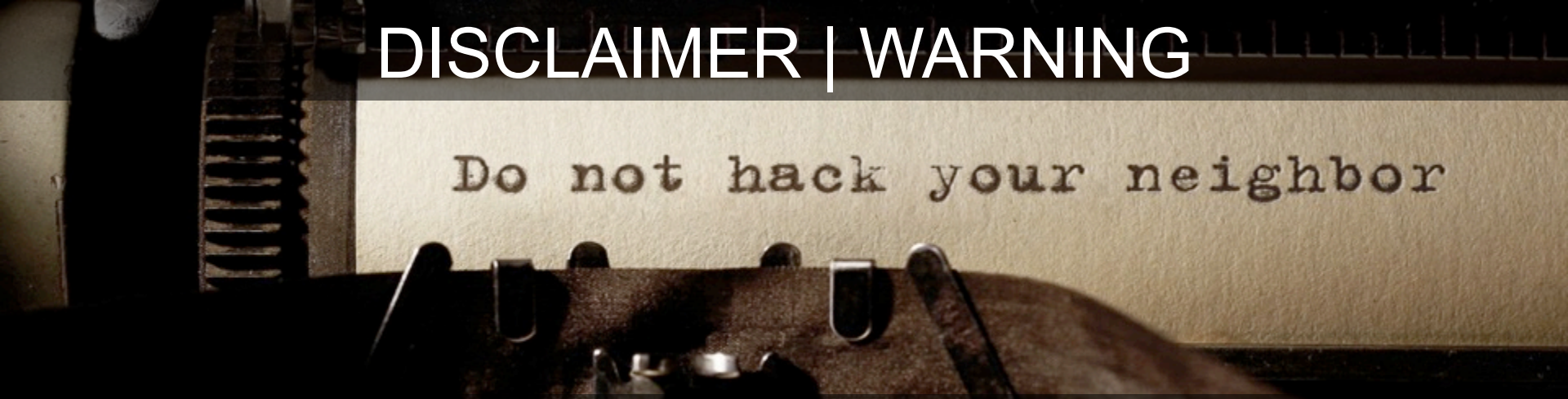
INTRODUCTION TO ETHICAL HACKING AND PENETRATION TESTING (DAY 2)

OMAR SANTOS
PRINCIPAL ENGINEER, PSIRT
SECURITY RESEARCH & OPERATIONS
CISCO SYSTEMS
Follow @santosomar


ETHICAL
THE ART OF
Hacking
Omar Santos
THEARTOFHACKING.ORG

Let’s Review…

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

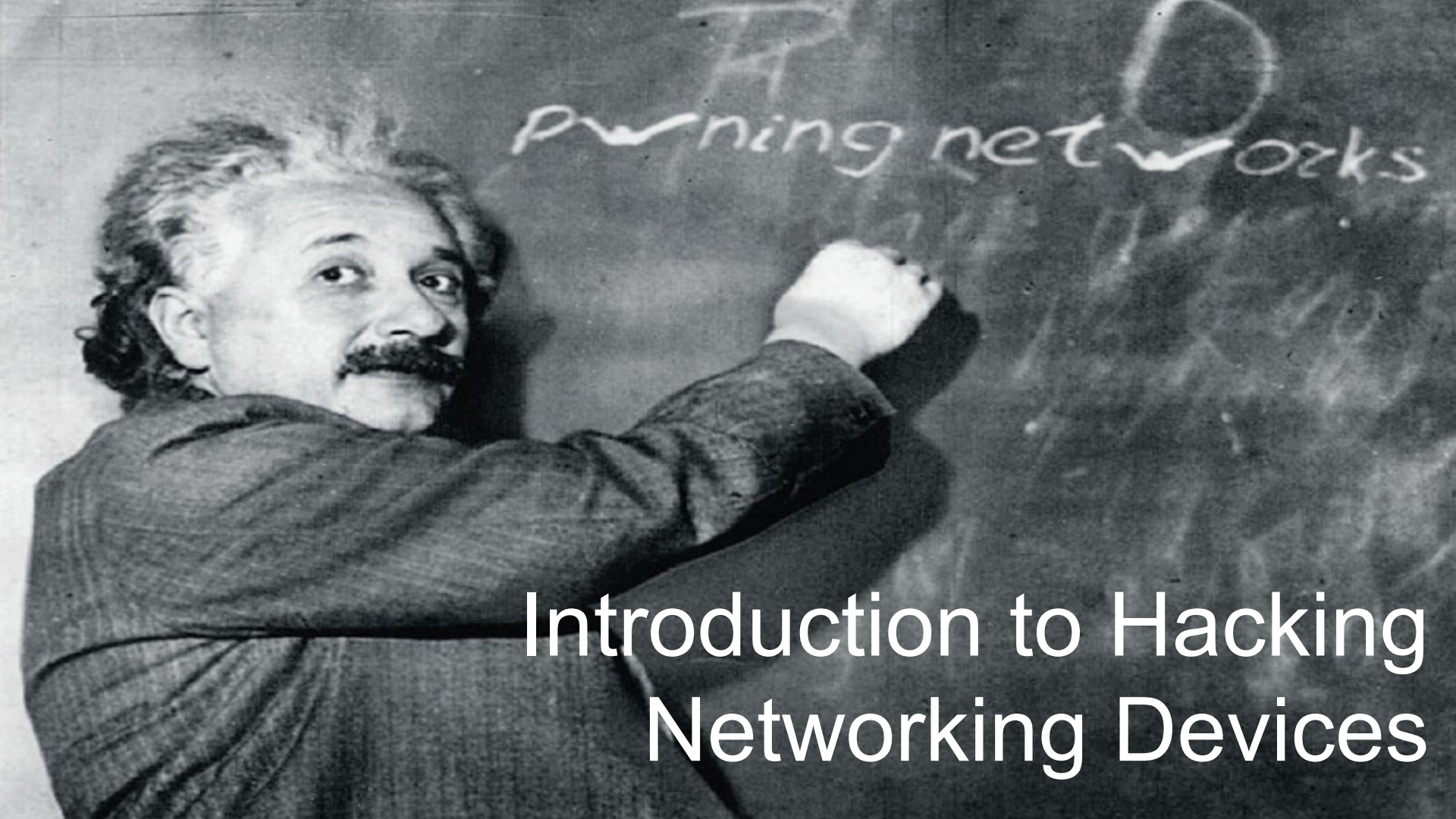
VIDEO COURSES IN SAFARI AND TONS OF REFERENCES

```
>> theartofhacking.org

>> theartofhacking.org/guide
```

EXERCISES AND LIVE TRAINING REFERENCES

- Introduction to Hacking Networking Devices
- Fundamentals of Wireless Hacking
- Introduction to Buffer Overflows
- Fundamentals of Evasion and Post Exploitation Techniques
- Introduction to Social Engineering
- How to Write Penetration Testing Reports



