



Automated Reconnaissance Tool

Submitted in the partial fulfillment for the award of

the degree of

BACHELOR OF ENGINEERING

IN

CSE IBM (Information Security)

Submitted by:

PPRANAY RAO PINNINTY

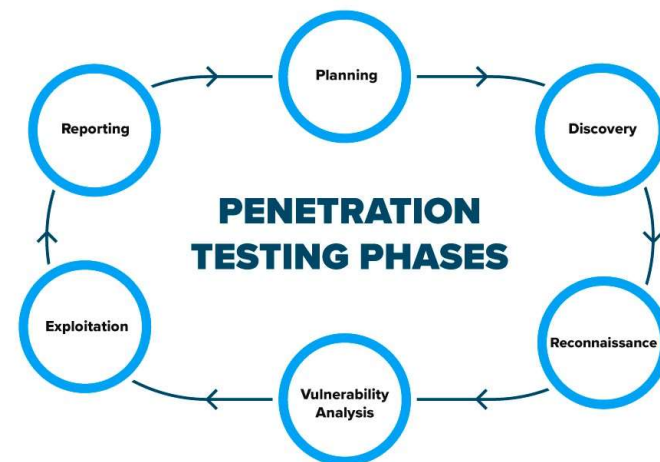
Department of AIT-CSE

DISCOVER . LEARN . EMPOWER

- Introduction to Project
- Problem Formulation
- Objectives of the work
- Methodology used
- Results and Outputs
- Conclusion
- References

Introduction to Project

Reconnaissance refers to the preparatory phase where a penetration tester seeks to gather as much information as possible about a target of evaluation prior to launching a penetration test. It involves three phases: footprinting, scanning, and enumeration of the network. In this research, we will be dealing with automating footprinting of an organization. Footprinting is the blueprint of the security profile of an organization, undertaken in a methodological manner. It discovers all information available about the target that is available through public domain sources. It is a time-consuming process to browse through web pages and collect information; hence in this paper, we investigate the problem of tedious web search and propose an efficient way to extract, organize and store data from search engines using a new command line tool search simplified.



Information gathering techniques can be roughly classified into the following:

- **Active:** This includes intrusive reconnaissance that sends (specifically crafted) packets to the targeted system, for example, port-scanning. Advanced networking enumeration techniques avoid direct communication with the targeted host.
- **Passive:** This includes reconnaissance that either does not communicate directly to the targeted system or that uses commonly available public information, not normally identifiable from standard log analysis.

This reconnaissance tool finds the subdomains of a domain, after finding the subdomains by vulnerability scanning we find the ports which are vulnerable. Having a unsecured subdomain can lead to a serious risk to website, there were some security incidents where the hacker used subdomain tricks to hack into the website.

Hardware Specifications:

- 4GB ram and 10GB laptop or computer
- Virtual Machine Support

Software Specifications

- Windows 10
- Kali Linux
- Python installed in linux



Problem Formulation

- In [computer security](#), a vulnerability is a weakness which can be exploited by a [threat actor](#), such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the [attack surface](#).
- [Vulnerability management](#) is the cyclical practice that varies in theory but contains common processes which include: discover all assets, prioritize assets, assess or perform a complete vulnerability scan, report on results, remediate vulnerabilities, verify remediation - repeat. This practice generally refers to software vulnerabilities in computing systems.





Objectives

Network Domain:

- A **network domain** is an administrative grouping of multiple private [computer networks](#) or hosts within the same [infrastructure](#). Domains can be identified using a [domain name](#); domains which need to be accessible from the public [Internet](#) can be assigned a globally unique name within the [Domain Name System](#) (DNS).

SubDomain:

- Subdomains are often used by internet service providers supplying web services. They allocate one (or more) subdomains to their clients who do not have their own domain name. This allows independent administration by the clients over their subdomain.

Port Filtering:

- Port-filtering definitions. Filters. Allowing or blocking network packets into or out of a device or the network based on their application (port number).





