Kali Linux Lab: Penetration Test

Spring 2025

Chengyi Qu

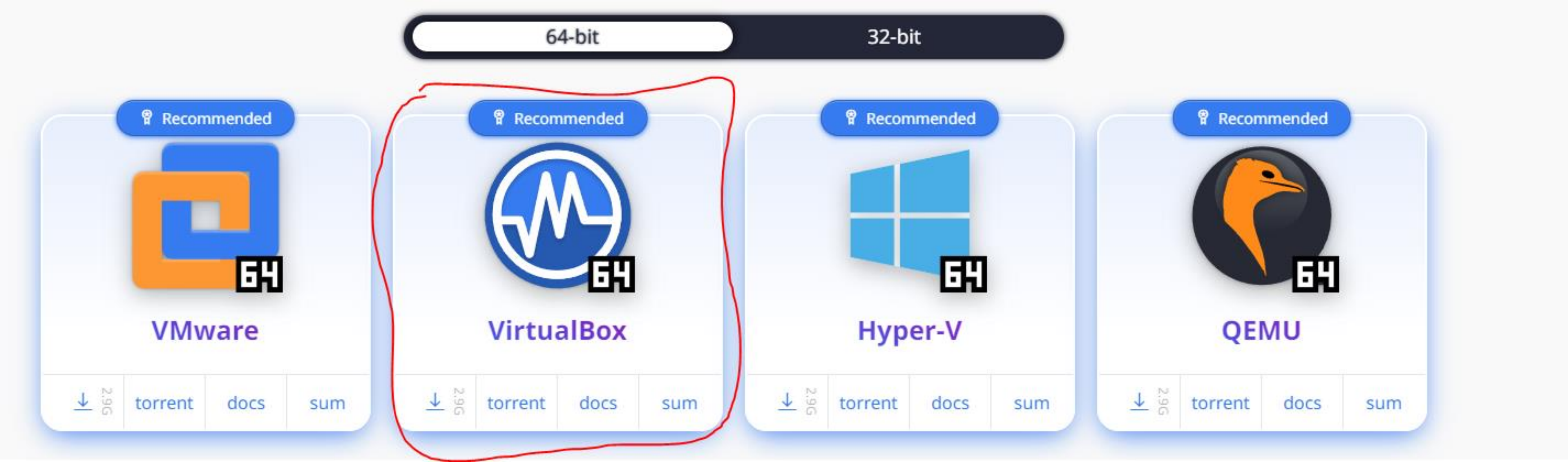
Submission Due: March 11th

Background

- Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.
- In this lab, we will working on several apps inside Kali Linux and process a series of penetration test.

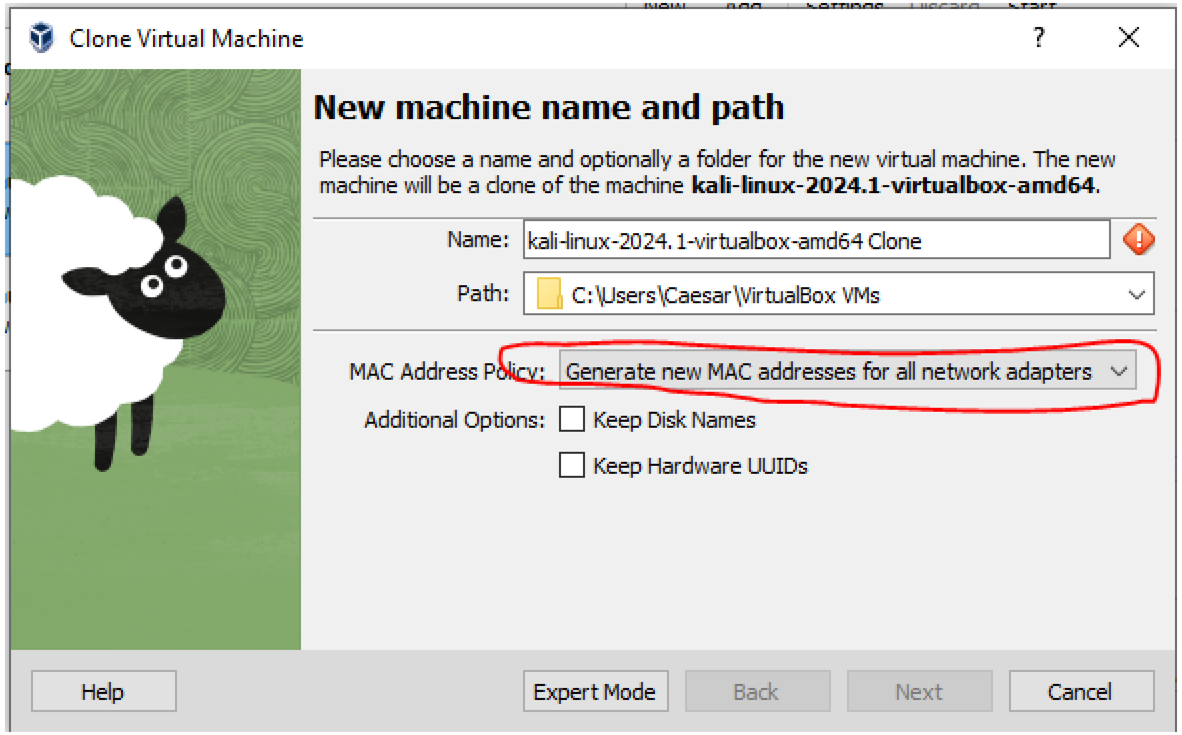
Basic Setup

- Download the virtual box version Kali Linux: https://www.kali.org/get-kali/#kali-virtual-machines
- You can check the doc here: https://www.kali.org/docs/virtualization/import-premade-virtualbox/



Clone the Kali Linux machine on Virtual Box

- Power off the machine. Select the VM, on the top menu, select Machine -> Clone, select Generate new MAC for network adapters and Full clone. Click **finish** to clone.



