Methodology of OSINT tools and their usage in Cyber Threat Intelligence.

Georgii Moiseev

start date: April 20th, 2021
end date: May 15th, 2021.

1 Plagiarism statement

I confirm that all statements, words, ideas and paragraphs that I am going to write in my project/article were the state of my own mind. The work on that project is my own work and I didn't copy it, unless I used the books, articles, lecture notes, documents and other academic materials, then I put quotation marks and give a credit to the author and make a reference on his/her intellectual property. I didn't cheat by taking the work from the author of its work and declaring that it is mine.
I affirm that I don't violate copyrights and avoid various kinds of plagiarism:

- Global plagiarism: using someone's work and declaring that this work is mine own.
- Paraphrasing plagiarism: rephrasing someone's else ideas without reference on source.
- Verbatim plagiarism: copying text without citation on that source.
- Mosaic plagiarism: combining the mix of idea and compiling in one own work.
- Self-plagiarism: reusing your own work from previous work that were done.
- Incorrect citation.
- Fake citation.

2 Abstract

Abstract

It is known that there exist a great deal of cyber observables, which are shared and spread the information about known threats that happened lately. They are known and there is a chance they may occur again, but it doesn't give the real idea to predict. We can only read the articles or reports about accidents and after, decide what potential threat may be. Besides that, we should know ***attack surface*** and ***attack vector***[1]. So in this project, I provide research articles and practical usage of Open-source intelligence for finding vulnerabilities. I have a report of some common methods and tools used for causing potential cyber threats. Also, I want to show the methodology of tools. Moreover, all collected, analyzed and summarized information provided with knowledge of Cyber Threat Intelligence could help, potentially, for trying to reach the goal of developing and training an AI model. This model would create the opportunity to foresee the future cyber threats scenarios.

