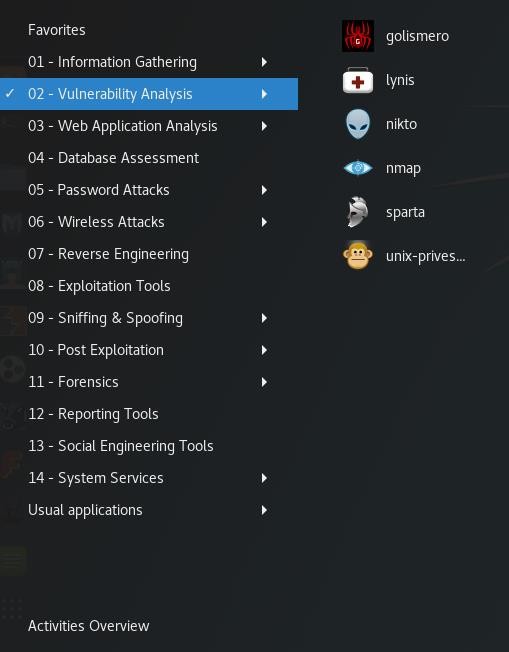
# 1-) İnformation Gathering

İlk Bölüm bilgi toplama araçlarından(**information gathering**) olup herhangi bir sistem üzerinde aktif veya pasif bilgiler elde etmek için farklı farklı araçlar geliştirilmiştir.

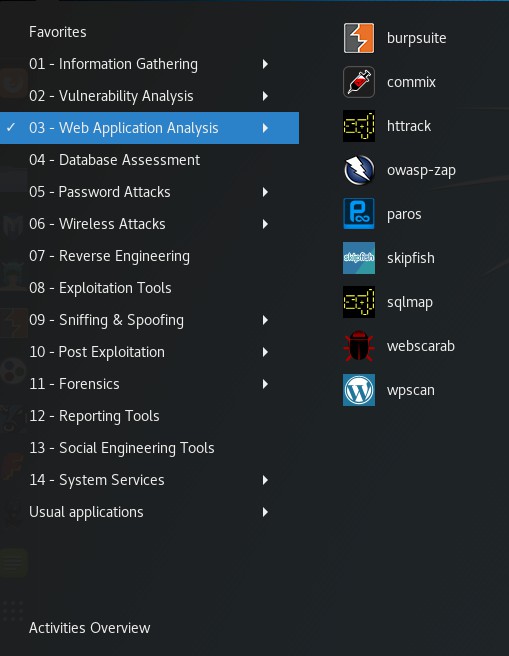
# 2-) Vulnerability Analysis

Güvenlik analizleri ile ilgili tüm araçlar burada yer alır. Örnek olarak nmap aracı ile aynı ağ içerisindeki bir bilgisayar üzerinde tarama yapıp port açıklarını veya sistem güvenlik açıklarına erişebilirsiniz.



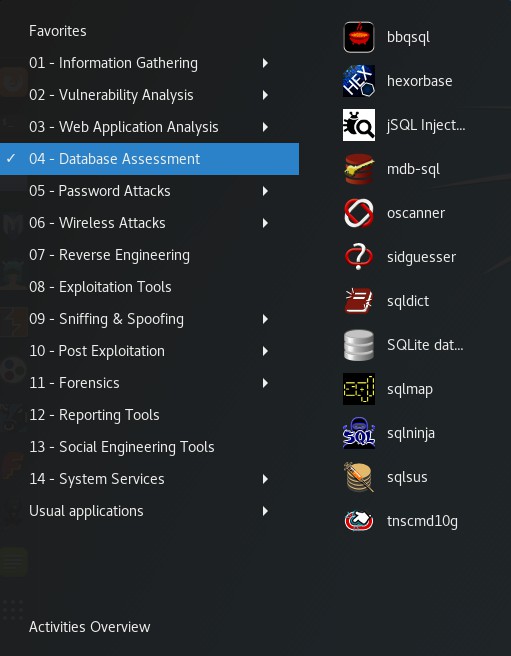
# 3-)Web Application Analysis

Burada WeB uygulama analizleri üzerinde geliştirilmiş araçlar mevcut- tur. Örnek olarak owasp-zap aracını kullanarak herhangi bir site üze- rinde zafiyet taramasını gerçekleştirip sistem açıklarına erişebilirisiniz. Veya wpscan aracı ile wordpres sitelerde admin şifre ve kullanıcı adını elde edebilirsiniz.