New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **kali-linux-2024.1-virtualbox-amd64**.

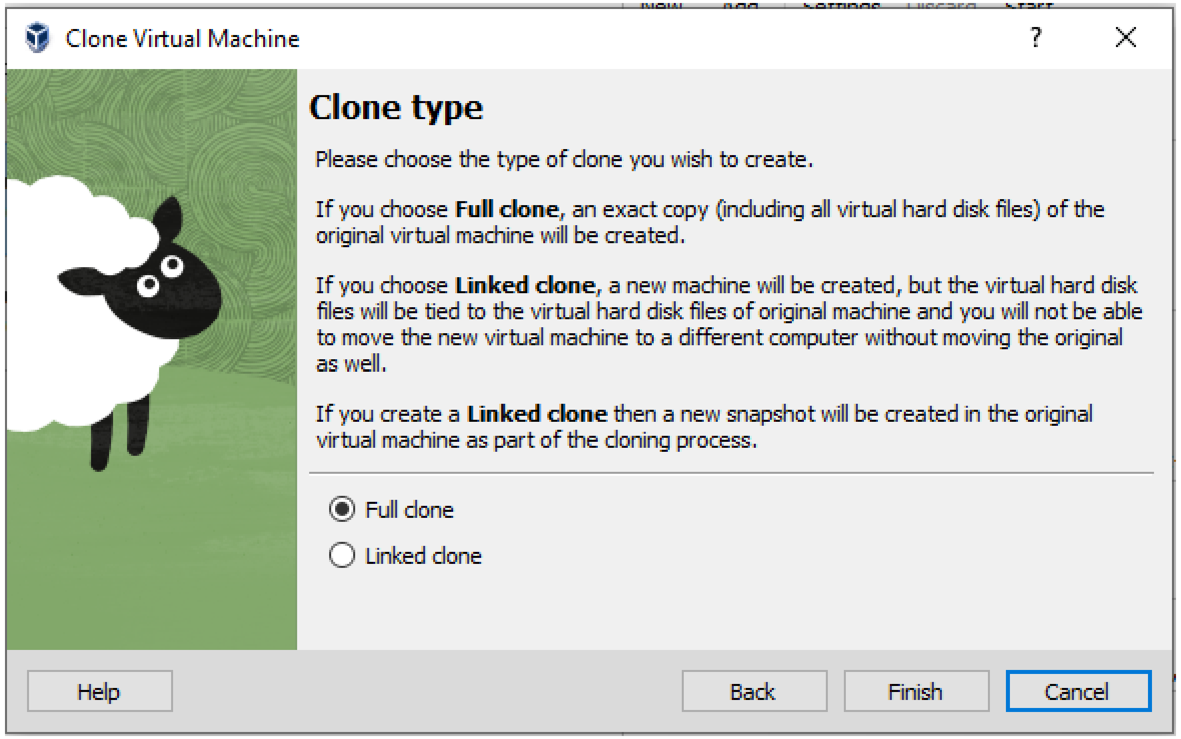
Name: kali-linux-2024.1-virtualbox-amd64 Clone

Path: C:\Users\Caesar\VirtualBox VMs

MAC Address Policy: Generate new MAC addresses for all network adapters

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs



Clone type

Please choose the type of clone you wish to create.

If you choose **Full clone**, an exact copy (including all virtual hard disk files) of the original virtual machine will be created.

If you choose **Linked clone**, a new machine will be created, but the virtual hard disk files will be tied to the virtual hard disk files of original machine and you will not be able to move the new virtual machine to a different computer without moving the original as well.

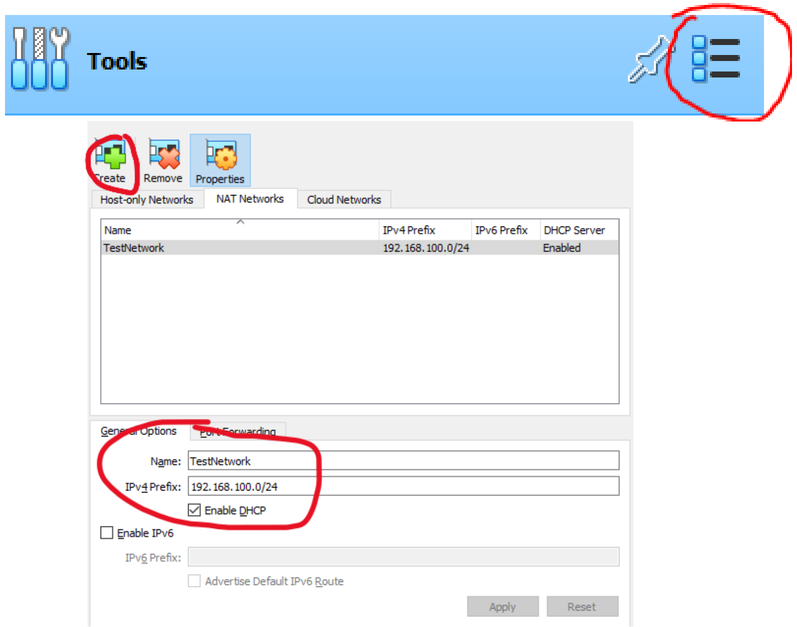
If you create a **Linked clone** then a new snapshot will be created in the original virtual machine as part of the cloning process.