Methodology used

- In the Automated Reconnaissance Tool First we have to know how to script the tool with using language python.
- First we have to check the hardware and software requirements which are required.
- Then we have to check the ram requirements in the software and install windows 10 latest version in the laptop.
- Then software should have virtual machine support where we will install virtualbox or vmware
- The next step will be checking the memory requirements and installing kali linux in our virtual machine .
- The Automated Reconnaissance Tool will be running by language python in kali linux terminal.
- First we have to gather the libraries when we are ready build the tool.

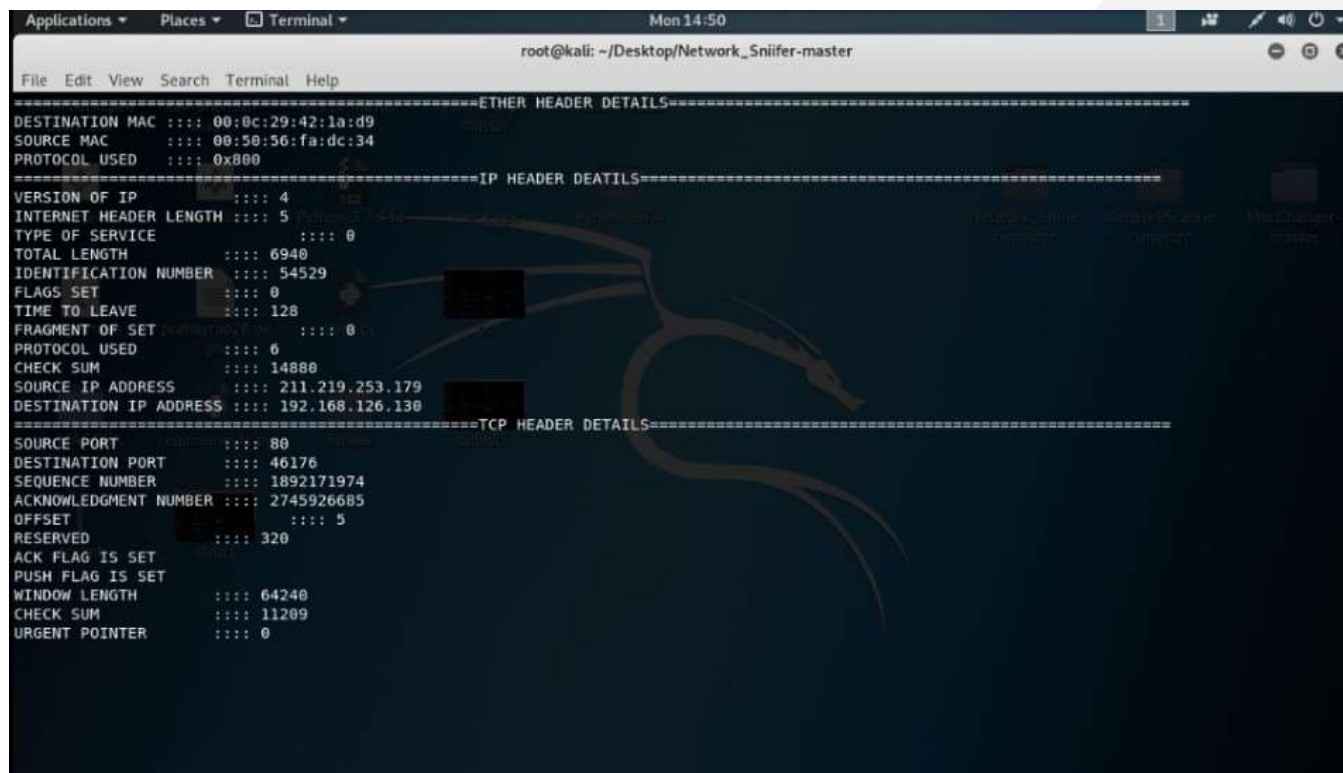


- We have to figure out that features that we are adding to the tool should be included in the tool.
- In the process of building team members who are good in networking and cyber security help to develop code and find the right use cases to be included in the script.
- In this phase team members who are building the tool write code in python which will be tested in various stages and software development life cycle is followed here.
- When the script is written perfectly it is checked for any bug fixes or errors and testing will be done .
- After the tool is ready to launch in kali linux we will ensure that this python scripted which will give excellent results.

