Ethical Hacking Bootcamp with Hands-on Labs

Omar Santos
Twitter: @santosomar

Agenda Day 1

- Introduction to Ethical Hacking, Building Your Own Lab, and Setup
- Penetration Testing Linux Distributions
- Passive Reconnaissance
- Active Reconnaissance

Agenda Day 2

- Social Engineering
- Buffer Overflows
- Introduction to Web Application Hacking
- Exploiting Cross-Site Scripting (XSS) Vulnerabilities
- Cross-site Request Forgery (CSRF)
- Bypassing Authentication and Authorization
- Exploiting XXE Vulnerabilities
- Hacking Databases

Agenda Day 3

- Hacking Wired and Wireless Networks
- Password Attacks
- Post-Exploitation
- PWNing the VMs: Exercises of Completely Compromising the RAVEN and VTSEC VMs

DISCLAIMER / WARNING

The information provided on this training is **for educational purposes only**. The **author**, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.

Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

RESOURCES FOR THIS CLASS

Class website:
https://bootcamp.h4cker.org

GitHub Repository:
https://h4cker.org/github

Additional Training:
https://h4cker.org/training

POLL QUESTION

What is your familiarity with Ethical Hacking and Penetration Testing?

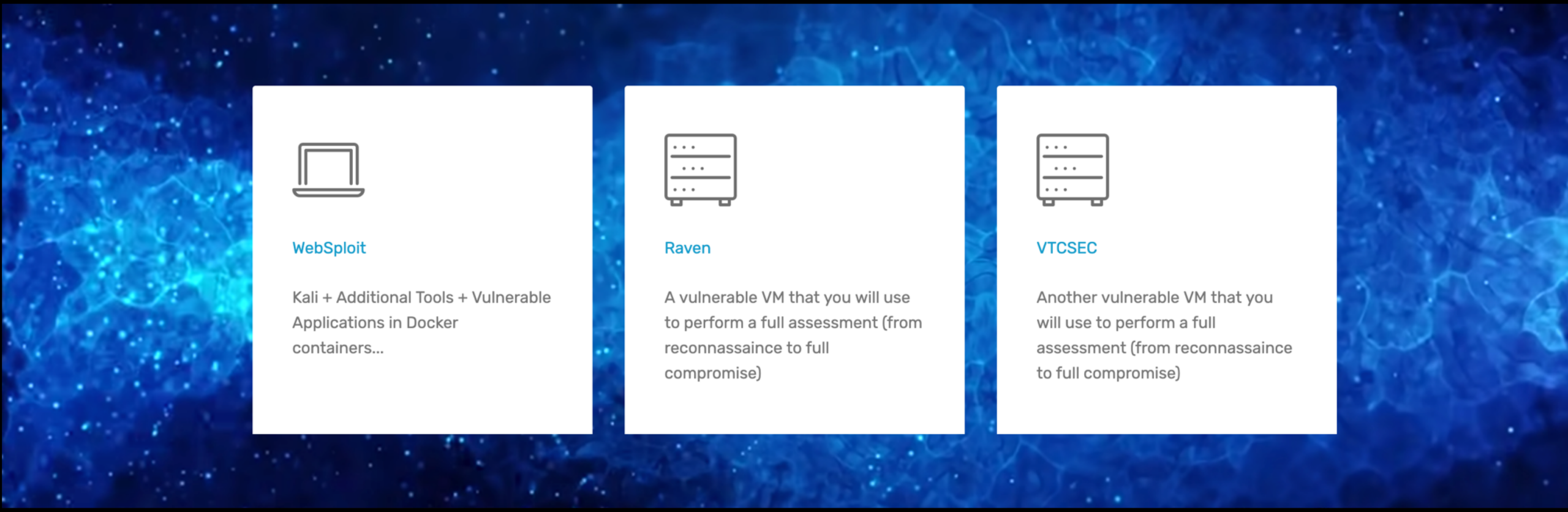
a. Just started
b. Intermediate (1-2 years of experience)
c. Significant experience