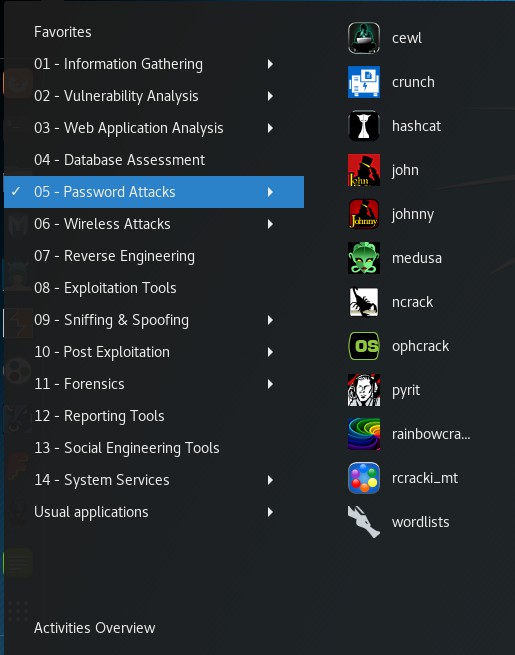
# 4-)Database Assessment

Veritabanı ile ilegili tüm araçlar burada yer alır.Bu bölüm çok önemli olup açıklı sitelerde veri tabana sızma işleminden tutun web site site- nin zafiyetlerini taramaya kadar tüm işlemler burada yer alan araçlar ile gerçekleştirmektedir.



# 5-)Password Attacks

Burada Şifre saldırıları ile ilgili araçlar yer alır.burada kullancı şifreleri- ne saldırı , sistem şifresine saldırı,wordlist ile saldırı vb diğer bütün

saldırı çeşitleri burada yer almaktadır.

# 6-)Wireless Attacks

Burada wi-fi ağlarına yönelik saldırılar yapmak için geliştirilmiş araçlar mevcut.Örnek olarak sahte bir ağ yaymak , etraftaki ağları tarama ,

kullanıcıları ağdan atma, wi-fi ağına yönelik saldırılar gibi birçok araç burada yer almaktadır.



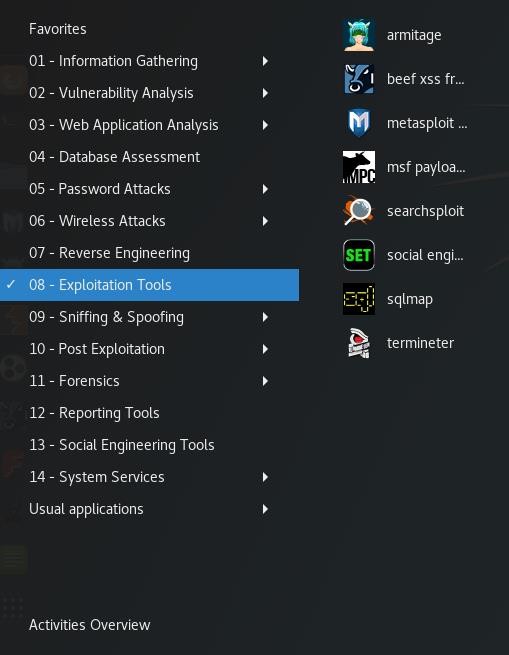
# 7-)Reverse Engineering

Ters mühendislik dediğimiz bu alan günlük hayatta sık kullanacağımız araçlardan pek sayılmaz.Burada bu araçlarla en çok yapılabilen şeyler arasında yapılmış olan bir aracı incelemek sistemin nasıl çalıştığını anlamak için kullanabileceğimiz araçlardır.



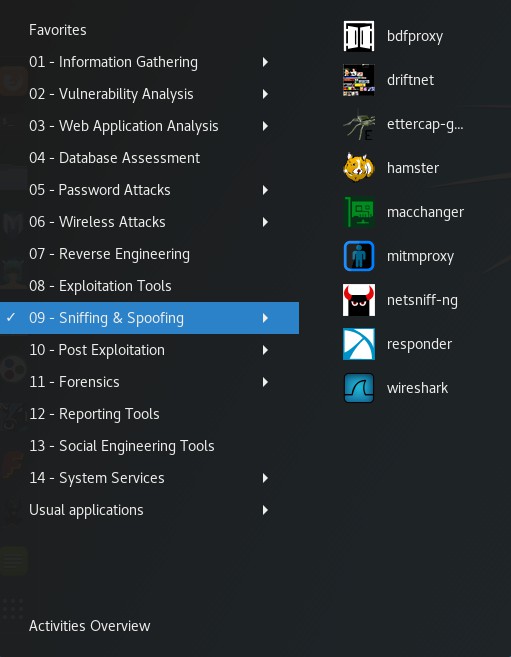
# 8-)Exploitation Tools

Burada Daha çok sistem üzerinde sömürme işlemleri için geliştirilmiş araçlar yer alır.Örnek olarak burada sık kullanılan araçlardan metasp- loit aracı sistem üzerindeki açıklardan faydalanıp sisteme sızmamızı

sağlayan araçlardan biridir.

