
One
PenTest Course
FOR ETHICAL HACKERS AND SYSTEM ADMINISTRATORS
INFORMATION GATHERING
Discover Vulnerabilities And Fix Them Quickly
Know Tricks To Fight Against Black Hackers
MoTech CyberSec

INTRODUCTION

This is security short course which is direct towards system administrator and different university students taking computer security , software developers and various people interested in the field of computer security, for the purpose of producing and ensuring the security of different system, for the side administrators it will an essential course as managing systems you need to know various tricks used by black hackers to com promise the systems, this security course series will help a reader to gain knowledge of securing different system , for them system administrator taking this security course should be a first step after job arrival, as I can “We Can Easily Stop Thieves If We Know Their Ways” ,so for them system administrator should consider taking Ethical Hacking Courses so that they can prevent their systems from them black hackers.

WHY YOU SHOULD TAKE THIS SECURITY COURSE.

It is based on current methodologies used by hackers, it is more based on real examples of the working places, requirement for this course is almost affordable for everyone.

Cybersecurity is the current trending issue on the ground of Information Technology, only machine learning, deep learning and artificial intelligence can compete with cybersecurity, but if you have covered one the technologies mentioned above, together with cybersecurity then you are luck.

INFORMATION GATHERING

This is very simple, for us to protect resources we must know what resources we own and what are the valuable resources or with high risk of being stolen by thieves.

This is the same I our real life. System admin should know ports present on the system, should know vulnerabilities of ports which might be easily exploited by black hackers.

NOTE:

FOR SYSTEM ADMIN ➔ Make you sure that, you are able to gather information of your computer and by knowing which ports are prone to be attacked, it will be simple to control system and keep black hacker in hard situation though do not trust yourself 100%.

FOR PENTESTER ➔ Before testing system, make sure you Don not jump the steps , gathering information about your target before scanning vulnerability is considered as undesirable in computer security point of view, knowing which port is open can help you to brute-force the port and gain access direct to the system, also knowing the version of device running on system will help you to know the vulnerabilities of device and exploit them easily.

Important Information To Gather Before End Of this Section

- ⇨ Number of ports running in a system
- ⇨ Types of services running in ports of system
- ⇨ Devices and their names
- ⇨ Ip address of a site
- ⇨ Subdomains Of a site
- ⇨ DNS information

InfoGather.sh IS THE TOOL OF TRADE

Alternative tool to used ➔ **Nmap**

➔ **Zenmap**

InfoGather.sh is used for gathering information, it is not only because the tool was coded by author but working with scripts, brings job automation.

WHERE TO GET THIS TOOL

This tool is currently on github.com by clicking this link

https://github.com/MoTechStore/InfoGather

Just download it for free but if you have github.com account you can follow MoTechStore on github.com, MoTechStore is an account on which different phases of this course for ethical hackers and system administrator will be updated and added, so better get in touch with MoTechStore.

HOW TO USE InfoGather

cd InfoGather

After downloading InfoGather from github.com, extract it and then, mean change to InfoGather directory or within InfoGather directory you can open terminal.

```
┌─[✗]─[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $ls
InfoGather.sh  readme.txt  requirements.txt
┌─[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $sudo chmod +x InfoGather.sh
┌─[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $sudo chmod +x requirements.txt
┌─[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $pip install -r requirements.txt
```