Results and Outputs

Network Packet Analyzer:

- The act of capturing data packet across the computer network is called **packet sniffing**.
- It is similar to as wire tapping to a telephone network.
- It is mostly used by *crackers and hackers* to collect information.
- Also used by the ISP(Internet Service Providers).



```

Applications ▾ Places ▾ Terminal ▾ Mon 14:50
root@kali: ~/Desktop/Network_Sniifer-master

File Edit View Search Terminal Help

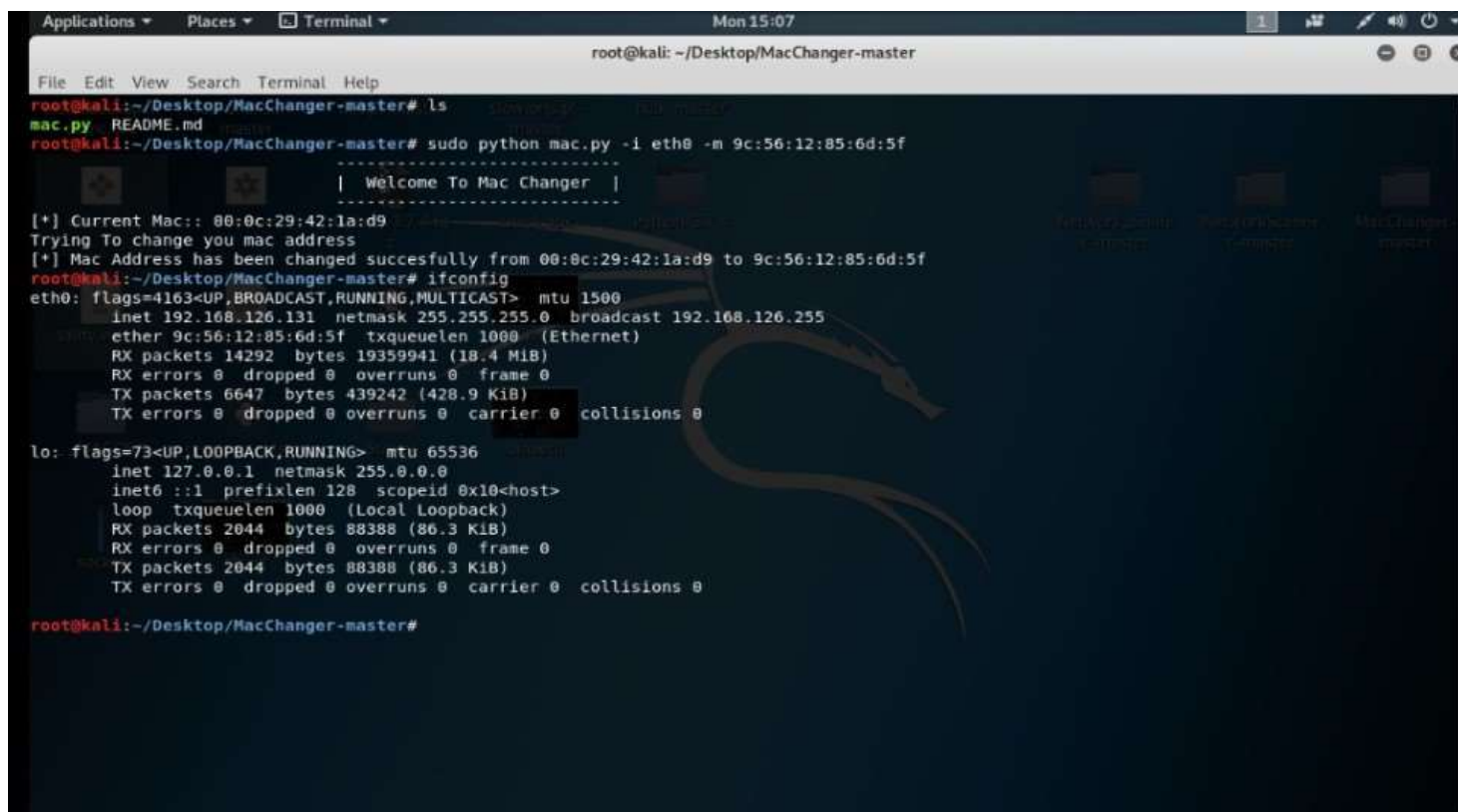
=====ETHER HEADER DETAILS=====
DESTINATION MAC ::: 00:0c:29:42:1a:d9
SOURCE MAC      ::: 00:50:56:fa:dc:34
PROTOCOL USED   ::: 0x800

=====IP HEADER DEATILS=====
VERSION OF IP   ::: 4
INTERNET HEADER LENGTH ::: 5
TYPE OF SERVICE ::: 0
TOTAL LENGTH    ::: 6940
IDENTIFICATION NUMBER ::: 54529
FLAGS SET       ::: 0
TIME TO LEAVE   ::: 128
FRAGMENT OF SET ::: 0
PROTOCOL USED   ::: 6
CHECK SUM       ::: 14880
SOURCE IP ADDRESS ::: 211.219.253.179
DESTINATION IP ADDRESS ::: 192.168.126.130

=====TCP HEADER DETAILS=====
SOURCE PORT      ::: 80
DESTINATION PORT ::: 46176
SEQUENCE NUMBER  ::: 1892171974
ACKNOWLEDGMENT NUMBER ::: 2745926685
OFFSET           ::: 5
RESERVED         ::: 320
ACK FLAG IS SET
PUSH FLAG IS SET
WINDOW LENGTH    ::: 64240
CHECK SUM        ::: 11209
URGENT POINTER    ::: 0
  