● Full clone

○ Linked clone

Generate new Nat Networks and make two machine talk to each other

- Power off all machines, Go to tools -> little list icon -> network, click Nat Network tab -> click ‘Create’ on top.
- Under General options -> Name your Nat Network as ‘TestNetwork’ (can be others) -> Type Ipv4 prefix into 192.168.100.0/24 -> Enable ‘DHCP’, click Apply.



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
TestNetwork	192.168.100.0/24		Enabled

Name: TestNetwork

IPv4 Prefix: 192.168.100.0/24

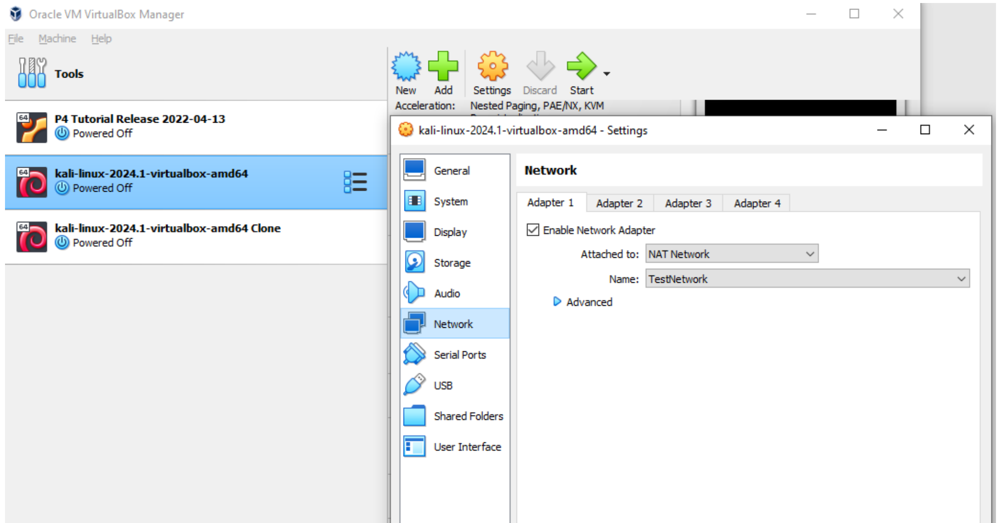
☑ Enable DHCP

☐ Enable IPv6

IPv6 Prefix:

☐ Advertise Default IPv6 Route

- On each Kali Linux, select Settings -> Network -> Nat Network with the name of ‘TestNetwork’



Acceleration: Nested Paging, PAE/NX, KVM

P4 Tutorial Release 2022-04-13
Powered Off

kali-linux-2024.1-virtualbox-amd64
Powered Off

kali-linux-2024.1-virtualbox-amd64 Clone
Powered Off

kali-linux-2024.1-virtualbox-amd64 - Settings

☑ Enable Network Adapter

Attached to: NAT Network

Name: TestNetwork

Task 1:Show IP assigned and communications (10 points)

- Login on each Kali Machine (user: kali, password: kali), open terminal and check the ip address and show successful communication.
- Thinking about how to check IP address? How to test a successful communication?

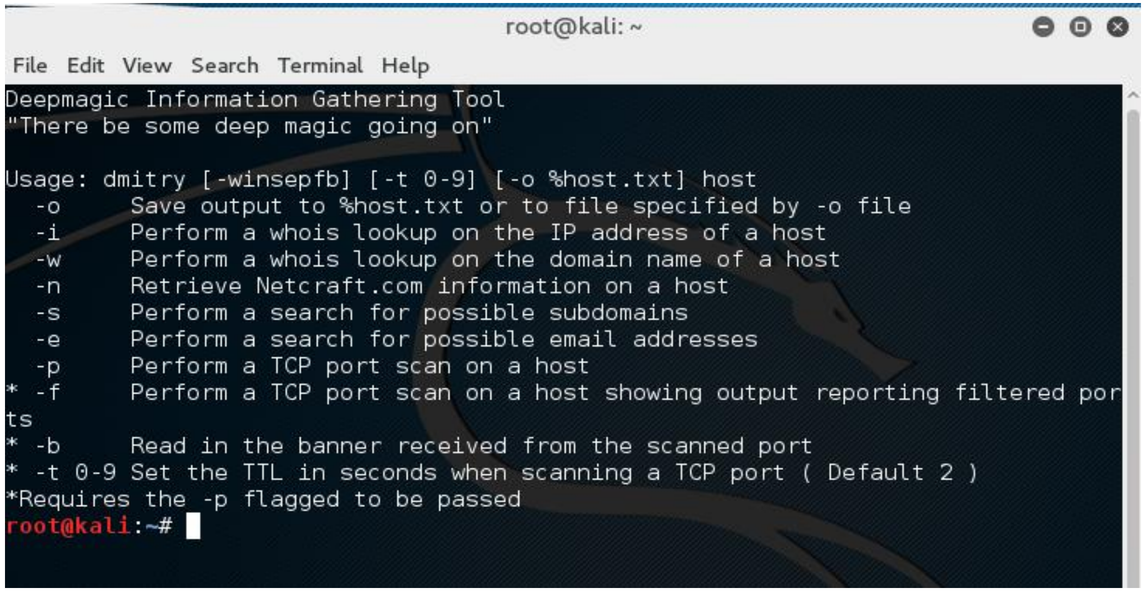
- What to include in your report on this question?
  - Screenshots on terminal shows the IP address on each Kali machine;
  - Show communication between each other with some command
  - Your name typed in the terminal to avoid cheat ☺

