

Create a free Shodan account and login.

In the search bar look for os: "Windows XP"



Flag: Norway

shodan - 2

100

All challenges in the OSINT Shodan series c

The telnet service is notorious for its unencrypted communications. According to Shodan, which city in the United States places second in utilizing this plaintext service?


Unlock Hint for 1 points

Unlock Hint for 30 points

Flag

Submit

Search for "US" and port "23"


 SHODAN

country:"US" port:"23"

TOTAL RESULTS

502,543

TOP COUNTRIES

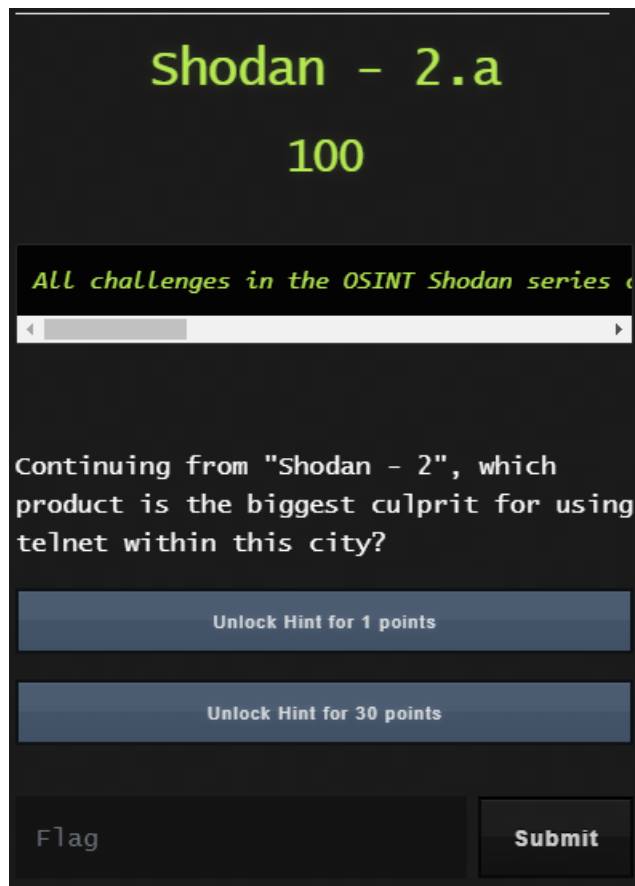


United States	502,543
---------------	---------

TOP CITIES

Phoenix	5,431
Las Vegas	5,249
Los Angeles	4,482
Prior Lake	4,096
Columbia	2,319

Flag: Las Vegas



Continuing from shodan-2 look further down on the left side to products

TOP PRODUCTS	
Cisco router telnetd	14,195
OpenSSH	5,861
Cisco catalyst swit...	1,912
Microsoft ftpd	176
CCProxy telnet co...	119

Flag: Cisco router telnetd

shodan - 3

100

All challenges in the OSINT Shodan series

Which country has the most public-facing PlayStation 4 consoles?

