

## Metasploit Framework

Metasploit, güvenlik testlerinde kullanılan bir araçtır. Bilgisayar sistemlerindeki zayıf noktaları tespit etmek ve güvenlik açıklarını istismar etmek için kullanılır. Aynı zamanda exploit geliştirme ve otomatik saldırılar için geniş bir veritabanı sunar.



# Wireshark

Wireshark, ağ trafigini analiz etmek için kullanılan bir araçtır. Bu sayede ağdaki iletişimini yakalayabilir, paketleri inceleyebilir ve hataları veya güvenlik zayıflıklarını tespit edebilirsiniz.



@Linux.pro.tr

# Nmap

**Nmap, ağ taraması yapmak için kullanılan bir araçtır.**  
**Bir ağdaki cihazları ve açık portları taramanıza olanak sağlar.**  
**Ayrıca hedef sistemlerin işletim sistemini belirleyebilir**  
**ve ağdaki güvenlik açıklarını saptayabilirsiniz.**



@Linux.pro.tr

# Burp Suite

Burp Suite, web uygulamalarını test etmek ve güvenlik açıklarını tespit etmek için kullanılan bir pakettir. Proxy, tarayıcı ve zafiyet tarama gibi araçlar içerir. Bu sayede web uygulamalarınızın güvenliğini değerlendirebilir ve koruyabilirsiniz.



@Linux.pro.tr

# Nessus

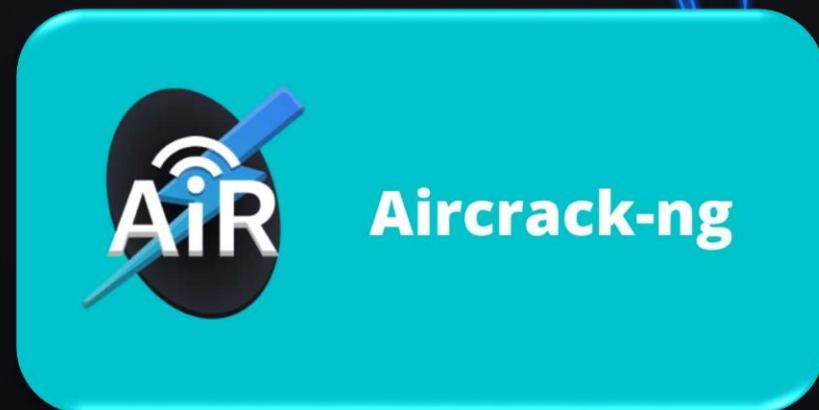
Nessus, zafiyet taraması yapmak için kullanılan bir araçtır. Sistemlerdeki güvenlik açıklarını otomatik olarak tespit eder ve raporlar oluşturur. Bu sayede bilgisayar ağınızdaki zayıf noktaları belirleyebilir ve düzeltici önlemler alabilirsiniz.



@Linux.pro.tr

# Aircrack-ng

Aircrack-ng, kablosuz ağların güvenliğini test etmek için kullanılan bir araçtır. Şifre kırma ve ağ trafigini analiz etme yetenekleri sunar. Bu sayede güvenliğinizinizi sağlamak için kablosuz ağınızı test edebilirsiniz.



@Linux.pro.tr

# Hydra

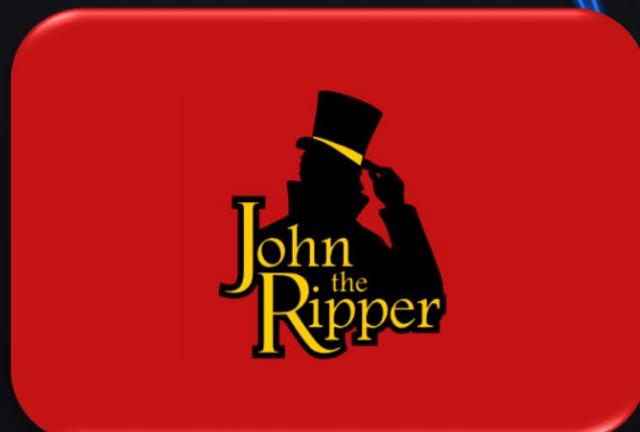
Hydra, kaba kuvvet saldırıları gerçekleştirmek için kullanılan bir araçtır.