Introduction to Kali Linux

- The successor to Backtrack, a popular penetration testing distribution that was first released in 2006.
- https://www.kali.org/
- It has a HUGE number of tools. A few are listed here:
  - BBQSQL
  - Jsql
  - Reaver
  - Nmap
  - dnsenum
  - dnsrecon
  - sigguesser
  - cisco-orc

Task 2: learn Dmitry

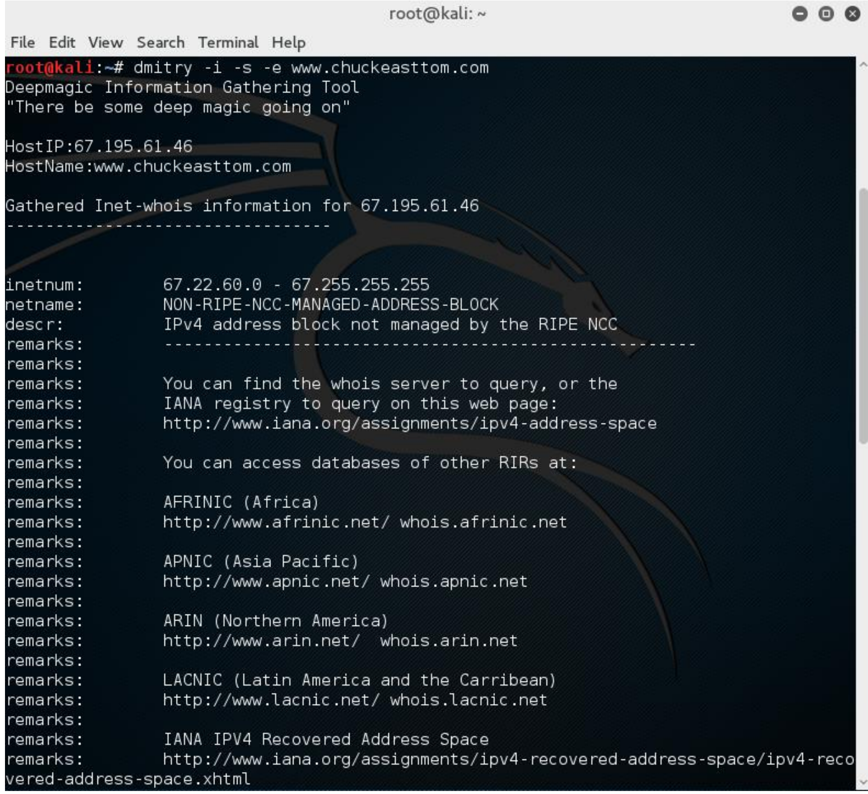
Dmitry is Deepmagic Information Gathering Tool. It is essentially a search and scanning tool.



```
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered por
ts
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~# 
```

Analysis using Dmitry (20 points)



```
root@kali:~# dmitry -i -s -e www.chuckeasttom.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:67.195.61.46
HostName:www.chuckeasttom.com

Gathered Inet-whois information for 67.195.61.46
---------------------------------


inetnum:        67.22.60.0 - 67.255.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        You can find the whois server to query, or the
remarks:        IANA registry to query on this web page:
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:        You can access databases of other RIRs at:
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/  whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        IANA IPV4 Recovered Address Space
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space/ipv4-reco
vered-address-space.xhtml
```

Let’s use Dmitry on my own website again and type the following:

```
dmitry –i –s –e chengyiqu.com
```

-i is a whois lookup.