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

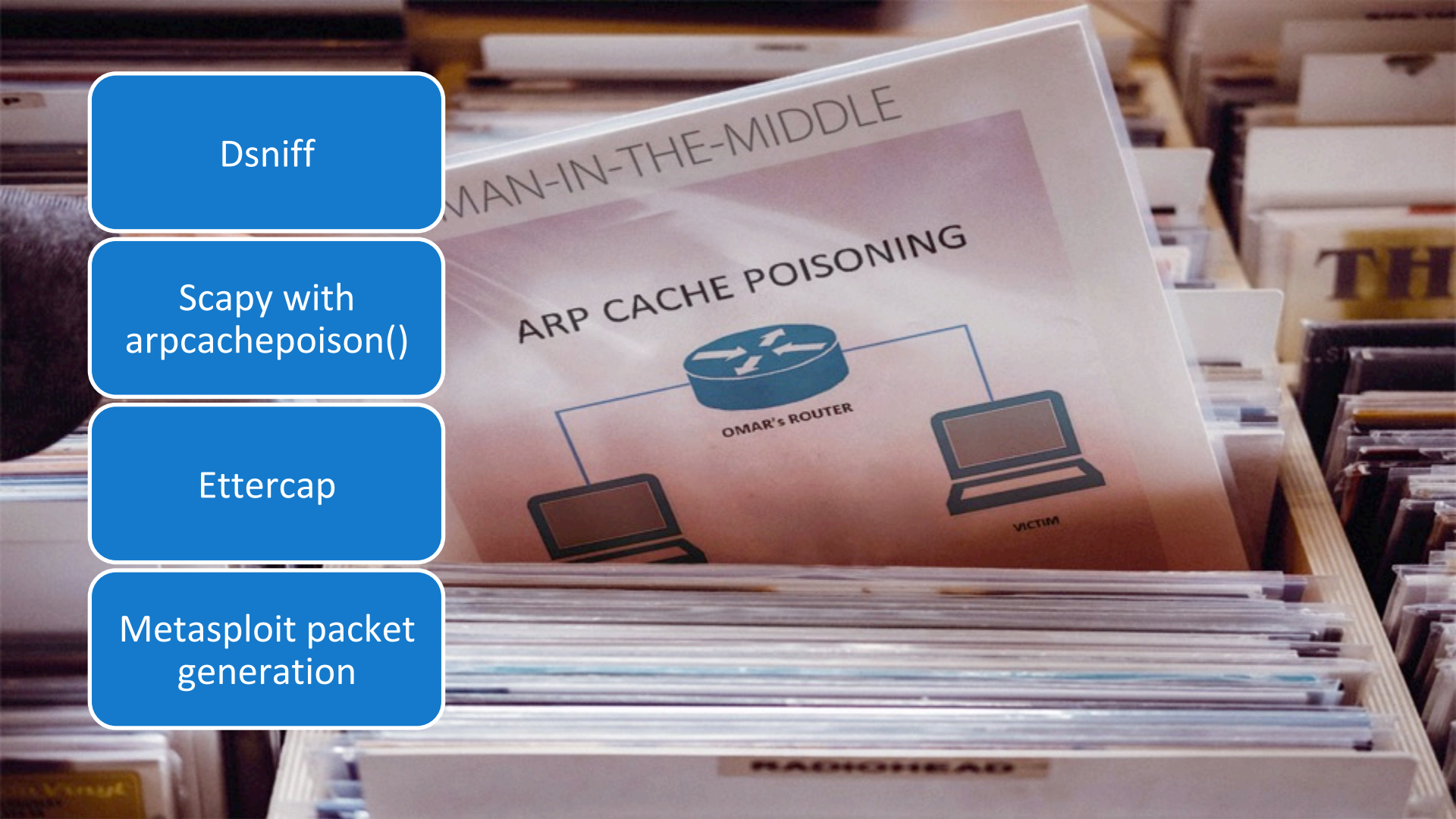
VIRL

- Virtual Internet Routing Lab Personal Edition
- Powerful network virtualization and orchestration platform that enables the development of highly accurate models of existing or planned networks.
- You can use it to learn network penetration testing too!

http://get.virl.info

Example Attacks:

- 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

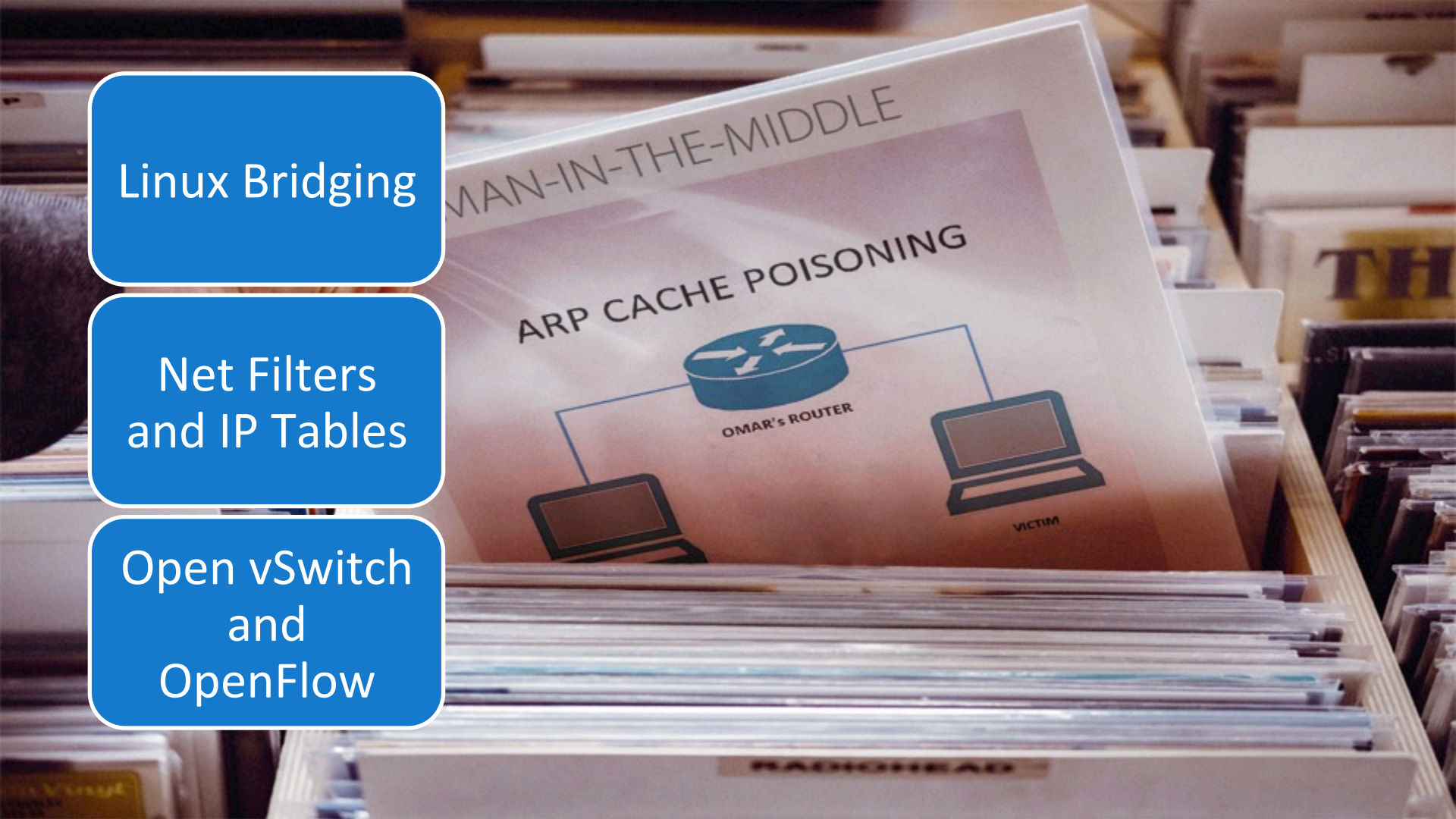


- Dsniff
- Scapy with arpcachepoison()
- Ettercap
- Metasploit packet generation

Linux Bridging

Net Filters and IP Tables

Open vSwitch and OpenFlow



How can I detect that Omar’s firewall?