Kullanıcı adı ve parola kombinasyonlarını deneyerek sistemlere yetkisiz erişim sağlamaya çalışır. Bu sayede zayıf parolaları tespit edebilir ve güvenlik önlemlerinizi güçlendirebilirsiniz.



# John the Ripper

**John the Ripper, parola kırma saldırıları için kullanılan bir araçtır. Şifrelenmiş parolaları kırmak veya kaba kuvvet saldırıları yapmak için kullanılır. Bu sayede sistemlerinizdeki zayıf parolaları keşfedebilir ve daha güçlü parolalar kullanabilirsiniz.**



# Maltego

Maltego, OSINT (Açık Kaynak İstihbarat) analizi için kullanılan bir araçtır. Bilgi toplama, veri görselleştirme ve ağ analizi yetenekleri sunar.

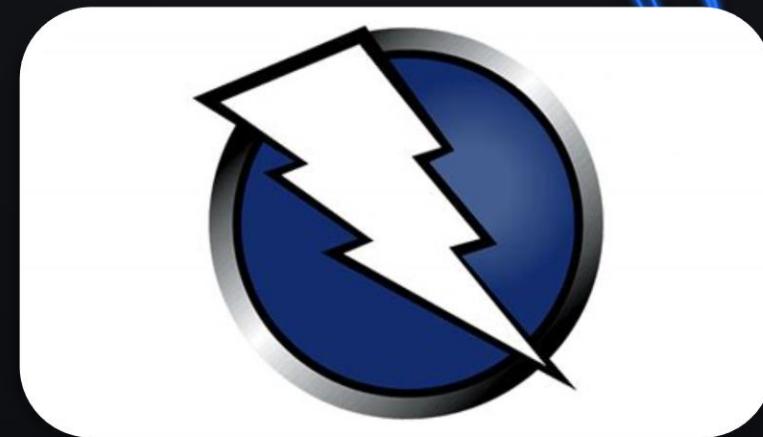
Bu sayede hedefleriniz hakkında daha fazla bilgi edinebilir ve güvenlik açıklarını belirleyebilirsiniz.



@Linux.pro.tr

# OWASP Zap

OWASP Zap, web uygulamalarında güvenlik testleri yapmak için kullanılan bir açık kaynaklı araçtır. Zafiyet taraması, sızma testleri ve web uygulama güvenliği analizi gibi özelliklere sahiptir. Bu sayede web uygulamalarınızı güvenli tutmak için potansiyel güvenlik açıklarını tespit edebilirsiniz.



@Linux.pro.tr

# sqlmap

**sqlmap**, web sitelerindeki güvenlik açıklarını tespit etmek için kullanılan bir araçtır.

Özellikle SQL enjeksiyonu adı verilen saldırılara karşı korunma sağlar. Bu sayede web sitelerindeki zayıf noktaları bulabilir ve bilgi sizıntılarına engel olabilirsiniz.



@Linux.pro.tr

# Dirb

**Dirb, web sitelerinde gezinirken gizli veya saklanmış dosyalara erişimi kolaylaştırın bir araçtır. Bir web sitesindeki dizin yapılarını tarar ve kullanıcılaraya yetkisiz erişime yol açabilecek potansiyel dosyalara ulaşmanızı yardımcı olur.**



```
root@kali:~# dirb http://192.168.1.106/
[...]
JIRB v2.22
By The Dark Raver
[...]
START TIME: Sat Oct 13 11:46:45 2018
URL_BASE: http://192.168.1.106/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[...]
GENERATED WORDS: 4612
[...]
---- Scanning URL: http://192.168.1.106/ ----
+ http://192.168.1.106/cgi-bin/ (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.1.106/dav/
+ http://192.168.1.106/index (CODE:200|SIZE:891)
+ http://192.168.1.106/index.php (CODE:200|SIZE:891)
+ http://192.168.1.106/phpinfo (CODE:200|SIZE:48077)
+ http://192.168.1.106/phpinfo.php (CODE:200|SIZE:48089)
==> DIRECTORY: http://192.168.1.106/phpMyAdmin/
+ http://192.168.1.106/server-status (CODE:403|SIZE:299)
==> DIRECTORY: http://192.168.1.106/test/
==> DIRECTORY: http://192.168.1.106/twiki/
[...]
--- Entering directory: http://192.168.1.106/dav/ ---
) WARNING: Directory IS LISTABLE. No need to scan it anyway.
```



