TPOT LOCAL KURULUMU

<https://github.com/telekom-security/tpotce/releases> öncelikle verilen linkten iso dosyamızı indiriyoruz.

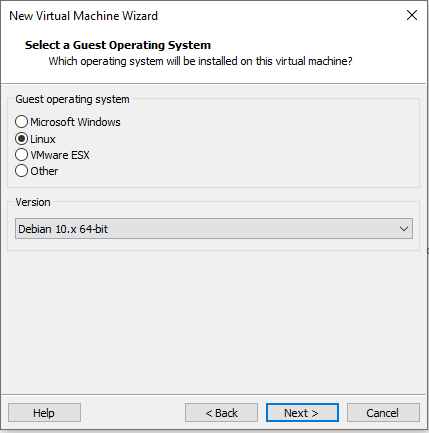
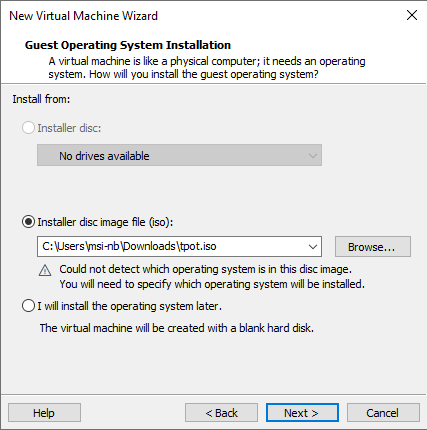
VMware Workstation uygulaması açılarak “Create New Virtual Machine” butonu seçilir. Aynı işlem “**File > New Virtual Machine**” adımları izlenerek de yapılabilir.

Sanal makine oluşturma sihirbazı başladıktan sonra kurulum için ‘Typical’ ve ‘Custom’ olarak iki seçenek sunulmaktadır.  Tipik kurulum seçeneği önerilen olduğu için bu seçenekle devam edilir.

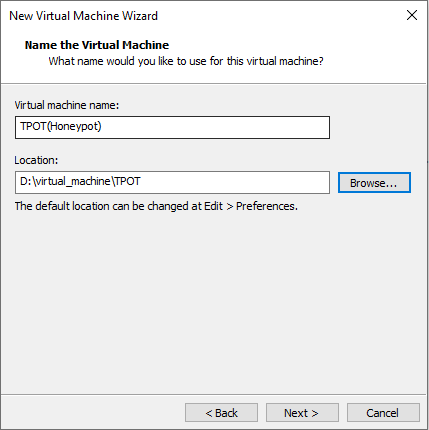


Sanal makine oluşturma sihirbazı başladıktan sonra kurulum için ‘Typical’ ve ‘Custom’ olarak iki seçenek sunulmaktadır.  Tipik kurulum seçeneği önerilen olduğu için bu seçenekle devam edilir.

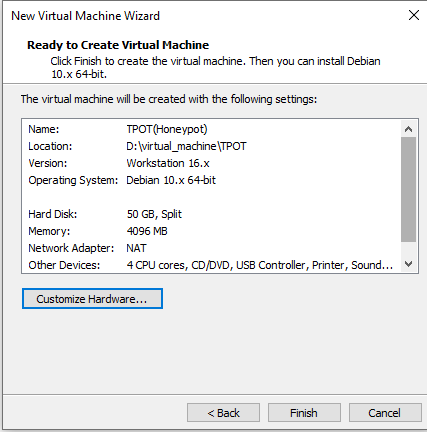
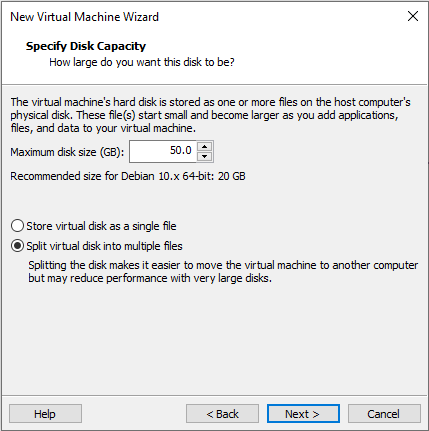
Gelen ekranda kurulum dosyası için ‘**Installer disc image file (iso)**’seçeneği seçilerek dosya yolu gösterilir. Devamında iso dosyası seçilerek devam edilir. Ardından işletim sistemi ve versiyonu seçilerek devam edilir.