ls

This is long listing to see the content of the folder InfoGather

sudo chmod +x InfoGather.sh

Adding Execute permission to the Script

pip install -r requirements.txt

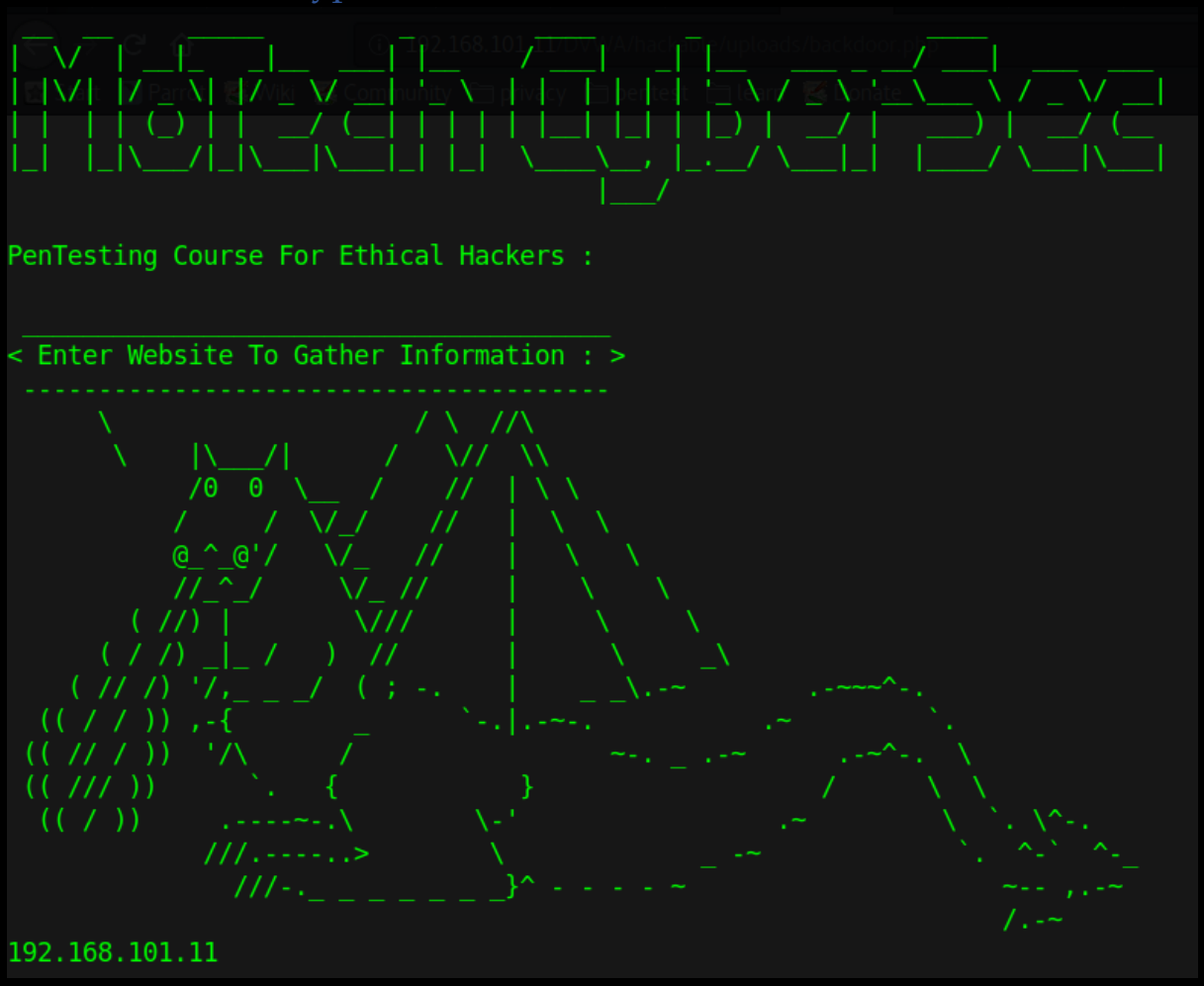
Installing the requirements

./InfoGather.sh

```
┌──[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $ls
InfoGather.sh  readme.txt  requirements.txt
┌──[forensic5@parrot]─[~/Desktop/InfoGather]
└──╼ $./InfoGather.sh
```

After that run the script InfoGather.sh

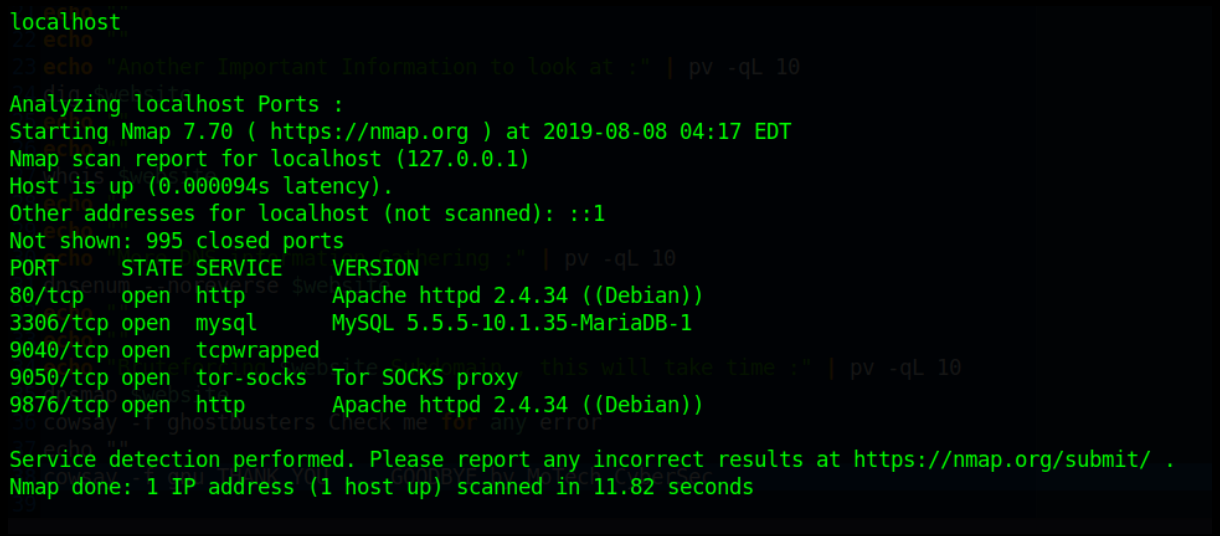
After the script to run you can type ip address of the target or domain name for the trial type 127.0.0.1 and see the results first.



or use localhost

Wait for a moment it will soon start to gather information.

