|  |
| --- |
| ***LDAP*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| LDAP nedir ve Web for Pentester laboratuvarı üzerinde LDAP zafiyeti nasıl uygulanır bunun hakkında bilgi vereceğim. |

**30.07.2021**

***LDAP(Hafif Dizin Erişim Protokolü)***

-LDAP’ı kabaca Kimlik doğrulama sistemi üzerinden yetkilendirme diyebiliriz.

-LDAP,389 ve 636 no’lu portlarda çalışır.

-Önceki yaptığımız uygulamalarda 80 ve 443 portlarında çalışan Web Uygulamalarının açıklarıydı.

LDAP ile ilgili WFP üzerinden 2 adet uygulama deneyeceğiz.

**Uygulama 1 :** Kimlik doğrulama sistemi. Bu uygulama üzerinde 3 farklı yol deneyeceğiz.

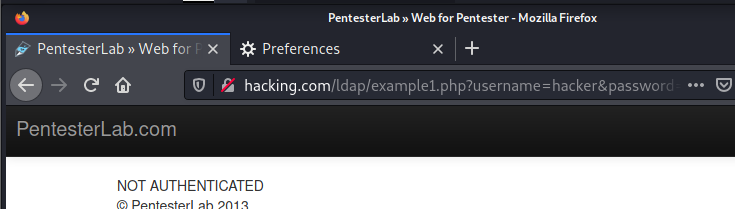
1-)Kullanıcı adı ve parola boş bırakmak

2-)Wordlist ile bruteforce

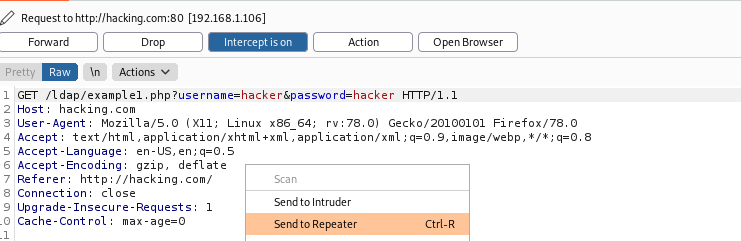
3-)Kullanıcı adı ve parolayı ortadan kaldırmak.

-Tüm işlemler Burpsuite üzerinden gerçekleşeceği için önce Burpsuite’i açıyorum.Gerekli proxy ayarlarını yapıyorum.

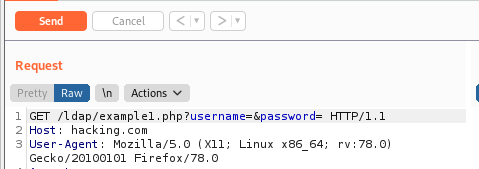
**1-)** Kullanıcı adı ve parola boş bırakma.



-WFP üzerinden zafiyet içeren Web sitesini görüntülüyorum ve URL’i kopyalıyorum.Bu esnada arka planda Burpsuite çalışmaktadır. Burpsuite üzerinden intercept ayarını on konumuna getirip sayfayı yeniliyorum ve bilgileri burpsuite üzerine çekiyorum.



-WFP üzerinden yapmış olduğum işlem sonrasında bütün bilgileri Burpsuite üzerine çekebildim.Ardından “send to repeater” ile bilgileri repeater a aktarıyorum.Burada sayfayı adım adım izleyebileceğim.

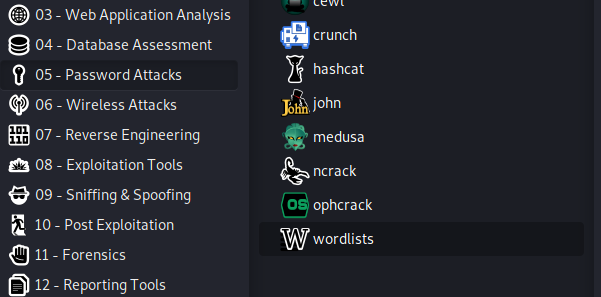


-Repeater üzerine geçiş yapıyorum ve burada Kullanıcı adı ve şifre kısmını boş bırakıyorumArdından Send ile “Response” bölümüne gönderiyorum.

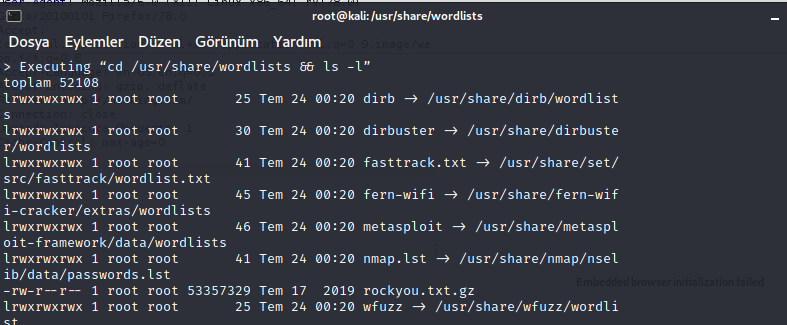


-Response bölümünde Render işlemi gerçekleştirip Web üzerinde ki görünümüne bakıyorum fakat başarısız olduğunu görüntülüyorum.

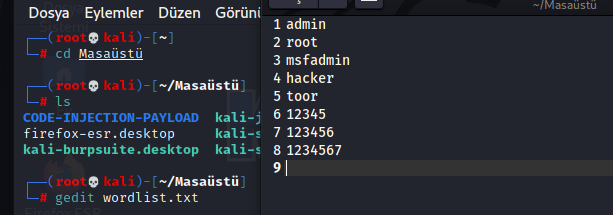
**2-)** Wordlist ile Brute Force işlemi.



