

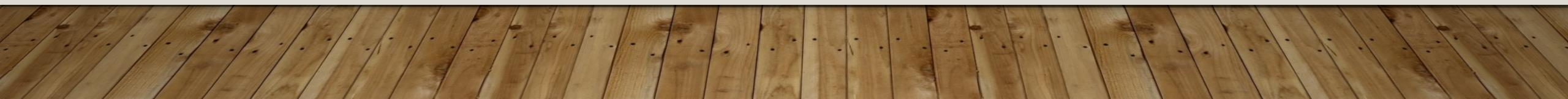
# FIRAT ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ YAZILIM MÜHENDİSLİĞİ İŞ YERİ EĞİTİMİ SUNUMU

---

MEHMET DURUK

190542016

KRIPTARIUM AR-GE YAZILIM DANIŞMANLIK SAVUNMA SANAYİ VE TİCARET LTD.ŞTİ.



# KRİPTARİUM AR-GE YAZILIM DANIŞMANLIK SAVUNMA SANAYİ VE TİCARET LTD. ŞTİ.

---

- Remote olarak stajyer olduğum Kriptarium Firmasında Ar-Ge ve Yazılım Danışmanlık hizmeti vermesinin yanında güvenlik alanında da danışmanlık ve ürün hizmeti vermektedir.
- Fırat Teknokent merkezli olup aktif bir şekilde faaliyet göstererek diğer şirketler ile çalışmaktadır.
- Şirketin asıl amacı güvenlik zayıflıklarını açığa çıkarmak için yaratıcı testleri kullanarak cip ve cihaz güvenliği için bir fırsat sunmaya çalışmaktadır



# İŞ YERİ EĞİTİMİ KAPSAMINDA KULLANILAN PROGRAMLAR VE PLATFORMLAR

- Staj kapsamında en çok aktif olarak Python 3-2 dili kullanmanın yanında Go ve Bash dilleri ile de çalışılmıştır.
- IDE olarak programlama dillerini kullanmak amacıyla Visual Studio Code kullanıldı.
- Aktif olarak Kali Linux üzerinde çalışmanın yanında gerektiği zamanlarda VMware Workstation üzerinde Windows 10 ve Windows 7 sistemlerini kullanmanın yanında hedef makine olarak Metasploitable2 ve bWapp makineleri kullanıldı



# KAZANIMLAR VE DENEYİMLER

- İlk hafta yaptığımız araştırmalar kapsamında adli bilişim araçlarının amaçlarını, etki alanlarını, etkinlik düzeylerini ve çalışma mantıklarını öğrendim.
- Kişisel gelişim amacıyla çalışmalarımın olan Linux eğitimlerimde orta-ileri seviye Linux kullanım becerisini kazandım, araştırdığım ve öğrendiğim konular Linux'ta Süreç işlemleri ve Ağ yöneticiliği işlemleridir.





# KAZANIMLAR VE DENEYİMLER

- Staj kapsamında ekibim ile her hafta toplantı yaparak bilgi alışverişinde bulunduk
- İleriki haftalarda depreme ait verileri, Twitter'da o gün ve ertesi günde atılan deprem anahtar kelimesinin kullanıldığı mesajların çekilmesi, hasar tespit sitesi üzerinde gösterilen hasarsız, az-orta-ağır hasarlı binalara ait verilerin çekilmesi ve son olarak depreme ait görselleri il-il ilçe-ilçe şeklinde çekilmesini yaptık.



# KAZANIMLAR VE DENEYİMLER

- Kişisel gelişim amacıyla araştırdığım ve uygulama yaparak öğrendiğim Siber Güvenlik araçları

- Mimikatz
- Macof
- TCPCDump
- Wifiphisher
- Aircrack
- SpiderFoot
- Ngrok
- Snort
- ArpWatch

```
Extensions feed:
Sending 60 known beacons (OnAir ... HAM AIRPORT FREE WIFI)
Sending 60 known beacons (AEROPUERTO WIFI ... XFINITY)
Sending 60 known beacons (cablewifi ... backup)
Victim f4:91:      probed for WLAN with ESSID: 'Stargate' (KARMA)
Victim 40:f3:      probed for WLAN with ESSID: 'Telekom_FON' (Known Beacons)
DHCP Leases:
1533330793 40:f3:      android-6c      01:40

Wifiphisher 1.4GIT
ESSID: Free WiFi
Channel: 6
AP interface: wlan0
Options: [Esc] Quit

HTTP requests:
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] POST request from 10.0.0.94 with wifphshr-email=Victim@victim.com&wifphshr-password=crippledblackphoenix
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
```

```
(owlking@sensei)-[~]
$ sudo nmap -F 192.168.1.100 -oX /home/owlking/Desktop/yeni.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 16:50 +03
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.59 seconds
```



# SONUÇLAR VE DEĞERLENDİRMELER

---

- İş yeri eğitimi kapsamında gerek teorik gerek uygulamalar ile bilgi ve birikimimi artırdığımı inanıyorum
- Bu önümdeki yol haritasında hangi kararları verirken nelere dikkat edeceğimi daha iyi biliyorum
- Siber güvenlik alanında hangi eksikliklerimin olduğunu daha iyi kavradım ve bu amaçla hangi araç ve gereçleri pratikte kullanmam gerektiğine dair yol haritası yaptım
- Sektörde dikkat edilmesi gereken hususlar nelerdir ve nasıl yapılır öğrendim
- Başta Fatih Özkaynak hocam olmak üzere ekip arkadaşlarım ve mentor lerimden aldığım verim için teşekkür ederim

# KAYNAKÇA

---

- [https://github.com/DURUK-Mehmet/Is\\_Yeri\\_Kodlar](https://github.com/DURUK-Mehmet/Is_Yeri_Kodlar)
- <https://chat.openai.com/>
- <https://www.btkakademi.gov.tr/>
- <https://www.youtube.com/>
- [https://docs.google.com/spreadsheets/d/1\\_wIakARJIKzCxMQnlv9ZObM7m-yXu\\_XJn-\\_SvjR6j74/edit](https://docs.google.com/spreadsheets/d/1_wIakARJIKzCxMQnlv9ZObM7m-yXu_XJn-_SvjR6j74/edit)
- <https://hasartespit.csb.gov.tr/>
- <https://www.kali.org/docs/>
- <https://gelecegiyazanlar.turkcell.com.tr/>
- <https://github.com/BunyaminUcar/earthquakedatacollection>