For it to load.



Those above are the open ports scanned, from above results mysql port is open, one can think about direct exploiting , ad access the port , not yet it will be done in the next phases of exploitation.

Information Gathered

Ip address ➔ 127.0.0.1

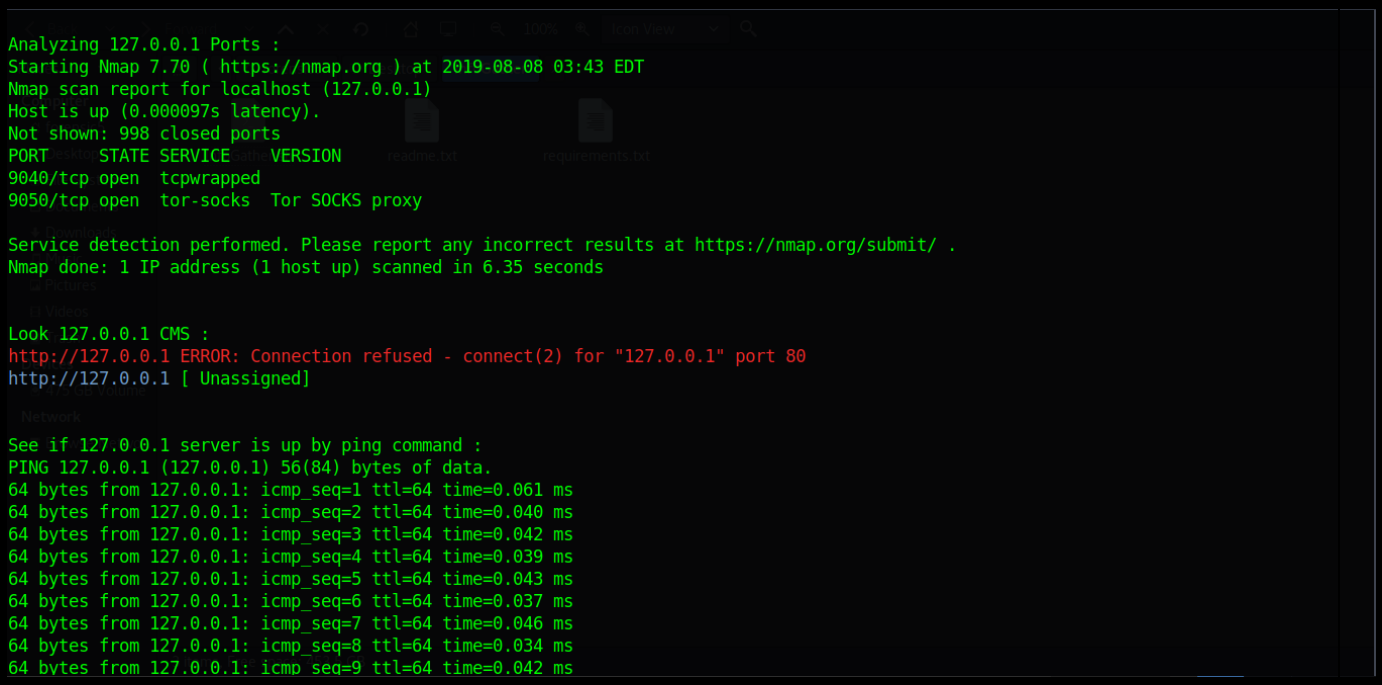
MySql port ➔ open

Web Server ➔ Apache

Version of Web Server ➔ 2.4.34

Hostname ➔ Debian

Running proxy ➔ port 9050



ping and packets are received directly means the server is up, you can't do penetration testing if server is down so ping command is very essential.

```
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
```

On behalf of MoTech CyberSec Cow Say Goodbye .... See You Next Phase, Do not miss next phases.

CONCLUSION

Thank you and welcome for the next PenTest Course Series For PenTester and System Admin, as we we have yet to find our official website for giving update on when next phases of this course, All updates will be published at MoTech YouTube Channel, so it is better to subscribe at MoTech YouTube Channel where and news and updated about will course will be displayed, also you can follow MoTechStore at GitHub.com series.

Name of the author ➔ Noel Moses Mwadende

But there are other contributors and experts for the whole journey of this course.

WAYS TO HOOK MoTech /MoTech CyberSec

YouTube

https://www.youtube.com/channel/UCtuaigKZF3okQnKON5RM1qQ

GitHub

https://github.com/MoTechStore/

Amazon

https://www.amazon.com/s?k=noel+moses+mwadende&ref=nb_sb_noss