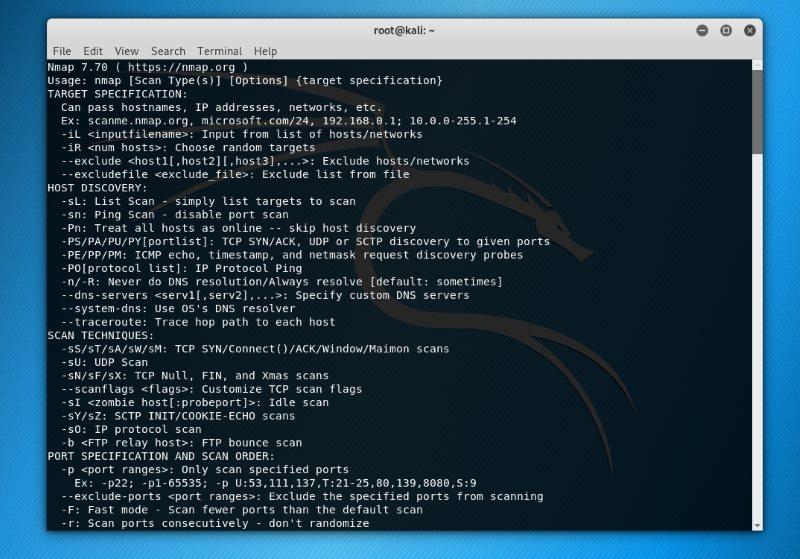
1. Nmap

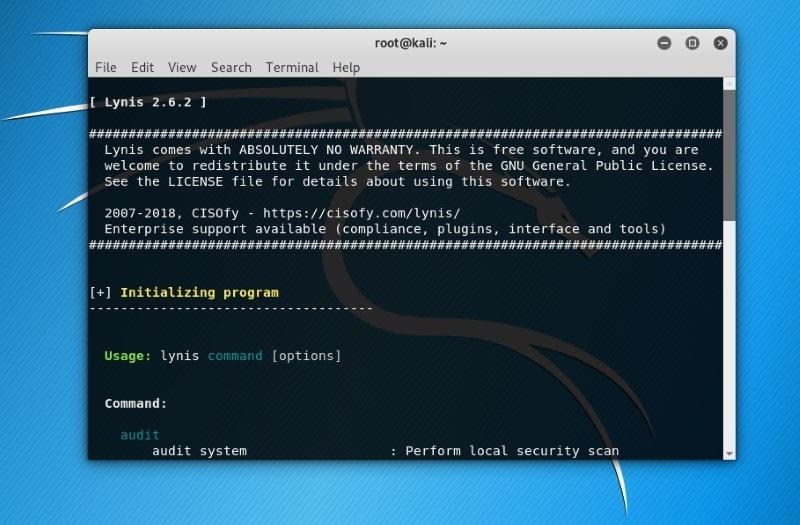


Kali Linux Nmap

[Nmap](https://justpaste.it/redirect/7k3rd/https://nmap.org/) veya "Network Mapper", bilgi toplama için Kali Linux'taki en popüler araçlardan biridir. Başka bir deyişle, ana bilgisayar, IP adresi, işletim sistemi algılama ve benzer ağ güvenliği ayrıntıları (açık bağlantı noktalarının sayısı ve ne oldukları gibi) hakkında bilgi almak için.

Ayrıca güvenlik duvarından kaçınma ve sahtekarlık için özellikler sunar.

2. Lynis



Lynis Kali Linux Aracı

[Lynis](https://justpaste.it/redirect/7k3rd/https://cisofy.com/lynis/) , güvenlik denetimi, uyumluluk testi ve sistem sağlamlaştırma için güçlü bir araçtır. Elbette bunu güvenlik açığı tespiti ve sızma testi için de kullanabilirsiniz.

Sistemi algıladığı bileşenlere göre tarayacaktır. Örneğin, Apache'yi algılarsa, kesin nokta bilgisi için Apache ile ilgili testleri çalıştıracaktır.

