International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

OPEN SOURCE INTELLIGENCE AND TECHNIQUES FOR PASSIVE RECONNAISSANCE IN LINUX ENVIRONMENT

Prof. Vinit A. Sinha
Assistant Professor
PGDCA (PRMITR, Badnera- Amravati MS(INDIA))
vinit.sinha84@gmail.com

ABSTRACT: -

Open Source Intelligence (OSINT) or simply Information Gathering, the idea behind passive reconnaissance is to gather information about a target using only publicly available resources. As valuable as open source intelligence can be, information overload is a real concern. Most of the tools and techniques used to conduct open source intelligence initiatives are designed to help security professionals (or threat actors) focus their efforts on specific areas of interest.
In this article methods for reconnaissance specially in kali linux are discussed.

Keyword: - OSINT, Kali, Linux, Security

I. INTRODUCTION: -

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analysing it to produce actionable intelligence.

Open Source Intelligence (OSINT) takes three forms; Passive, Semi-passive and Active.

A. Passive Information Gathering: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.
B. Semi-passive Information Gathering: The goal for semi-passive information gathering is to profile the target with methods that would appear like normal Internet traffic and behavior. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, we aren't searching for "unpublished" servers or directories. We aren't running network level portscans or crawlers and we are only looking at metadata in published documents and files; not actively seeking hidden content. The key here is not to draw attention to our activities. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.
C. Active Information Gathering: Active information gathering should be detected by the target and suspicious or malicious behavior. During this stage, we are actively mapping network infrastructure (think full port scans nmap –p1-65535), actively enumerating and/or vulnerability scanning the open services, we are actively searching for unpublished directories, files, and servers. Most of this activity falls into your typically "reconnaissance" or "scanning" activities for your standard pentest.

OSINT TECHNIQUES FOR PASSIVE RECONNAISSANCE

1. **Maltego**

Figure 1 . Maltego

Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

Maltego uses the idea of transforms to automate the process of querying different data sources. This information is then displayed on a node based graph suited for performing link analysis.
Currently there are three versions of the Maltego client namely Maltego CE, Maltego Classic and Maltego XL. This page will focus on Maltego Community Edition (CE).

The focus of Maltego is analysing real-world relationships between information that is publically accessible on the Internet. This includes foot printing Internet infrastructure as well as gathering information about the people and organisation who own it.

2. **Shodan**

Figure 2- Shodan

Google is the search engine for all but shodan is the search engine for hackers. Instead of presenting the result like other search engines it will show the result that will make more sense to a security professional. As a certified information security professional one of the important entity is digital asset and network. Shodan provides you a lot of information about the assets that have been connected to the network. The devices can vary from computers, laptops, webcams, traffic signals, and various IOT devices. This can help security analysts to identify the target and test it for various vulnerabilities, default settings or passwords, available ports, banners, and services etc.

3. **Google Dorks**

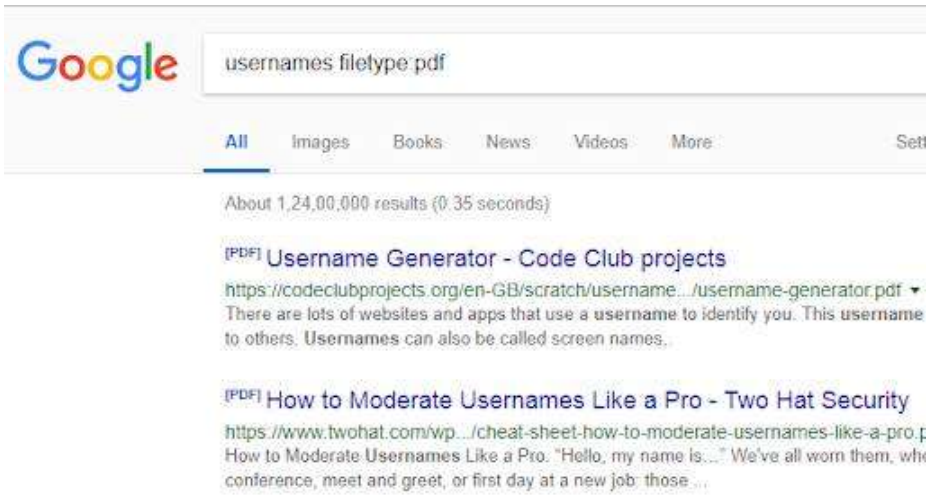

Figure 3 – Google dorks

Google is one of the most commonly used search engine when it comes to finding stuff on the internet. For a single search, the results can be of various hundred pages sorted in order of relevance. The results vary from ads, websites, social media posts, images etc. Google Dorks can help a user to target the search or index the results in a better and more efficient way. Let us say that the user wants to search for the word usernames but only requires the results with PDF files and not websites.