- ICMP
- TRACEROUTE

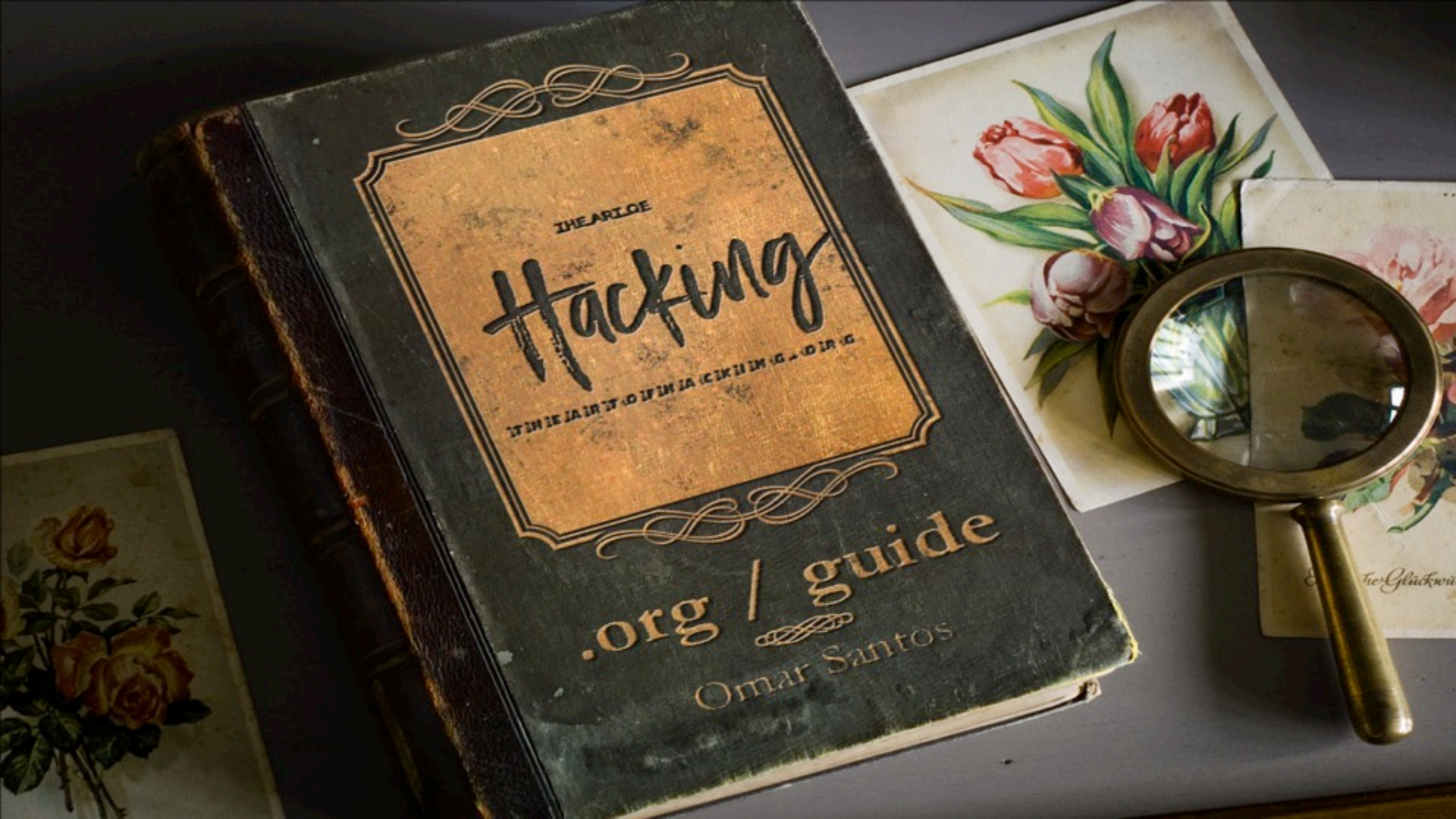
How can I bypass Omar’s firewall?

