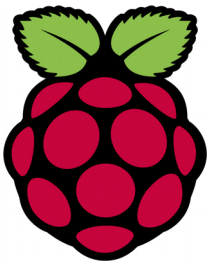


Raspberry Pi 3 ile Snort Entegrasyonu

(05.09.2017)

Emre Övünç

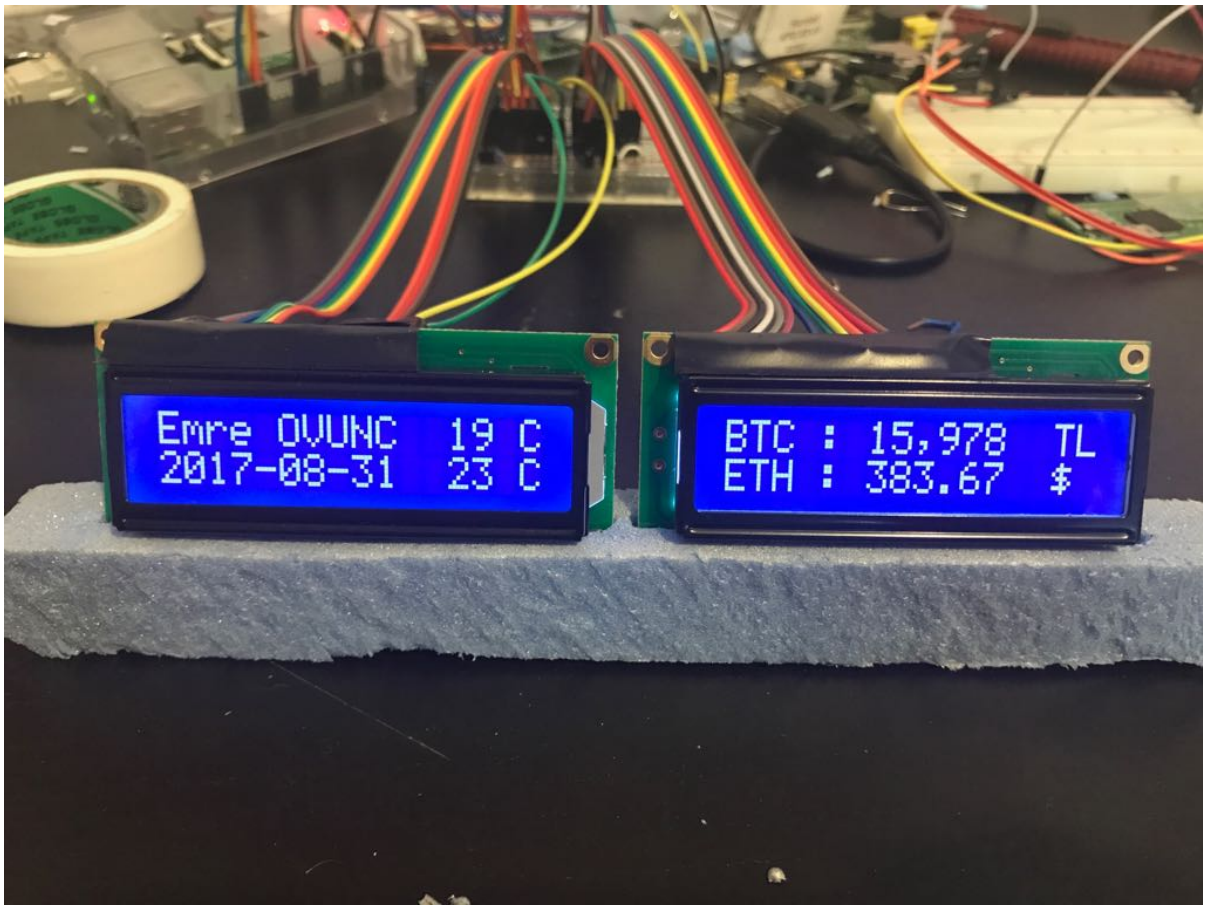
Siber Güvenlik Mühendisi

İçerik

1. Giriş

Elektronikle uğraşmayı seviyorsanız ve kendiniz için önemli olan bilgileri kolaylıkla takip edebilmek istiyorsanız bu yazım tam size göre. İşim dışında kalan boş zamanlarda genellikle IoT ve Ağ Güvenliği üzerine çalışmalar yaparım. Bilgisayar başındayken vazgeçilmezlerim arasında Snort ve Iptables bulunmaktadır, sürekli kurallar yazarak veya değiştirerek ağda neredeyse görünmez bir şekilde dolaşmak bile mümkün.

