Lecture 4: Information Gathering

BKACAD’s Security Training

Table of Content

Foot-printing Concept

Passive Information Gathering

Active Information Gathering

Table of Content

Foot-printing Concept

Passive Information Gathering

Active Information Gathering

Foot-printing Concept

Concept

1st step in the evaluation of the security posture.

Through foot-printing, one can gather maximum information about a computer system or a network and about any devices connected to that network

Table of Content

Foot-printing Concept

Passive Information Gathering

Active Information Gathering

Passive Information Gathering

Concept

A.K.A Open-source Intelligence/OSINT is the process of collecting openly avaiable information about a target, without any direct interaction with that target.

Passive Information Gathering

Two types

- In the strictest interpretation, NEVER communicate with target directly. Rely on 3rd party for information but wouldn't access any of the target's systems or servers.
    - pros: High level of secrecy
    - cons: Limit results
- In a looser interpretation, might interact with the target, but only as a normal Internet user would.

Passive Information Gathering

Website Recon

If the client has a website, we can gather basic information by simply browsing the site. Small organizations may only have a single website, while large organizations might have many, including some that are not maintained.

This section will be reminded in “Web Security Lecture”.

https://www.megacorpone.com/

Passive Information Gathering

whois Enumeration

Whois is a TCP service, tool, and a type of database that can provide information about a domain name, such as the name server.