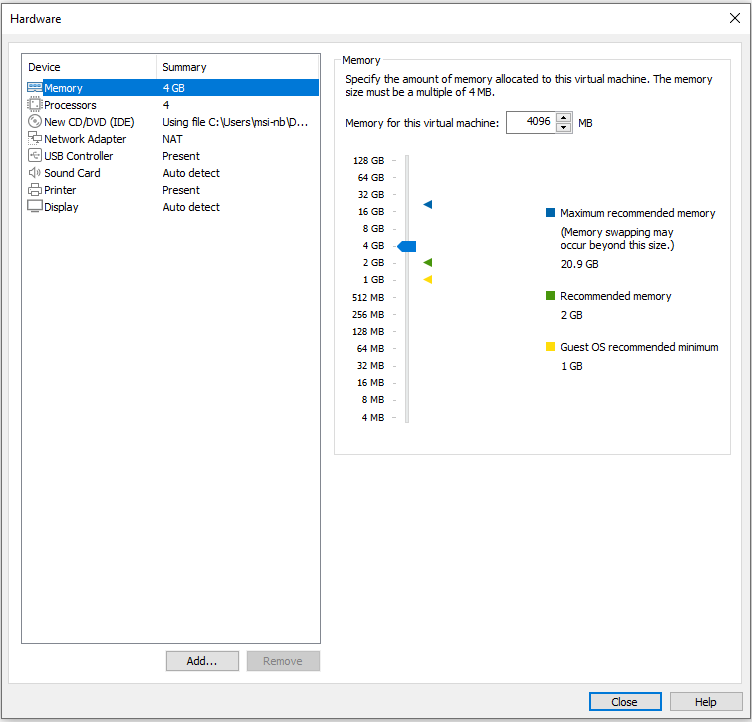
Devamında kurduğumuz makineye isim verilir ve kurulum konumu seçilir.



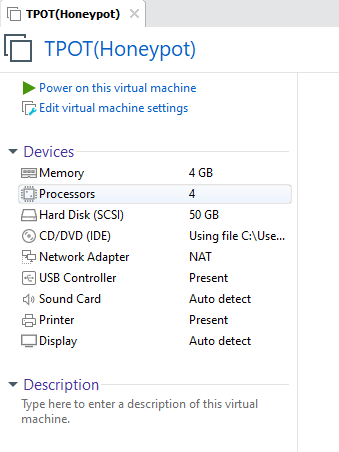
Solda, sanal makinenin disk boyutu ve saklama tipi seçilerek devam edilir. Disk boyutunu sanal makinada kullanılacak uygulama ve verilere göre değiştirilebilir. Sağda, donanım özelliklerinde değişiklik yapılmak istenirse **‘Customize Hardware’**seçeneği ile işlemler gerçekleştirilir ve **‘finish’**butonu ile bitirilir.



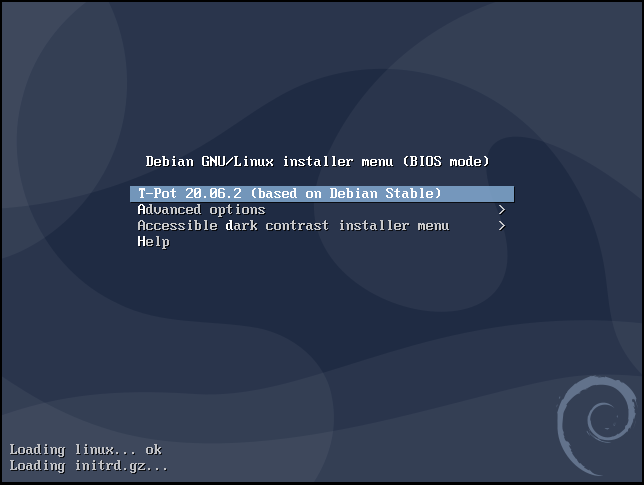
Honeypot için verdiğimiz özellikler bu şekildedir.