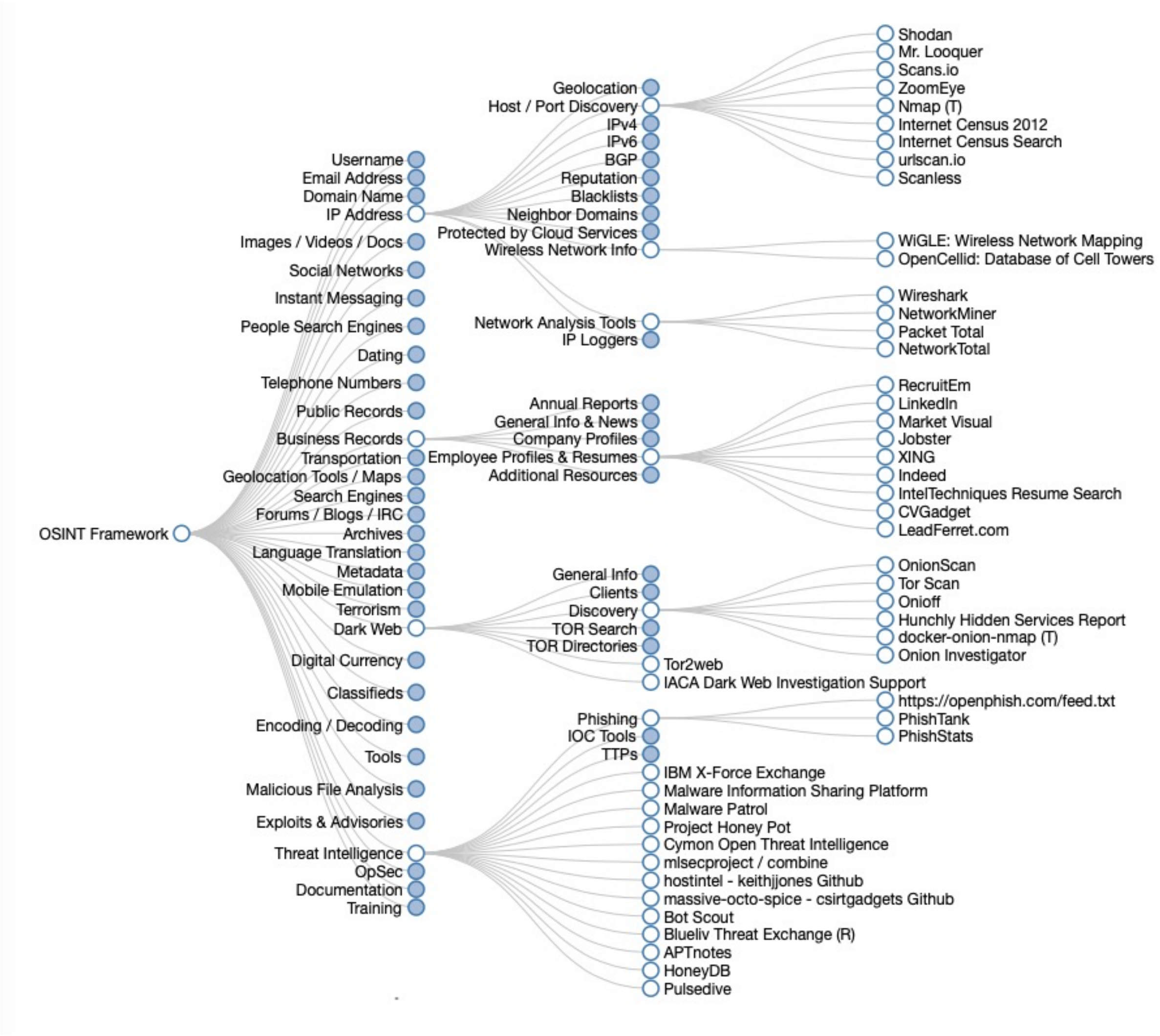
Contents

3 Main body Page:

Introduction:

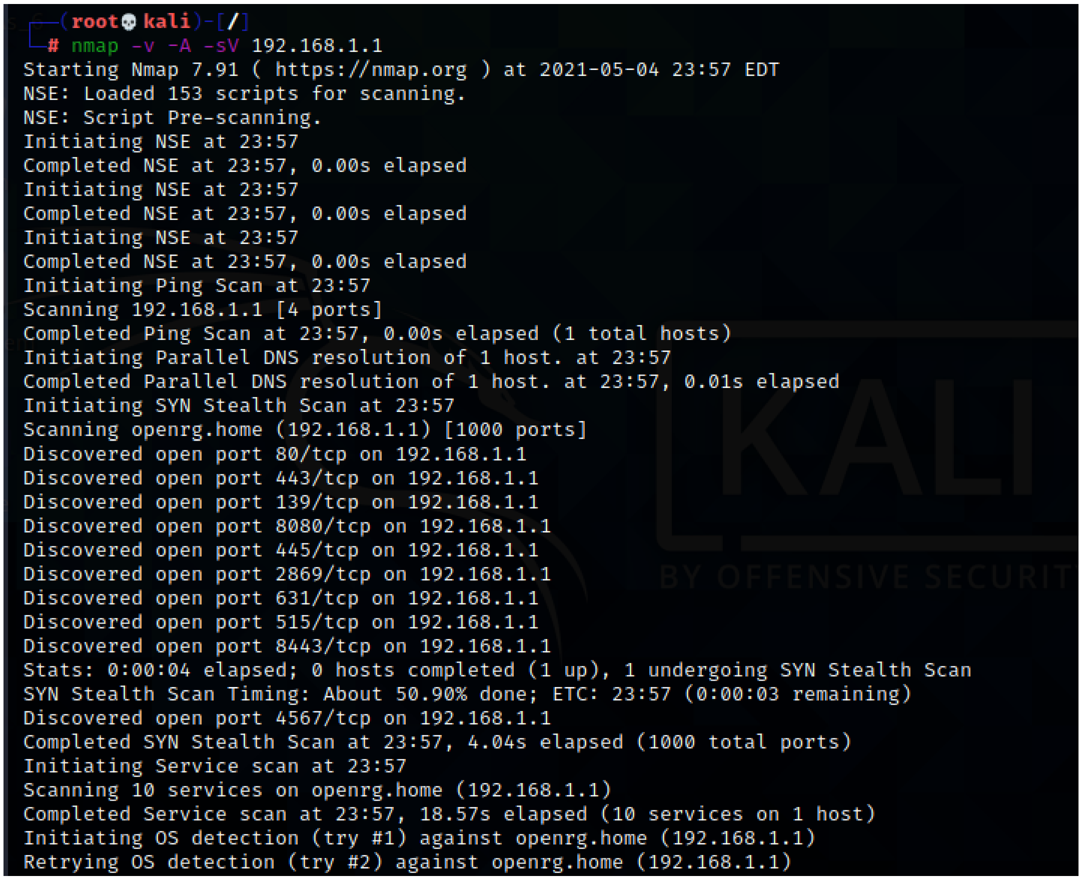
My goal is writing about the most commonly used OSINT tools for cyber intelligence threats and making my own report about the frequency of utilization. I want to demonstrate the abilities of those tools and their potential usage, when those tools should be used, for what purposes and what commands I used. Besides that, I am going to write about the methodology of other tools, but touch following topic slightly. Moreover, usage of OSINT is a very important topic because it covers *attack surface*. The first tool that I am going to use is *nmap*. Besides that in project, I can provide a detailed report and how the tool can be used and in which cases. Other tools most likely will be used are *Metagoofil*, *nikto* and explain why social media might be dangerous in terms of privacy and safety aspects.