4. **The Harvester**

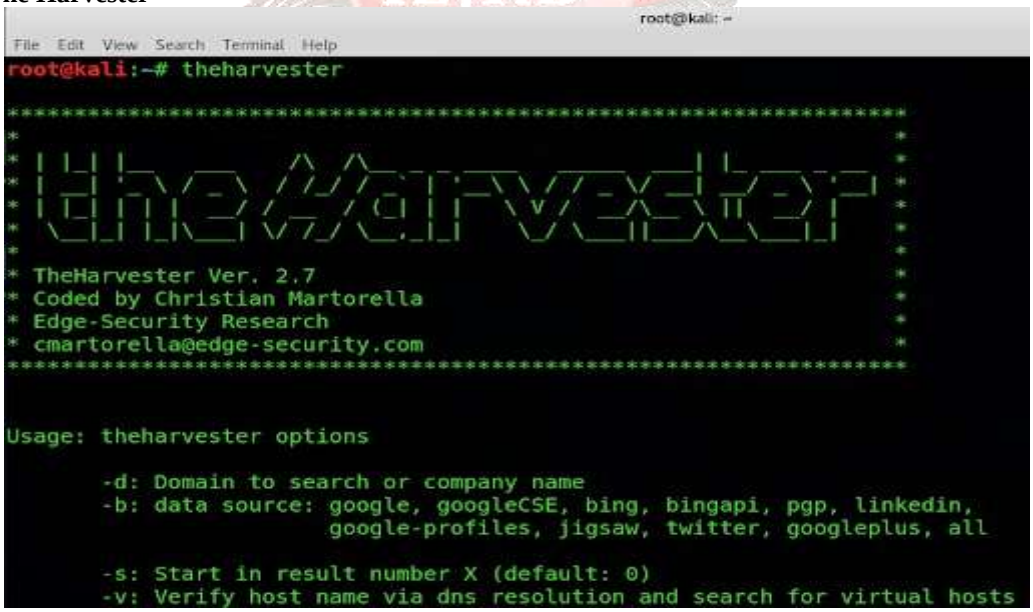

Figure 4 – The Harvester

The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.

This is a complete rewrite of the tool with new features like:

- Time delays between request
- All sources search
- Virtual host verifier
- Active enumeration (DNS enumeration, Reverse lookups, TLD expansion)
- Integration with SHODAN computer database, to get the open ports and banners
- Save to XML and HTML
- Basic graph with stats
- New sources

5. **Metagoofil**

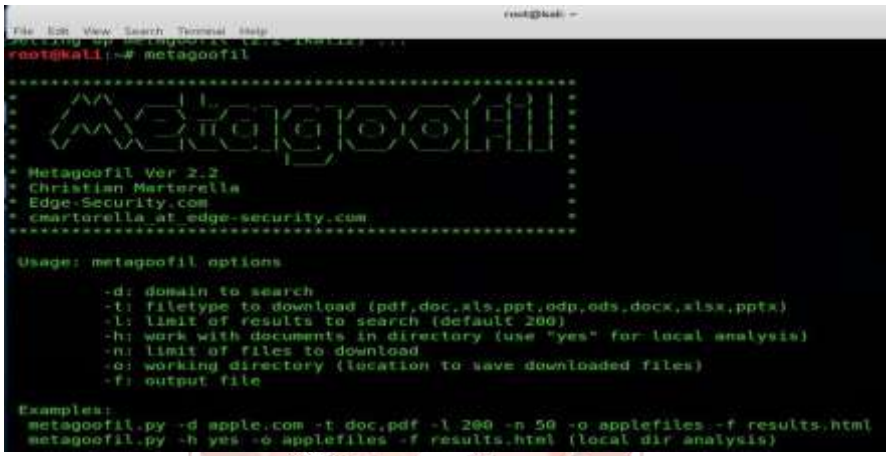

Figure 5 - Metagoofil

Metagoofil is written by Christian Mattarella and is a command line tool that is used to gather metadata of public documents. The tool is pre-bundled in Kali Linux and has a lot of features searching for the document type on the target, local download, extraction of metadata and reporting the results. For example: Users can scan for a particular kind of documents on a particular domain. Metagoofil –d nmap.org –t pdf.

