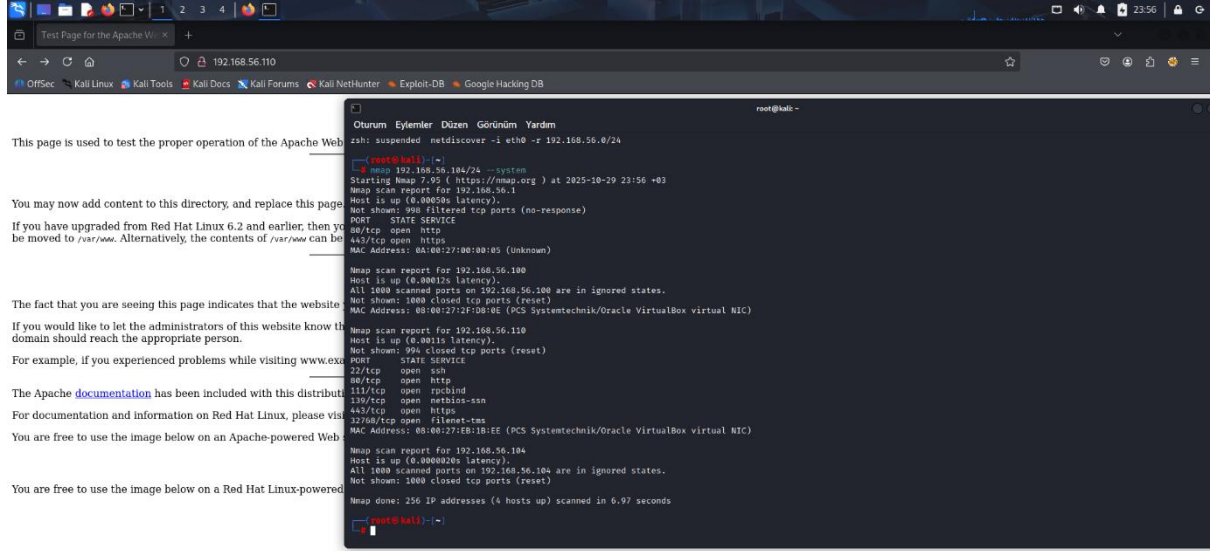
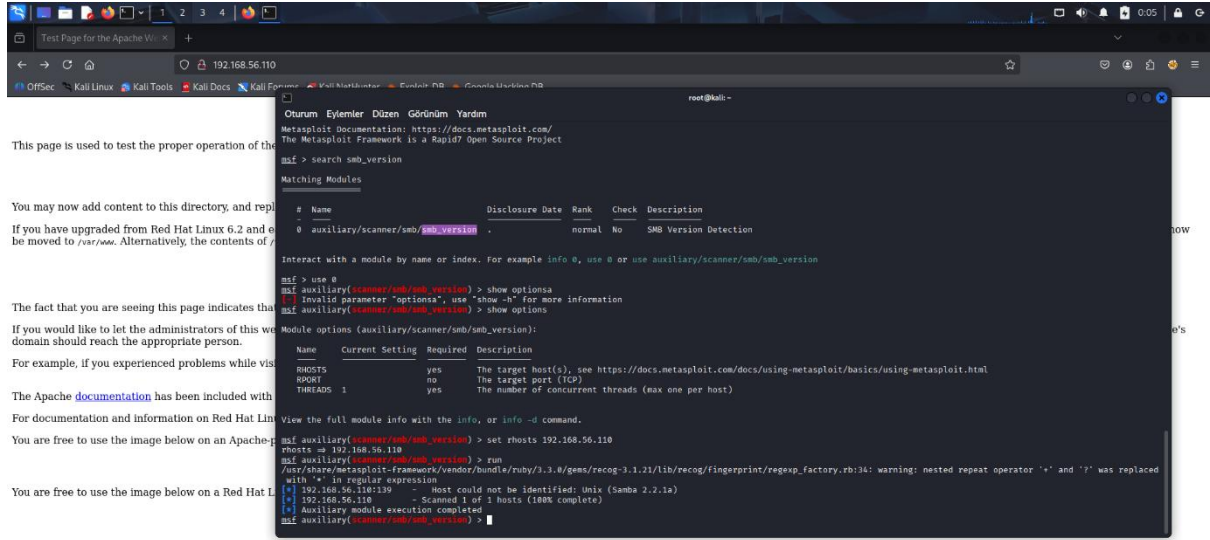