3. WPScan



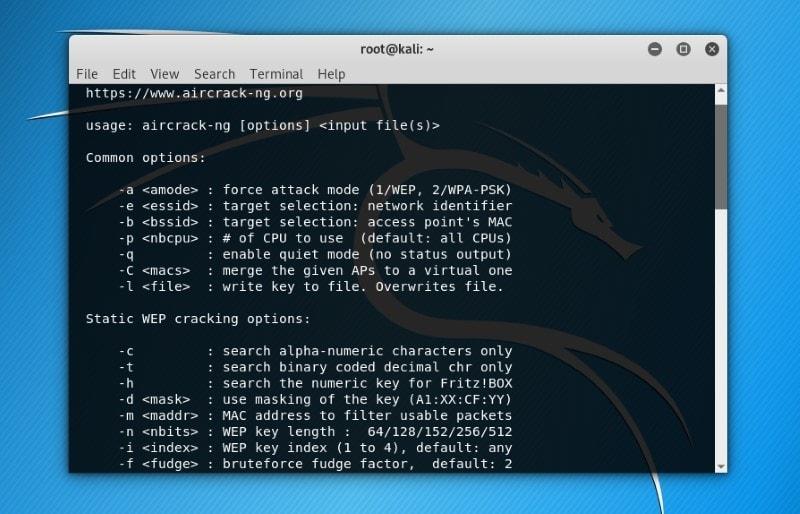
Wpscan Kali Linux

WordPress, en iyi açık kaynaklı CMS'lerden biridir ve bu, en iyi ücretsiz WordPress güvenlik denetleme aracı olacaktır. Ücretsizdir ancak açık kaynak değildir.

Bir WordPress blogunun bir şekilde savunmasız olup olmadığını bilmek istiyorsanız, [WPScan](https://justpaste.it/redirect/7k3rd/https://wpscan.org/) arkadaşınızdır.

Ek olarak, size aktif eklentilerin ayrıntılarını da verir. Elbette, güvenli bir blog size çok fazla ayrıntı vermeyebilir, ancak yine de WordPress güvenlik taramalarının olası güvenlik açıklarını bulması için en iyi araçtır.

4. Aircrack-ng

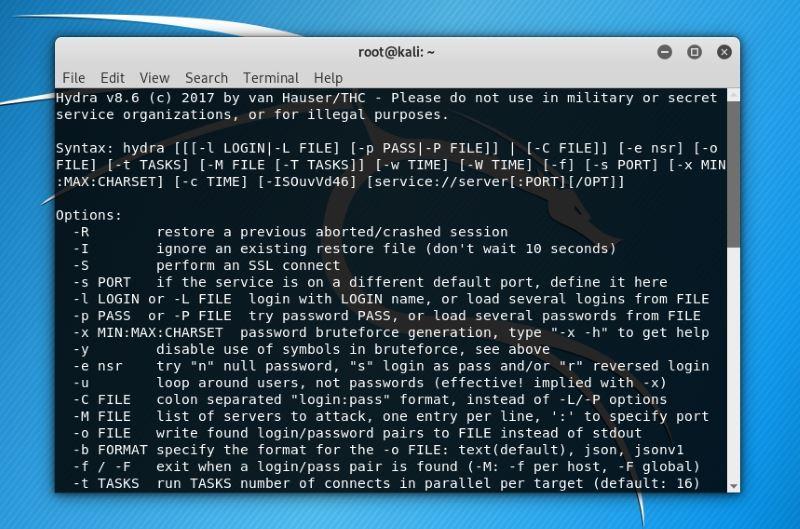


Aircrack Ng Kali Linux Aracı

[Aircrack-ng](https://justpaste.it/redirect/7k3rd/https://www.aircrack-ng.org/) , WiFi ağ güvenliğini değerlendirmek için kullanılan bir araç koleksiyonudur. Yalnızca izlemek ve içgörüler elde etmekle sınırlı değildir, aynı zamanda bir ağı tehlikeye atma yeteneğini de içerir (WEP, WPA 1 ve WPA 2).

Kendi WiFi ağınızın şifresini unuttuysanız - yeniden erişim kazanmak için bunu kullanmayı deneyebilirsiniz. Ayrıca, güvenliğini artırmak için bir WiFi ağını hedefleyebileceğiniz / izleyebileceğiniz çeşitli kablosuz saldırıları da içerir.