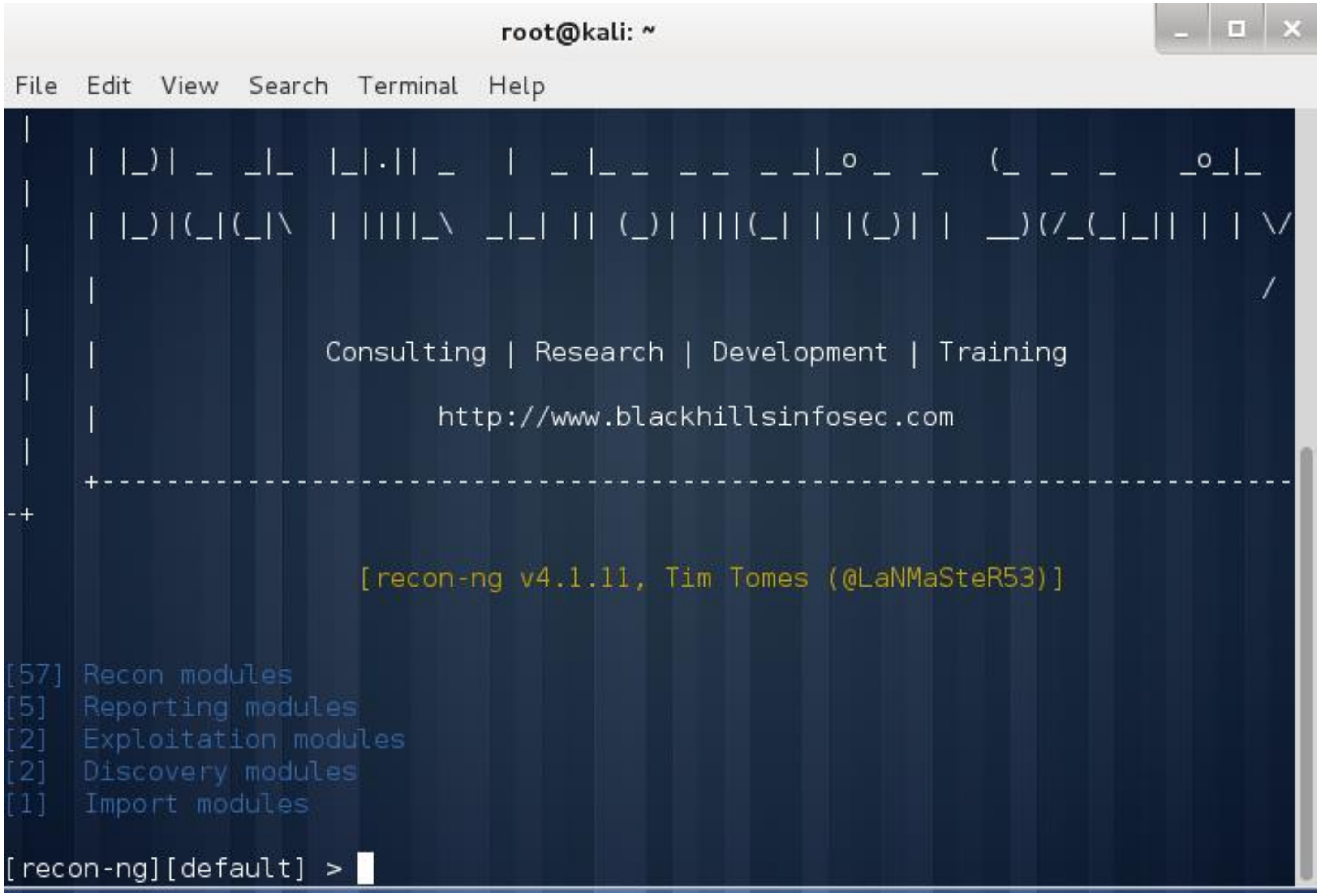
-s is a search for subdomains.

-e is a search for email addresses.

- What you need to submit:
  - Show screenshot of the Dmitry on the above command and explain the output.
  - Which name server my website is using? Which port I’m opening for access?
  - Any other information you find from this website scanning?

Task 3: Learn Recon-ng

Type **Recon-NG** at the shell, or select from menu.



```
|
    | |_)| _  _|_  |_|.|| _   |  _ |_ _  _ _  _ _|_o _  _   (_  _  _    _o_|_
|
    | |_)|(_|(_|\  | ||||_\  _|_| || (_)| |||(_| | |(_)| |  __)(/_(_|_|| | | \/
|
    |                                                                          /
|
    |               Consulting | Research | Development | Training
|
    |                     http://www.blackhillsinfosec.com
|
    +--------------------------------------------------------------------------
-+


                  [recon-ng v4.1.11, Tim Tomes (@LaNMaSteR53)]


[57] Recon modules
[5]  Reporting modules
[2]  Exploitation modules
[2]  Discovery modules
[1]  Import modules

[recon-ng][default] > 
```

Recon-ng test (30 points)

- Use this tutorial: https://medium.com/@bibinrajbs/using-recon-ng-in-kali-2020-cc76aa3a4a6d to generate a Car report

- What you need to submit:
  - Change two different car titles instead of Tesla and BMW (make sure you type the current domain name);
  - Save in your own file location, name it as report.html;
  - A HTML report screenshot, include the address URL.

  - Note that you need to build the report.html first in order to let Recon-ng find the location

Task 4: Lean the basic of Metasploit

- Following this tutorial to hack inside the Metasploitable VM:

https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b

Hints:

- To build a new Metasploitable VM in Vmbox, check this link: https://smallbusiness.chron.com/open-wfc-file-18909.html
- You will need to test the connection between Kali linux to Metasploitable VM before hacking
- Use right ctrl to release from Mataspoitable VM.