- TCP TRACEROUTE
- IODINE
- Corkscrew

DEMO


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

Fundamentals


Hacking
.org / guide
Omar Santos

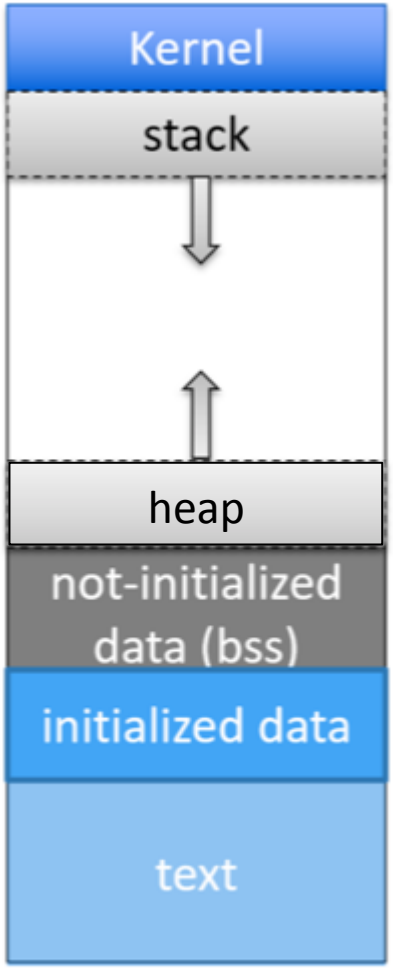
XXXX

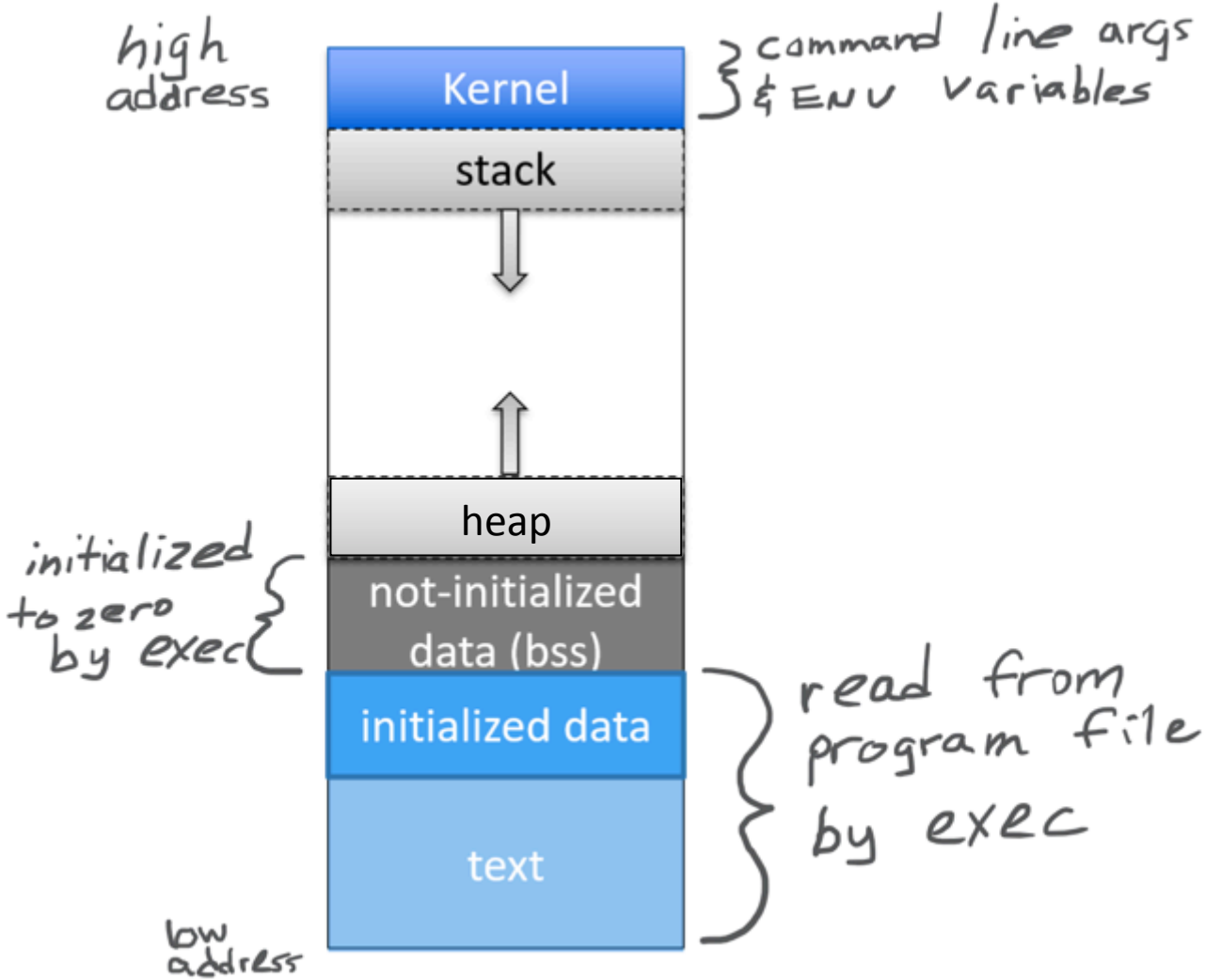
- Hacktivists are defined as group of hackers that hack into computer systems for a cause or purpose.
- The purpose may be political gain, freedom of speech, human rights, and so on.

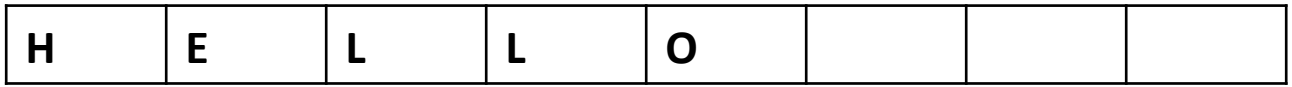
BREAK

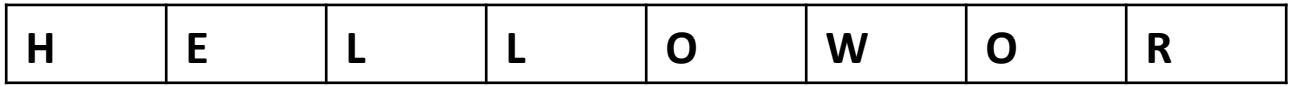
10 MINUTES

Introduction to Buffer

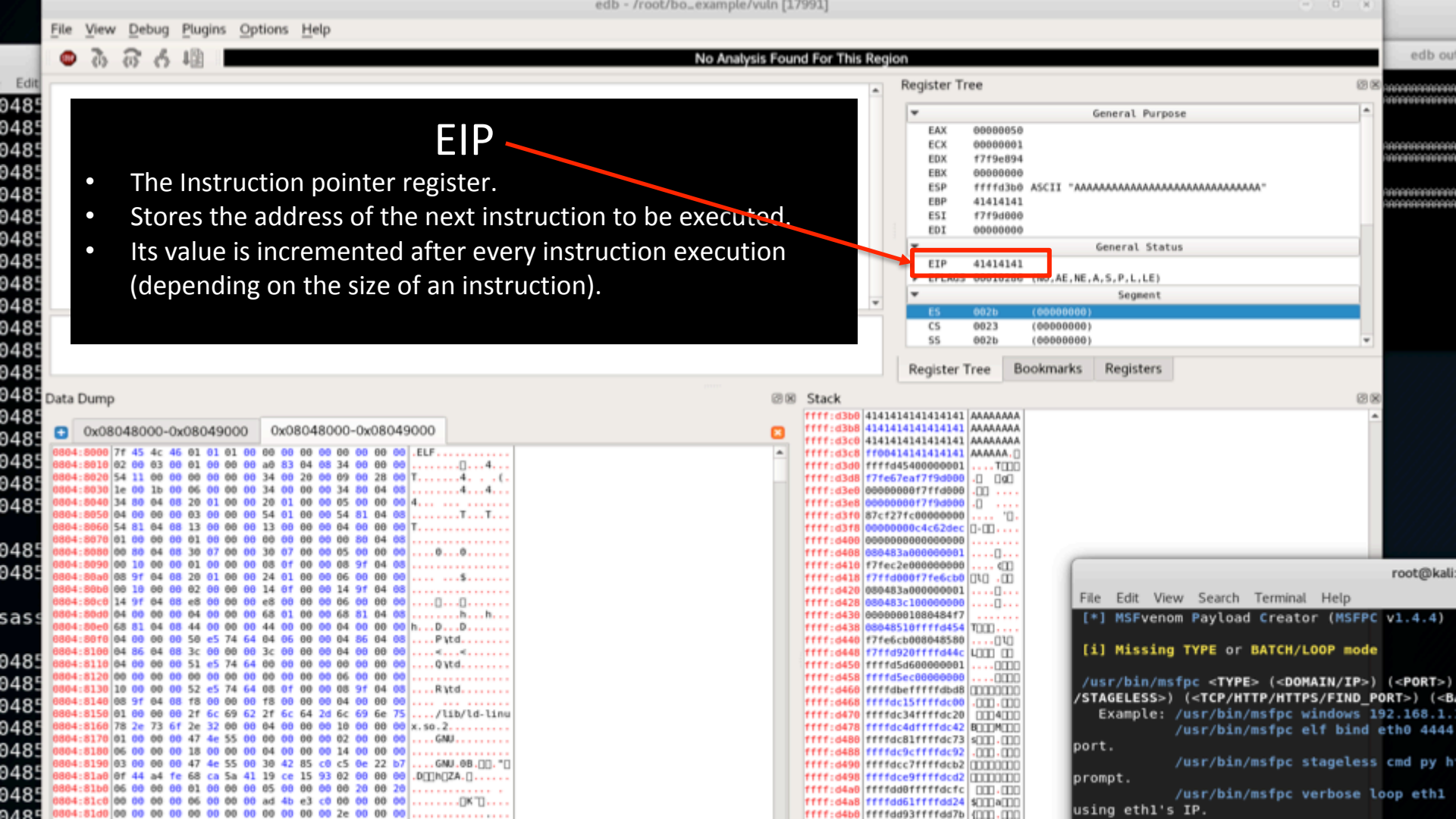

Kernel
stack
heap
not-initialized
data (bss)
initialized data
text


high address
Kernel
command line args & ENV variables
stack
heap
initialized to zero by exec
not-initialized data (bss)
initialized data
text
read from program file by exec
low address



