Ethical Hacking Bootcamp with Hands-on Labs (Day 3)

Omar Santos
Twitter: @santosomar

What we covered on day 1…

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

What we covered yesterday…

- 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.

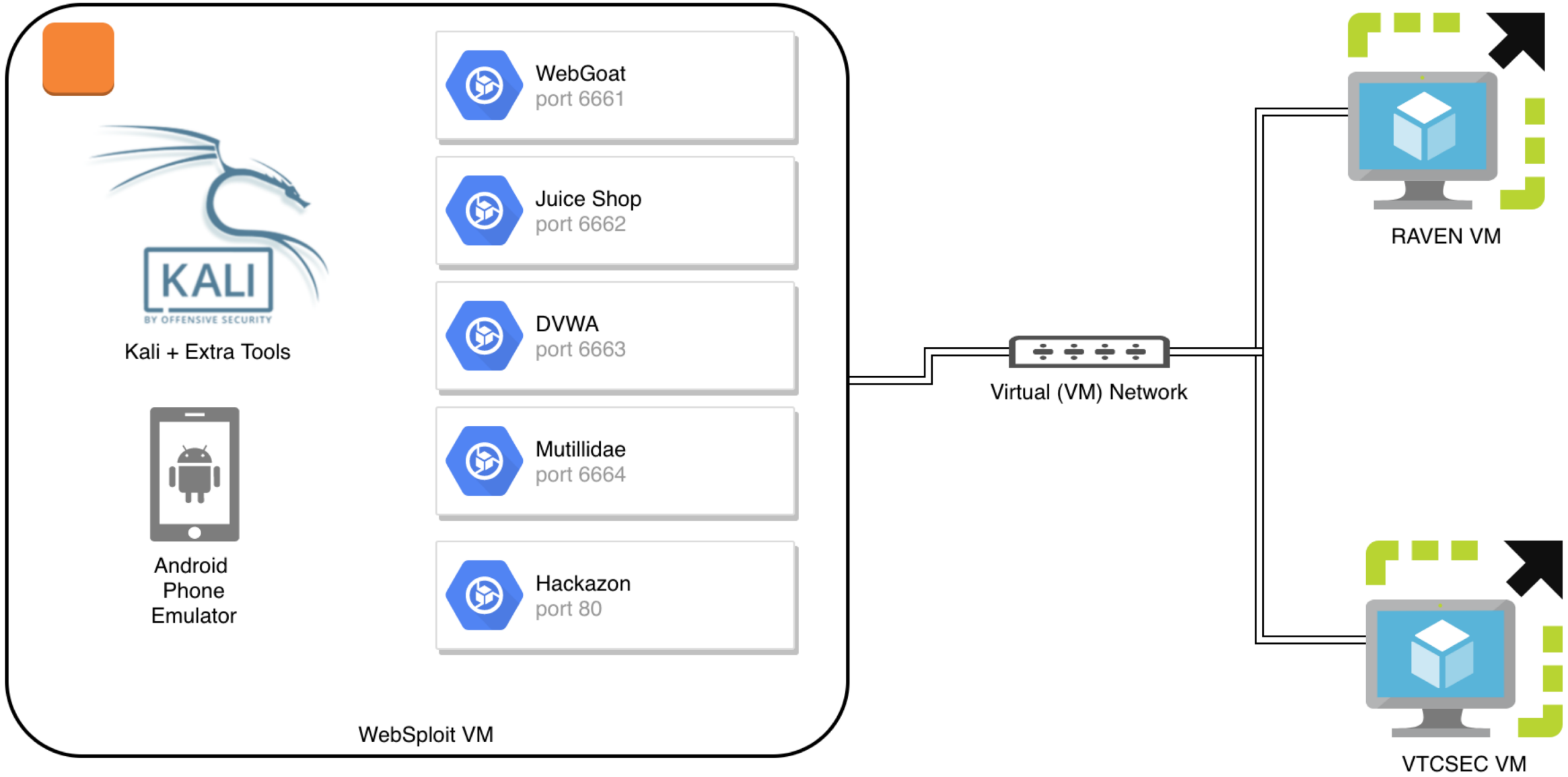
RESOURCES FOR THIS CLASS