OSINT methodology[2]:



3.1 Nmap

Nmap is open-source for scanning a computer network and used specifically for discovering hosts and services on a computer network.[2]
This useful tool can help to define availability of specific host, services of those hosts, Operating system and even firewall details.[3]
Nmap often used for scanning of vulnerabilities[4] and asset management. For example, if take a look at the details about my IP address and related hosts, by typing 192.168.1.1 for my private IP address through router, we are getting the following result:



```
┌──(root💀kali)-[/]
└─# nmap -v -A -sV 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-04 23:57 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating NSE at 23:57
Completed NSE at 23:57, 0.00s elapsed
Initiating Ping Scan at 23:57
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 23:57, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:57
Completed Parallel DNS resolution of 1 host. at 23:57, 0.01s elapsed
Initiating SYN Stealth Scan at 23:57
Scanning openrg.home (192.168.1.1) [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 139/tcp on 192.168.1.1
Discovered open port 8080/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.1
Discovered open port 2869/tcp on 192.168.1.1
Discovered open port 631/tcp on 192.168.1.1
Discovered open port 515/tcp on 192.168.1.1
Discovered open port 8443/tcp on 192.168.1.1
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.90% done; ETC: 23:57 (0:00:03 remaining)
Discovered open port 4567/tcp on 192.168.1.1
Completed SYN Stealth Scan at 23:57, 4.04s elapsed (1000 total ports)
Initiating Service scan at 23:57
Scanning 10 services on openrg.home (192.168.1.1)
Completed Service scan at 23:57, 18.57s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against openrg.home (192.168.1.1)
Retrying OS detection (try #2) against openrg.home (192.168.1.1)
```

My input was **nmap -v -A -sV 192.168.1.1** in which -v used for verbosity, -A which allows you to define OS, version, trace route and -sV is checking for open ports. So, while we are using *nmap* we can define what physical devices with their OS are connected to scanned networks and even routers and switches. Also, what ports are opened. It gives an opportunity to predict future attacks because open ports increase *attack surface*. Especially, with *attack vectors* the *actor* can find vulnerabilities, then write the malicious code or an *exploit* and run it. It will give the ability for the attacker to take control of the whole system.[5] Besides that, he can use *malware or ransomware*. For instance, with the *nmap*, the attacker might find out the hosts, open ports, servers, their function and the version of OS. So, the attacker can already know what *malware* he needs to use. It is a pretty practical tool for monitoring the traffic, which is going in and out. I would say *nmap* is a great sniffing tool, which can be used on "dark" side, ethical hacking or usual analysis and monitoring.

