

Forum:[Hack Forums](#)

Thread: [Extremely subjective assessment of the Criminal IP](#)

Deepfaker345 - September 12, 2022, 10:05 pm

OSINT is one of the must-to-check in bug bounty, infringement response, security blue&red team. Exposure of important information due to unnecessary port browsing and insufficient auth process can be confirmed as a representative. In addition, as cloud services are used a lot recently, storage database leakage and exposure of instance information are increasing.

I got shodan Premium for \$5 lifetime and have ever used Shodan only. However, by chance, I came across a tool called Criminal IP at Reddit, and I share what I felt while using the Criminal IP Tool over the past few weeks.

First of all, from the point of view of using Exploit search the most, Shodan is quite limited when searching for vulnerabilities and it is quite difficult if you're noob. In addition, it seems that update cycle of CVE result information is very slow or late. In the case of Criminal IP, the latest vulnerability information updates are well made. And various tags are applied to facilitate further search. It's very convenient to be able to see the safety of incoming and outgoing traffic.

The exploit search in Criminal IP seems that data is imported from the Exploit DB. But the speed at which results are retrieved is very fast compared to Exploit DB. And the part where statistics can be checked in Exploit DB is difficult to check out except for the total number of results at the bottom of search result. However, in the case of Criminal IP, detailed statistics can be checked according to vulnerability information.

Looking at the exploit code, it was easy to see how information relevant to metasploit is included at glance. And it's possible to check the latest trends of exploit, such as how many metasploit codes are being created out of a total 40,000 exploit information. Even noobs can see that recent exploit codes are strongly associated with metasploit. And more, it's possible to confirm that which environments has the most vulnerabilities. It's confirmed that most in the php environment.

Although it is now a beta, but if API officially provided and linked in Criminal IP later, it seems that automated assessment can be conducted integrated with Python or others like Searchsploit. It's very promising tool as far as I know.

<https://criminalip.io>

Edit : This is real my subjective opinion. You can check yourself by googling Criminal IP. And sorry for my poor english.