POLL QUESTION

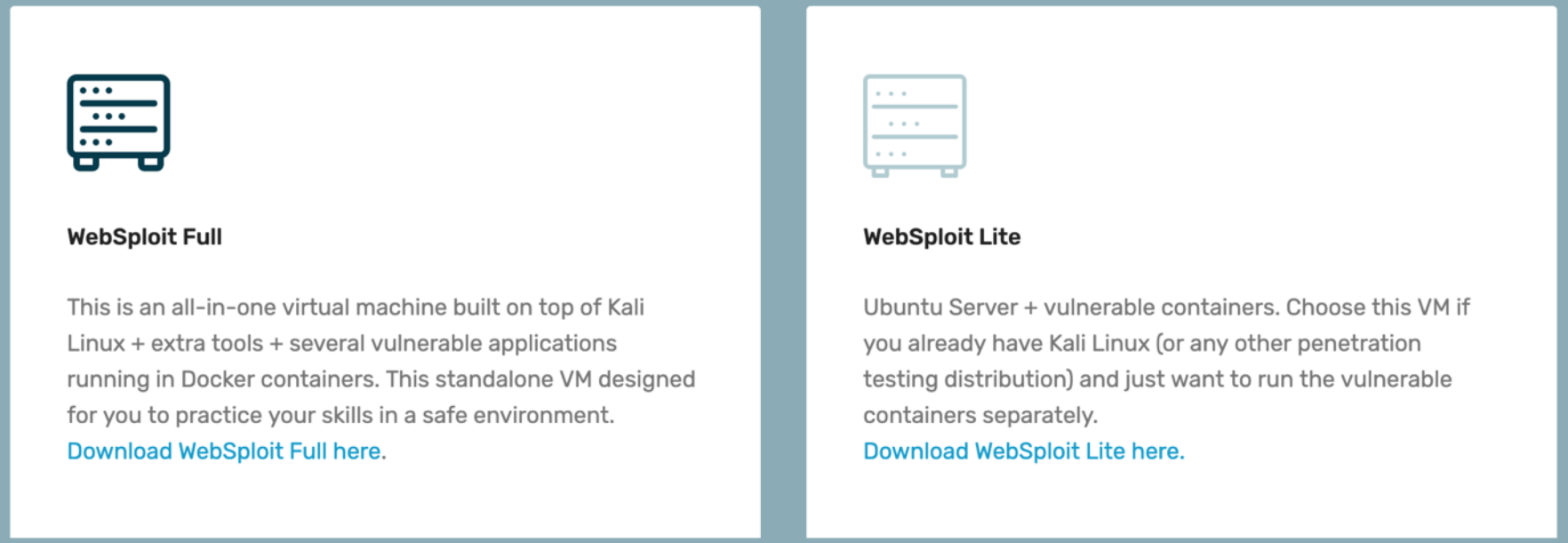
Why are you interested in this class?

a. Just curious about pen testing
b. Preparing for a certification
c. My job is pen testing (ethical hacking)