Task 4: Lean the basic of Metasploit (40 points)

- What you need to submit:
  - Screenshots on successfully hacking inside the Metasploitable VM.
  - Create a file with ‘your name.txt’ with any content inside the file from Kali Linux, and check back on the Metasploitable to see if the file exists.
  - Take screenshots on the file name with your name and content using ‘cat’ command on Metasploitable.
  - (15 points) Run at least one more tool in Metasploit and explain the results, e.g.,
    - scanner/smb/smb_version
    - auxiliary/scanner/mssql/mssql_ping
    - scanner/ssh/ssh_version
    - auxiliary/scanner/ftp/anonymous
    - or others…

Additional tasks

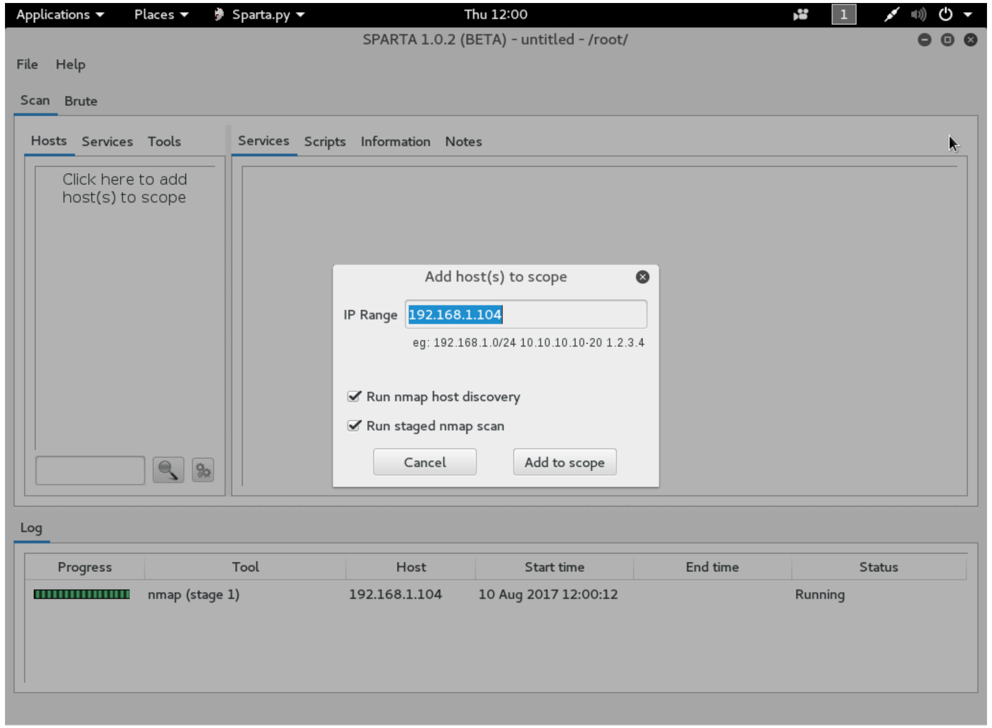
- There are a lot of tools pre-installed in Kali. Try to explore some other tools listed in the following slides and get extra points by including your findings.
- You may gain at most 20 extra points on this exploration.
- You need to provide a detailed report on at least 2 (10 points each) of the tools from the following list and show screenshots on successfully use these tools to explore.

Sparta

Sparta is a tool that gives you access to many vulnerability scanners in one, including

- Mysql-default
- Nikto
- Snmp-enum
- Smtp-enum-vrfy
- Snmp-default
- Snmp-check

Sparta is also an easy-to-use GUI tool rather than a command line.



SPARTA 1.0.2 (BETA) - untitled - /root/

Add host(s) to scope

IP Range: 192.168.1.104

eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4

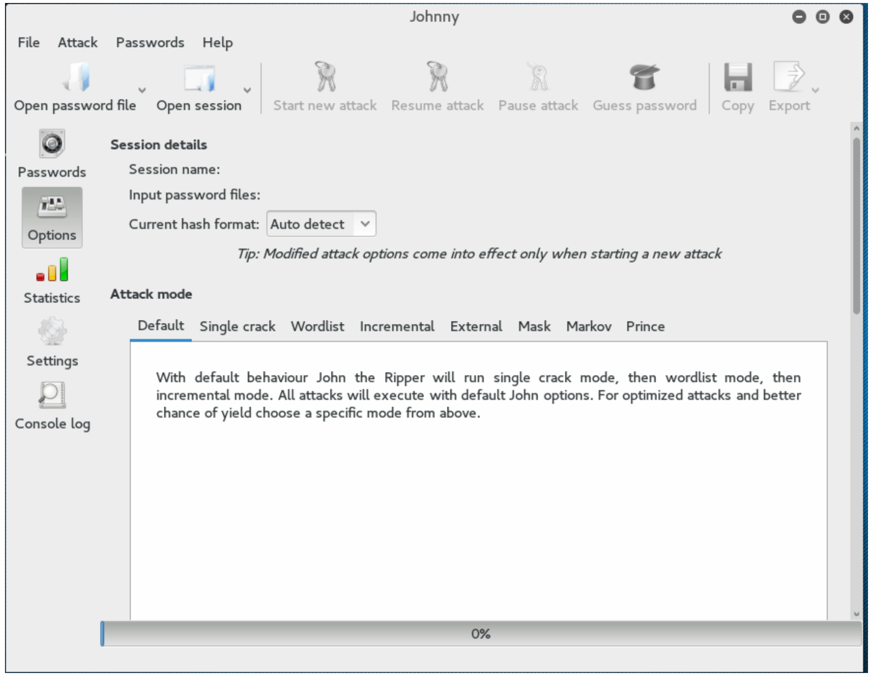
☑ Run nmap host discovery

☑ Run staged nmap scan

Progress	Tool	Host	Start time	End time	Status
	nmap (stage 1)	192.168.1.104	10 Aug 2017 12:00:12		Running