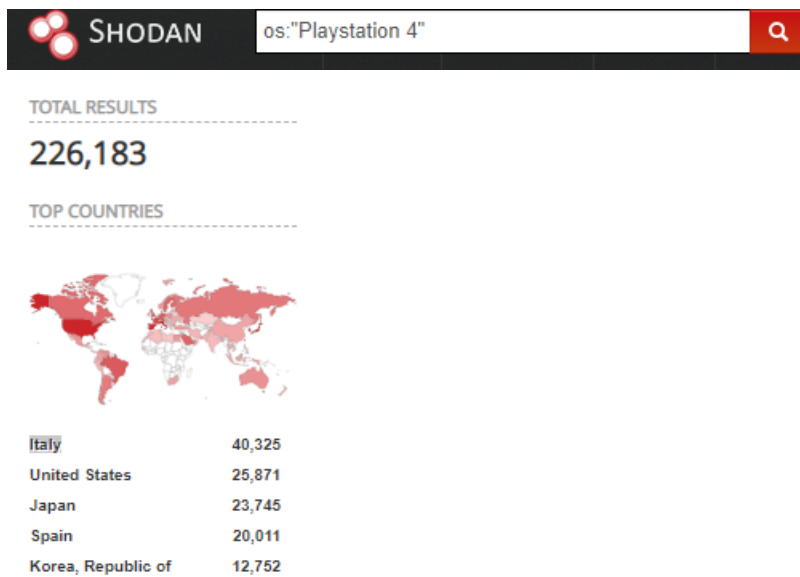
Unlock Hint for 1 points

Unlock Hint for 30 points

Flag

Submit

Search for the os of playstation 4



Flag: Italy

Shodan - 3.a

100

All challenges in the OSINT Shodan series c

Based on the information from "Shodan-3"'s results, can you determine which PlayStation feature is responsible?

Unlock Hint for 1 points

Unlock Hint for 50 points

Flag

Submit

Port 9295

TOP SERVICES

9295	222,574
52889	2



playstation 4 port 9295

PS4: Remote Play and Second Screen for PS Vita

System Features : PlayStation Apps & Features

Learn how to connect and control the PlayStation Vita for PlayStation 4 for Remote Play and Second Screen play.

Flag: Remote Play

Shodan – 4

100

All challenges in the OSINT Shodan series c

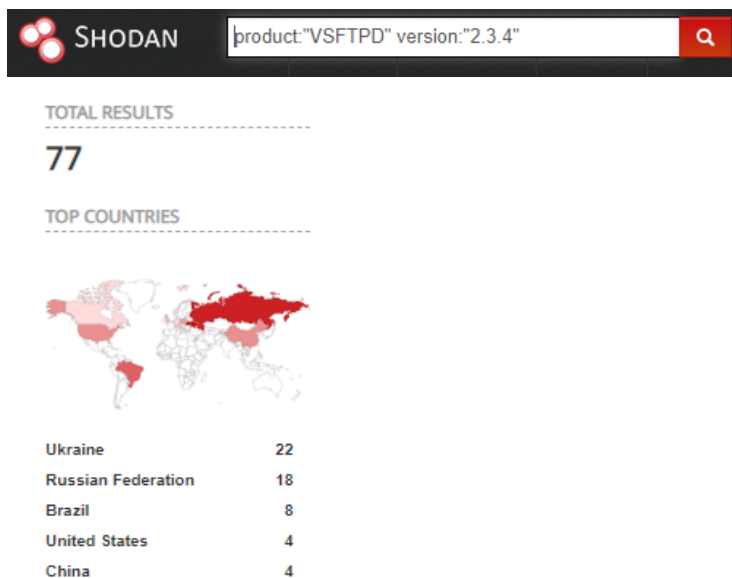
So far we've looked at general information in relation to Shodan queries, but now we'll start to look at it from a more security minded focus. A certain version of vsftpd is known to have a malicious backdoor built into it which can allow remote code execution. If we assume all instance of vsftpd of this version are affected, which country is most vulnerable to this backdoor?

Unlock Hint for 1 points

Unlock Hint for 30 points

Flag Submit

2.3.4 has a backdoor and is loaded into Metasploitable 2 VM



Flag: Ukraine

Shodan - 4.a

100

All challenges in the OSINT Shodan series c

The vsftpd service is not the only FTP service which has exploitable vulnerabilities. A particular version of ProFTPD had command execution exploits published in early-mid 2015. If we assume all instance of ProFTPD of this version are susceptible to this exploit, which country is most vulnerable?

Unlock Hint for 1 points

Unlock Hint for 30 points

<https://www.bleepingcomputer.com/news/security/proftpd-vulnerability-lets-users-copy-files-without-permission/>

1.3.6 and earlier are exploitable