# SET (Social Engineering Toolkit)

SET, sosyal mühendislik saldırısını gerçekleştirmeye yönelik bir araçtır. Sosyal mühendislik, insanların güvenini kazanarak hassas bilgilere erişmeyi hedefleyen bir saldırı türüdür. SET, bu tür saldırıları otomatize ederek kullanıcılarına bu konuda bilinç kazandırmayı amaçlar.



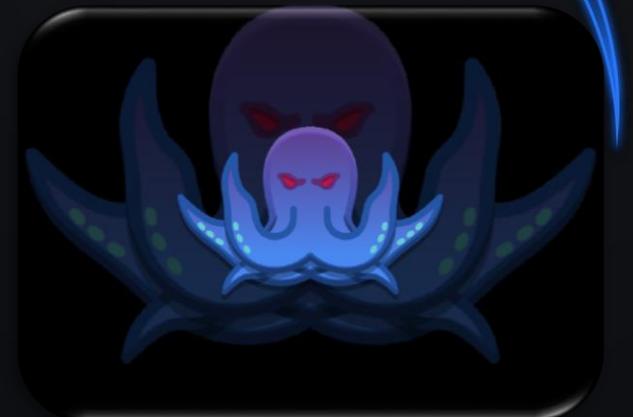
## Cain and Abel

Cain and Abel, ağ güvenliğini test etmek için kullanılan bir araçtır. Özellikle ağdaki parolaları kırma ve ağ trafigini izleme gibi yeteneklere sahiptir. Bu sayede ağınızdaki zayıf noktaları keşfedebilir ve güvenlik önlemlerini artırabilirsiniz.



@Linux.pro.tr

Wfuzz, web sitelerinde brute force saldırıları yapmaya yönelik bir araçtır.  
Brute force saldırıları, kullanıcı adları, parolalar veya dizinler  
gibi hedefe özgü parametreleri deneyerek güvenlik açıklarını bulmayı hedefler.  
Bu sayede web sitelerinizin güvenliğini test edebilirsiniz.



# hping

hping, ağ paketlerini manipüle etmeye ve analiz etmeye yarayan bir araçtır. Ağdaki cihazları veya sunucuları test etmek, port taraması yapmak veya ağ performansını değerlendirmek için kullanılabilir. Bu sayede ağınızdaki güvenlik açıklarını tespit edebilirsiniz.



@Linux.pro.tr

## Medusa

Medusa, parola kırma saldırıları gerçekleştirmek için kullanılan bir araçtır. Özellikle SSH, FTP veya Telnet gibi protokollerde zayıf parolaları tespit etmek için kullanılır. Bu sayede sistemlerinizde güçlü parolalar kullanabilir ve güvenliğinizin artırılabilirsiniz.



# WPScan

WPScan, WordPress tabanlı web sitelerinde güvenlik taraması yapmak için kullanılan bir araçtır. Zayıf parolaları tespit etmek, güvenlik açıklarını kontrol etmek ve web sitenizin güvenliğini artırmak için kullanılabilir.



**WPScan**



@Linux.pro.tr

# THC-Hydra

THC-Hydra, kaba kuvvet saldırıları yapmak için kullanılan bir araçtır. Kullanıcı adı ve parola kombinasyonlarını deneyerek sistemlere yetkisiz erişim sağlamaya çalışır. Özellikle farklı protokoller ve servisler üzerinde kullanılabilir.



@Linux.pro.tr

BeEF, tarayıcı tabanlı saldırılar gerçekleştirmek için kullanılan bir araçtır. XSS (Cross-Site Scripting) saldırıları yapabilir, tarayıcı oturumlarını ele geçirebilir ve çeşitli saldırı senaryolarını simüle edebilir. Bu sayede web uygulamalarının güvenliğini değerlendirebilirsiniz.