5. Hydra

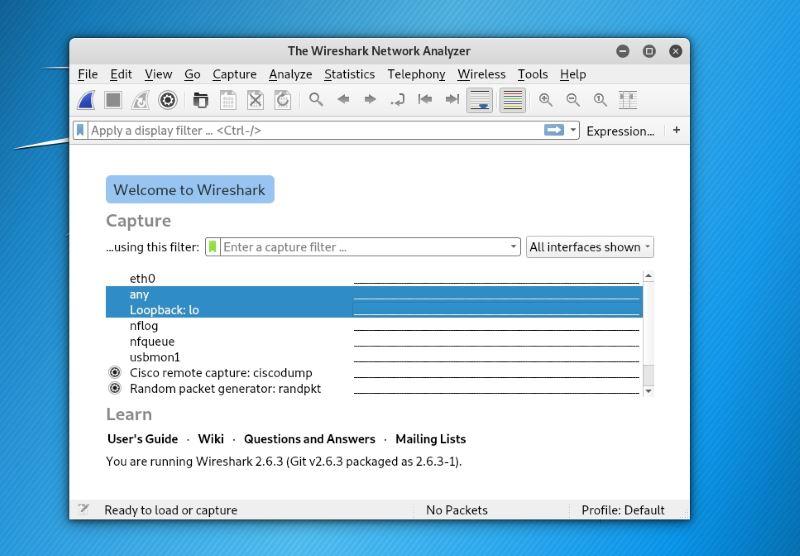


Hydra Kali Linux

Giriş / şifre çiftlerini kırmak için ilginç bir araç arıyorsanız, [Hydra](https://justpaste.it/redirect/7k3rd/https://github.com/vanhauser-thc/thc-hydra) önceden yüklenmiş olarak gelen en iyi Kali Linux araçlarından biri olacaktır.

Artık aktif olarak bakımı yapılmayabilir - ancak şimdi [GitHub'da](https://justpaste.it/redirect/7k3rd/https://github.com/vanhauser-thc/THC-Archive) , böylece üzerinde çalışmaya da katkıda bulunabilirsiniz.

6. Wireshark

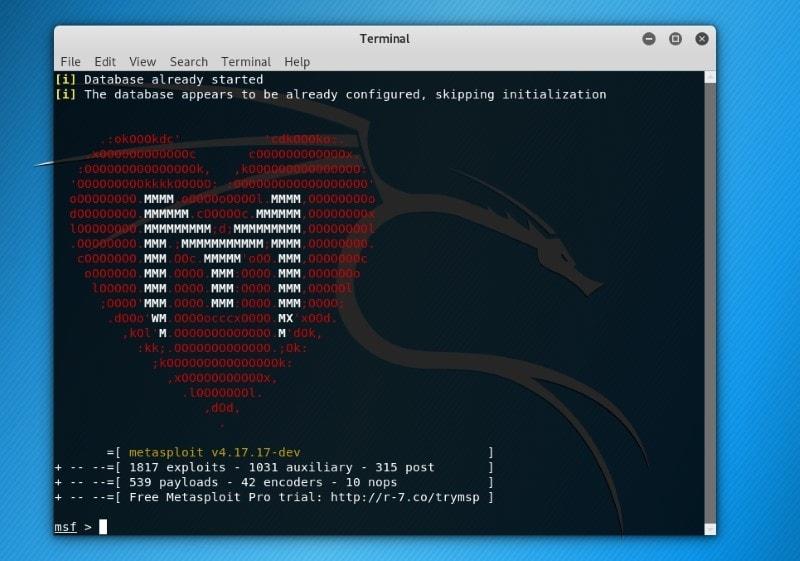


Wireshark Ağ Analizcisi

[Wireshark](https://justpaste.it/redirect/7k3rd/https://www.wireshark.org/) , Kali Linux ile birlikte gelen en popüler ağ analizcisidir. Ağ koklama için de en iyi Kali Linux araçlarından biri olarak kategorize edilebilir.

Aktif olarak bakımı yapılmaktadır, bu yüzden bunu denemenizi kesinlikle tavsiye ederim.

7. Metasploit Framework

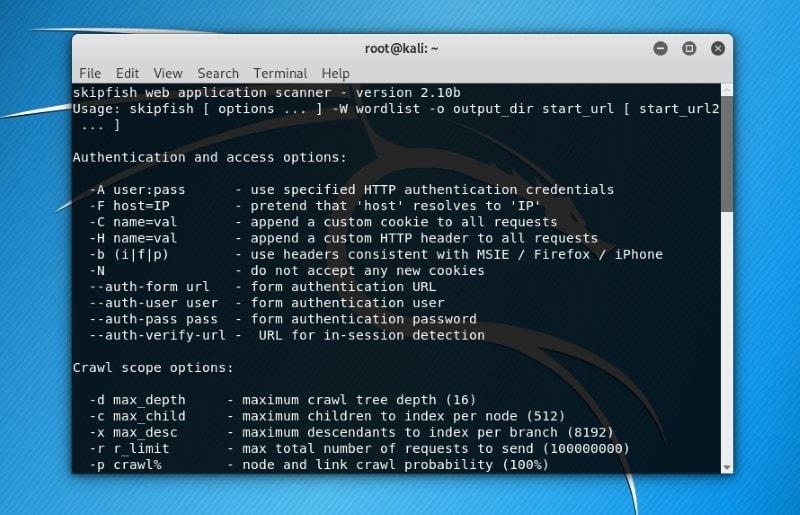


Metasploit Çerçevesi

[Metsploit Framework](https://justpaste.it/redirect/7k3rd/https://github.com/rapid7/metasploit-framework) , en çok kullanılan sızma testi çerçevesidir. İki sürüm sunar - biri (açık kaynak) ve ikincisi bunun pro sürümüdür. Bu araçla, güvenlik açıklarını doğrulayabilir, bilinen açıkları test edebilir ve eksiksiz bir güvenlik değerlendirmesi gerçekleştirebilirsiniz.