Düzenli olarak Snort'un bildirimlerini takip ederek ağımda olan bitenleri görmek her zaman ilgimi çekmiştir. Elimdeki sensörleri ve ekranları kullanarak yeni bir proje yapıp, Snort uyarılarını daha iyi bir şekilde takip etmeyi düşündüm. Hem daha okunaklı bir biçimde uyarıları takip edebilmek hem de bilgisayar ekranımda daha fazla yer açmak için oldukça faydalı bir çalışma olduğunu söyleyebilirim.



2. Malzemeler

- Python3
- Raspberry Pi 3
- Jumper kablolar
- 10K ve 480 Ohm dirençler
- 16x2 LCD ekranlar
- Breadboard
- Ultrasonic mesafe sensörü
- Sıcaklık ve nem sensörü
- İsteğe bağlı potans
- Havya ekipmanları
- Snort veya benzeri IPS&IDS
- Bolca sabır ve el emeği :)

3. LCD

3.1 Hazırlık

Malzemeleri bir araya getirip masama yığdıktan sonra ilk hedefim ekranları bağlayarak herhangi bir yazı göndermek oldu. Bunun için internetten yapacağınız küçük bir araştırma ile gerekli şemaları bulabilirsiniz, ufak farklılıklar yaparak aşağıdaki şemayı kullandım. Burada asıl önemli olan nokta ekran ile kablolar arasındaki lehim işini çok iyi bir şekilde yapmak. Sağlamlaştırmak isterseniz silikon da kullanabilirsiniz.

3.2 LCD Pinleri

LCD pinlerinin yerlerini belirletmek gerekirse;

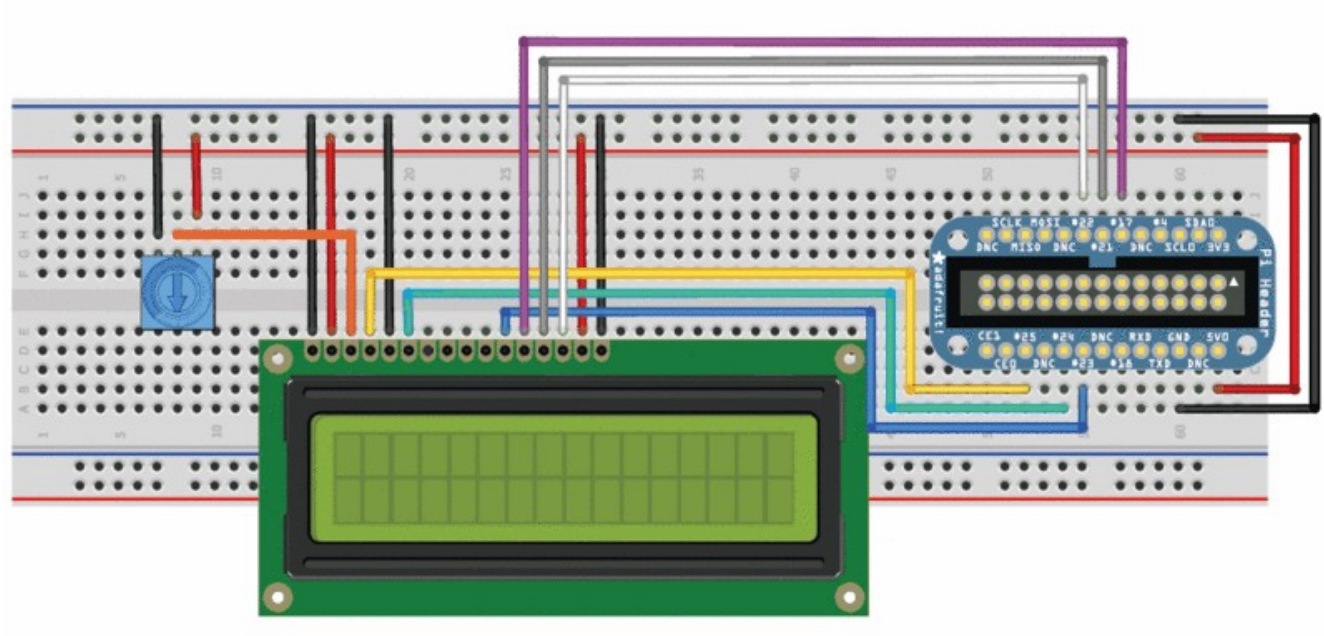
1 , 5, 16	–	GND
2 , 15	–	5V+
3	–	Parlaklık
4 , 6 , 11 , 12 , 13 , 14	–	GPIO Pin