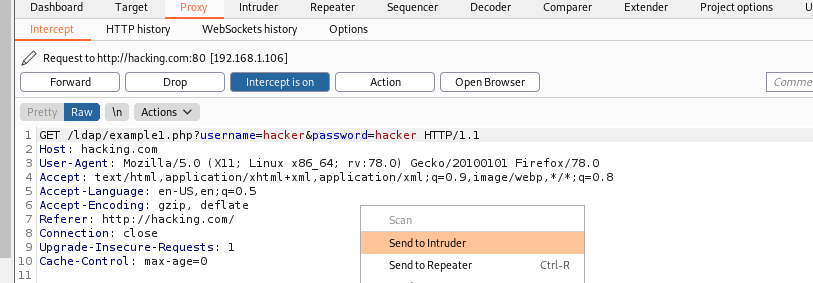
-Kali linux üzerinde hazır olarak bulunan wordlistlerden yararlanabilirim.Wordlist uygulamasını açıyorum.



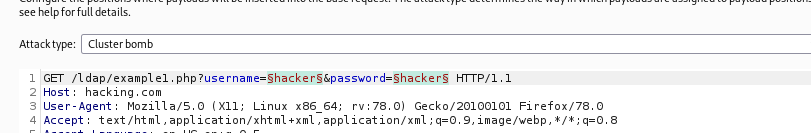
-Karşıma gelen komut istemci üzerinden istediğim listeyi kullanabilirim fakat bu işlem çok uzun sürecektir.



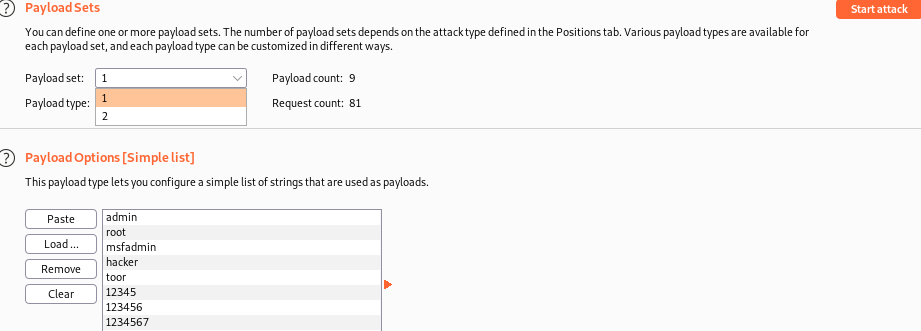
-Bu yüzden kendim bir wordlist oluşturmak istiyorum.Gedit komutu ile bir .txt dosyası oluşturuyorum.İçerisine random olarak şifre ekliyorum.



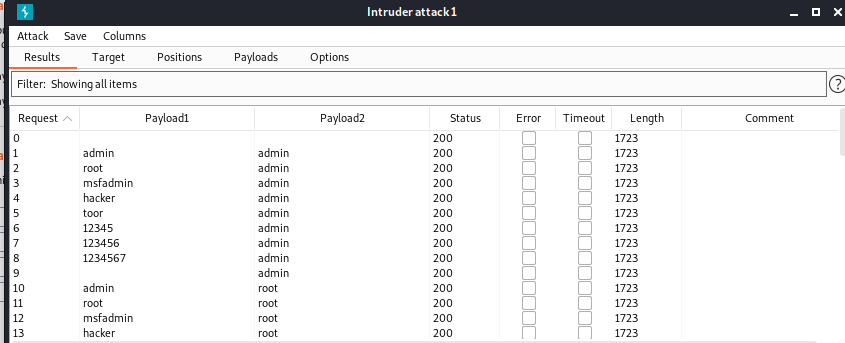
-Ardından Burpsuite üzerine geçiş yapıyorum ve proxy bölümünden “send to intruder” yapıyorum.



-Açılan sekmede brute force uygulayacağım kısım doğru burada işlem yapmıyorum.

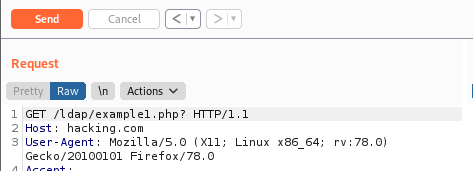


-Şimdi ise payloads kısmına listemi ekliyorum.Ardından “start attack” butonu ile işlemi başlatıyorum.

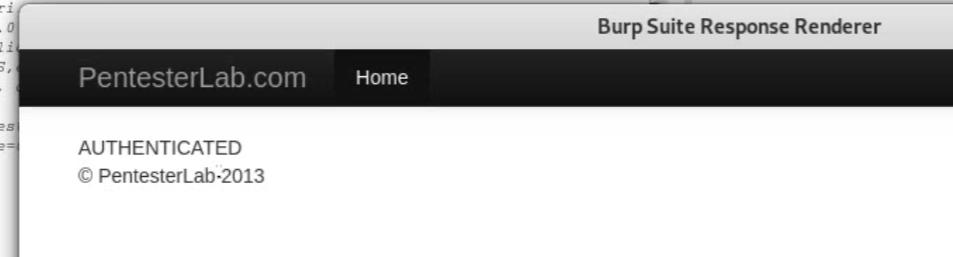


-Ardından length değeri diğerlerinden farklı olan doğru olandır.Ben rastgele bir liste oluşturduğum için başarılı olamadım.

**3-)** Kullanıcı adı ve parolayı ortadan kaldırma.



**-**Şimdi ise Burpsuite üzerinden repeater ksımına geçiş yapıyorum ve kullanıcı adı ve şifre bölümünü silip send diyerek siteyi çalıştırıyorum.



-Şuanda bağlantıyı kurabildim bunu da yapacağımız testler içerisine eklememizde fayda var.