Elbette, ücretsiz sürüm tüm özelliklere sahip olmayacak, bu nedenle ciddi konularla ilgileniyorsanız, sürümleri [burada](https://justpaste.it/redirect/7k3rd/https://www.rapid7.com/products/metasploit/download/editions/) karşılaştırmalısınız .

8. Skipfish

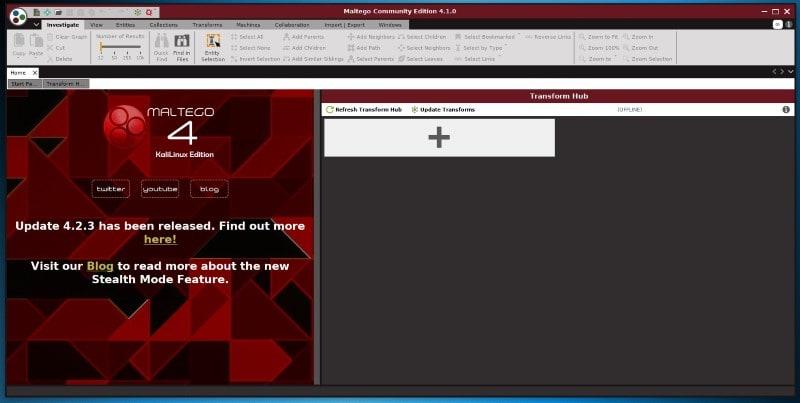


Skipfish Kali Linux Aracı

WPScan'e benzer, ancak sadece WordPress'e odaklanmadı. [Skipfish](https://justpaste.it/redirect/7k3rd/https://gitlab.com/kalilinux/packages/skipfish/) , hemen hemen her tür web uygulaması için size fikir verecek bir web uygulaması tarayıcısıdır. Hızlı ve kullanımı kolaydır. Ek olarak, yinelemeli tarama yöntemi onu daha da iyi hale getirir.

Profesyonel web uygulaması güvenlik değerlendirmeleri için, Skipfish tarafından oluşturulan rapor kullanışlı olacaktır.

9. Maltego



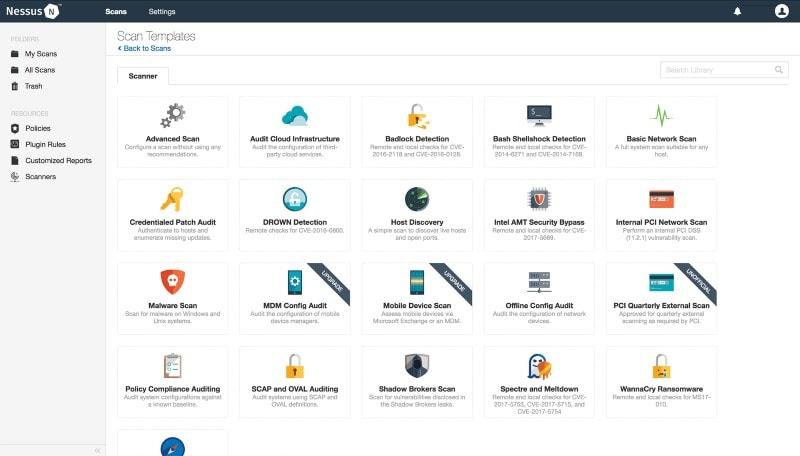
Maltego

[Maltego](https://justpaste.it/redirect/7k3rd/https://www.paterva.com/web7/buy/maltego-clients*.*php) , bilgileri çevrimiçi olarak analiz etmek ve noktaları (varsa) birleştirmek için etkileyici bir veri madenciliği aracıdır. Bilgiye göre, bu veri parçaları arasındaki bağlantıyı analiz etmeye yardımcı olacak yönlendirilmiş bir grafik oluşturur.

Bunun açık kaynaklı bir araç olmadığını unutmayın.

Önceden yüklenmiş olarak gelir, ancak kullanmak istediğiniz sürümü seçmek için kaydolmanız gerekecektir. Kişisel kullanım için topluluk sürümü yeterli olacaktır (sadece bir hesap için kaydolmanız gerekir), ancak ticari amaçla kullanmak istiyorsanız, klasik veya XL sürümüne aboneliğiniz olması gerekir.