# Zed Attack Proxy (ZAP)

ZAP, web uygulamalarının güvenlik testlerinde kullanılan bir araçtır. Web sitelerini tarayarak güvenlik açıklarını tespit eder ve size bu açıkların nasıl giderileceği konusunda öneriler sunar. Bu sayede web sitenizin güvenliğini artırabilirsiniz.



@Linux.pro.tr

# Evilginx

Evilginx, phishing saldırıları için kullanılan bir araçtır. Bu araç, saldırganlara hedef kullanıcıların kimlik bilgilerini çalmak için phishing saldırılarını otomatize etme imkanı sağlar. Dikkatli olmanız ve bilinçli bir şekilde bu aracı kullanmanız önemlidir.



@Linux.pro.tr

# Fern Wifi Cracker

Fern Wifi Cracker, kablosuz ağlarda güvenlik testleri yapmak için kullanılan bir araçtır. Ağınıza bağlı olan cihazların güvenlik seviyesini değerlendirmenizi sağlar ve şifre kırma yetenekleri sunar. Bu sayede kendi kablosuz ağınızın güvenliğini kontrol edebilirsiniz.



# Snort

Snort, ağ tabanlı saldırıları tespit etmek için kullanılan bir Intrusion Detection System (IDS) aracıdır. Ağ trafigini izleyerek bilinen saldırı kalıplarını tespit eder ve size alarm verir. Bu sayede ağınızın güvenliğini sağlamak için saldırıları erken aşamada tespit edebilirsiniz.



@Linux.pro.tr

# Nikto

**Nikto, web sunucularında güvenlik açıklarını taramak için kullanılan bir araçtır.**  
**Web sitelerinizi zafiyetlere karşı tarayarak potansiyel güvenlik**  
**açıklarını ortaya çıkarır. Bu sayede web sitenizin güvenliğini**  
**artırabilir ve güvenlik önlemleri alabilirsiniz.**



W3af, web uygulamalarında güvenlik testleri yapmak için kullanılan bir araçtır. Web sitenizin güvenlik açıklarını tespit ederek size raporlar sunar. Bu sayede web sitenizin güvenliğini değerlendirebilir ve gereken önlemleri alabilirsiniz.



# Gobuster

**Gobuster, web sitelerinde dizin taraması yapmak için kullanılan bir araçtır.**  
**Web sitenizin alt dizinlerini tarayarak gizli veya saklanmış dosyalara**  
**erişim sağlamanıza yardımcı olur. Bu sayede web sitenizin güvenliğini**  
**test edebilir ve eksiklikleri gidermek için adımlar atabilirsiniz.**



# Sublist3r

**Sublist3r, bir alan adına ait alt alanları keşfetmek için kullanılan bir araçtır. Hedef alan adının alt alanlarını tarar ve size potansiyel hedefleri sunar.**

**Bu sayede daha kapsamlı bir saldırı yüzeyi oluşturabilir ve hedeflerinizi belirleyebilirsiniz.**



@Linux.pro.tr

# XSSStrike

XSSStrike, cross-site scripting (XSS) saldırılarını gerçekleştirmek için kullanılan bir araçtır. Web uygulamalarında güvenlik açıklarını tespit ederek XSS saldırılarını otomatize eder. Bu sayede web uygulamalarının güvenlik açıklarını tespit edebilir ve gerekli önlemleri alabilirsiniz.