Python kodlamasında ise küçük bir yardım olarak;

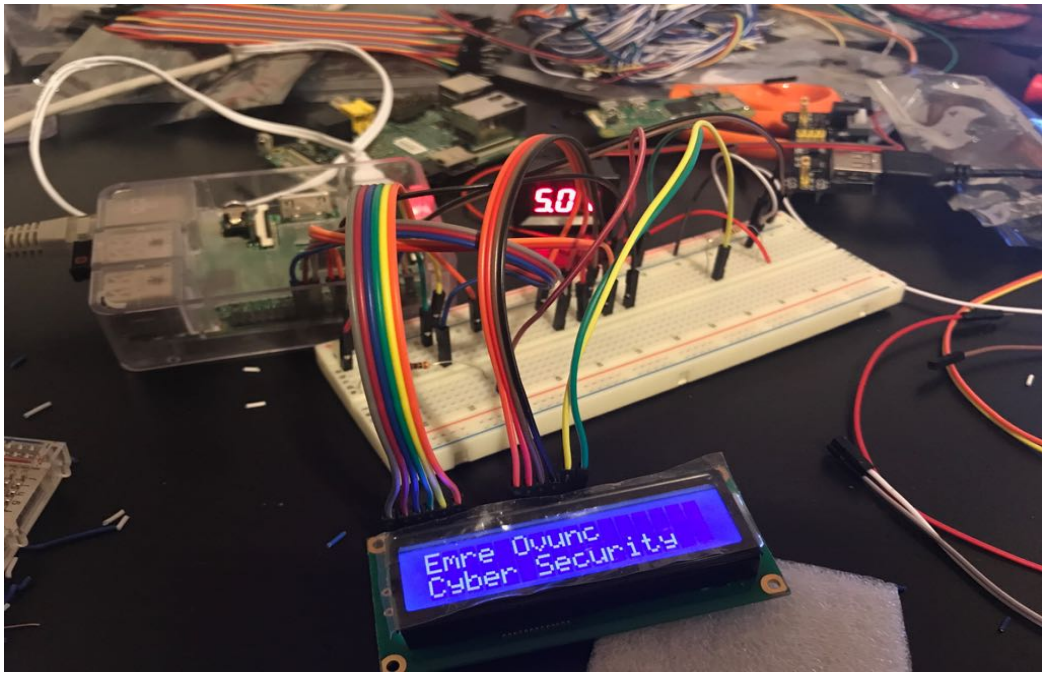
```
GPIO.setwarnings(False)
GPIO.setmode(GPIO.BCM)
GPIO.setup(LCD_GPIO_PIN , GPIO_PINLERI)
```

NOT: Ekranları doğru GPIO pinlerine bağladığınızdan emin olmalısınız aksi taktirde cihazlarınıza zarar verebilirsiniz sorumluluk tamamen size aittir.

3.3 Ekran Şeması



İlk ekranıma doğru bir şekilde görüntüyü gönderdikten sonra bağlantıları sağlamlaştırıp, farklı pinler kullanarak ikinci ekranımı da bağlamaya koyuldum.