Introduction to Ethical Hacking, Building Your Own Lab, and Setup

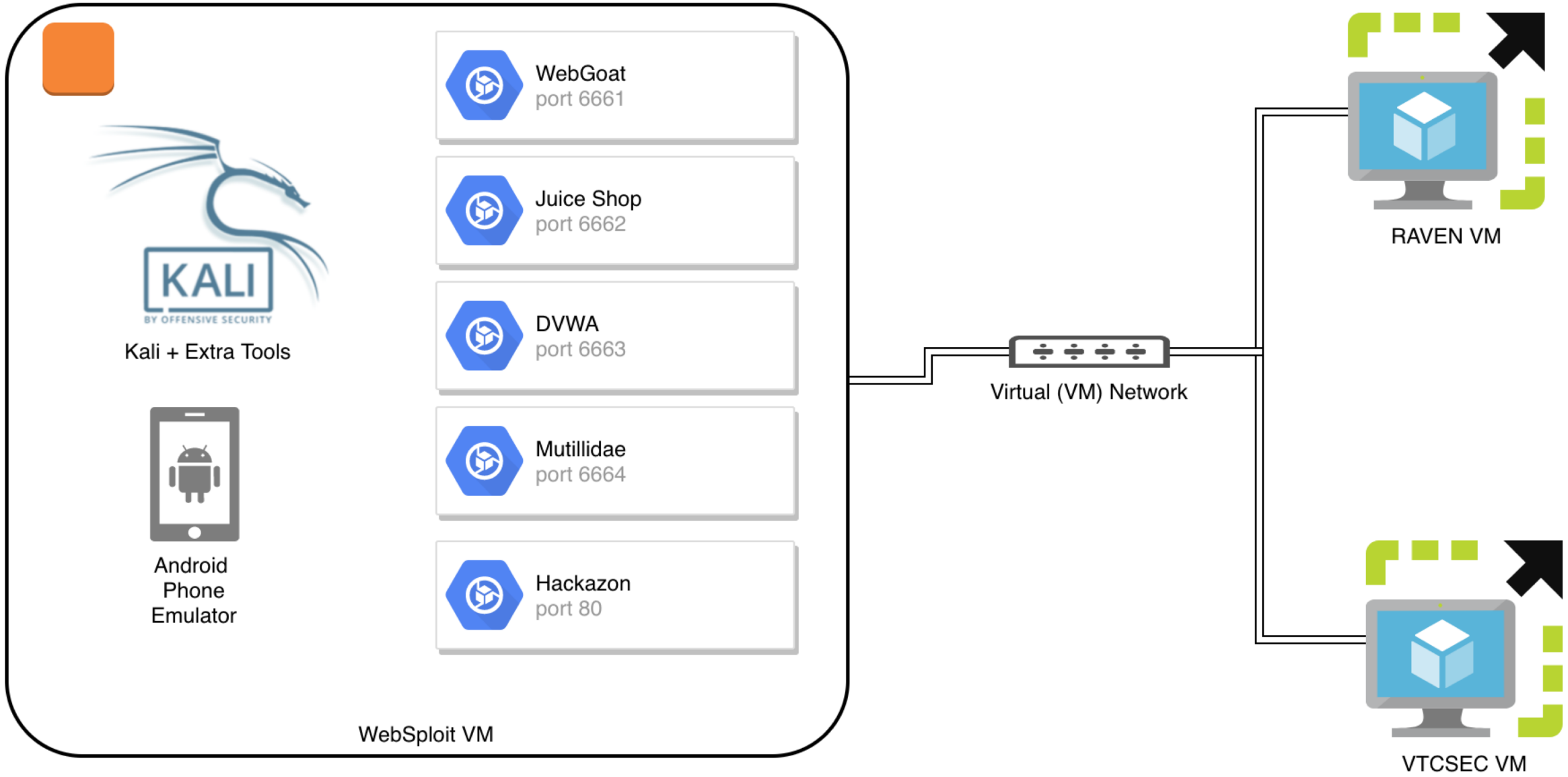


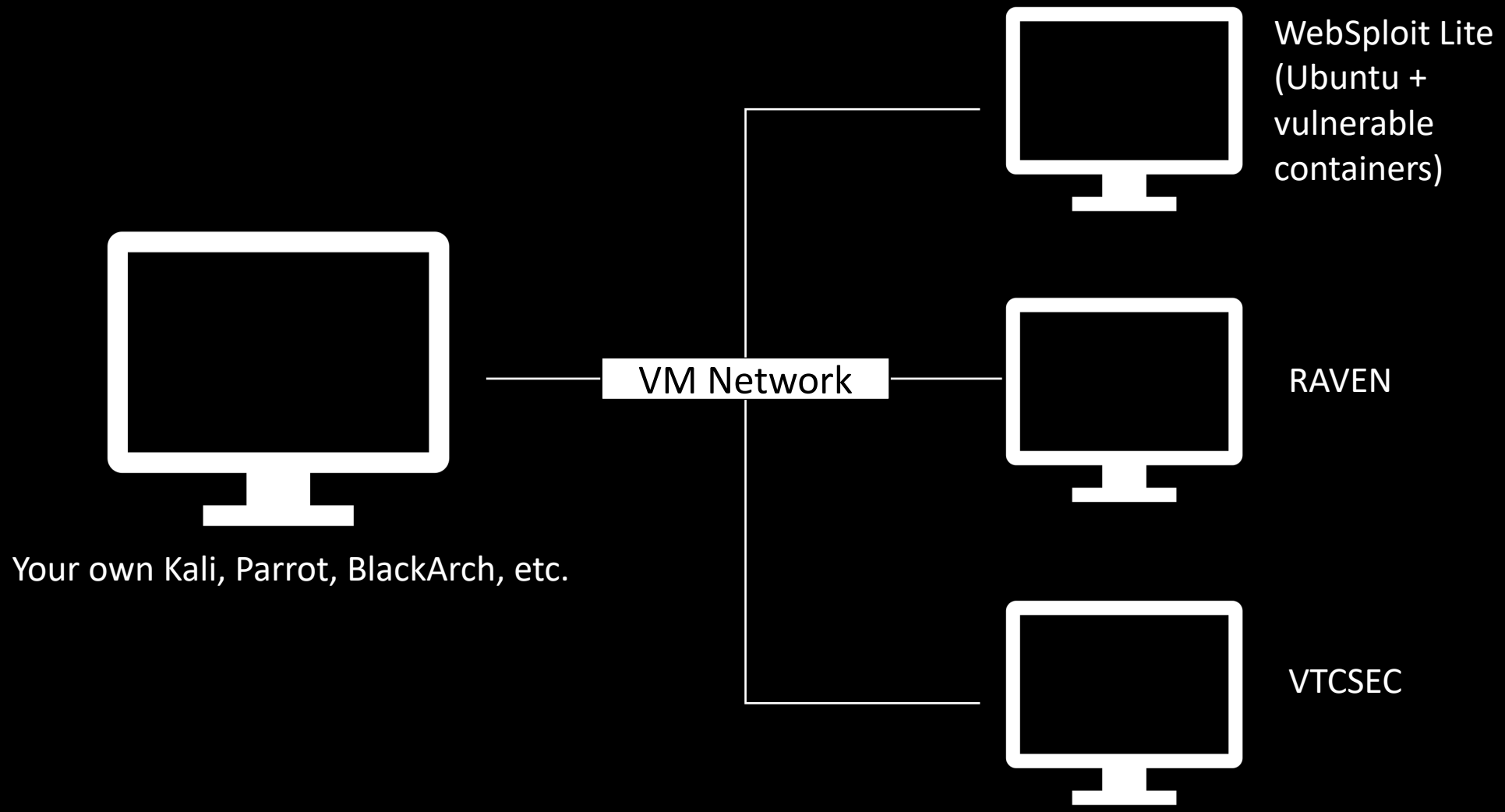
Virtual Machines



WebSploit

https://websploit.h4cker.org


KALI
BY OFFENSIVE SECURITY
Kali + Extra Tools
Android Phone Emulator
WebGoat
port 6661
Juice Shop
port 6662
DVWA
port 6663
Mutillidae
port 6664
Hackazon
port 80
WebSploit VM
Virtual (VM) Network
