Basic Search Practice Tasks for Shodan Learning

Each task helps students explore different types of devices, ports, services, and filters.

Task 1: Web Servers

- Search Queries:
  - http
  - port:80
  - apache
  - nginx

Goal: Identify types of web servers exposed to the internet and note their IPs, ports, and banner info.

Task 2: SSH Services

- Search Queries:
  - port:22
  - product:OpenSSH
  - country:"IN" port:22

Goal: Find systems that allow remote shell access. Observe versions and geographic spread.

Task 3: FTP Servers

- Search Queries:
  - port:21
  - anonymous login
  - vsFTPd

Goal: Identify exposed FTP servers and whether anonymous access is allowed.

Task 4: Exposed Cameras

- Search Queries:
  - webcamXP
  - netcam
  - port:81

Goal: Find live cameras accessible online. Observe device info and country.

Task 5: Remote Desktop (RDP)

- Search Queries:

  - port:3389
  - Microsoft Terminal Service
  - country:"IN" port:3389

Goal: Detect systems with RDP enabled and learn why it’s risky if left unsecured.

Task 6: Database Servers

- Search Queries:

  - port:27017 (MongoDB)
  - port:3306 (MySQL)
  - product:MongoDB

Goal: Find exposed databases. Understand risk of misconfigured data storage.

Task 7: SCADA/ICS Devices

- Search Queries:

  - SCADA
  - Siemens
  - port:102

Goal: Spot industrial control systems that should not be public. Discuss critical infrastructure risks.

Task 8: Internet Service Providers (ISPs)

- Search Queries:

  - org:"BSNL"
  - org:"Reliance Jio"
  - org:"Airtel"

Goal: Track devices exposed by ISP. Observe which services are common on their networks.

Task 9: City or Region-Specific Search

- Search Queries:

  - city:"Raipur"
  - country:"IN" port:80
  - region:"Chhattisgarh"

Goal: Understand local exposure and raise awareness of nearby threats.

Task 10: Search by Device Type

- Search Queries:

- device:webcam
- device:router
- device:printer

Goal: Discover common types of exposed IoT devices. Analyze manufacturer, model, and vulnerabilities.

What Students Should Submit for Each Task

Task :1

Field	Web Servers
Query Used	Http
Total Results	486,616,331
Top Countries	China , United States ,Singapore
IP Example	**47.108.43.109**
Banner Info	Undertow/1 , JBoss-EAP/7, 200
Risk Identified	A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

Task:2

Field	SSH Services
Query Used	Port:22
Total Results	20,599,289
Top Countries	United States ,China,Germany
IP Example	**54.39.180.53**
Banner Info	SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
Risk Identified	In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding.

Task:3

Field	FTP Servers
Query Used	Port:21
Total Results	7,455,903
Top Countries	United States ,China,Germany
IP Example	192.185.108.5
Banner Info	220-Local time is now 01:45. Server port: 21.
Risk Identified	A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

Task:4

Field	Exposed Cameras
Query Used	WebcamXP
Total Results	151
Top Countries	United States ,China,Russian Federation
IP Example	184.57.102.6
Banner Info	**webcamXP** 5, HTTP/1.1 200
Risk Identified	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue

Task:5

Field	Remote Desktop(RDP)
Query Used	Port:3389
Total Results	3,559,202
Top Countries	United States ,China,Singapore
IP Example	194.88.196.77
Banner Info	OS: Windows 11 OS Build: 10.0.26100 Target Name: KTZHPRODAPP01

Risk Identified	

Task:6

Field	Remote Desktop(RDP)
Query Used	Port:27017 (MongoDB)
Total Results	97,468
Top Countries	China,United States,Germany
IP Example	**144.76.65.51**
Banner Info	Authentication partially enabled
Risk Identified	

Task:7

Field	SCADA/ICS Devices
Query Used	Port:102
Total Results	871,275
Top Countries	United States,China,Israel
IP Example	**34.110.199.222**
Banner Info	No data returned
Risk Identified	

Task:8

Field	Internet Service Provider
Query Used	org:"Airtel"
Total Results	247,728
Top Countries	India,Kenya,Nigeria
IP Example	**105.112.252.143**
Banner Info	SNMP: Versions:3
Risk Identified	

Task:9

Field	City or Region-Specific Search
Query Used	city:"Raipur"
Total Results	8,296
Top Countries	
IP Example	**103.242.186.62**
Banner Info	HTTP/1.1 200 OK Server: nginx
Risk Identified	

Task:10

Field	Search by Device Type
Query Used	device:router
Total Results	706,126
Top Countries	China,United States,Pakistan
IP Example	**14.171.33.218**
Banner Info	220 MikroTik FTP server (MikroTik 6.47.4) ready
Risk Identified	