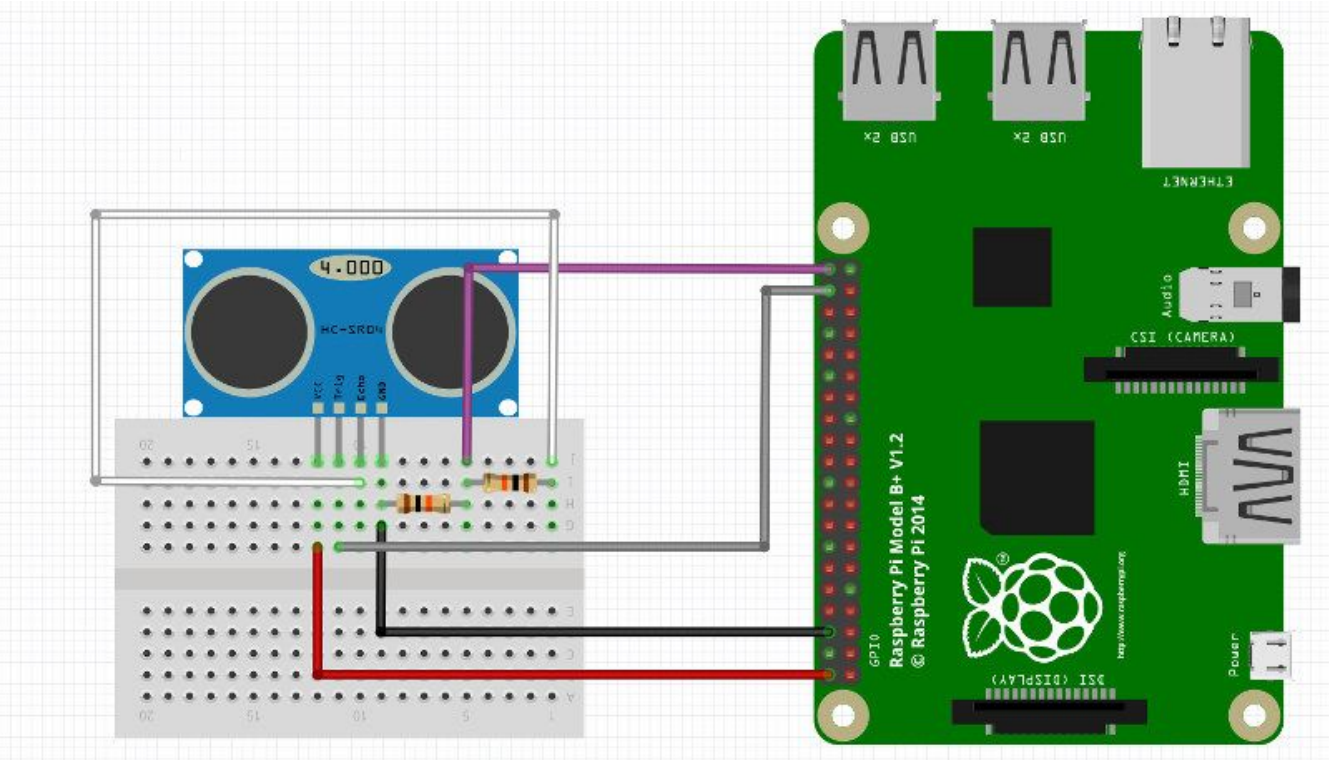
4. Sensörler

4.1 Sensörler Hazırlık

Şimdi sıra ultrasonic mesafe sensörünü bağlayıp, masa başında ben yokken boşu boşuna Snort bildirimlerini aktarmak yerine, hava durumu, haberler gibi bilgileri aktararak çeşitlilik sağlamaya geldi.

LCD ekranlarıyla karşılaştırdığımız zaman sensörleri bağlamak gerçekten çok daha kolay. HC-SR04 sensörüyle ilgili pek çok detaylı yazı ve tasarım dökümanını ufak bir araştırma ile bulabilirsiniz.

4.2 Sensör Şemaları



5. LCD ve Sensörleri Birleştirme

Tüm malzemelerimizi çalışır hale getirdikten sonra şimdi uzaklık sensörü ile LCD ekranlarını ayarlamak kalıyor. Aşağıdaki ufak örneklerle bu konuyu da rahatlıkla çözebilirsiniz. Ayrıca *Nmap* kullanarak kendi açık servislerinizi de ekranlardan öğrenebilirsiniz.

```
#1 Distance:
        while True:
                sleep(3)
                 if 0 < distance < 100:
                        LCDs_near()
                else:
                        LCDs_far()
```