RAVEN VM
VTCSEC VM



Option 2: Your Own Kali + WebSploit Lite and other VMs

BREAK

10 MINUTES

Don’t forget about the resources at: https://h4cker.org

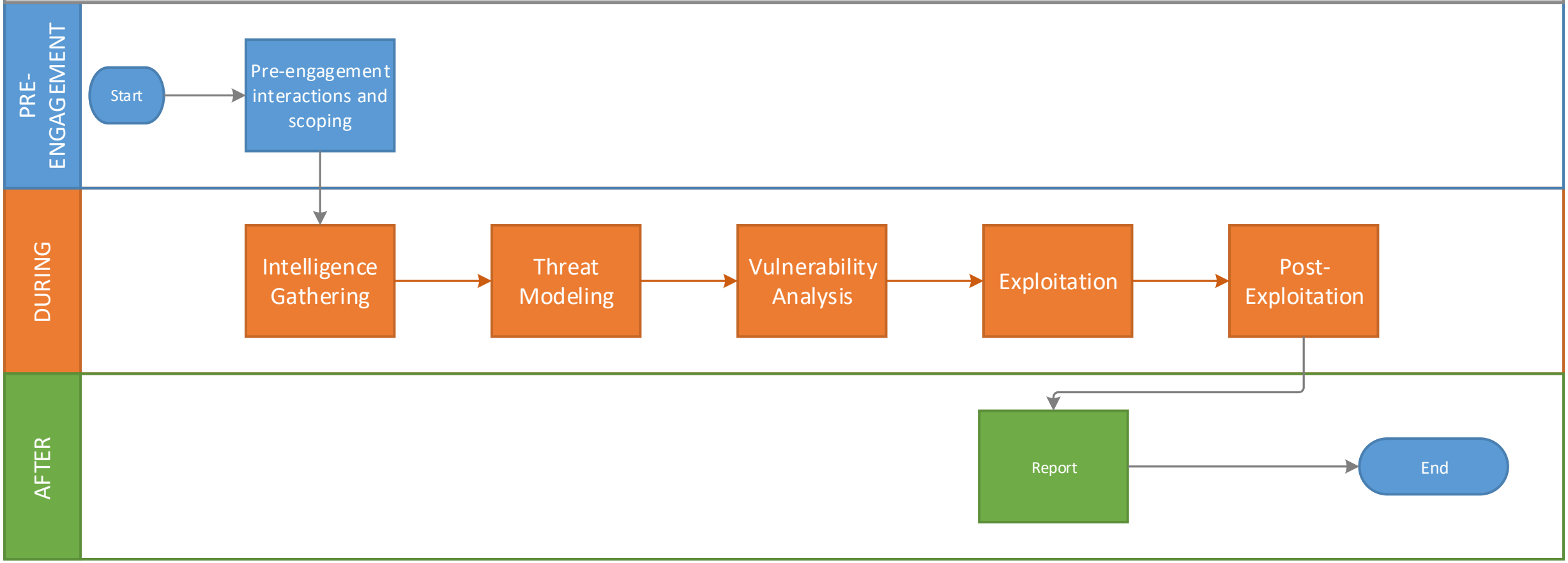
You can deploy and configure your VMs using

- Virtual Box (Windows, Linux, Mac)
- VMWare Workstation Player (Windows)
- VMWare Workstation Pro (Windows)
- VMWare Fusion (Mac)
- vSphere Hypervisor (free ESXi server)