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

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

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

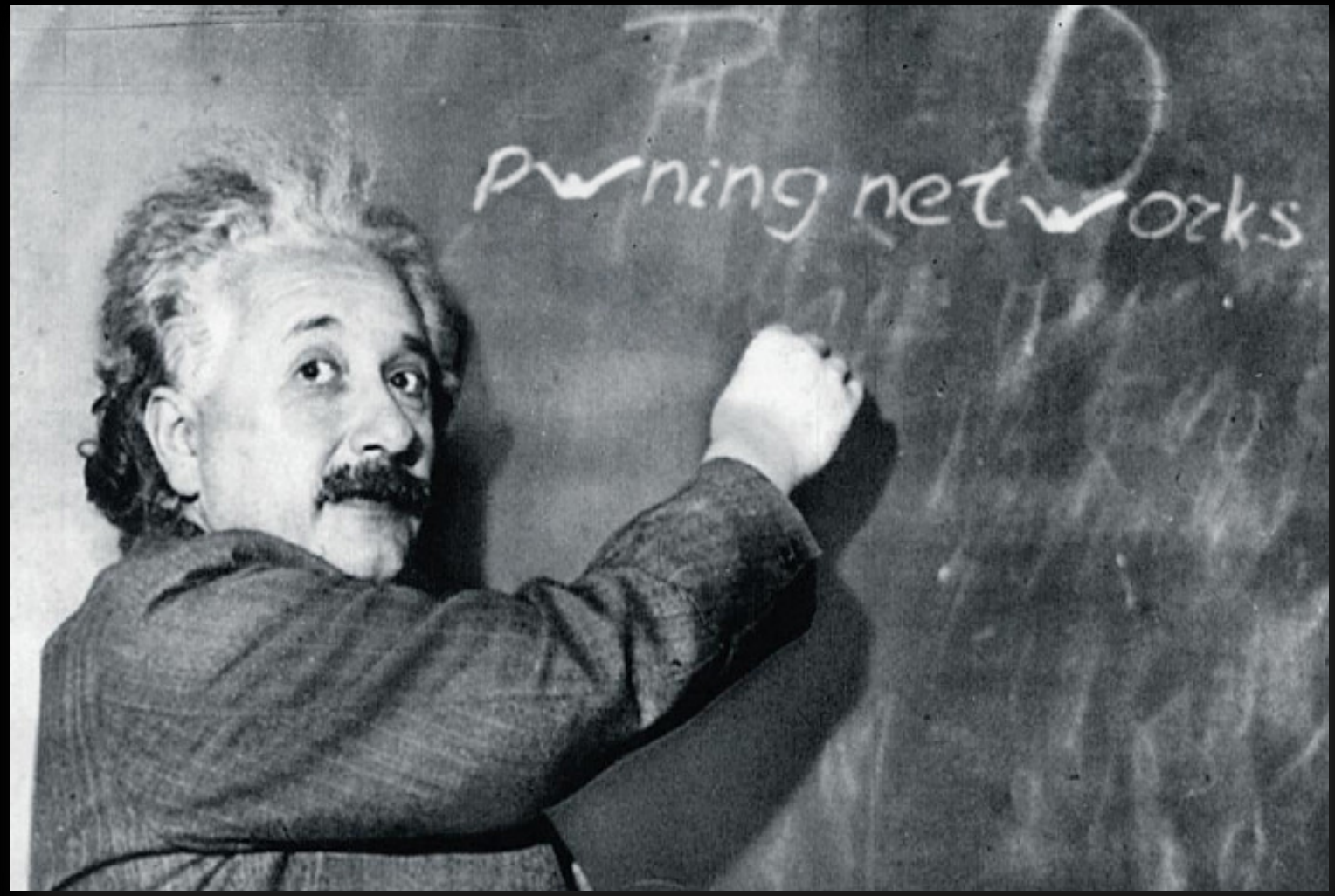
VM Lab and Setup


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

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)