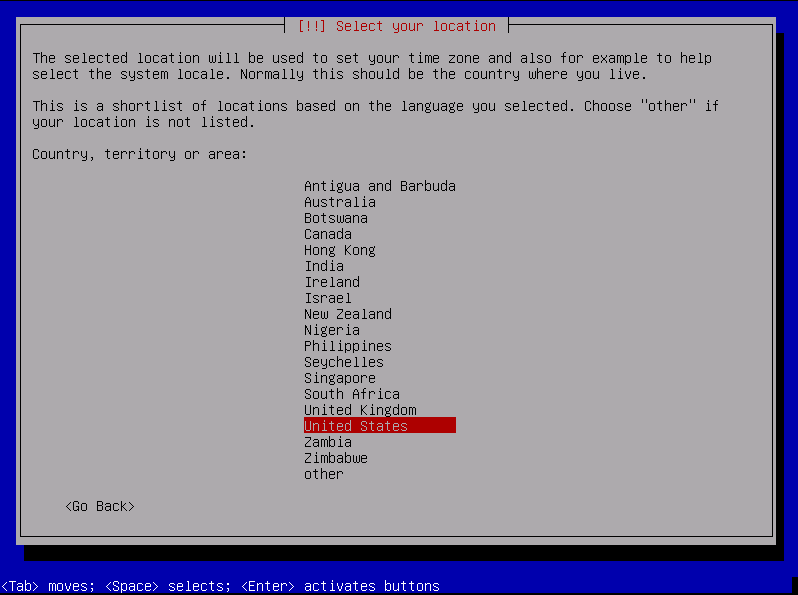
Sanal makine üstüne yapılan yapılandırmadan sonra kurulum için TPOT başlatılır.



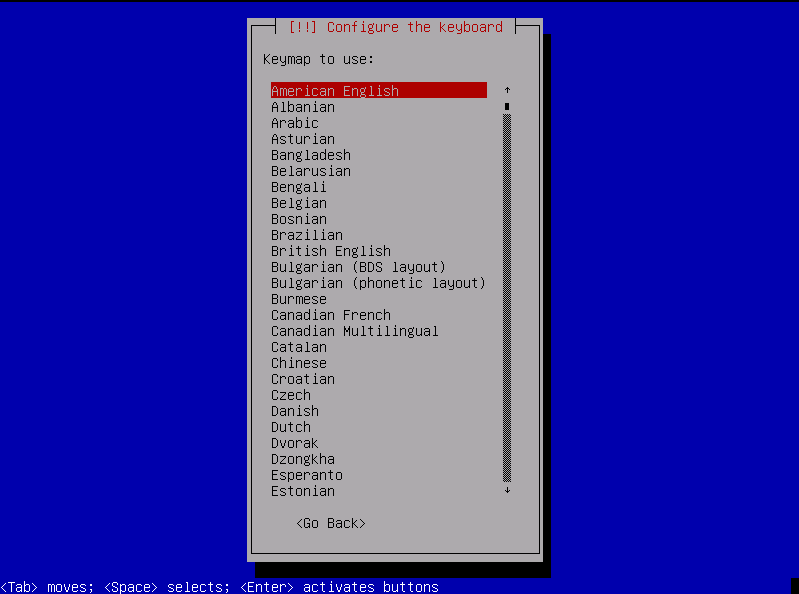
Gelen Boot ekranında ilk seçenek seçilerek ile devam edilir.



Bundan sonra ki kısım temel kurulum adımları enter yaparak devam edebilirsiniz.