10. Nessus

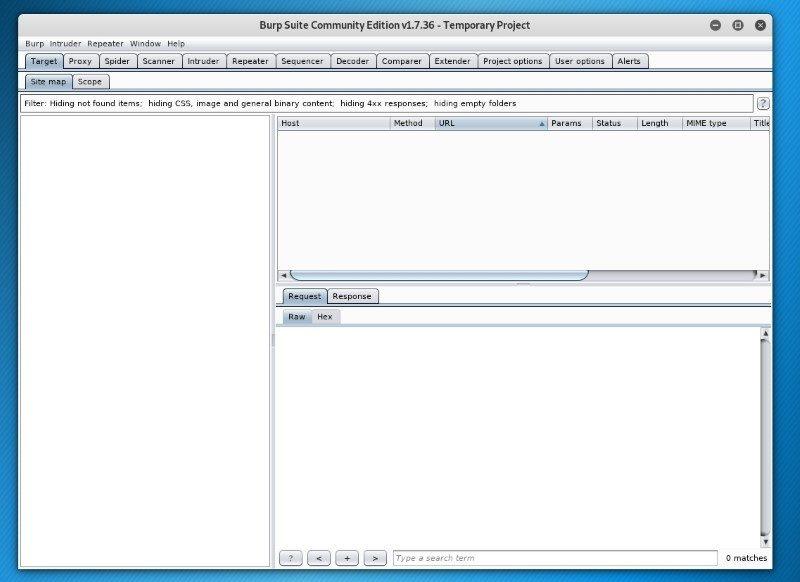


Nessus

Ağa bağlı bir bilgisayarınız varsa, Nessus, potansiyel bir saldırganın yararlanabileceği güvenlik açıklarını bulmanıza yardımcı olabilir. Elbette, bir ağa bağlı birden fazla bilgisayarın yöneticisi iseniz, onu kullanabilir ve bu bilgisayarların güvenliğini sağlayabilirsiniz.

Ancak, bu artık ücretsiz bir araç değil, [resmi web sitesinden](https://justpaste.it/redirect/7k3rd/https://www.tenable.com/try) 7 gün boyunca ücretsiz deneyebilirsiniz .

11. Burp Suite Scanner



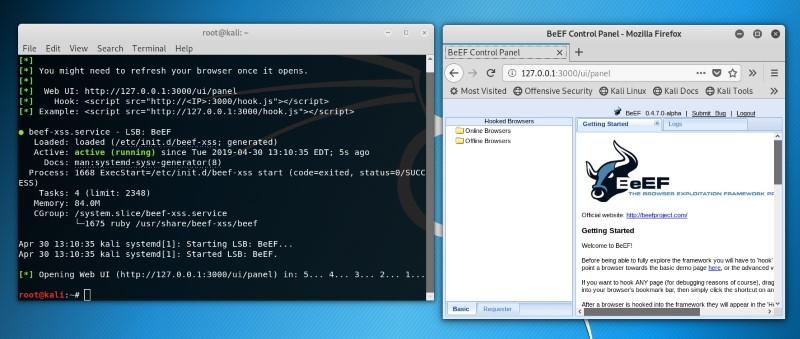
Burp Suite Community Edition

[Burp Suite Scanner](https://justpaste.it/redirect/7k3rd/https://portswigger.net/burp) , harika bir web güvenliği analiz aracıdır. Diğer web uygulama güvenlik tarayıcısının aksine, Burp bir GUI ve epeyce gelişmiş araçlar sunar.

Bununla birlikte, topluluk sürümü, özellikleri yalnızca bazı temel manuel araçlarla sınırlar. Profesyoneller için, yükseltmeyi düşünmeniz gerekecek. Önceki araca benzer şekilde, bu da açık kaynak değildir.

Ücretsiz sürümü kullandım, ancak bununla ilgili daha fazla ayrıntı istiyorsanız, [resmi web sitelerinde](https://justpaste.it/redirect/7k3rd/https://portswigger.net/burp) bulunan özelliklere göz atmalısınız .