Introduction to Hacking Networking Devices

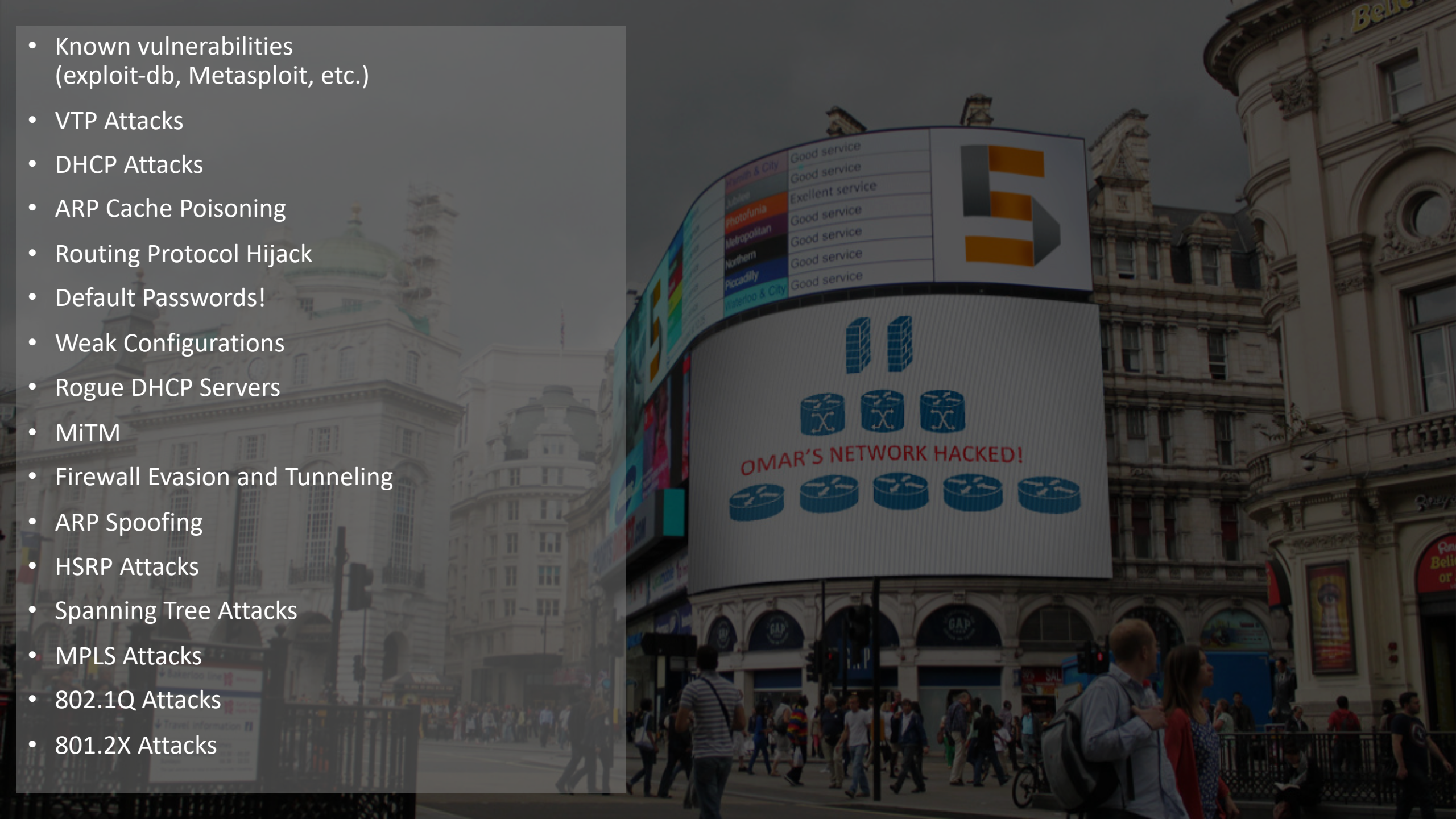


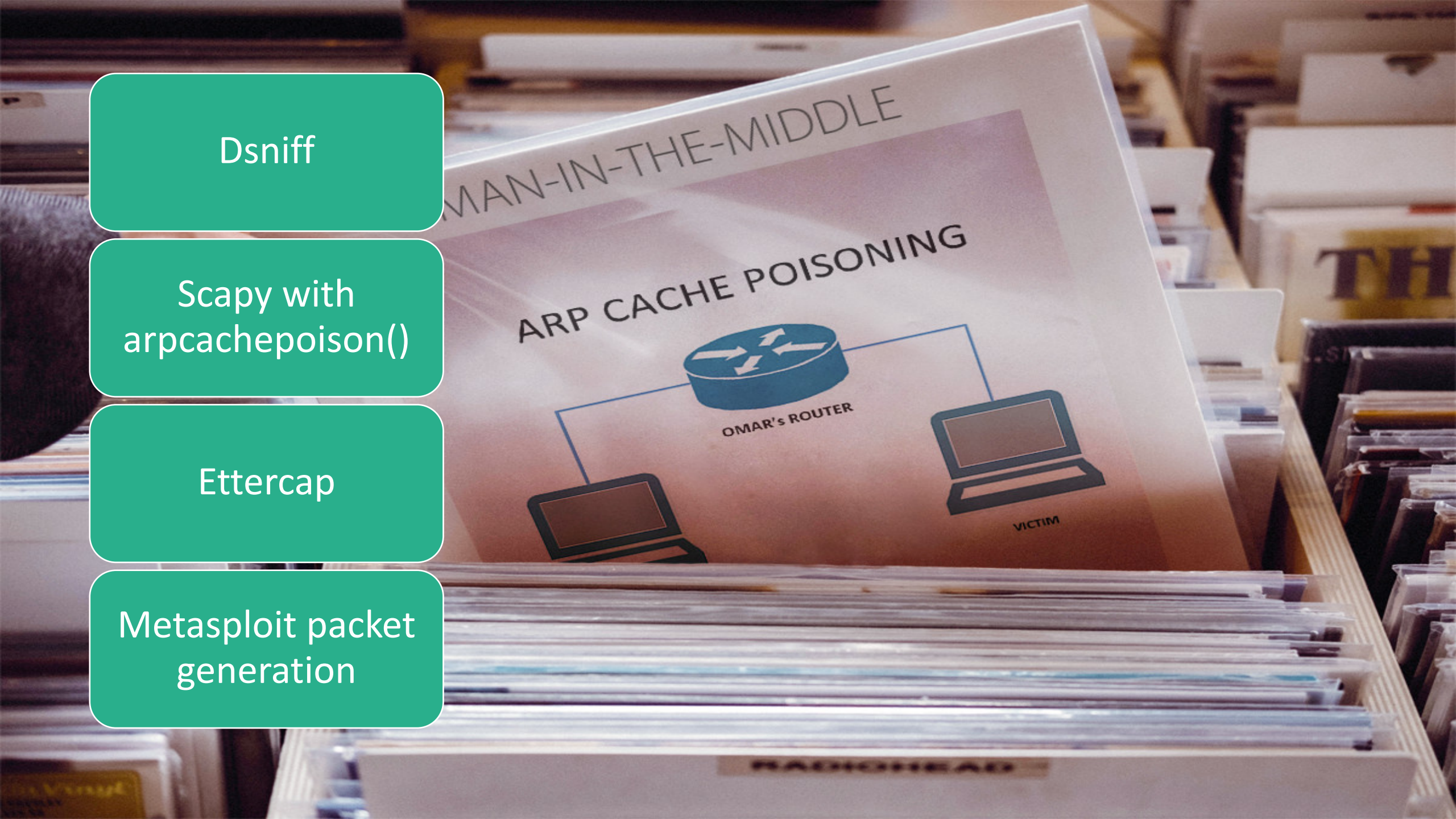
Why Hack Network Devices?

- Used as stepping stones.
- Mass surveillance.
- Sometimes not monitored as closed as your hosts.
- Longer system lifecycle.
- No malware detection.
- Sometimes running protocols designed back in the 80's.
- Take advantage of features like port mirroring, tunneling, lawful intercept to infiltrate and exfiltrate data.