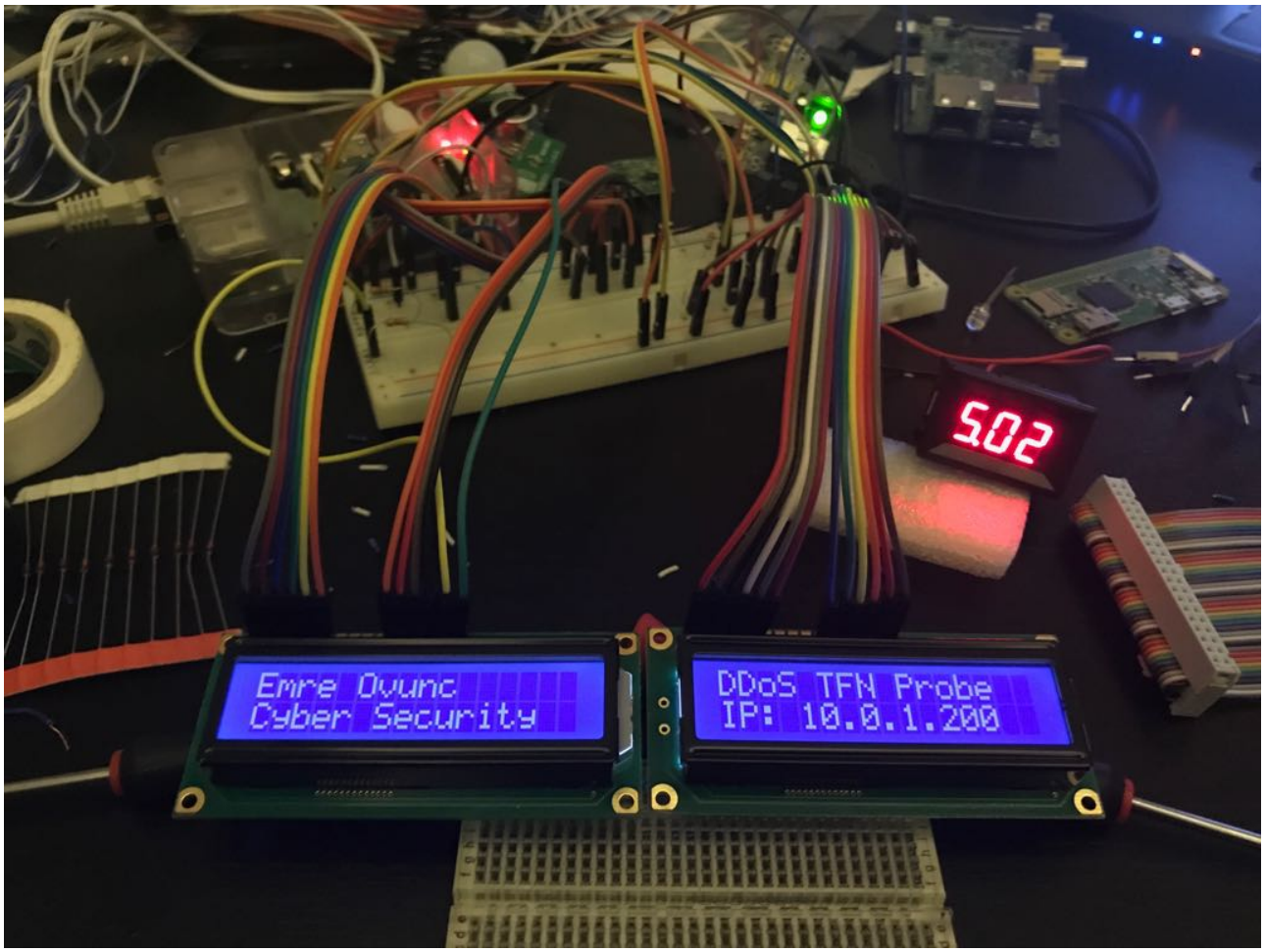
```
#2 LCDs_near:
         (out, err) = SnortProc.communicate()
         LCD1_Upper(outParser1)
         LCD1_Lower(outParser2)
```

```
#3 LCDs_far:
        from requests import get
        weather_request = get(url=weatherUrl)
        C = (weather_request.text.split(weatherParser)[1].split(weatherParser2)[0])
        LCD2_Upper(C)
        LCD2_Lower(geTime())
```

6. Programlama

Kodlama ile ilgili takıldığınız yerleri mail atarak sorabilirsiniz. Hazıra ve ezbere karşı olduğum için yaptığım projenin kodlarını github'a koymadım ancak yardımcı olması açısından aşağıdaki linklerden faydalanabilirsiniz.

- https://github.com/EmreOvunc/Hacktrick2017
- https://github.com/EmreOvunc/MyDailyScripts
- https://github.com/adafruit/Adafruit-Raspberry-Pi-Python-Code



7. Sonuç

Sonuç olarak ekranlarımda bilgisayar başındayken Snort processinden gelen uyarılar, uzaktayken ise hava durumu ve bilgisayarımdaki açık servisler gibi bilgileri alarak işlerimi kolaylaştırmaya başladım. Bu projeden yola çıkarak pek çok hayatınızı kolaylaştıracak fikirlere doğru yönelebilirsiniz, unutulmaması gerekenler arasına *sabır* ve *çalışmayı* ekleyerek yazıma son veriyorum.