PEN TESTING METHODOLOGIES

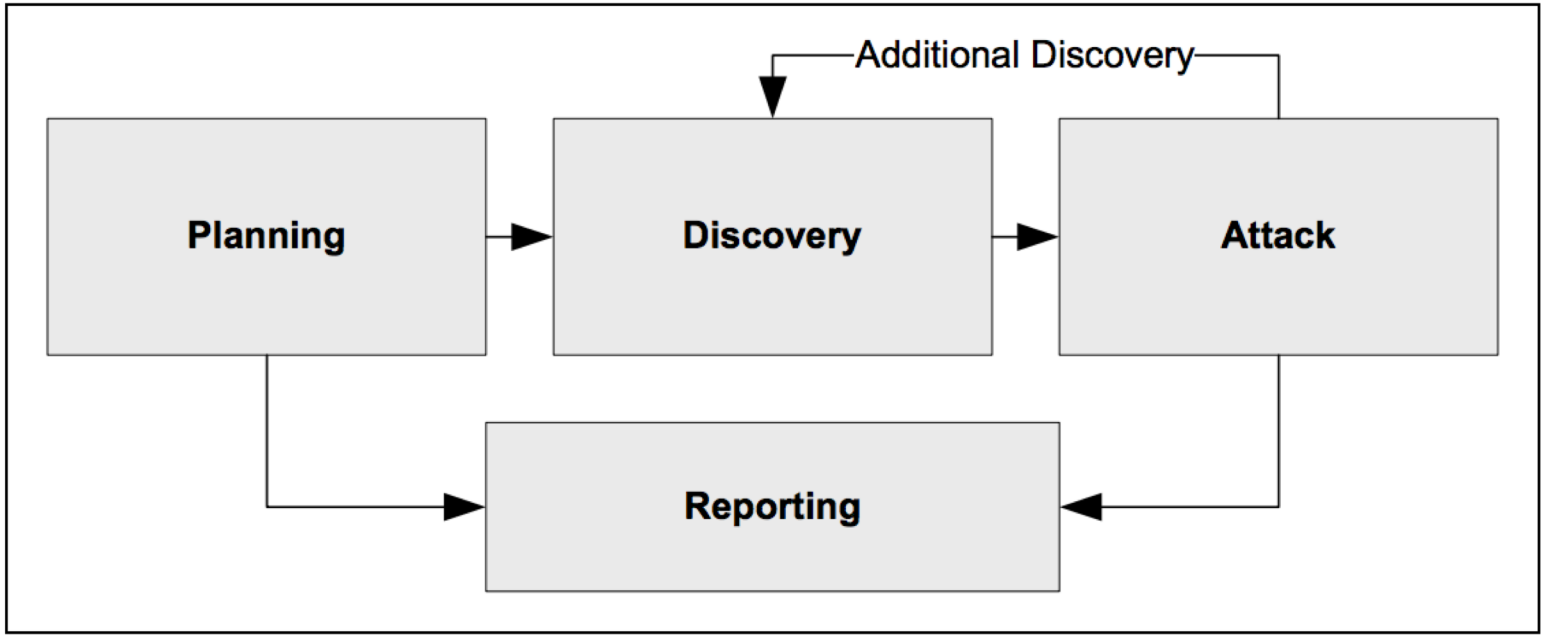
- Penetration Testing Execution Standard
  http://www.pentest-standard.org
- OWASP Testing Guide
  https://www.owasp.org/index.php/OWASP_Testing_Project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- Open Source Security Testing Methodology Manual (OSSTMM)
  http://www.isecom.org/research/