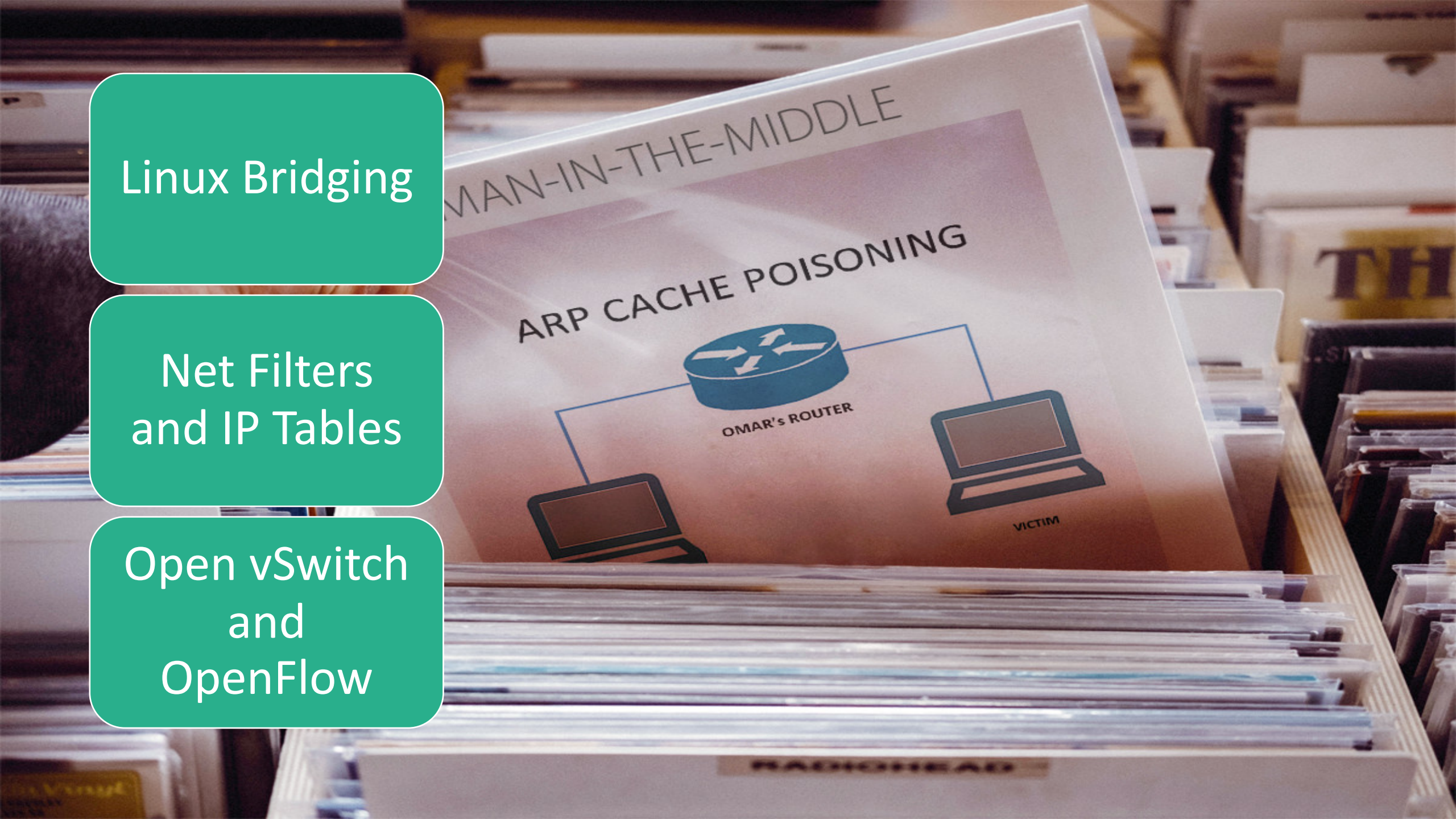
https://theartofhacking.org/go/hacking_networks.html

- Known vulnerabilities (exploit-db, Metasploit, etc.)
- VTP Attacks
- DHCP Attacks
- ARP Cache Poisoning
- Routing Protocol Hijack
- Default Passwords!
- Weak Configurations
- Rogue DHCP Servers
- MiTM
- Firewall Evasion and Tunneling
- ARP Spoofing
- HSRP Attacks
- Spanning Tree Attacks
- MPLS Attacks
- 802.1Q Attacks
- 801.2X Attacks





- Dsniff
- Scapy with arpcachepoison()
- Ettercap
- Metasploit packet generation



Linux Bridging

Net Filters and IP Tables

Open vSwitch and OpenFlow

How can I detect Omar’s firewall?

- ICMP
- TRACEROUTE

How can I bypass Omar’s firewall?

- TCP TRACEROUTE
- IODINE
- Corkscrew


Applications
Places
Terminal
Sat 14:22
root@kali: ~/bo_example
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - VTP mode
[14:19:24]
Code Domain MD5 Iface Last seen
YERSINIA DEMO
Attack Panel
No DoS Description
0 sending VTP packet
1 X deleting all VTP vlans
2 X deleting one vlan
3 adding one vlan
4 X Catalyst zero day
Select attack to launch ('q' to quit)
Total Packets: 0
VTP Packets: 0
MAC Spoofing [X]
Those strange attacks...
VTP Fields
Source MAC 02:C2:DC:7F:8E:F3 Destination MAC 01:00:0C:CC:CC:CC
Version 01 Code 03 Domain
MD5 00000000000000000000000000000000 Updater 010.013.058.001
Revision 0000000001 Timestamp Start value 00001
Followers 001 Sequence 001


WIRELESS HACKING
Fundamentals

Rogue Access Points

Evil Twins

Attacking the Preferred Network List (PNL)