12. BeEF

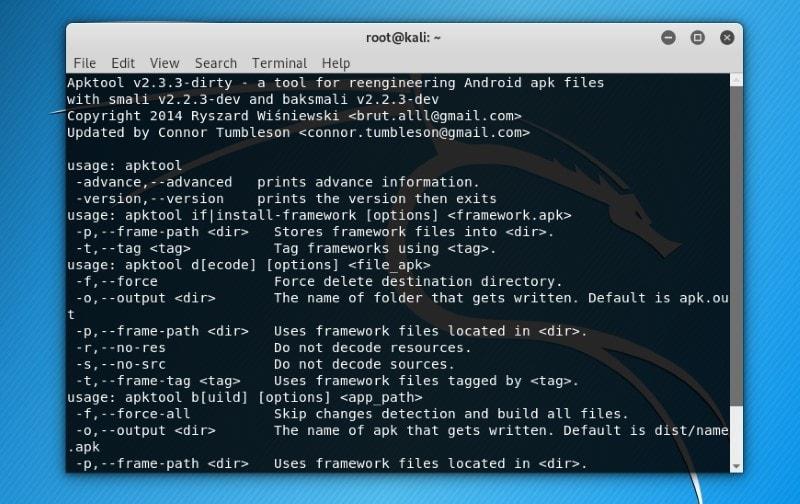


Sığır Eti Çerçevesi

BeEF (Browser Exploitation Framework) bir başka etkileyici araçtır. Bir web tarayıcısının güvenliğini değerlendirmek için sızma testi uzmanları için özel olarak tasarlanmıştır.

Bu, en iyi Kali Linux araçlarından biridir çünkü birçok kullanıcı, web güvenliği hakkında konuşurken istemci tarafındaki sorunları bilmek ve düzeltmek ister.

13. Apktool

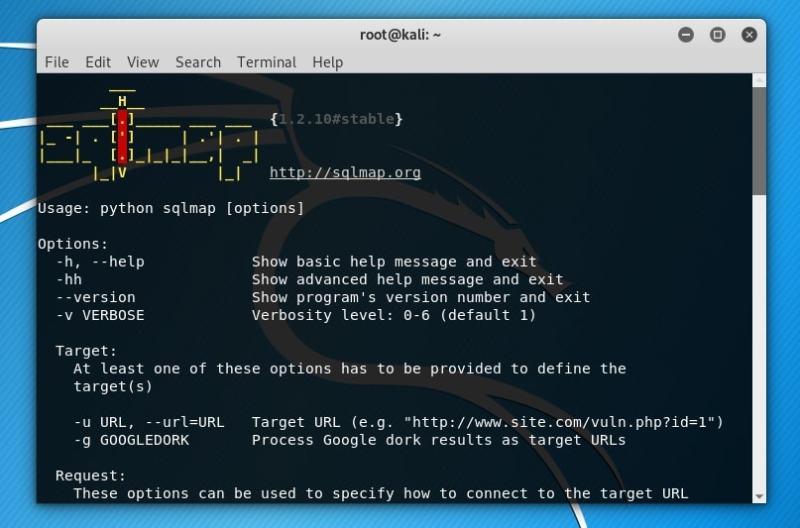


Apktool

[Apktool](https://justpaste.it/redirect/7k3rd/https://github.com/iBotPeaches/Apktool) , tersine mühendislik Android uygulamaları için Kali Linux'ta bulunan popüler araçlardan biridir. Tabii ki, eğitim amaçlı olarak onu iyi kullanmalısınız.

Bu araçla bazı şeyleri kendiniz deneyebilir ve orijinal geliştiricinin fikriniz hakkında bilgi sahibi olmasını sağlayabilirsiniz.

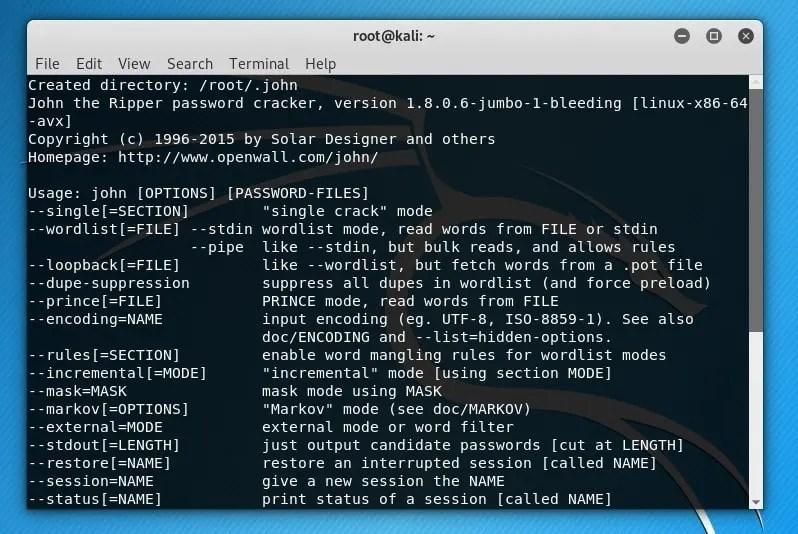
14. sqlmap



Sqlmap

Açık kaynak kodlu bir penetrasyon testi aracı arıyorsanız - [sqlmap](https://justpaste.it/redirect/7k3rd/http://sqlmap.org/) en [iyilerden](https://justpaste.it/redirect/7k3rd/http://sqlmap.org/) biridir. SQL enjeksiyon kusurlarından yararlanma sürecini otomatikleştirir ve veritabanı sunucularını ele geçirmenize yardımcı olur.