John the Ripper

John the Ripper is a well-known password cracking tool. Kali Linux has a shell version of John the Ripper and a GUI version named Johnny.



Session details

Session name:

Input password files:

Current hash format: Auto detect

Tip: Modified attack options come into effect only when starting a new attack

Attack mode

With default behaviour John the Ripper will run single crack mode, then wordlist mode, then incremental mode. All attacks will execute with default John options. For optimized attacks and better chance of yield choose a specific mode from above.

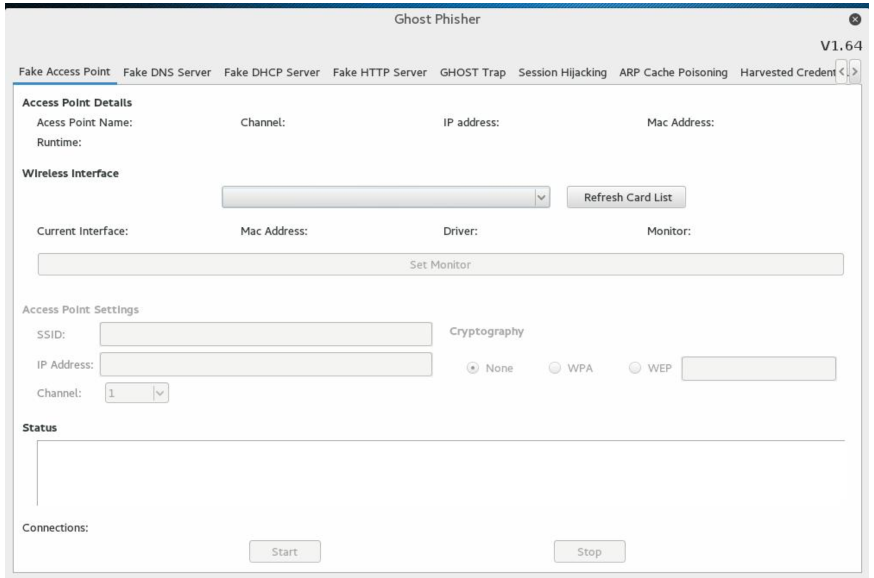
Ghost Phisher

This is a very versatile tool, with several interesting functions.

Each tab has settings to turn your Kali Linux machine into

- A fake wireless access point
- A fake DNS server
- A fake DHCP server
- A fake HTTP server

And more. There are tabs for session hijacking and harvesting credentials.