Cracking WEP

Cracking WPA and WPA2 PSKs

Additional Attacks Against WPA and WPA2 Networks

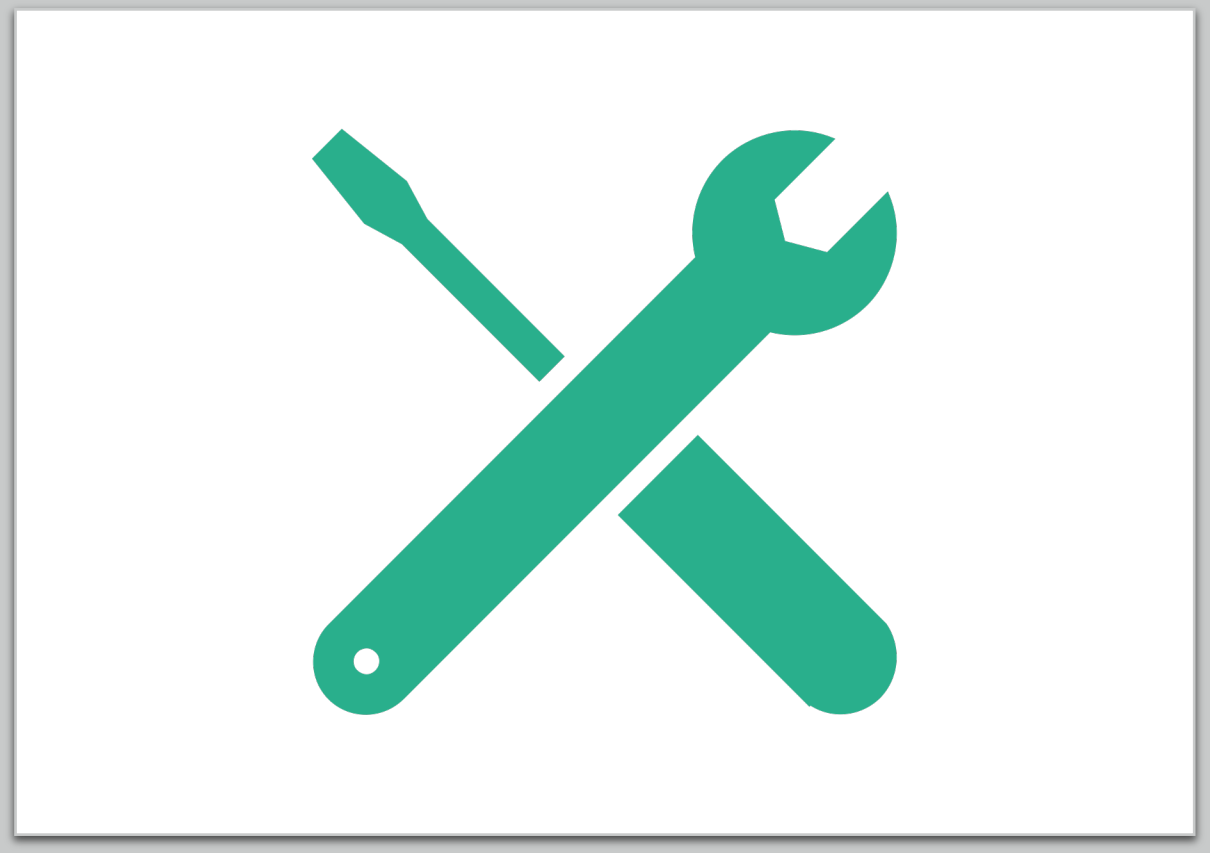
Free with Your Safari Subscription

BREAK

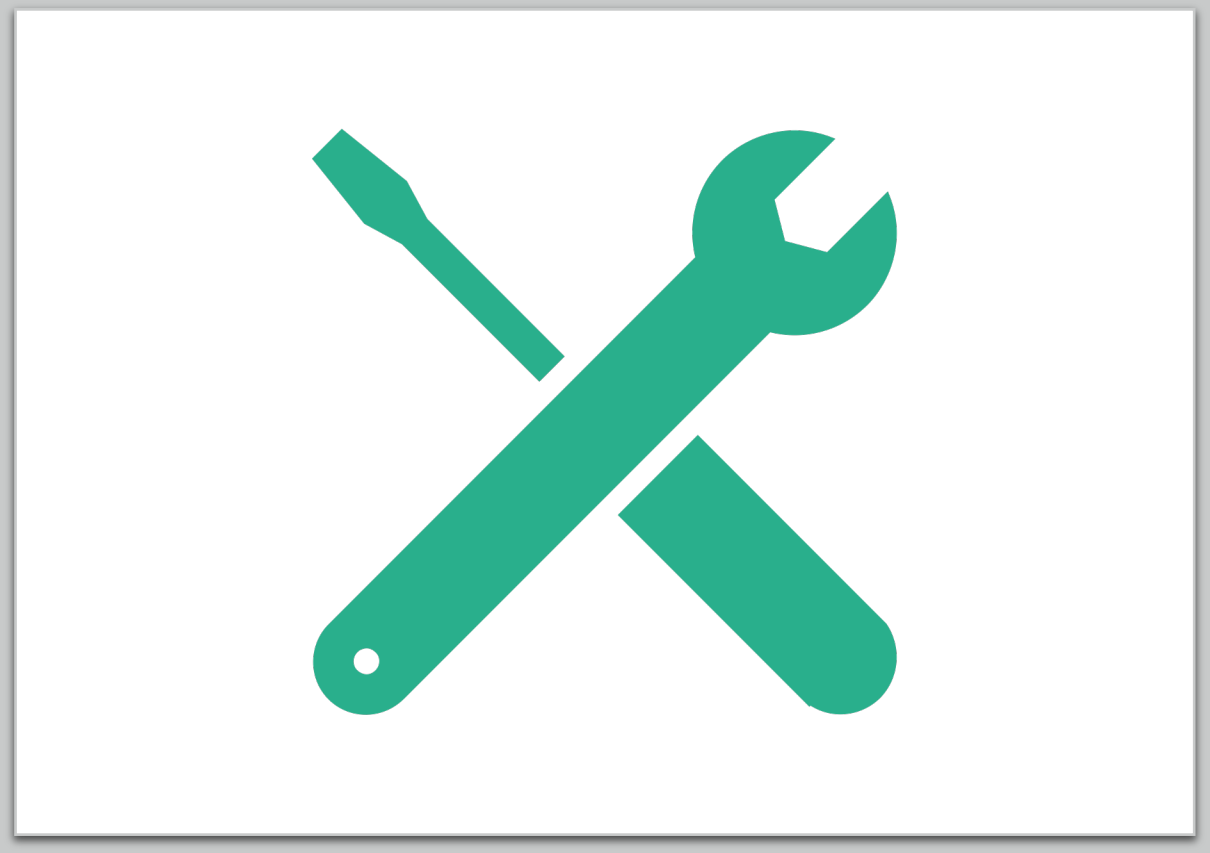
10 MINUTES

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

Password Attacks