PEN TESTING LIFECYCLE



Aligned with: http://www.pentest-standard.org

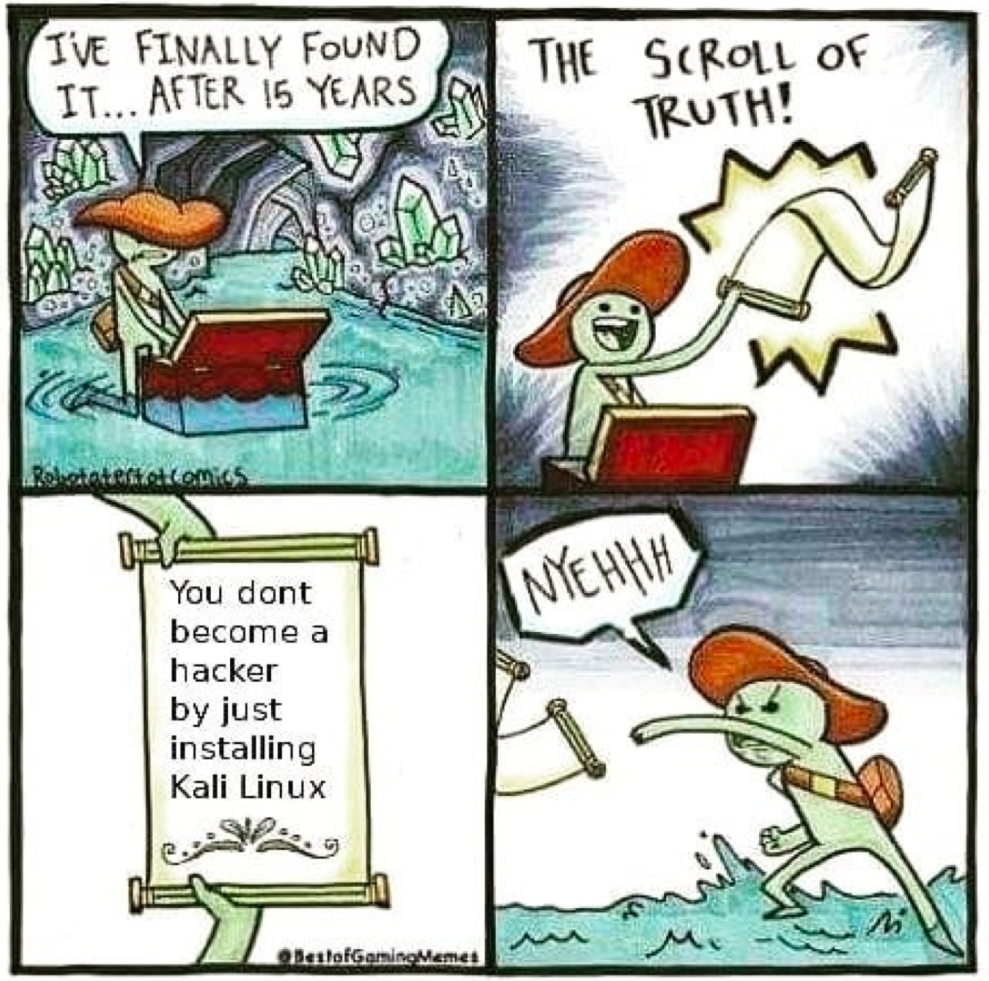
NIST 800-115



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

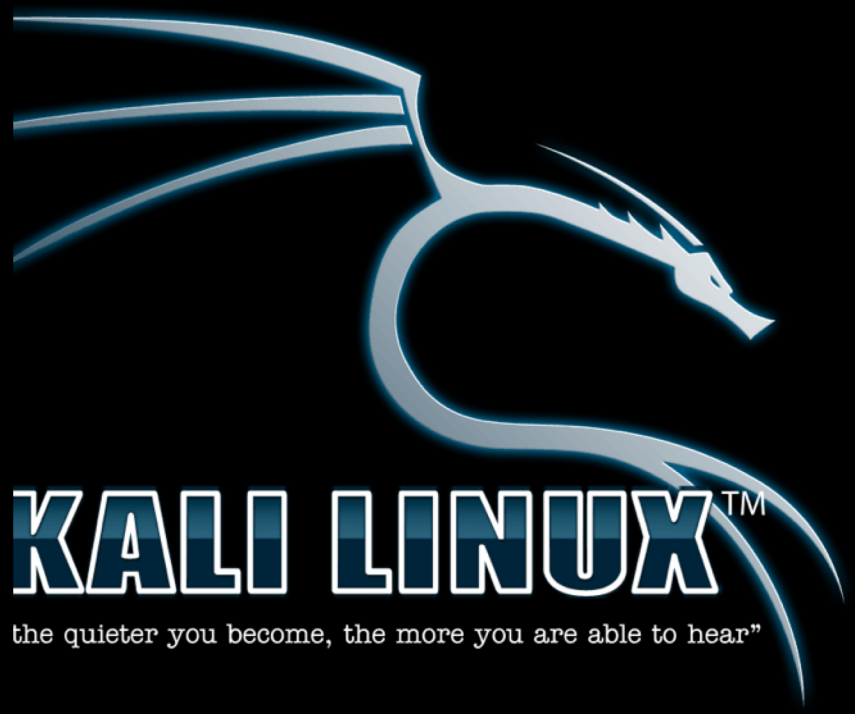
Penetration Testing Linux Distributions

Kali Linux

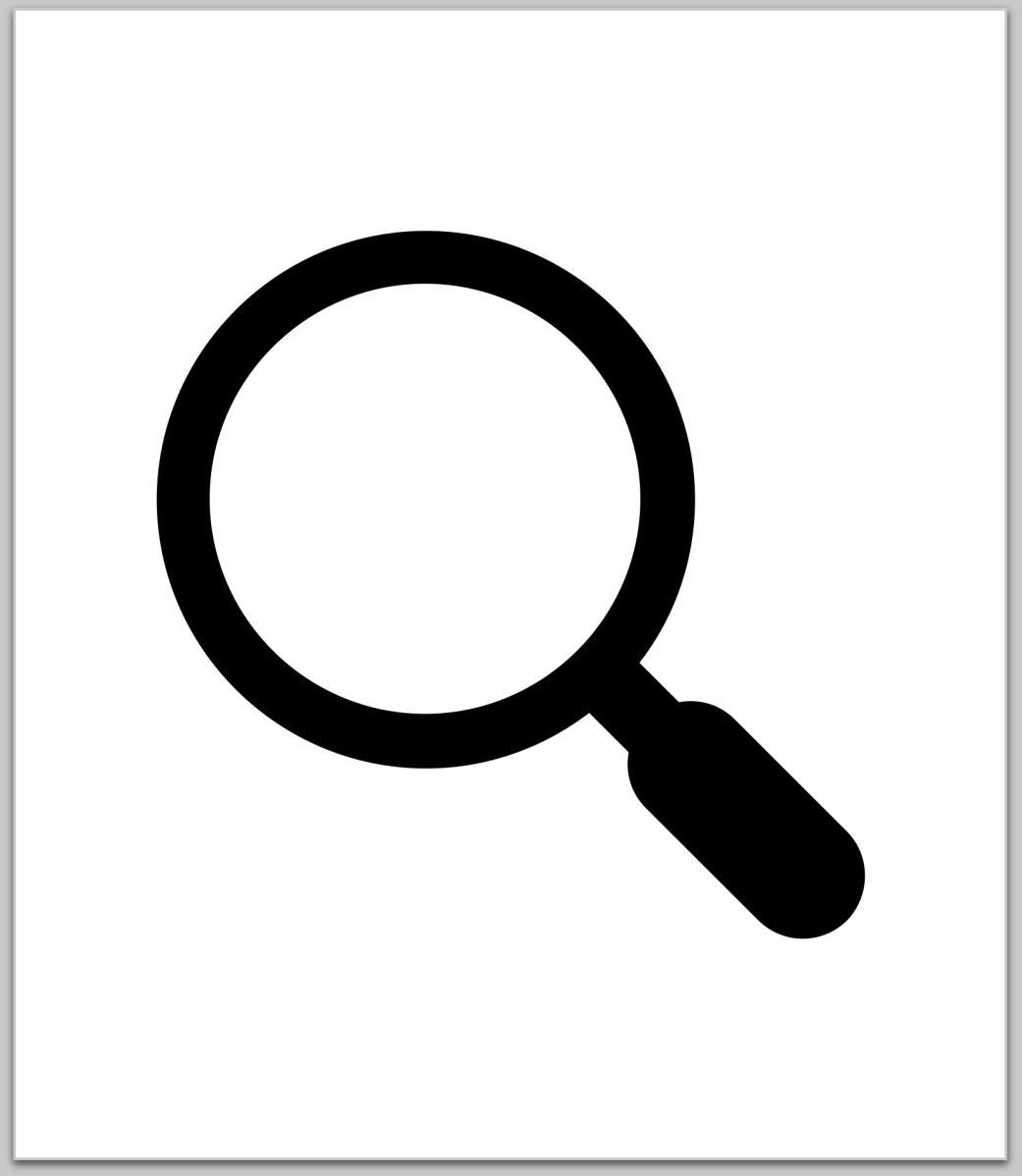

I'VE FINALLY FOUND IT... AFTER 15 YEARS
THE SCROLL OF TRUTH!
You dont become a hacker by just installing Kali Linux
NYEHHH
@BestofGamingMemes

Penetration Testing Linux Distributions

- Kali Linux: You can download Kali Linux from https://www.kali.org. Offensive Security released a free open source book and course about how to install, customize, and use Kali Linux. The book and the course can be accessed at https://kali.training.
- Parrot Security OS: You can download Parrot from https://www.parrotsec.org and access the documentation at https://docs.parrotsec.org.
- Black Arch: You can download BlackArch Linux from https://blackarch.org and access the documentation at https://blackarch.org/guide.html. BlackArch Linux source code can be accessed at https://github.com/BlackArch/blackarch.