6. **Recon-ng**

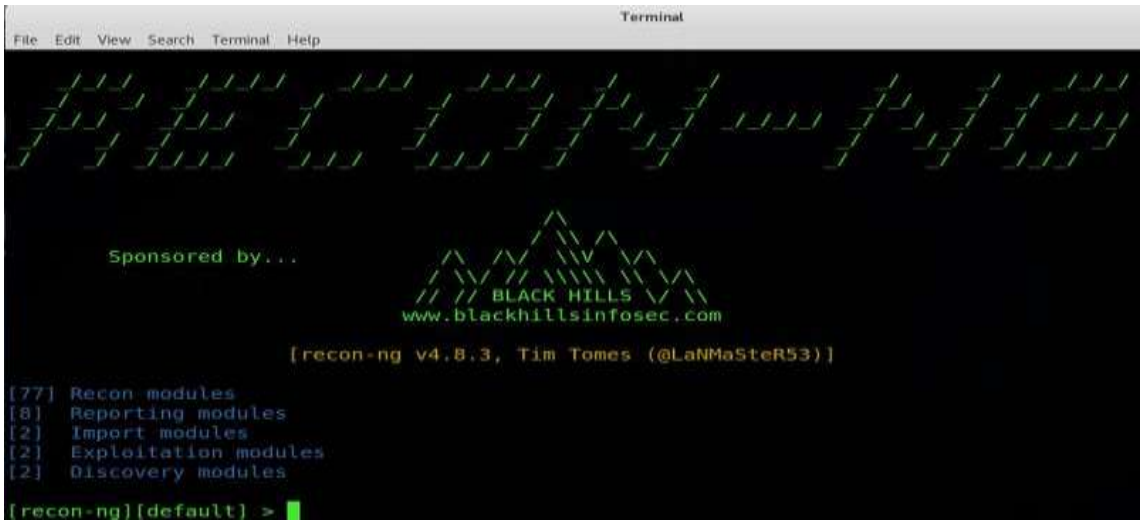

Figure 6 - Recon-ng

Recon-ng is a great tool for target information collection. This is also pre-bundled in Kali. The power of this tool lies in the modular approach. For those who have used Metasploit will know the power of modular tools. Different modules can be used on the target to extract information as per need. Just add the domains in the workspace and use the modules.

7. **Check Usernames**

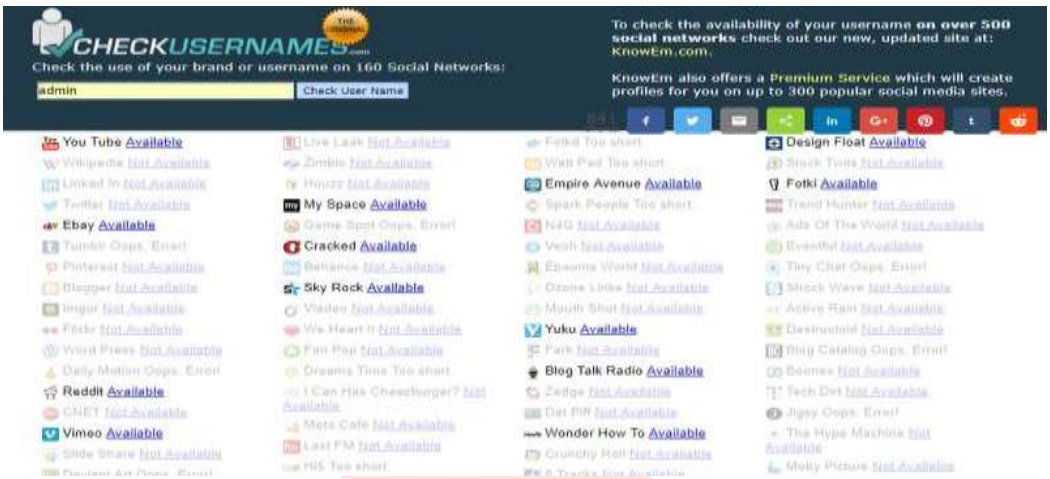

Figure 7 – Check Usernames

Social networking websites hold a lot of information but it will be really boring and time taking task if you need to check whether a particular username is present on any social media website. To get such information there is a website www.checkusernames.com. It will search for the presence of a particular username on more than 150 websites. The users can check for the presence of a target on a particular website so as to make the attack more targeted.

TinEye

Figure 8 - TinEye

Tineye is used to perform an image related search on the web. It has various products like tineye alert system, color search API, mobile engine etc. Any one can search if an image has been available online and where that image has appeared. Tineye uses neural networks, machine learning, and pattern recognition to get the results. It uses image matching, watermark identification, signature matching and various other parameters to match the image rather than keyword matching. The website offers API extensions and browser extensions as well.