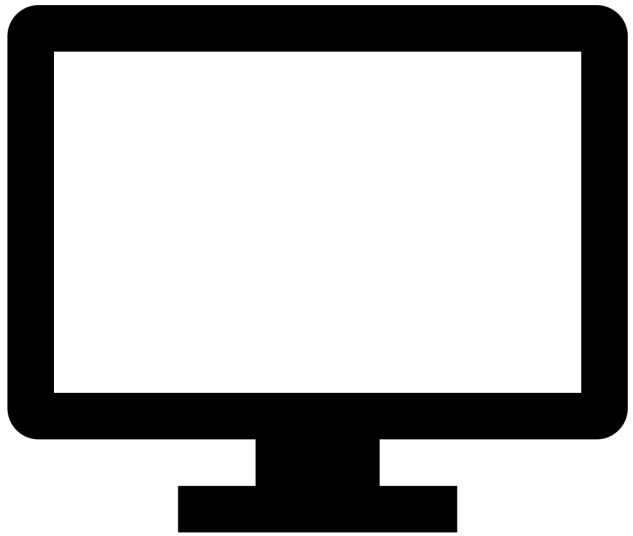


Exercise 1.1: Cracking Passwords with John the Ripper



Exercise 1.2: Cracking Passwords with Hashcat

DEMO: Cracking Passwords



Compromising the Raven VM

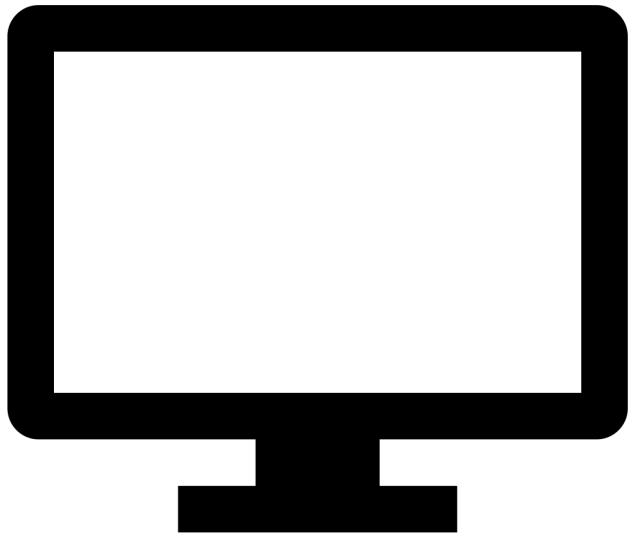
Complete Exercises 2.1 through 2.3