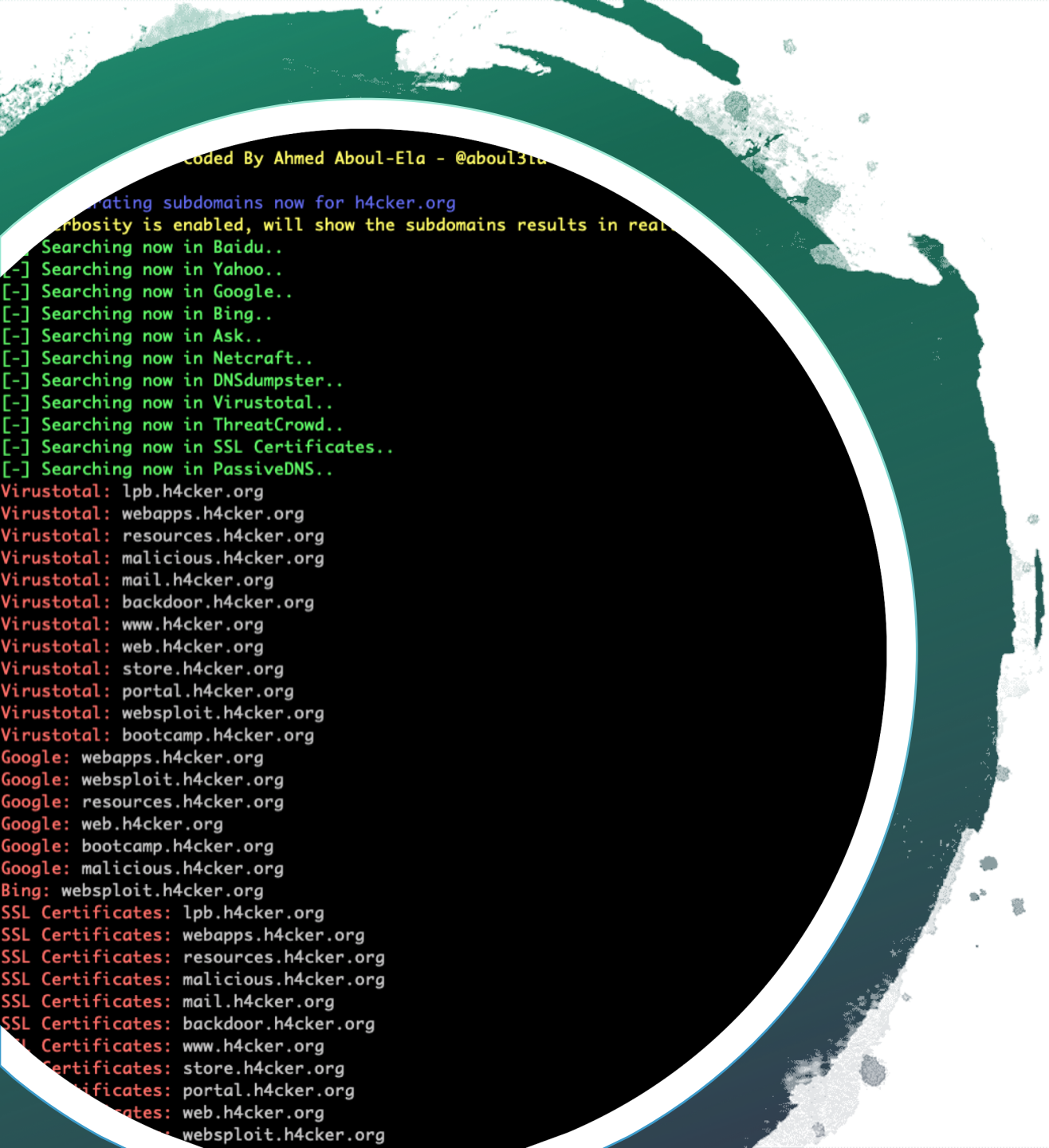
Exercise 1.0: Kali Linux Top Post Install Customizations and Tips



Passive Reconnaissance

Demos

- Google Hacking DB
- Shodan
- Recon NG
- Maltego
- SpiderFoot
- Sublist3r
- Buscador


Coded By Ahmed Aboul-Ela - @aboul3la
rating subdomains now for h4cker.org
rbosity is enabled, will show the subdomains results in real
Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Virustotal: lpb.h4cker.org
Virustotal: webapps.h4cker.org
Virustotal: resources.h4cker.org
Virustotal: malicious.h4cker.org
Virustotal: mail.h4cker.org
Virustotal: backdoor.h4cker.org
Virustotal: www.h4cker.org
Virustotal: web.h4cker.org
Virustotal: store.h4cker.org
Virustotal: portal.h4cker.org
Virustotal: websploit.h4cker.org
Virustotal: bootcamp.h4cker.org
Google: webapps.h4cker.org
Google: websploit.h4cker.org
Google: resources.h4cker.org
Google: web.h4cker.org
Google: bootcamp.h4cker.org
Google: malicious.h4cker.org
Bing: websploit.h4cker.org
SSL Certificates: lpb.h4cker.org
SSL Certificates: webapps.h4cker.org
SSL Certificates: resources.h4cker.org
SSL Certificates: malicious.h4cker.org
SSL Certificates: mail.h4cker.org
SSL Certificates: backdoor.h4cker.org
Certificates: www.h4cker.org
Certificates: store.h4cker.org
ificates: portal.h4cker.org
ates: web.h4cker.org
websploit.h4cker.org

Sublist3r

Complete Exercises 2.1, 2.2, 2.3, and optionally 2.4 (you can do 2.4 in your own time)

BREAK

10 MINUTES

Don’t forget about the resources at: https://h4cker.org

Active Reconnaissance

Demos and Explanations

- Netdiscover
- Nmap
- Zenmap
- Commercial Scanners
- OpenVAS

Exercise 3.1: Netdiscover

Exercise 3.2: Nmap

Python and Nmap

python™

3. root@kali: ~ (ssh)

```
root@kali:~# cat congrats
```

YOU HAVE COMPLETED DAY 1!

TOMORROW YOU
WILL RECEIVE
ANOTHER LAB GUIDE
AND A SEPARATE
SET OF SLIDES.

```
root@kali:~#
```

Thank you!

Don’t forget about the additional resources at:
https://h4cker.org