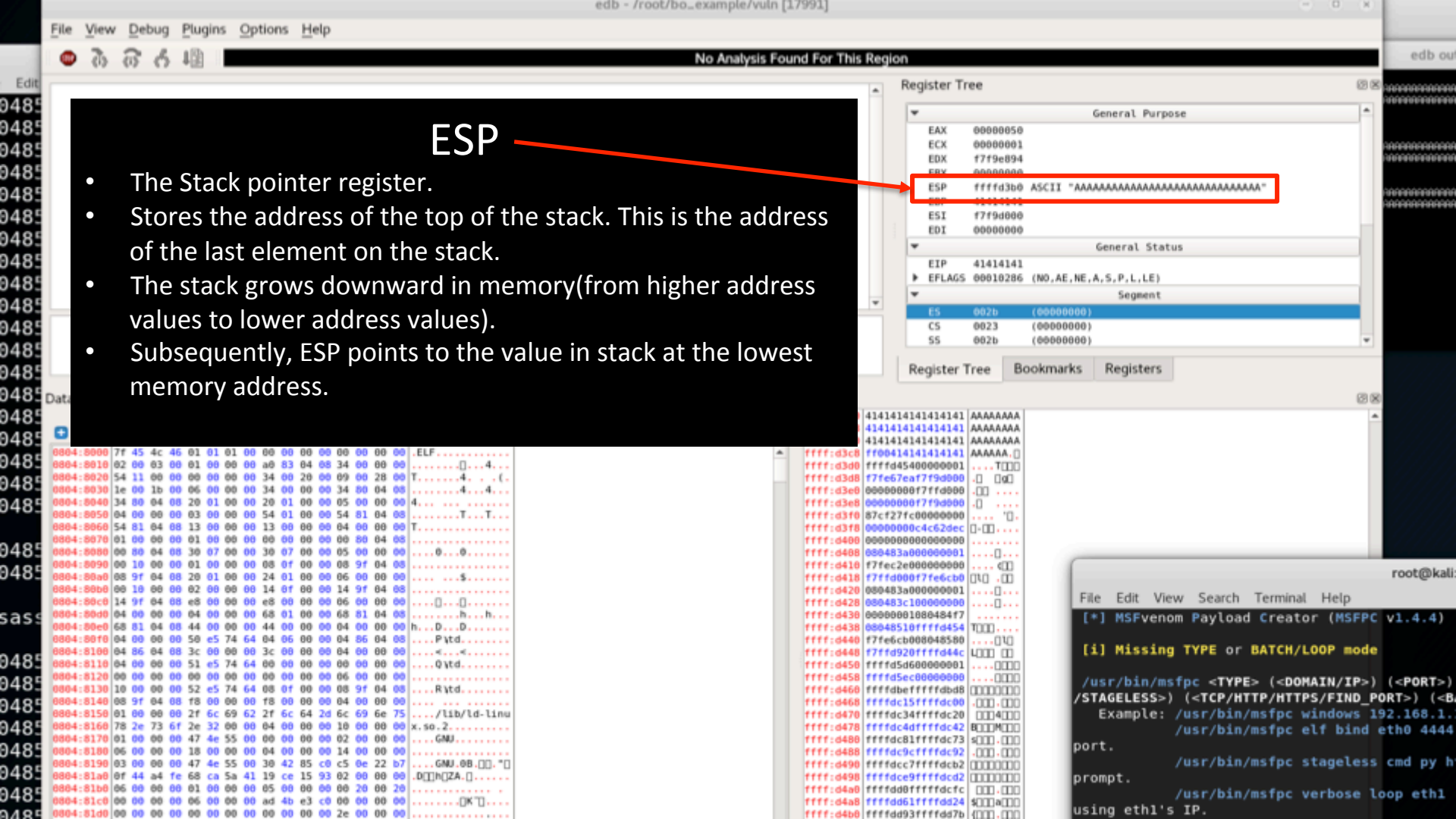


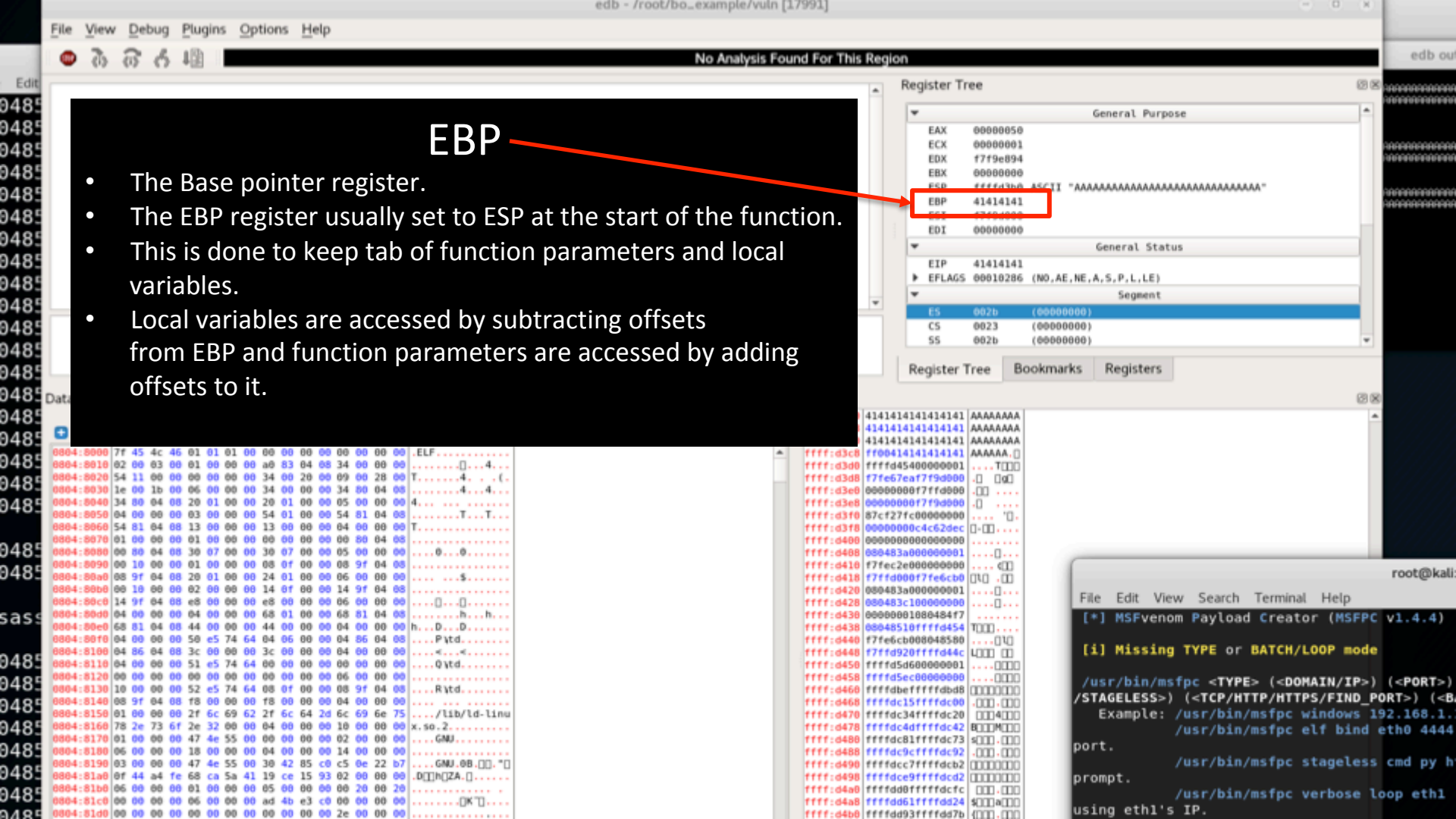
L D


EIP
The Instruction pointer register.
Stores the address of the next instruction to be executed.
Its value is incremented after every instruction execution (depending on the size of an instruction).
edb - /root/bo_example/vuln [17991]
File View Debug Plugins Options Help
No Analysis Found For This Region
Register Tree
General Purpose
EAX 00000050
ECX 00000001
EDX f7f9e894
EBX 00000000
ESP ffffd3b0 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EBP 41414141
ESI f7f9d000
EDI 00000000
General Status
EIP 41414141
Segment
ES 002b (00000000)
CS 0023 (00000000)
SS 002b (00000000)
Register Tree
Bookmarks
Registers
Data Dump
0x08048000-0x08049000
0x08048000-0x08049000
Stack
root@kali
File Edit View Search Terminal Help
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] Missing TYPE or BATCH/LOOP mode
/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>)
/STAGELESS>) (<TCP/HTTP/HTTPS/FIND_PORT>) (<B
Example: /usr/bin/msfpc windows 192.168.1.
/usr/bin/msfpc elf bind eth0 4444
port.
/usr/bin/msfpc stageless cmd py h
prompt.
/usr/bin/msfpc verbose loop eth1
using eth1's IP.

