookup
  ncalrpc: ...
```

194.75.101.150
BT Infrastructure Layer
United Kingdom, Bristol

```
Microsoft RPC Endpoint Mapper
```

You can also find the user accounts related to RDP by appending the username beside the port filter, as shown below.



-port:3389 "Administrator"

TOTAL RESULTS
400,048

TOP COUNTRIES

Germany	124,560
United States	89,539
Japan	32,443
China	13,541
United Kingdom	12,441

More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

194.87.10.39
Reliable Communications s.r.o.
United Kingdom, London

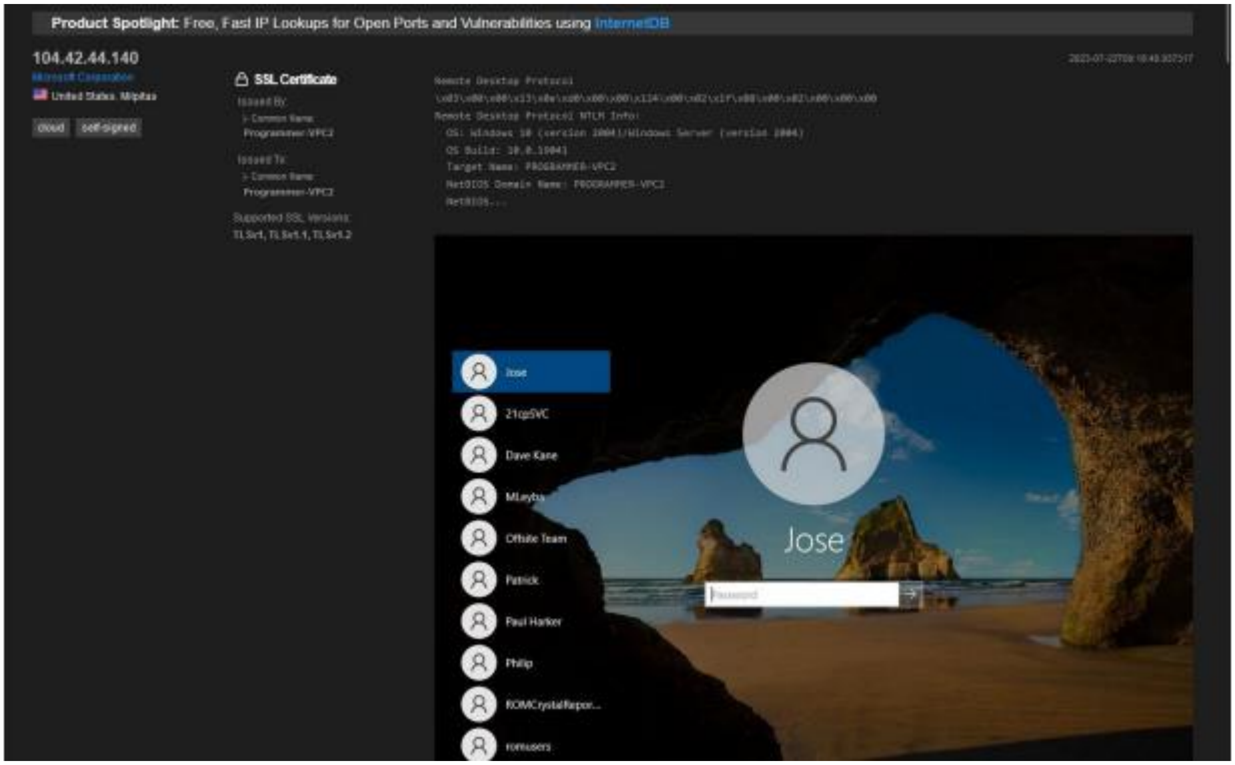
```
HTTP/1.1 400 Bad Request
Date: Fri, 21 Jul 2023 09:49:27 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3319
Content-Language: en
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" con...
```

195.133.195.83
barber.midatlanticlabel.com
Reliable Communications s.r.o.
Germany, Berlin