15. John the Ripper



John The Ripper

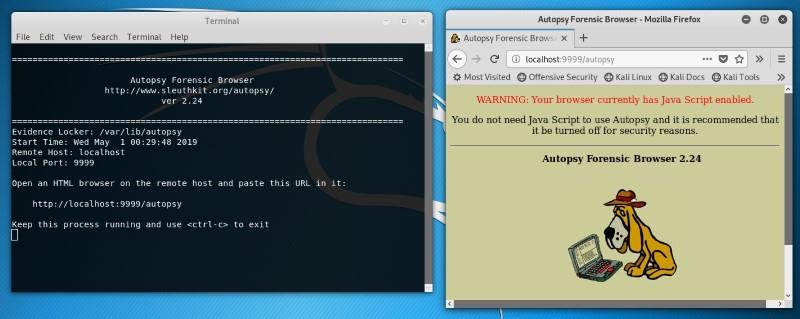
[John the Ripper](https://justpaste.it/redirect/7k3rd/https://github.com/magnumripper/JohnTheRipper) , Kali Linux'ta bulunan popüler bir şifre kırma aracıdır. Ücretsiz ve açık kaynaklıdır. Ancak, [topluluk tarafından geliştirilmiş sürümle](https://justpaste.it/redirect/7k3rd/https://github.com/magnumripper/JohnTheRipper) ilgilenmiyorsanız, ticari kullanım için [profesyonel sürümü](https://justpaste.it/redirect/7k3rd/https://www.openwall.com/john/pro/) seçebilirsiniz .

16. Snort

Gerçek zamanlı trafik analizi ve paket kaydı özelliği mi istiyorsunuz? [Snort](https://justpaste.it/redirect/7k3rd/https://www.snort.org/) arkanı [kolladı](https://justpaste.it/redirect/7k3rd/https://www.snort.org/). Açık kaynaklı bir saldırı önleme sistemi olmasına rağmen, sunabileceği çok şey var.

[Resmi web sitesi](https://justpaste.it/redirect/7k3rd/https://www.snort.org/%23get-started) Zaten yoksa yüklü almak için prosedür bahseder.

17. Autopsy Forensic Browser



Otopsi Adli Tarayıcı

[Autopsy](https://justpaste.it/redirect/7k3rd/https://www.sleuthkit.org/autopsy/) , bilgisayarınızda neler olduğunu araştırmak için dijital bir adli tıp aracıdır. Peki, SD karttan görüntüleri kurtarmak için de kullanabilirsiniz. Ayrıca kolluk kuvvetleri tarafından da kullanılıyor. Bununla neler yapabileceğinizi keşfetmek için [belgeleri](https://justpaste.it/redirect/7k3rd/https://www.sleuthkit.org/autopsy/docs*.*php) okuyabilirsiniz .

Ayrıca [GitHub sayfalarına](https://justpaste.it/redirect/7k3rd/https://github.com/sleuthkit/autopsy) da bakmalısınız .

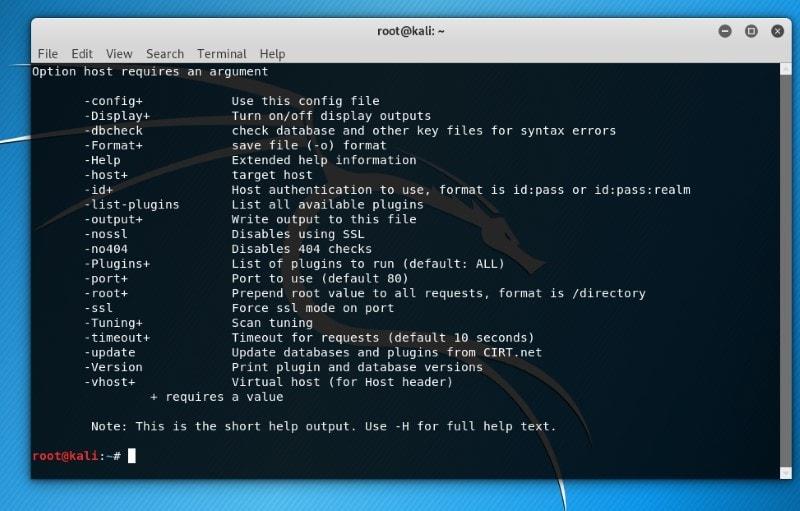
18. King Phisher



Kral Phisher

Kimlik avı saldırıları günümüzde çok yaygındır. Ayrıca [King Phisher aracı](https://justpaste.it/redirect/7k3rd/https://github.com/securestate/king-phisher) , gerçek dünyadaki kimlik avı saldırılarını simüle ederek test etmeye ve kullanıcı farkındalığını artırmaya yardımcı olur. Açık nedenlerden dolayı, bunu bir kuruluşun sunucu içeriğinde simüle etmek için izne ihtiyacınız olacaktır.