DEMO: Compromising the Raven VM

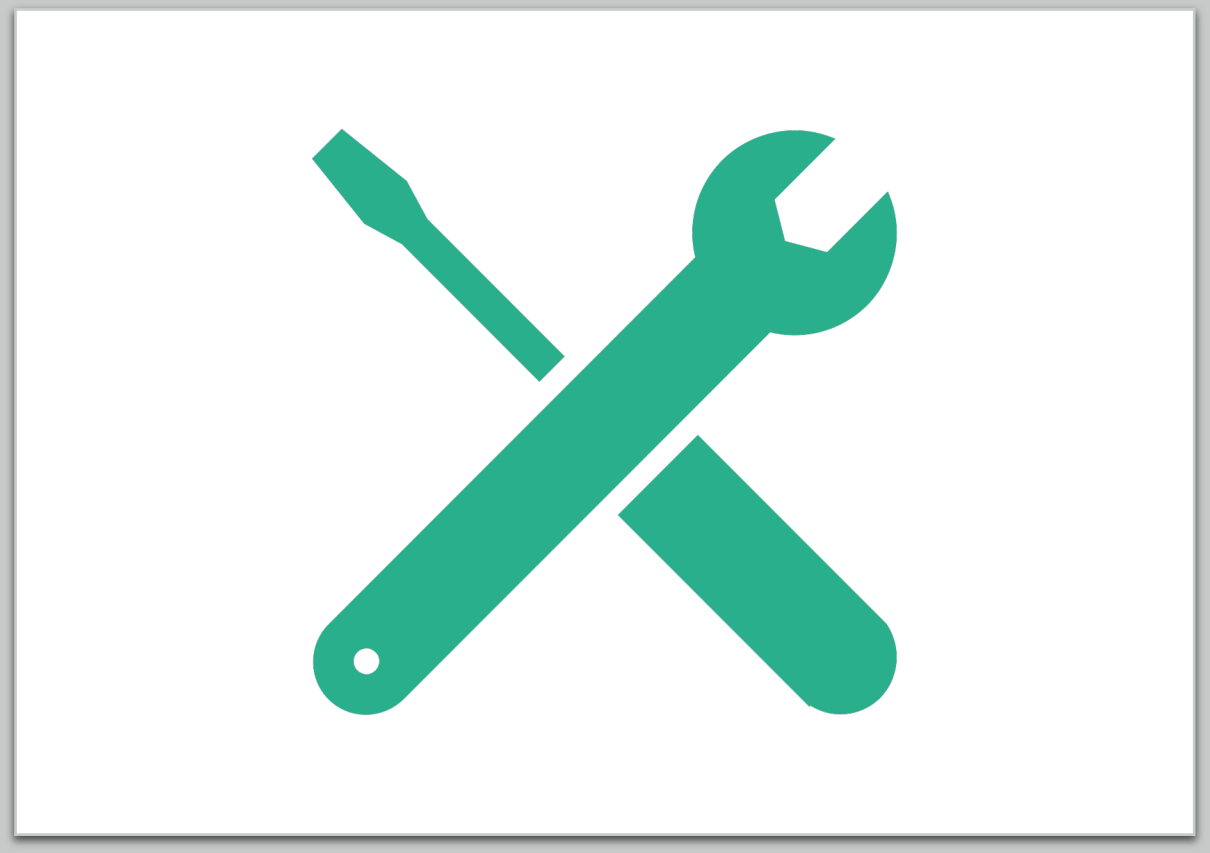
BREAK

10 MINUTES

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



Compromising the VTCSEC VM



Complete Exercises 3.1 through 3.4

DEMO: Compromising the VTCSEC VM

Thank you!

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