@Linux.pro.tr

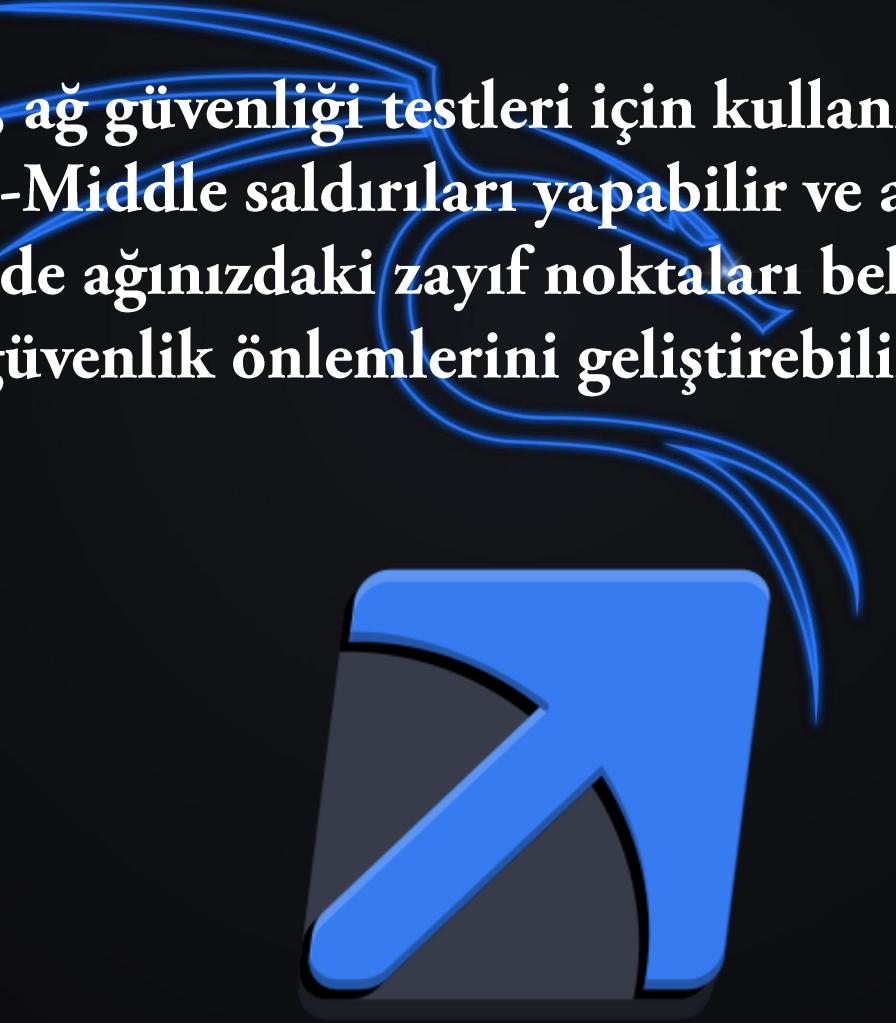
## Kismet

**Kismet, kablosuz ağlarda güvenlik testleri yapmak için kullanılan bir araçtır.**  
**Ağınızda tespit edilen kablosuz cihazları izler ve potansiyel güvenlik açıklarını belirler.**  
**Bu sayede kablosuz ağınızın güvenliğini değerlendirebilir**  
**ve gereken önlemleri alabilirsiniz.**



## Responder

Responder, ağ güvenliği testleri için kullanılan bir araçtır. Bir ağda Man-in-the-Middle saldırıları yapabilir ve ağ trafigini takip edebilir. Bu sayede ağınızdaki zayıf noktaları belirleyebilir ve güvenlik önlemlerini geliştirebilirsiniz.



# openVAS

OpenVAS, bir ağın güvenlik açıklarını taramak için kullanılan bir araçtır.  
Sistemdeki zayıf noktaları tespit eder ve raporlar sunar.  
Bu sayede bilgisayar sistemlerinizi daha güvenli hale getirebilirsiniz.



@Linux.pro.tr

# Volatility

Volatility, bilgisayar belleği analizi yapmak için kullanılan bir araçtır. Bellek görüntülerini inceleyerek kötü amaçlı yazılımların izlerini sürer ve saldıruları tespit eder. Bu sayede bilgisayarlarınızın güvenliğini sağlamak için önlemler alabilirsiniz.



Patator, kaba kuvvet saldırıları yapmak için kullanılan bir araçtır. Kullanıcı adı ve parola kombinasyonlarını deneyerek giriş yetkisi elde etmeyi amaçlar. Bu sayede güçlü parolalar kullanarak hesaplarınızın güvenliğini sağlayabilirsiniz.



# Maltrail

Maltrail, ağdaki kötü niyetli aktiviteleri izlemek için kullanılan bir araçtır. Sistemdeki potansiyel saldırıları tespit eder ve size uyarılar gönderir. Bu sayede ağınızdaki güvenlik açıklarını belirleyebilir ve önlem alabilirsiniz.