```
HTTP/1.1 400 Bad Request
Date: Fri, 21 Jul 2023 09:49:22 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3340
Content-Language: en
Connection: close
```

Doing this results in the following screenshots exposing administrator accounts within RDP.



Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

104.42.44.140
Microsoft Corporation
United States, Milpitas

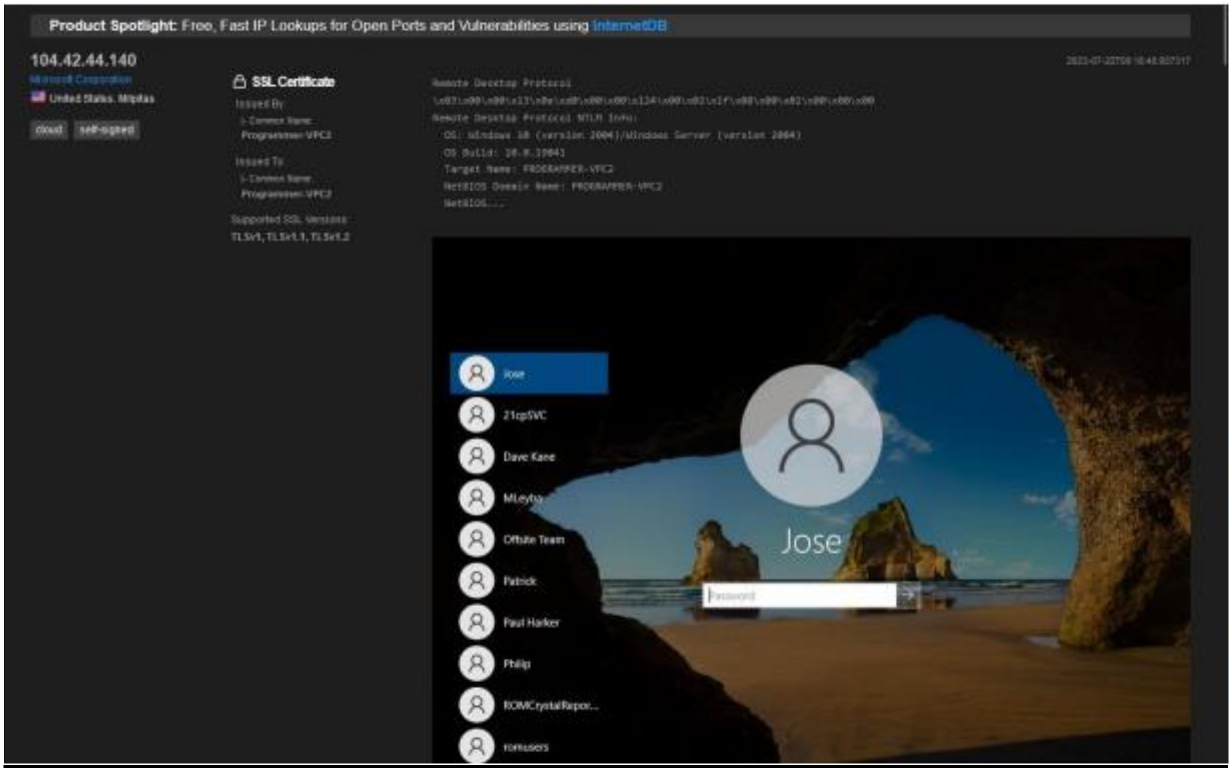
2023-07-22T09:10:49.307517

SSL Certificate
Issued By:
|- Common Name:
Programmer-VPC2
Issued To:
|- Common Name:
Programmer-VPC2
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 2004)/Windows Server (version 2004)
  OS Build: 10.0.19041
  Target Name: PROGRAMMER-VPC2
  NetBIOS Domain Name: PROGRAMMER-VPC2
  NetBIOS...
```

The screenshot above shows a Windows machine in United States, with the Administrator account prompting a login password.

Understanding Shodan Vulnerability Assessment



Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

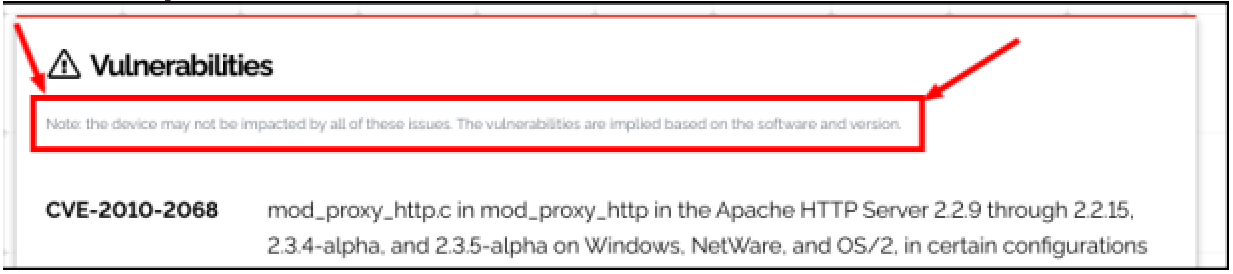
104.42.44.140
Microsoft Corporation
United States, Milpitas
cloud self-signed

2023-07-22T08:10:48.937317

SSL Certificate
Issued By:
|- Common Name:
Programmer-VPC2
Issued To:
|- Common Name:
Programmer-VPC2
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 2004)/Windows Server (version 2004)
  OS Build: 10.0.19041
  Target Name: PROGRAMMER-VPC2
  NetBIOS Domain Name: PROGRAMMER-VPC2
  NetBIOS...
```

There are 2 types of vulnerabilities that can be attached to the banners in Shodan: verified and unverified. Unverified vulnerabilities are vulnerabilities that are implied based on the metadata we've collected. For example, if a server is running an old version of Apache then we will associate known issues with that version and set the associated verified property in the banner to False. Shodan has increasingly also started to verify vulnerabilities when possible. If a verified vulnerability is discovered then we set the verified property to True. Unverified vulnerabilities can have significant false positives depending on the device/ software so they typically require additional verification to make sure the service is vulnerable. They should be seen as a starting point for further investigation. Note that Shodan Monitor only sends out notifications for verified vulnerabilities.



⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2068 mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations

Learning Outcomes: The student should have the ability to

LO1: Understand the concept of Google Dorks.

LO2: How they can be used to perform advanced searches on Google.

Course Outcomes: Upon completion of the course students will be able to understand the concept of Google Dorks and Shodan and will be able to use Google Dorking and Shodan Tools for security purposes.

Conclusion: Through this experiment we learned the concept of Google Dorks and Shodan and we used the Google Dorks and Shodan to find open ports, banner, and vulnerabilities using Shodan.

For Faculty Use:

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				