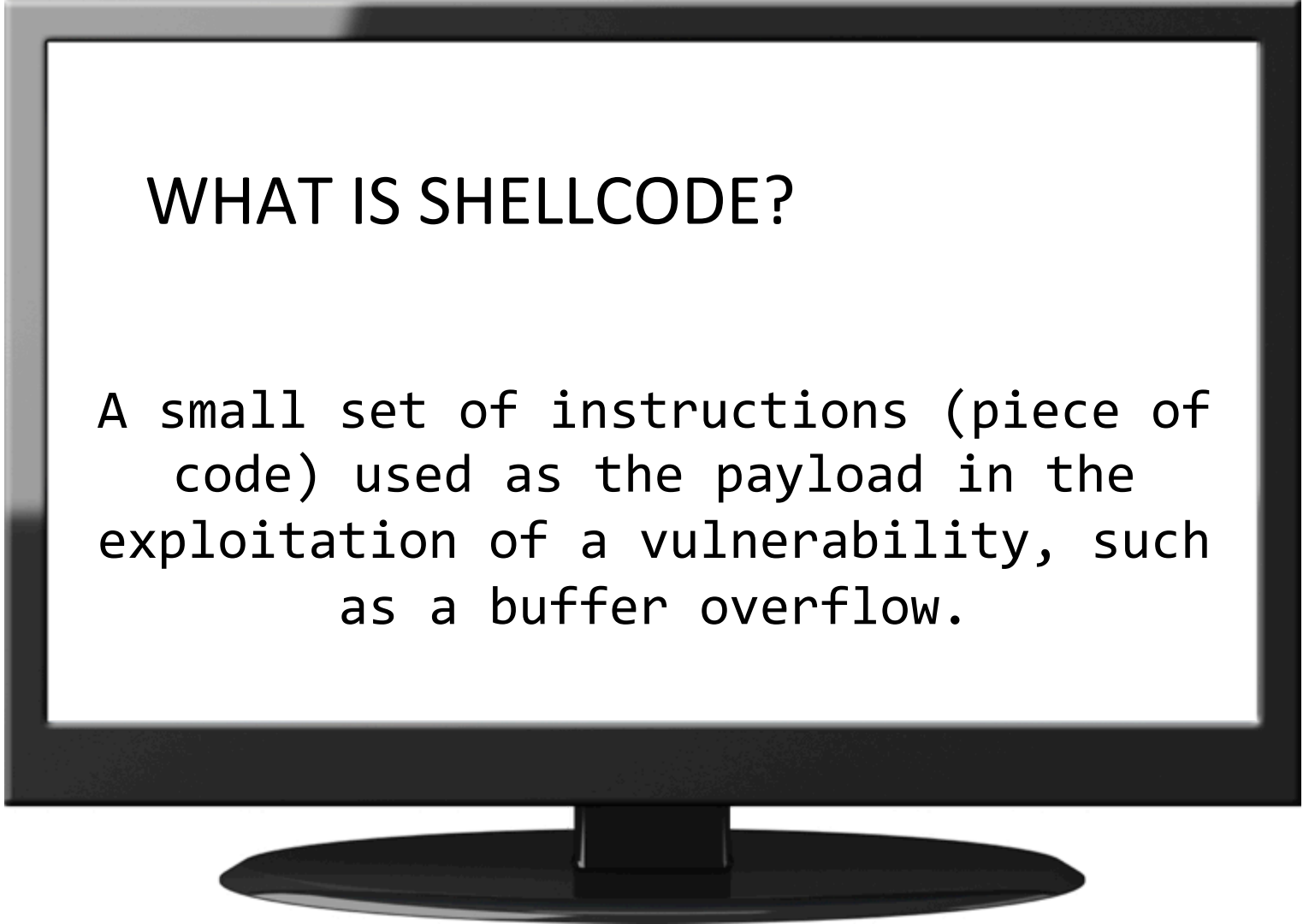
ESP

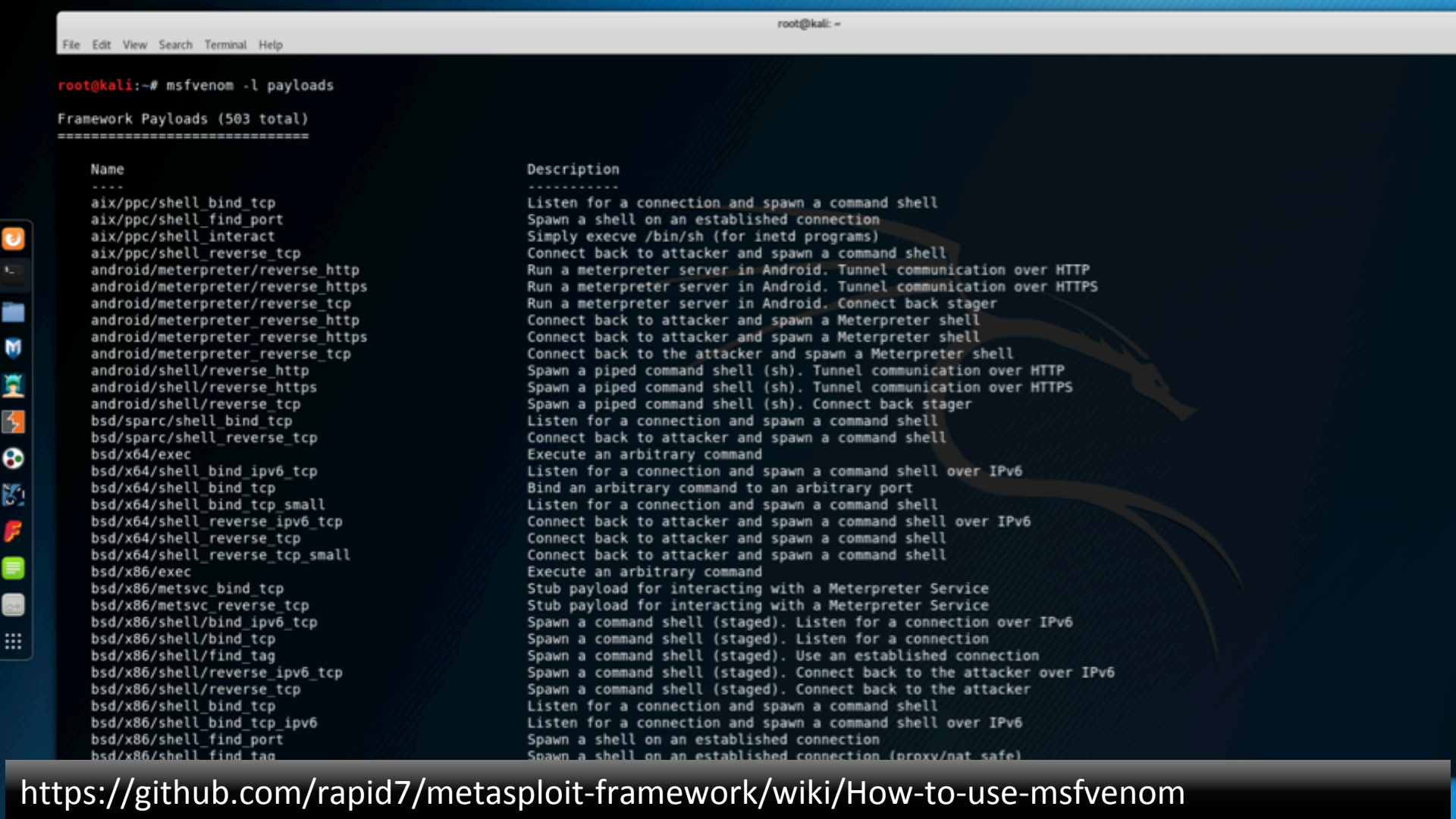
- The Stack pointer register.
- Stores the address of the top of the stack. This is the address of the last element on the stack.
- The stack grows downward in memory(from higher address values to lower address values).
- Subsequently, ESP points to the value in stack at the lowest memory address.




EBP
The Base pointer register.
The EBP register usually set to ESP at the start of the function.
This is done to keep tab of function parameters and local variables.
Local variables are accessed by subtracting offsets from EBP and function parameters are accessed by adding offsets to it.
File View Debug Plugins Options Help
No Analysis Found For This Region
Register Tree
General Purpose
EAX 00000050
ECX 00000001
EDX f7f9e894
EBX 00000000
EBP 41414141
EDI 00000000
General Status
EIP 41414141
EFLAGS 00010286 (NO,AE,NE,A,S,P,L,LE)
Segment
ES 002b (00000000)
CS 0023 (00000000)
SS 002b (00000000)
Register Tree
Bookmarks
Registers
root@kali
File Edit View Search Terminal Help
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] Missing TYPE or BATCH/LOOP mode
/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>)
Example: /usr/bin/msfpc windows 192.168.1.
/usr/bin/msfpc elf bind eth0 4444
/usr/bin/msfpc stageless cmd py h
/usr/bin/msfpc verbose loop eth1
using eth1's IP.


CINEMA
IN CINEMA TODAY
OMAR'S BUFFER
OVERFLOW DEMO


WHAT IS SHELLCODE?
A small set of instructions (piece of code) used as the payload in the exploitation of a vulnerability, such as a buffer overflow.