@Linux.pro.tr

# Netcat

Netcat, ağda veri iletişimini yapmak için kullanılan bir araçtır. Çok yönlü bir ağ aracıdır ve port taraması, dosya transferi ve ağ bağlantıları gibi işlemleri gerçekleştirebilir. Bu sayede ağınızdaki iletişimini yönetebilirsiniz.



drozer

Trozer, USB cihazlarını güvenlik testleri için kullanılan bir araçtır.  
USB cihazlarını tarar ve içerisindeki dosyaları analiz eder.  
Bu sayede bilgisayarınıza zararlı bir USB cihazı  
takılıp takılmadığını kontrol edebilirsiniz.

→ drozer →



@Linux.pro.tr

# RSMangler

RSMangler, parola kırma saldırıları için kullanılan bir araçtır.  
Parola kombinasyonları oluşturarak güçlü parolaları kırmayı hedefler.  
Bu sayede hesaplarınızı güvenli hale getirebilirsiniz.



# SpiderFoot

SpiderFoot, internet üzerindeki kaynakları tarayarak bilgi toplamak için kullanılan bir araçtır. Bir hedefle ilgili açık kaynak istihbaratı (OSINT) toplama yeteneğine sahiptir. Bu sayede hedefiniz hakkında daha fazla bilgi edinebilir ve güvenlik açıklarını belirleyebilirsiniz.