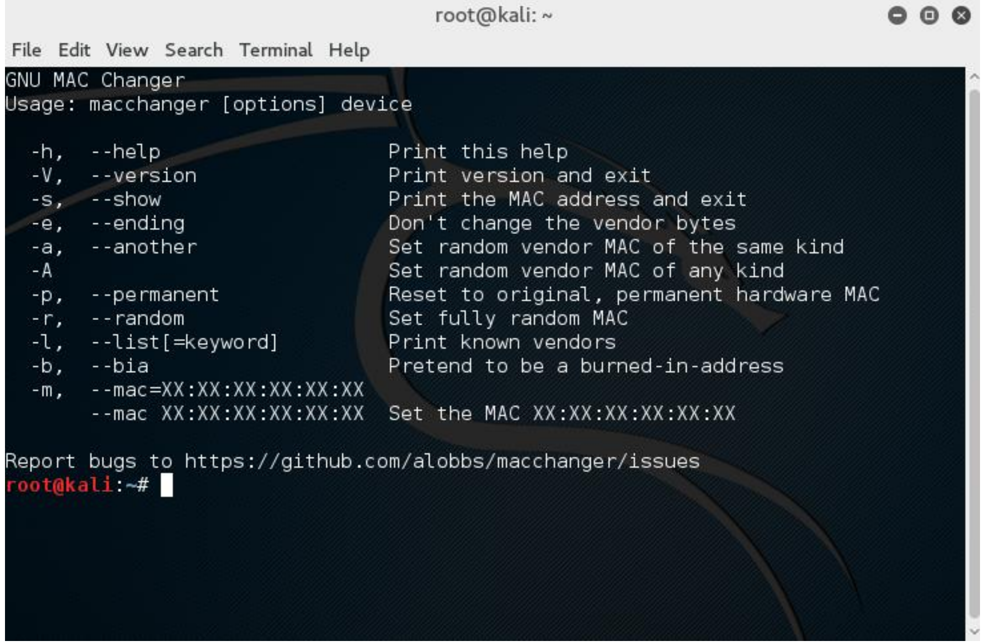


Channel: 1

● None ○ WPA ○ WEP

Macchanger

This tool changes the MAC address your Kali machine sends out, which makes it more difficult to trace the attack back to the Kali machine. Also, MAC spoofing can be a way to circumvent some forms of authentication.



```
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                   Print this help
  -V,  --version                Print version and exit
  -s,  --show                   Print the MAC address and exit
  -e,  --ending                 Don't change the vendor bytes
  -a,  --another                Set random vendor MAC of the same kind
  -A                            Set random vendor MAC of any kind
  -p,  --permanent              Reset to original, permanent hardware MAC
  -r,  --random                 Set fully random MAC
  -l,  --list[=keyword]         Print known vendors
  -b,  --bia                    Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
root@kali:~#
```

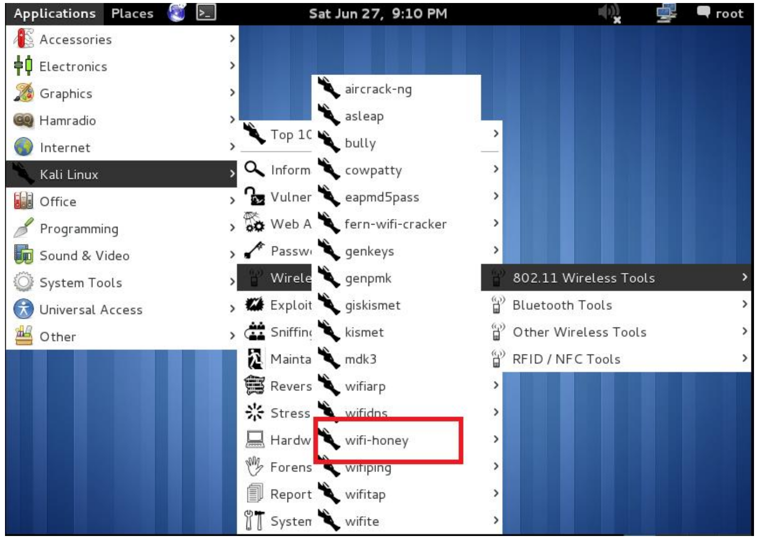
Wifi Honey

- Create your own fake AP with wifi-honey
- Generic example:

```
wifi-honey <essid> <channel> <interface>
```

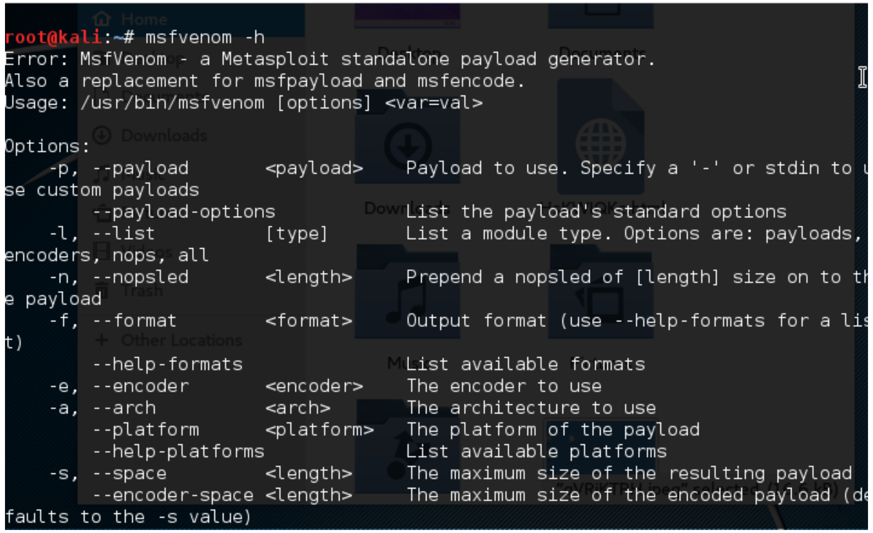
- Specific example:

```
wifi-honey FreeWiFi 6 eth0
```



msfvenom

Msfvenom essentially combines msfpayload and msfencode so that you can encode payloads and then send them to the target. It is a powerful tool, and a part of Metasploit you should be familiar with. It is used from the shell in Kali, not from inside Metasploit. You start by trying **msfvenom –h**.



```
root@kali:~# msfvenom -h
Error: MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
    -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to u
se custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads,
encoders, nops, all
    -n, --nopsled       <length>     Prepend a nopsled of [length] size on to th
e payload
    -f, --format        <format>     Output format (use --help-formats for a lis
t)
        --help-formats               List available formats
    -e, --encoder       <encoder>    The encoder to use
    -a, --arch          <arch>       The architecture to use
        --platform      <platform>   The platform of the payload
        --help-platforms             List available platforms
    -s, --space         <length>     The maximum size of the resulting payload
        --encoder-space <length>     The maximum size of the encoded payload (de
faults to the -s value)
```

Conclusion

- You need to provide both the screenshots and explanation to get full points.
- Please make sure to include your own information to avoid any cheat check, either on the screenshots or on the explanation.
- Submit one single PDF file.

Submission Due: March 11th