https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

https://www.offensive-security.com/metasploit-unleashed/msfpayload/

Fundamentals of Evasion and Post Exploitation Techniques

Evasion Techniques

Encryption & Obfuscation Demo Using the Eternalblue Exploit

Pivoting

Whiteboard Explanation

Pivoting

Meterpreter Demo

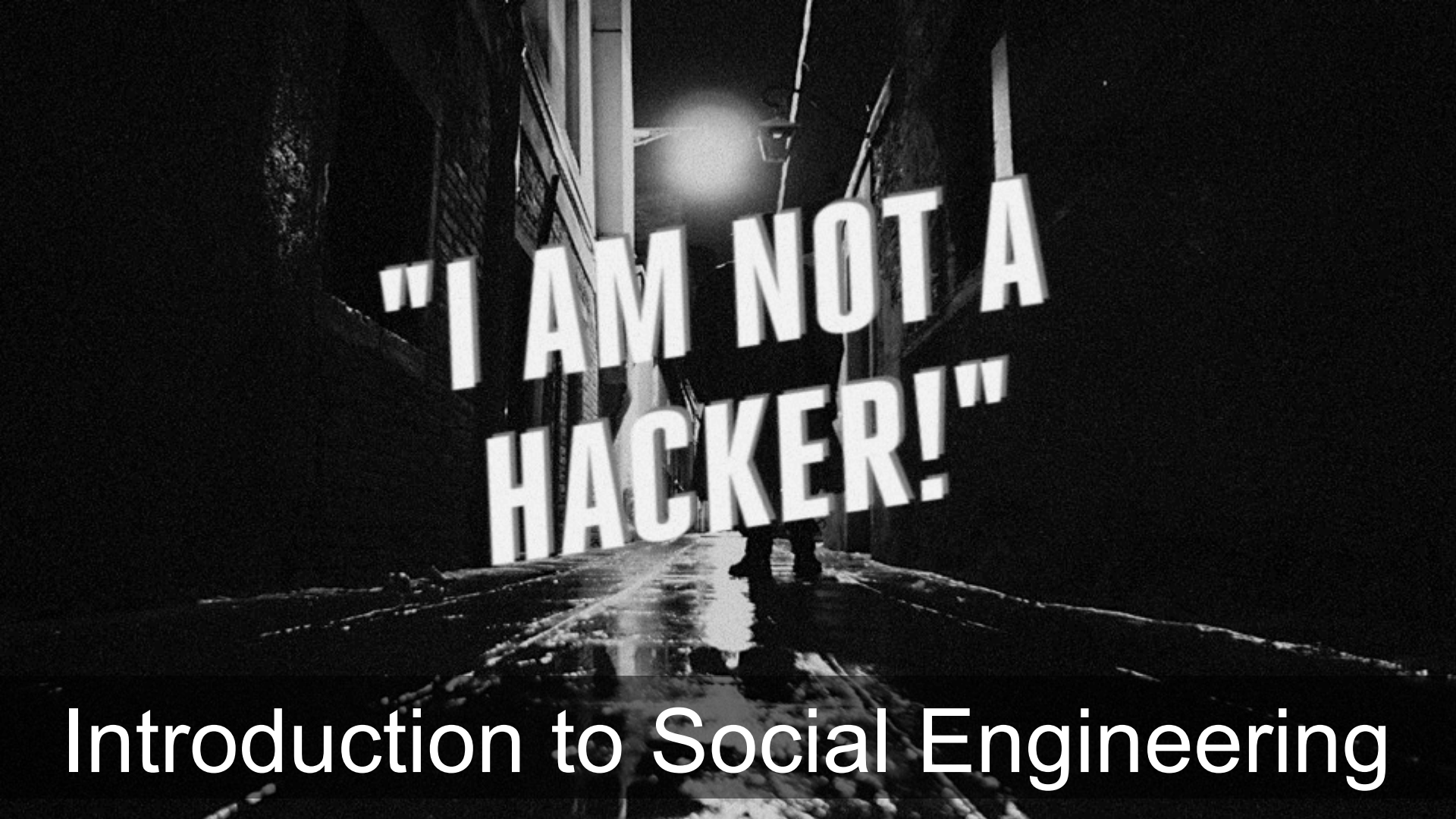
Exfil

egressbuster demo


Omar's
Demo & Whiteboard

BREAK

10 MINUTES

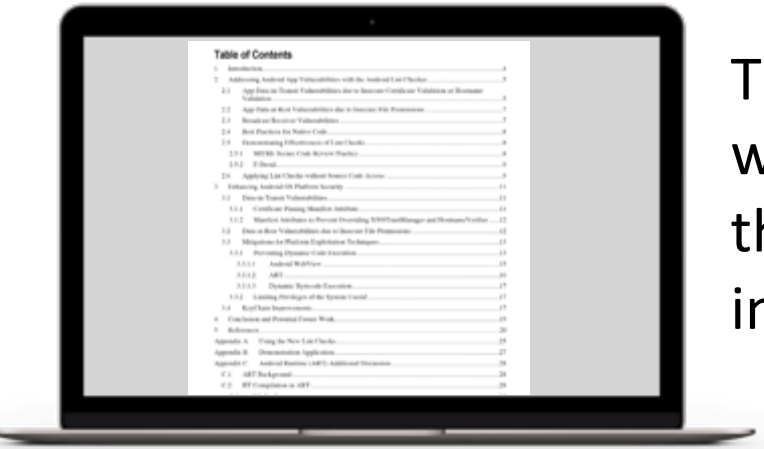


Introduction to Social Engineering


Omar's
Demo & Whiteboard

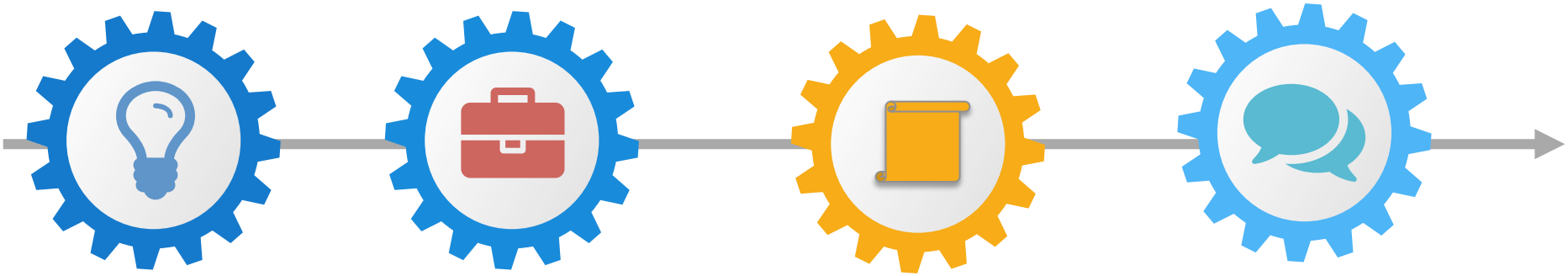
How to Write Penetration Testing Reports

The penetration testing report must be clear, detail the outcome of the tests, and in most cases include recommendations.



The audience will vary, executive summary will be read by the senior management and the technical details will be read by the IT or information security stakeholders.

Pen Testing Report Development Stages



Report Planning

Consider the target audiences

- Their need for the report (i.e. operational planning, resource allocation, approval),
- Position in the organization
- Knowledge of the report topic(i.e. purpose),
- Responsibility or authority to make decision based on the report, and
- Personal demographics (i.e. age, alliances, attitudes).

Report Planning

Report Classification

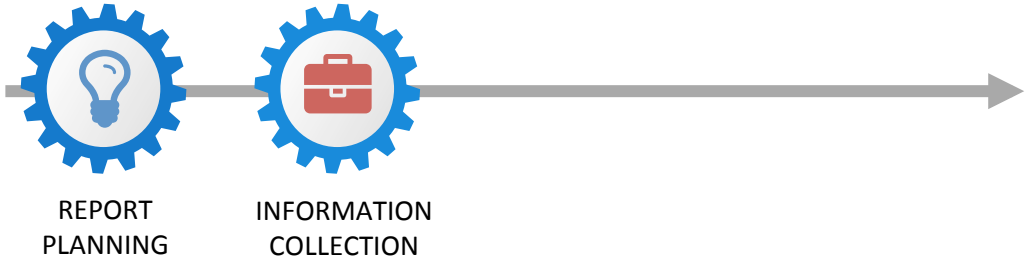
- Be aware of sensitive information