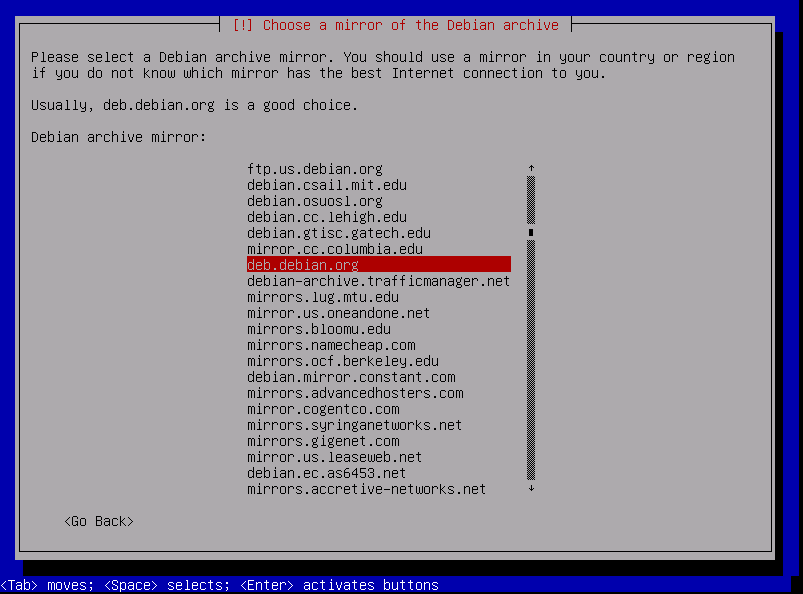
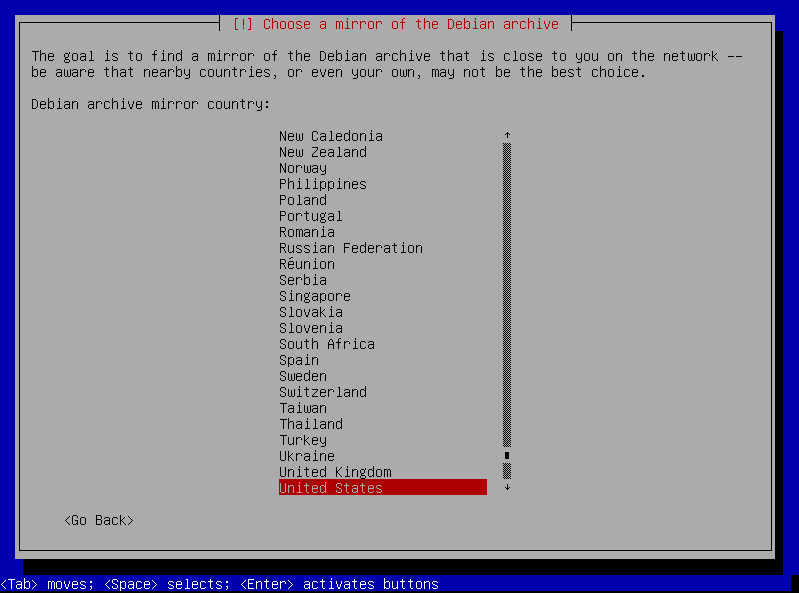


Klavye ayarları kısmından kullanmakta olduğunuz klavye türünü seçerek devam edebilirsiniz.

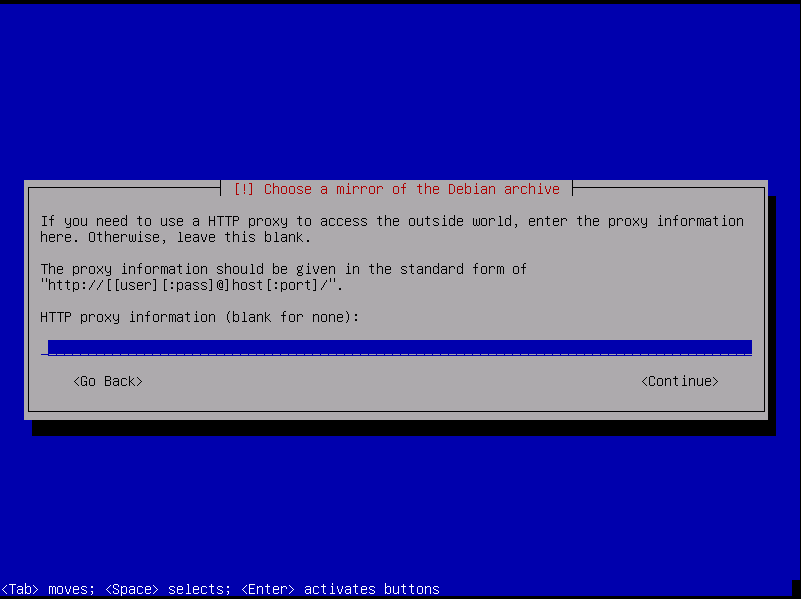


T-pot kurulum sihirbazı, paketleri indirmek için otomatik olarak bir debian arşiv aynası seçecektir.