https://whois.domaintools.com/

```
kali@kali:~$ whois www.bkacad.com
```

Passive Information Gathering

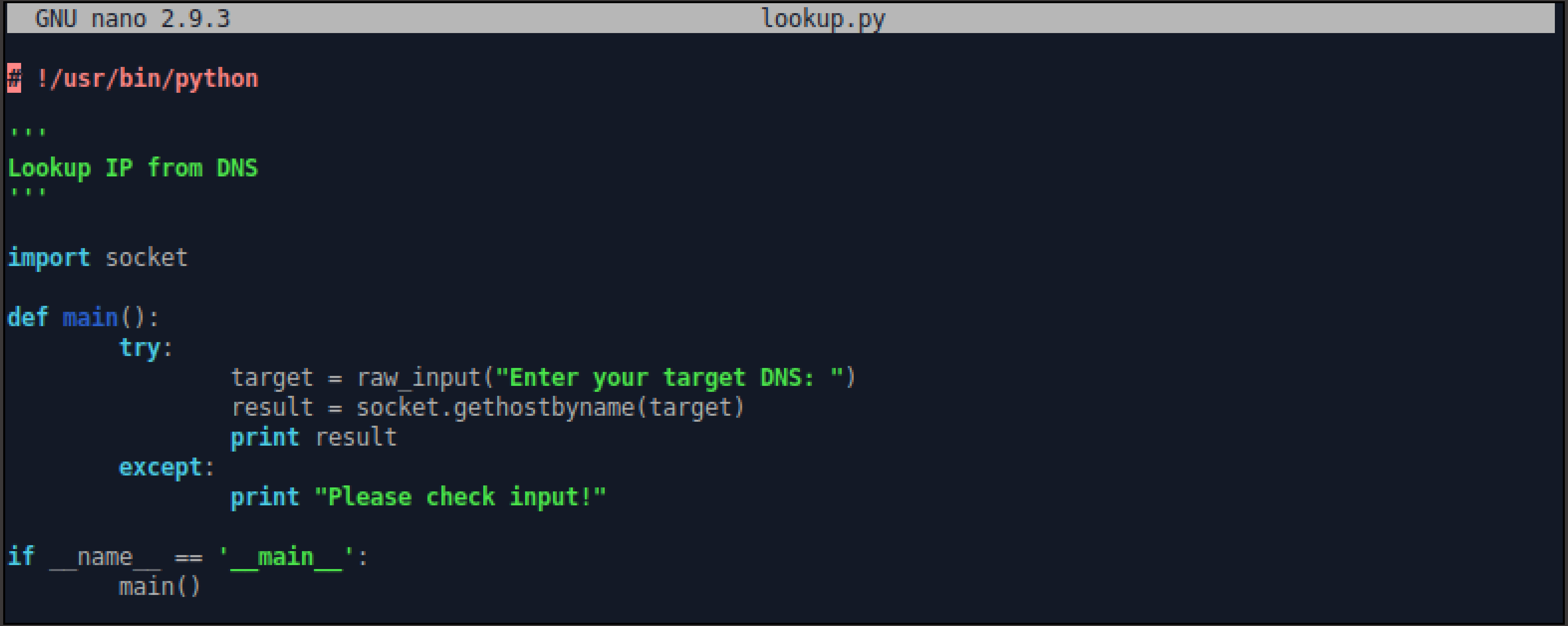
Exercises

1. Use the `whois` tool in Kali to identify the name servers of MegaCorp One.
2. Code a simple `lookup.py & reverse_lookup.py` script with Python `socket` module, that they can lookup IP from Domain name and reverse.

Hint: `raw_input(), gethostbyname(), gethostbyaddr()`

Passive Information Gathering

Exercises – Walk through



```
# !/usr/bin/python

'''
Lookup IP from DNS
'''

import socket

def main():
        try:
                target = raw_input("Enter your target DNS: ")
                result = socket.gethostbyname(target)
                print result
        except:
                print "Please check input!"

if __name__ == '__main__':
        main()
```

Passive Information Gathering

Google Hacking

Operator	Syntax	Description
Filetype	filetype:string	Search file with specific type “Ceh” + filetype:pdf
Index of	Index of /string	Display pages with directory listing vulnerability Index of /password
Intitle	intitle:string	Search for pages that contain string in the title intitle:"SQLiteManager" + intext:"Welcome to SQLiteManager version "
Inurl	inurl:string	Display pages within string in the url inurl:/host.txt + filetype:txt + "password"
Info	infor:string	Display information Google stores about the page itself
Link	link:string	Display linked pages based on search term
Site	site:domain	Display pages for specific website or domain holding search term.

Passive Information Gathering

Google Hacking – Demo

Target:

- https://stable.modified-shop.org/.svn/wc.db
- https://stable.modified-shop.org/.svn/pristine/

```
kali@kali:~$ wget http://www.sometarget.tgt/.svn/wc.db

kali@kali:~$ sqlite3 wc.db 'select local_relpath, ".svn/pristine/" ||
substr(checksum,7,2) || "/" || substr(checksum,7) || ".svn-base" as
alpha from NODES;'
```

Passive Information Gathering

Exercises

1. Reproduce pre-demo in Dolcera company with main web-site URL https://www.dolcera.com/
2. Make a dork to get all results from Google about this vulnerability

Passive Information Gathering

Netcraft

Netcraft is an Internet services company based in England offering a free web portal that performs various information gathering functions.