3.2 Metagoofil

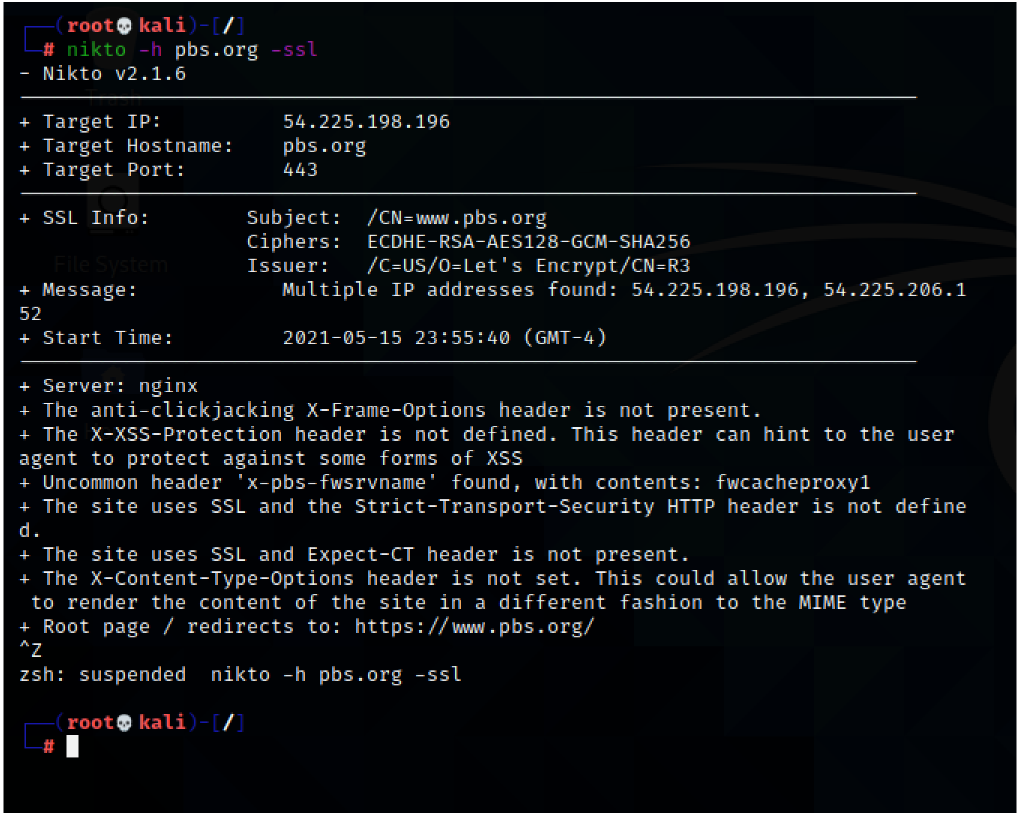
Another great tool for gathering and collecting public information is Metagoofil that collects *metadata* from the file. With that data, the actor can find enough data about the creator of the file. So, we can retrieve author's name, email, software which has been used, probably MAC address and the printer's information and information about servers, excel and pdf files, Word documents, and Powerpoint documents from the specific resource or domains[2]. Known this information, the *actor* can use exploits to crack the software on the system where the file was created, collect necessary information which is useful for the attack or used *social engineering* by using known emails[6]. So Metagoofil is a great tool for extracting the data from the files. It can be useful for analysis of collected data because we can know what information the *actor* can gain before launching his attack. It can help to prevent a potential attack.