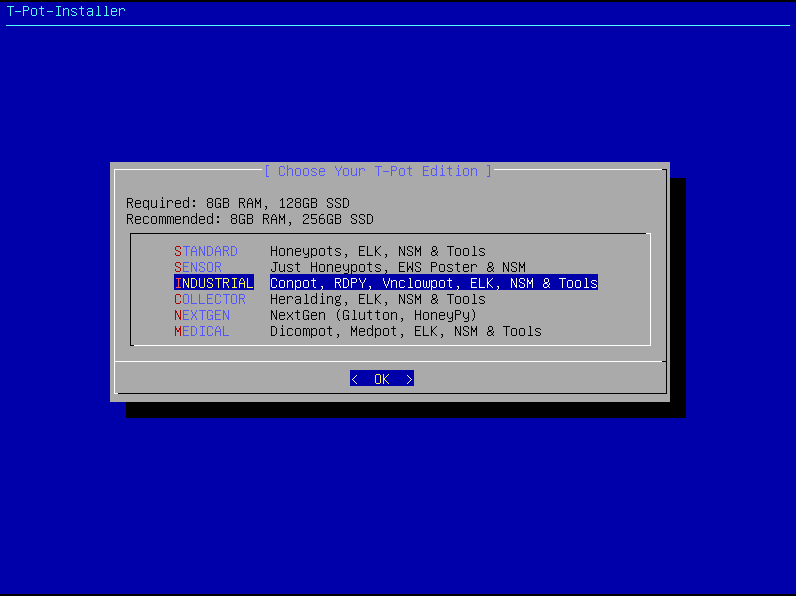
T-pot kurulumu için gerekli olan paketleri indirmek için debian arşivi seçiyoruz.



Proxy olmadığından dolayı **“Continue”** diyerek kuruluma devam edilir.



Önceden oluşturulmuş hazır kurulum türleri mevcuttur. Ben endüstriyel tpot kurmak istediğimden dolayı endüstriyeli seçip devam edilir.



Aşağıda ise hazır olarak oluşturulmuş kurulumların içerisinde hangi araçlar ve hangi honeypotlar var görmekteyiz.

**Standard**

* Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner
* Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

**Sensor**

* Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypy, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner
* Tools: cockpit, ewsposter, fatt, p0f & suricata
* Since there is no ELK stack provided the Sensor Installation only requires 4 GB of RAM.

**Industrial**

* Honeypots: conpot, cowrie, dicompot, heralding, honeysap, honeytrap, medpot & rdpy
* Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

**Collector**

* Honeypots: heralding & honeytrap
* Tools: cockpit, cyberchef, fatt, ELK, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

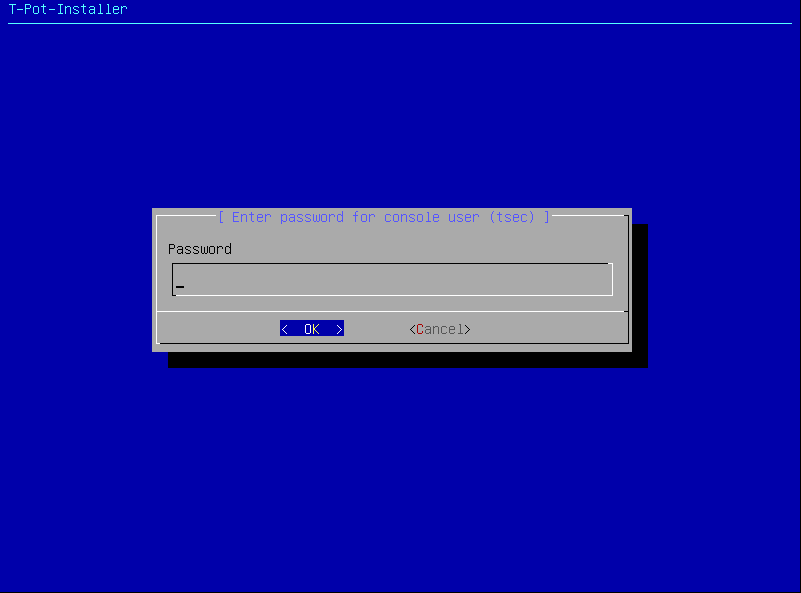
**NextGen**

* Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypy, honeysap, ipphoney, mailoney, medpot, rdpy, snare & tanner
* Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