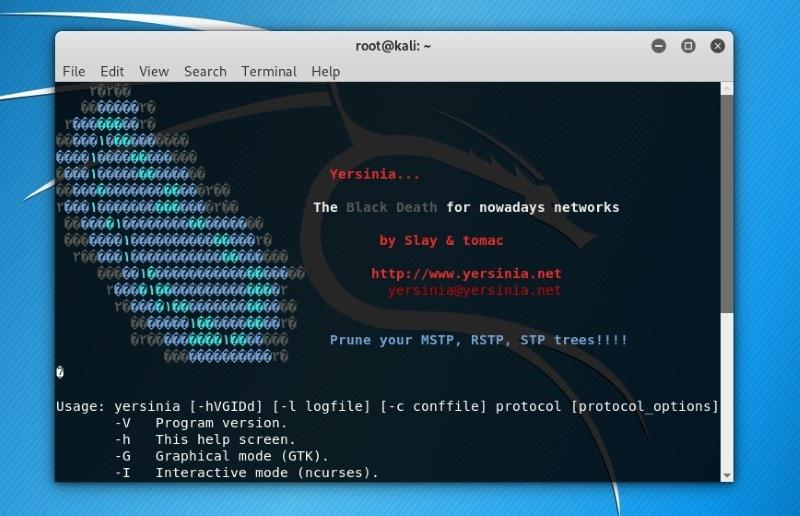
19. Nikto



Kimse

[Nikto](https://justpaste.it/redirect/7k3rd/https://gitlab.com/kalilinux/packages/nikto/) , onu mevcut en iyi Kali Linux araçlarından biri yapan güçlü bir web sunucusu tarayıcısıdır. Potansiyel olarak tehlikeli dosyalar / programlar, sunucunun eski sürümleri ve daha pek çok şeye karşı kontrol eder.

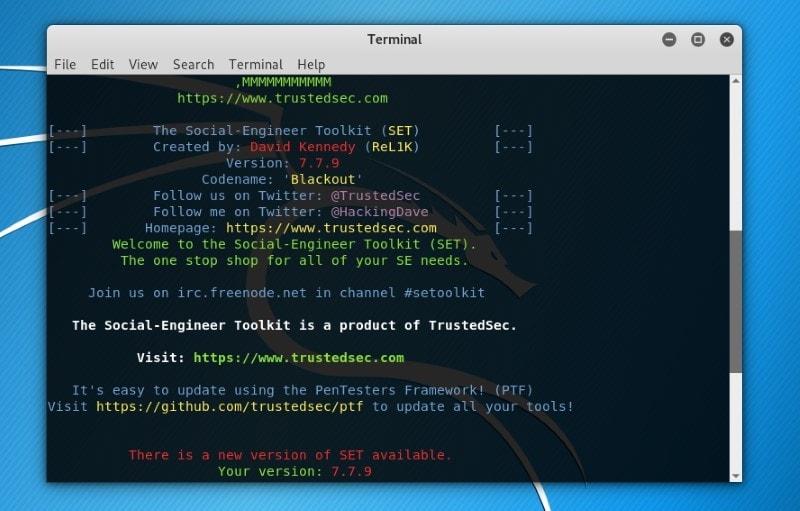
20. Yersinia



Yersinia

[Yersinia](https://justpaste.it/redirect/7k3rd/https://github.com/tomac/yersinia) , bir ağ üzerinde Katman 2 saldırıları (Katman 2, [OSI modelinin](https://justpaste.it/redirect/7k3rd/https://en.wikipedia.org/wiki/OSI_model) veri bağlantı katmanını ifade eder) gerçekleştirmek için ilginç bir çerçevedir . Elbette, bir ağın güvenli olmasını istiyorsanız, yedi katmanın tümünü göz önünde bulundurmanız gerekecektir. Ancak, bu araç Katman 2'ye ve STP, CDP, DTP ve benzerlerini içeren çeşitli ağ protokollerine odaklanır.

21. Social Engineering Toolkit (SET)



Sosyal Mühendislik Araç Seti

Oldukça ciddi penetrasyon testi işleriyle uğraşıyorsanız, kontrol etmeniz gereken en iyi araçlardan biri bu olmalıdır. Sosyal mühendislik çok önemlidir ve [SET](https://justpaste.it/redirect/7k3rd/https://www.trustedsec.com/social-engineer-toolkit-set/) aracı ile bu tür saldırılara karşı korunmaya yardımcı olabilirsiniz.