```

Mac changer

- This is the python scripted tool which changes the Mac address of our own system.
- In this tool we will give the Mac address which we want. To change



```
Applications ▾ Places ▾ Terminal ▾ Mon 15:07
root@kali: ~/Desktop/MacChanger-master
File Edit View Search Terminal Help
root@kali:~/Desktop/MacChanger-master# ls
mac.py  README.md
root@kali:~/Desktop/MacChanger-master# sudo python mac.py -i eth0 -m 9c:56:12:85:6d:5f
-----
| Welcome To Mac Changer |
-----
[+] Current Mac:: 00:0c:29:42:1a:d9
Trying To change you mac address
[+] Mac Address has been changed succesfully from 00:0c:29:42:1a:d9 to 9c:56:12:85:6d:5f
root@kali:~/Desktop/MacChanger-master# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.126.131 netmask 255.255.255.0 broadcast 192.168.126.255
    ether 9c:56:12:85:6d:5f txqueuelen 1000 (Ethernet)
    RX packets 14292 bytes 19359941 (18.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6647 bytes 439242 (428.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2044 bytes 88388 (86.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2044 bytes 88388 (86.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/Desktop/MacChanger-master#
```

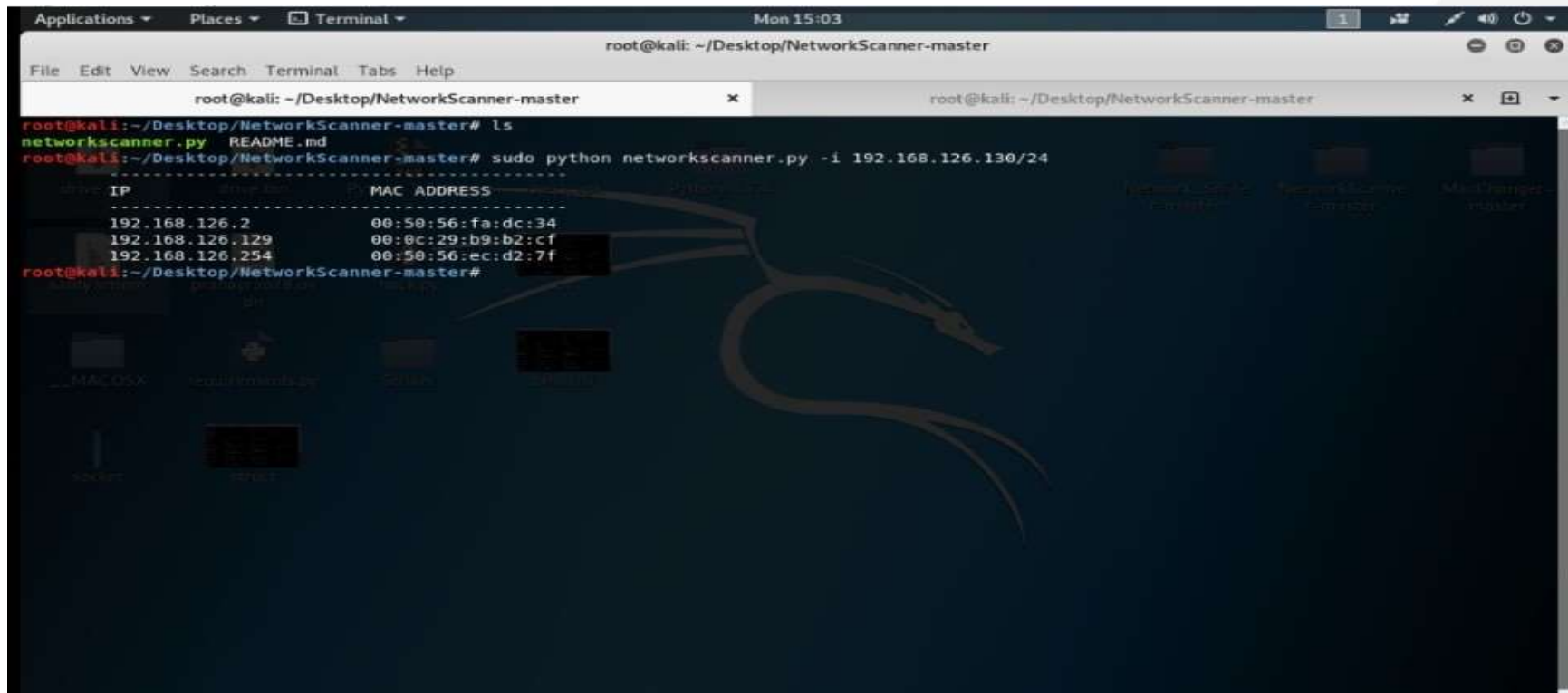
```
Applications ▾ Places ▾ Terminal ▾ Mon 15:05
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.126.130 netmask 255.255.255.0 broadcast 192.168.126.255
    inet6 fe80::20c:29ff:fe42:1ad9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:42:1a:d9 txqueuelen 1000 (Ethernet)