3.3 Socail media

Even the usual social media(without careful control) may cause vulnerability, which is a great help to OSINT. It is difficult to believe but LinkedIn, Indeed, XING, RecruitEm and similar job search websites are part of Cyber Intelligence threat because through them, hackers can gather the public information. All business records about employees are stored on social media platforms and can be the pathway to being hacked. Moreover, social media sites can be used for phishing attacks. The resume is always on open-source access. In the resume, we can find information such as email address, phone number, the previous work and victim's network would it be previous job or university. So it is not hard to use some tool for the collection of those resumes(where have enough data and emails). For example, sophisticated hackers can write a code which can be used as a bot with a searching engine. So all information can be complied with and used for a malicious purpose as sending malware, ransomware through emails or just using social engineering.

3.4 Nikto

Nikto is a well-known web server scanner. Also, it is an incredible tool for penetration testing of vulnerabilities. With nikto the analyst can predict *attack vectors*. Due to *nikto* we can find vulnerabilities that can be used as exploits on scanned websites. Moreover, this tool is not stealthy, so it means that the tool mostly should be used for scanning and detecting of vulnerabilities by the people who are authorized to make those scans. The *adversary* less likely will be using the tool for a reconnaissance. It is really great to for checking ssl, xss vulnerability and etc.[7]



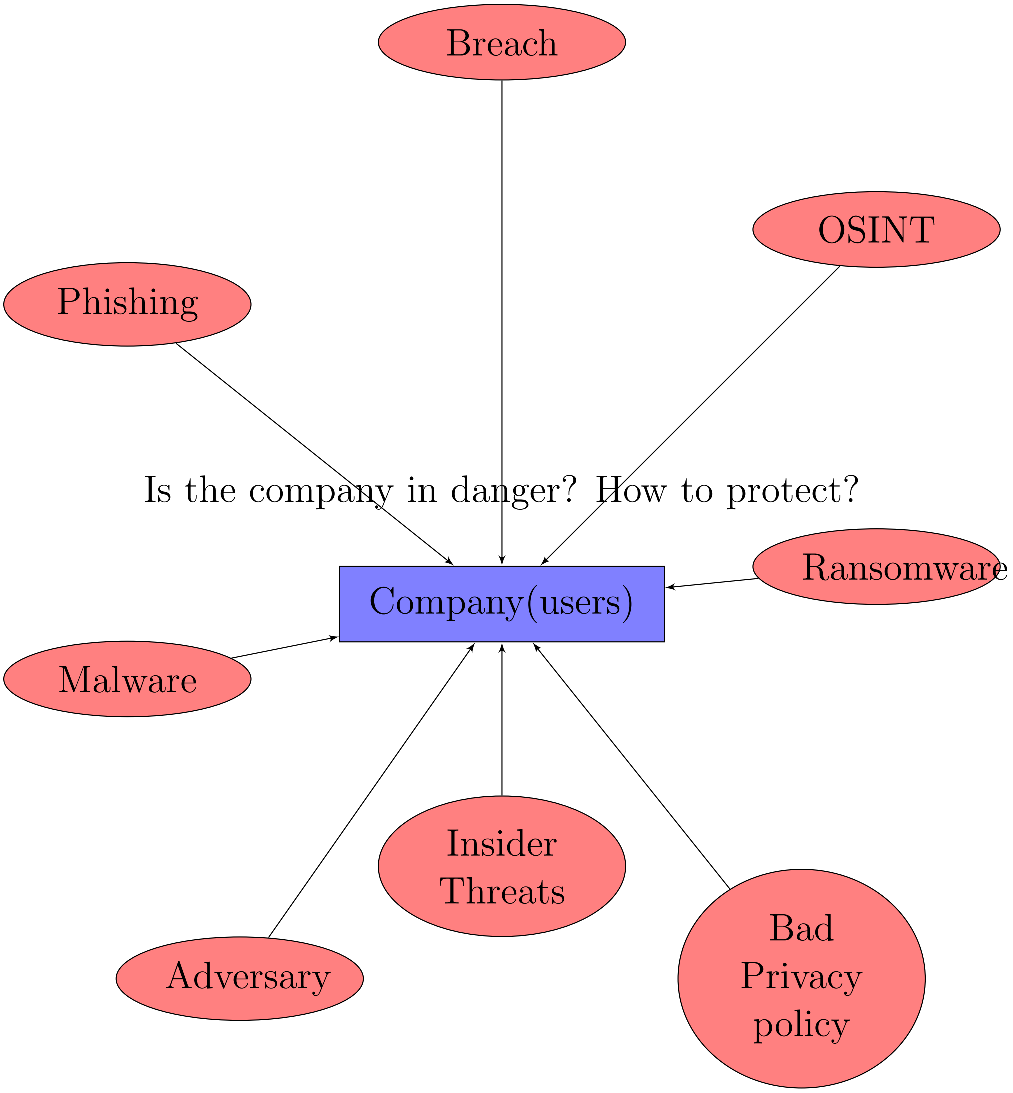
```
┌──(root💀kali)-[/]
└─# nikto -h pbs.org -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          54.225.198.196
+ Target Hostname:    pbs.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.pbs.org
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Message:            Multiple IP addresses found: 54.225.198.196, 54.225.206.1
52
+ Start Time:         2021-05-15 23:55:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ Uncommon header 'x-pbs-fwsrvname' found, with contents: fwcacheproxy1
+ The site uses SSL and the Strict-Transport-Security HTTP header is not define
d.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
 to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.pbs.org/
^Z
zsh: suspended  nikto -h pbs.org -ssl

┌──(root💀kali)-[/]
└─# █
```