KİOPTRİX

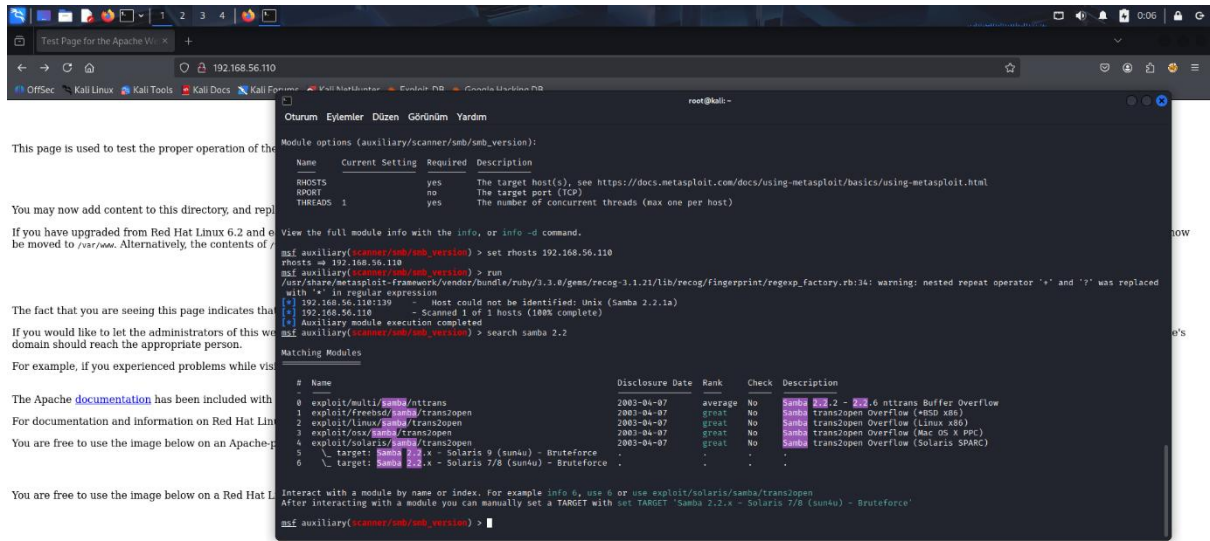
Önce bu ctf in kurulumu diğerleri gibi olmadı kurmak için yeni makine diyoruz ve ardından var olan diski kullan diyip bu makineyi ekliyoruz bu arada freebsd 32 bit seçmek gerekiyor diğer seçenekler ile başlatamadım makineyi denedim çoğunu (debian 32 bit vs). Bu işleri yaptıktan sonra bşr nmap taraması ile hemen açık portları ve ip adresini buluyorum sitenin.



Bu sayfada bize çok bir yol göstermiyor uygulama yani düzgün bir ekran yok karşımızda ben yine dirb taraması vs yaptım ordan da bir sonuç alamadım. Burada yeni bir durum ile karşı karşıya olduğumu anlayıp araştırmaya başladım. Sonra öğreniyorum ki sambanın açık olduğu uygulamalarda metasploit framework kullanılmalı. Buradan işe girişiyorum.



Msfconsole a giriş yaptıktan sonra sambanın versiyonunu öğrenmeye çalışıyorum. Sonra 0. satırı kullanarak bir exploit hazırlayacağım ve bu saldırıyı başlatıp root olacağım.



Burada bir sorunla karşılıyorum ki msfconsole benim RHOST umu okumuyor bu yöntemden vazgeçip her şeyi manuele döndürüyorum yani RHOST umu LHOST umu Payloadımı her şeyimi kendim set edip saldırı başlatıyorum ve sonucunda root oluyorum.