https://searchdns.netcraft.com/

https://searchdns.netcraft.com/?restriction=site+contains&host=*.megacorpone.com

Passive Information Gathering

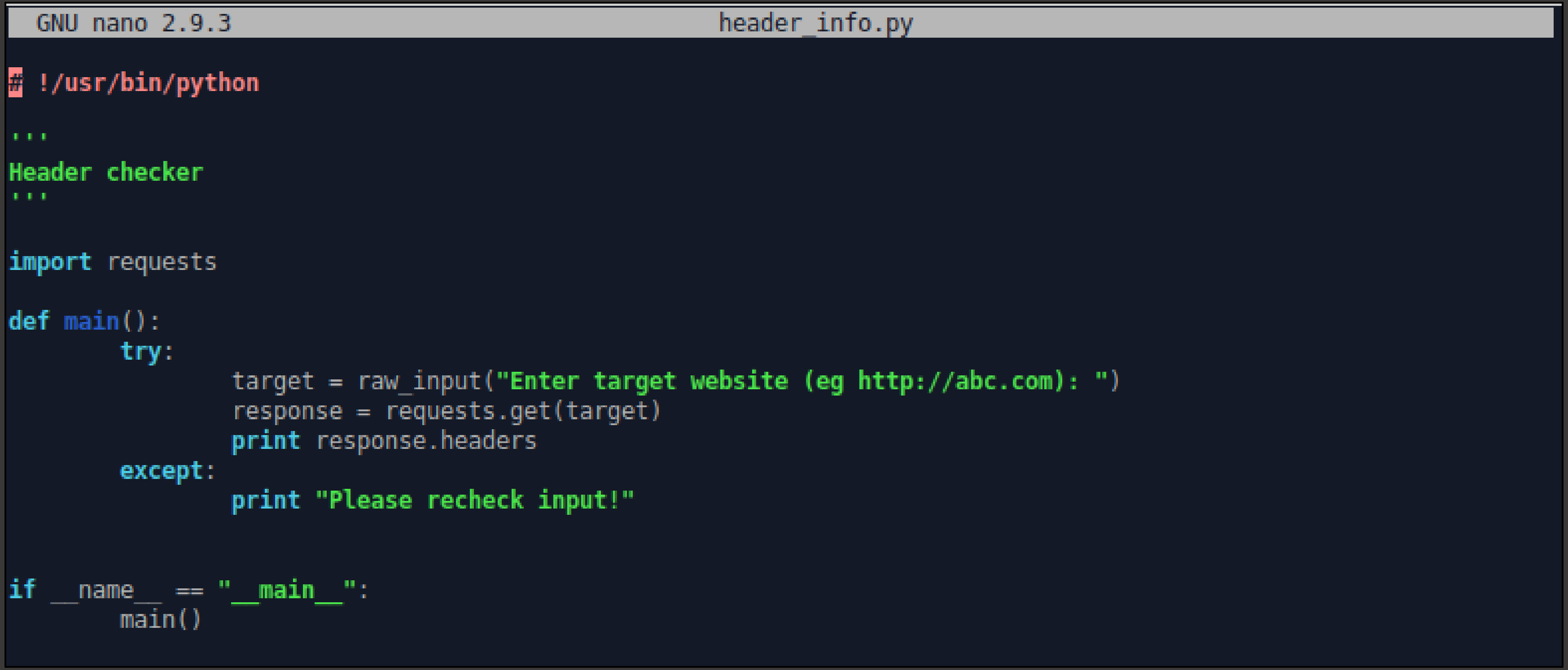
Exercises

1. Use Netcraft to determine what application server is running on www.bkacad.com
2. Code a simple `header_info.py` script with Python `requests` module, that they can check header of target website.

Hint: `import requests, dir(requests)`

Passive Information Gathering

Exercises – Walk through



```
  GNU nano 2.9.3                                   header_info.py

# !/usr/bin/python

'''
Header checker
'''

import requests

def main():
        try:
                target = raw_input("Enter target website (eg http://abc.com): ")
                response = requests.get(target)
                print response.headers
        except:
                print "Please recheck input!"


if __name__ == "__main__":
        main()
```

Passive Information Gathering

Open-Source Code

One such source of interesting information are open-source projects and online code repositories, such as GitHub, GitLab, and SourceForge.

Code stored online can provide a glimpse into the programming languages and frameworks used by an organization. In some rare occasions, developers have even accidentally committed sensitive data and credentials to public repos.

https://github.com/techgaun/github-dorks

Passive Information Gathering

Shodan

Shodan is a search engine that crawls devices connected to the Internet including but not limited to the World Wide Web. This includes the servers that run websites but also devices like routers and IoT devices.

https://www.shodan.io/

https://help.shodan.io/the-basics/search-query-fundamentals

Passive Information Gathering

Shodan – Demo Attack Un-authenticated ADB

Shodan LIVE demo

```
kali@kali:~$ This is live demo

kali@kali:~$ Nothing inside :’)
```

Test

Test

Test

```
kali@kali:~$ test
```