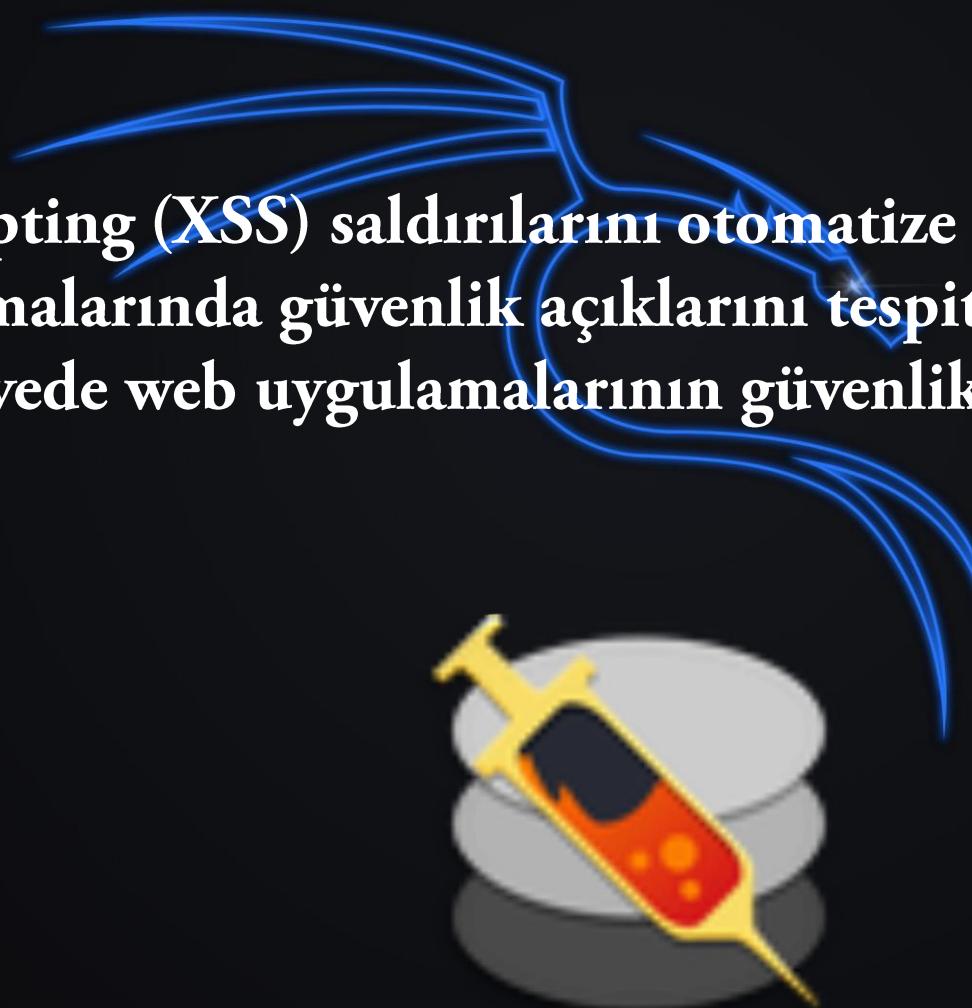
@Linux.pro.tr

# Bettercap

Bettercap, ağ güvenliği testleri için kullanılan bir araçtır. Man-in-the-Middle saldırılarını gerçekleştirebilir ve ağ trafigini manipüle edebilir. Bu sayede ağınızdaki güvenlik zayıflıklarını tespit edebilir ve önlemler alabilirsiniz.



XSSer, cross-site scripting (XSS) saldırılarını otomatize etmek için kullanılan bir araçtır. Web uygulamalarında güvenlik açıklarını tespit eder ve XSS saldırılarını gerçekleştirir. Bu sayede web uygulamalarının güvenlik açıklarını kontrol edebilirsiniz.



# Recon-ng

econ-**ng**, bilgi toplama (*reconnaissance*) için kullanılan bir araçtır. Farklı kaynaklardan veri toplar, hedefler hakkında bilgi edinir ve analizler yapar. Bu sayede hedefinizi daha iyi anlayabilir ve güvenlik açıklarını belirleyebilirsiniz.



@Linux.pro.tr

# Armitage

Armitage, Metasploit Framework'ün kullanıcı dostu bir grafik arayüzüdür. Sistem penetrasyon testleri ve saldırı simülasyonları yapmak için kullanılır. Bu sayede hedef sistemlere karşı saldırı senaryolarınızı yönetebilirsiniz.



@Linux.pro.tr

MITMf (Man-in-the-Middle Framework), ağ üzerinde Man-in-the-Middle saldırıları gerçekleştirmek için kullanılan bir araçtır. Ağ trafigini yönlendirir, paketleri manipüle eder ve kullanıcıların verilerini ele geçirir. Bu sayede ağ güvenliği açısından zayıf noktaları tespit edebilirsiniz.



# Dirbuster

Dirbuster, web sitelerinde gizli veya saklanmış dosyaları bulmak için kullanılan bir araçtır. Web sitesinin dizin yapısını tarayarak kullanıcılar yetkisiz erişime yol açabilecek potansiyel dosyalara ulaşmanızı yardımcı olur. Bu sayede web sitenizin güvenliğini test edebilirsiniz.



# Masscan

Masscan, ağ taramaları yapmak için kullanılan hızlı bir port tarama aracıdır.  
Büyük ağlarda portları taramak için optimize edilmiştir.  
Bu sayede ağınızdaki güvenlik açıklarını tespit edebilirsiniz.



@Linux.pro.tr

2sqlninja, SQL enjeksiyon saldırınızı otomatize etmek için  
kullanılan bir araçtır. Web uygulamalarının veritabanlarında  
güvenlik açıklarını tespit eder ve saldırılar gerçekleştirir.  
Bu sayede web uygulamalarının güvenliğini kontrol edebilirsiniz.



# BruteXSS

BruteXSS, cross-site scripting (XSS) saldırınızı gerçekleştirmek için kullanılan bir araçtır. XSS saldırınızı otomatize ederek web uygulamalarının güvenlik açıklarını tespit eder. Bu sayede web uygulamalarının güvenliğini test edebilirsiniz.



# Faraday

Faraday, sızma testi ve güvenlik analizi için kullanılan bir araçtır. Bilgi toplama, zafiyet taraması, saldırısı simülasyonu gibi özelliklere sahiptir. Bu sayede sızma testlerinizi yönetebilir ve güvenlik açıklarını belirleyebilirsiniz.



@Linux.pro.tr

# SSLStrip

sslstrip, ağ üzerindeki SSL/TLS bağlantılarını etkisiz hale getirmek için kullanılan bir araçtır. SSL/TLS korumasının olmadığı bağlantıları ele geçirir ve kullanıcıların verilerini çalabilir. Bu sayede ağ güvenliği açısından zayıf noktaları belirleyebilirsiniz.



SSLStrip



@Linux.pro.tr