- The report classification should be based on the underlying organization’s information classification policy.

Report Planning

Report Distribution

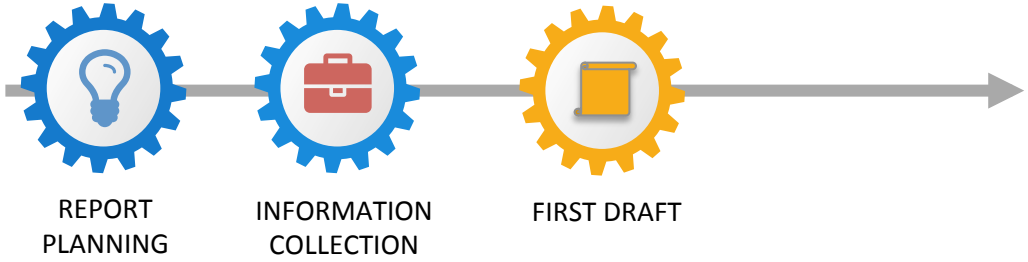
- The type of report delivery, recipients, number of copies and report distribution should be addressed in the scope of work.
- You should perform due diligence to ensure the confidentiality of the test results.

Information Collection



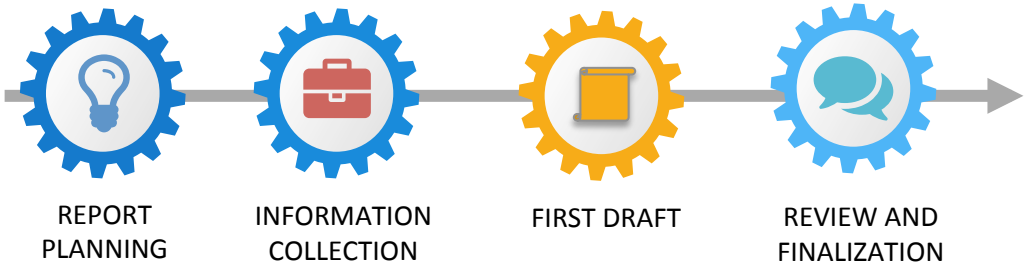
- Make sure that you collected all the information in all stages, system used and tools.
- Take notes, capture screenshots, log all activities, and keep all packet captures, scan reports, and any other results of your pen testing activities.

Report First Draft



Write a rough draft report using all relevant information gathered in the “information collection” stage.

Review and Finalization



- Peer review is very important!
- If you are a one-man pen testing shop, make sure to hire someone to proof read your report.

Risk Ratings

The most common risk rating for vulnerability assessment is the Common Vulnerability Scoring System (CVSS).

https://first.org/cvss

Risk Ratings

The standard risk model:

Risk = Likelihood * Impact

OWASP has a great resource that describes a risk rating methodology:

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology


Omar's
Demo & Whiteboard


THE ART OF
Hacking
THEARTOFHACKING.ORG
~ 325 ~

END OF DAY 2