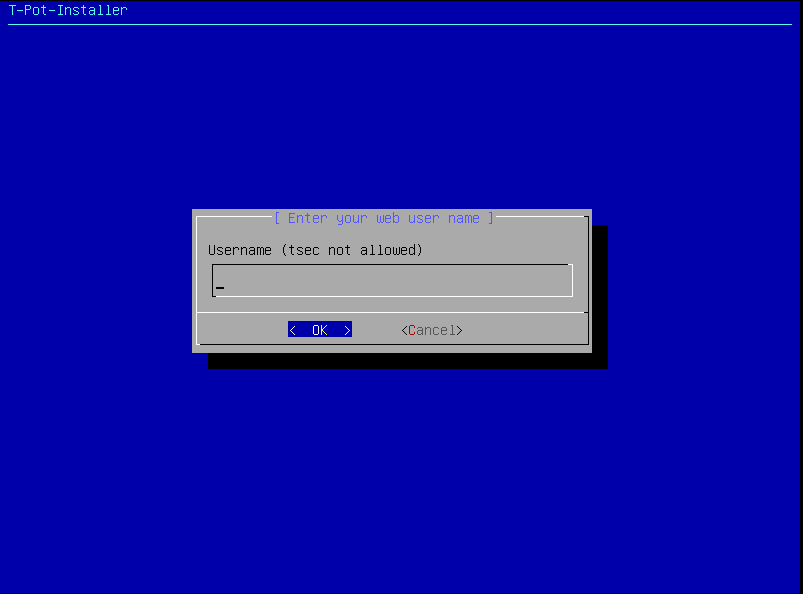
**Medical**

* Honeypots: dicompot & medpot
* Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

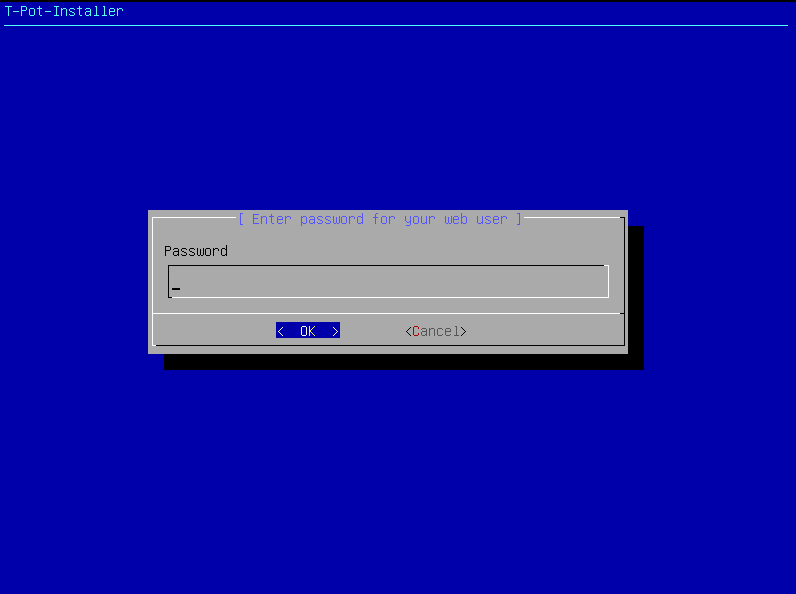
tsec kullanıcısı için bir parola vermemiz gerekiyor.



Şimdi de T-pot’un web arayüzüne erişmemiz için bir kullanıcı adı oluşturuyoruz.



Web arayüzü için vermiş olduğumuz kullanıcı için bir parola belirliyoruz.



Ardından kurulum işlemi başlıyor bu kısım biraz uzun sürebilir.



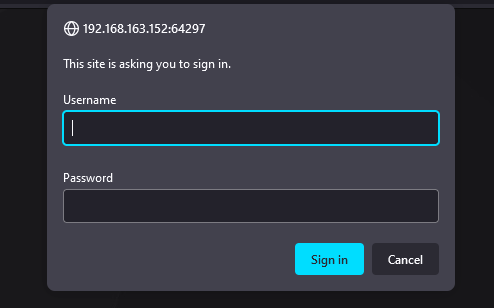
Kullanıcı adı tsec ve parola için de tsec için oluşturduğumuz parolayı veriyoruz.



Kurulum işlemi tamamlandı. T-pot artık aktif bir şekilde çalışmaktadır. Web ara yüzüne girmek için verilen ip adreslerinden girebiliriz.



Web arayüzü için vermiş olduğumuz kullanıcı adı ve parolasını girerek T-pot GUI açmış oluyoruz.



Web arayüzü de bu şekildedir web arayüzüne şu ip şu port üzerinden bağlanır.