    RX packets 11505 bytes 15396153 (14.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5843 bytes 389490 (380.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2044 bytes 88388 (86.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2044 bytes 88388 (86.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

Network scanner

- Network scanner is the python scripted tool which will search for the host that are available from the specified range of ip address. We will give the ip address in which we want to perform scan .



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
root@kali: ~/Desktop/NetworkScanner-master
root@kali:~/Desktop/NetworkScanner-master# ls
networkscanner.py  README.md
root@kali:~/Desktop/NetworkScanner-master# sudo python networkscanner.py -i 192.168.126.130/24
```

IP	MAC ADDRESS
192.168.126.2	00:50:56:fa:dc:34
192.168.126.129	00:0c:29:b9:b2:cf
192.168.126.254	00:50:56:ec:d2:7f

The terminal output shows a list of discovered hosts with their IP addresses and MAC addresses. The background of the terminal window features a Kali Linux dragon logo.

Conclusion

- This capturing data packet across the computer network and gives the details like version of IP, source port, destination port, check sum, source port, destination port,....etc.
- We can change the Mac address of our own system.
- This search for the host that are available from the specified range of ip address.
- This will give the ip address of hosts that are alive and their mac addresses



References

1. Kevin J. Connolly (2003). Law of Internet Security and Privacy. Aspen Publishers. p. 131. ISBN 978-0-7355-4273-0.
2. ^ "Network Segment Definition". www.linfo.org. Retrieved January 14, 2016