As can be seen, I used simple command **nikto -h pbs.org -ssl** for launching vulnerability scanner. In the following command, I scanned the website *pbs.org* and detected which port is opened and the number of code. Also checked for ciphers. The main point was to check the website for ssl protocol vulnerabilities because ssl is one of the most commonly used protocols for providing secure internet communication to users. Also, it is convenient that nikto command provides additional information about SSL such as what exact cipher was used, what multiple IP address the server has. So it is useful tool to discover potentially dangerous files and various problems on servers.

3.5 Diagram

[8]


Breach
OSINT
Phishing
Is the company in danger? How to protect?
Ransomware
Company(users)
Malware
Insider Threats
Adversary
Bad Privacy policy

3.6 Conclusion

So according to KSA paradigm, I gained knowledge related to analysis of OSINT tools and their potential usage. As for skills, I have learnt how to scan the computer network and find vulnerabilities, and a research on the topics that are necessary for cyber security intelligence. I have learnt some new statements and commands for *nmap and nikto.* And finally, for abilities now, I can mitigate the cyber threats, at least on basic level. I can organize the minimal risk management, basic penetration testing and prevent future attacks on port scanning on the company network. Also, I have learnt how to secure a private life through social media. Therefore, our goal as a part of cyber threat intelligence, to find the way to mitigate the potential danger. For that cases, we must analyze *attack surface* and make *countermeasure* in advance. It reduces the chances for *actors* to accomplish a *breach attack.*

References

[1] Raimo Streefkerk. 6 types of plagiarism and how to avoid them (with examples), January 17, 2018.

[2] Unknown. What is osint? (and how is it used?). July 17, 2019.

[3] Jeff Petters. How to use nmap: Commands and tutorial guide, May 20, 2020.

[4] Juliana DeGroot. 50 threat intelligence tools for valuable threat insights, December 31, 2020.

[5] Unknown. Cyber threat basics, types of threats, intelligence best practices, MAY 12, 2017.

[6] Staff Contributor. What is threat intelligence? definition and types, September 14, 2020.

[7] Sherif Koussa. 13 tools for checking the security risk of open-source dependencies, 2021.

[8] Joel Witts. The top 5 biggest cyber security threats that small businesses face and how to stop them, Mar 22, 2021.