Searchcode

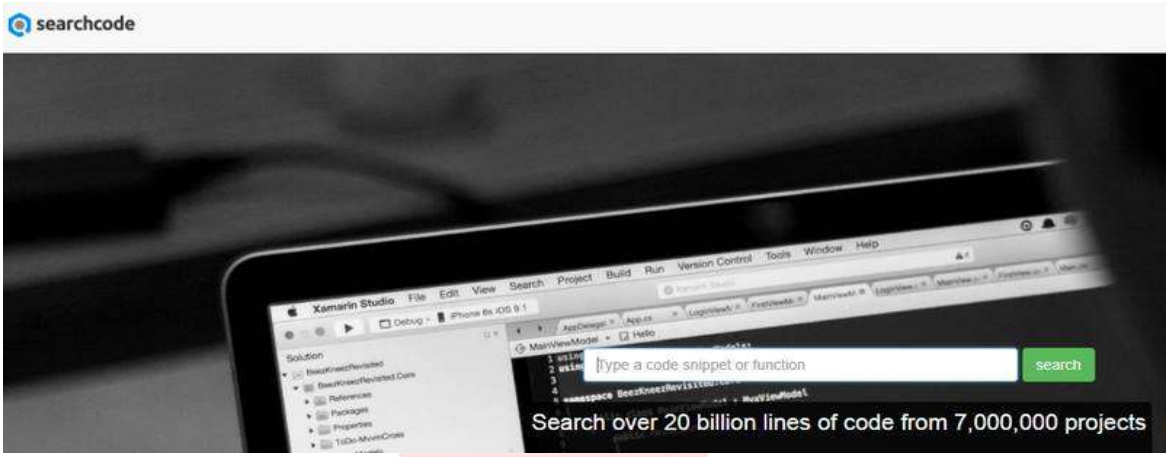

Figure 9 - Searchcode

Searching for text is easy as compared to searching for a code snippet. Try searching for a code sample on google and you will be prompted with no results or irrelevant results. Search code offers you a feature to search for a line of code which could have been present in various code sharing websites like Github etc. Users can search for functions or methods, variables, operations, security flaws and anything that can constitute a code segment. Users can search for strings as simple as "a++" too complex methods. The search results can be further filtered basis a particular repository or language.

8. **Recorded Future**

Figure – 10 Recorded Future

Recorded Future is an AI-based solution to trend prediction and big data analysis. It uses various AI algorithms and both structured and unstructured data to predict the future. The users can get past trends and future trends basis OSINT data.

CONCLUSION

This study brief outs how OSINT can help. Another is the power of OSINT that can help us in our day to day tasks. All discussed technologies are used to searching vulnerability and not for black hat hacking. So, A security professional can use the information for data protection, security testing, incident handling, threat detection etc. A threat actor, on the other hand, can gain information to perform phishing attacks, targeted information gathering, DDOS attacks and much more.

II. FUTURE SCOPE

Advancements in analytical tools, machine learning, deep learning, and artificial intelligence have made OSINT tools capable of discerning astute insights from large sets of unstructured data. The attitude of public sectors and government agencies to embrace the technology to combat and respond to real-time threats and thwart attacks can bode well for the market in the coming years. Lack of qualified personnel to handle the accumulation of data can act as a growth deterrent for the open source intelligence market.

The various techniques for getting information under OSIN can be improve by researching penetration methods as white hacking or ethical hacking.

III. REFERENCES

1. Robert Beggs - Mastering Kali Linux for Advanced Penetration Testing - Packt Publishing pg 45
2. James Broad Andrew Bindner - Hacking with Kali Practical Penetration Testing Techniques – First Edition
3. Jay LaCroix - Mastering Ubuntu Server
4. Tajinder Kalsi - Practical Linux Security Cookbook - Packt Publishing
5. Christopher Negus - Linux Bible – 9th Edition
6. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools
7. https://www.paterva.com/buy/maltego-clients/maltego-ce.php
8. https://tools.kali.org/information-gathering/theharvester
9. https://www.globenewswire.com/news-release/2018/09/10/1568680/0/en/Open-Source-Intelligence-OSINT-Market-Size-USD-7-000-Mn-by-2023-at-16-18-CAGR-OSINT-Industry-to-Expand-by-Fortifying-Defenses-of-Nations.html

E-ISSN NO:2349-0721