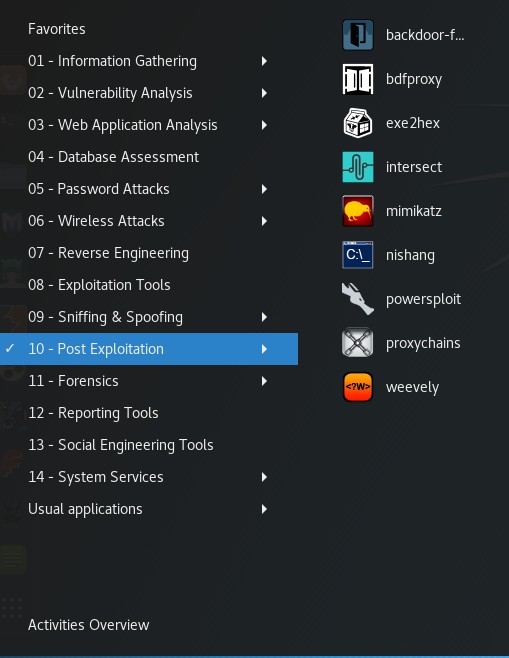
# 9-)Sniffing & Spoffing

Burada daha koklama, oltalama gibi yöntemlerle araçları kullanıp sistemde istenilen bilgilere erişme , servis dışı bırakma veya sistemi izleme gibi araçlar kullanılır.Örnek olarak driftnet aracı ile aynı ağdaki kullanıcıların girdiği web sitelerdeki resimleri görmemizi sağlar.



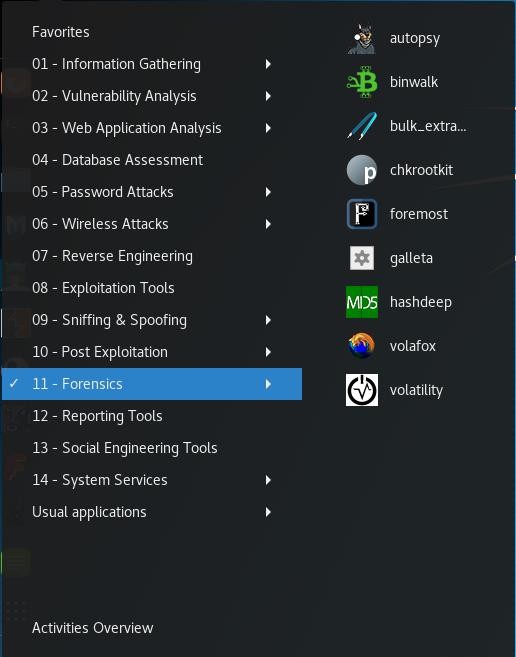
# 10-)Post Exploitation

Burada sistemi sömürdükten sonra kullanabilen araçlar yer alır.Örnek olarak backdoor faktory aracı ile yeni bir arka kapı oluşturup sisteme sızmamıza olanak sağlar.



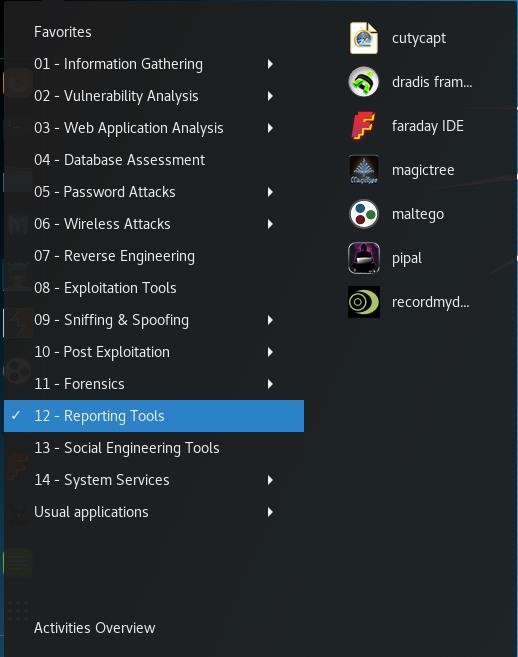
# 11-)Forensics

Adli bilişim alanı ile ilgili kullanılabilen tüm araçlar burada yer almak- tadır.Örnek olarak **volability** aracı ile suç işleyen bir bilgisayar korsa- nın bilgisayarın ram imajını alarak sistem açık iken yapılan tüm işlem- leri ram imajı üzerinden analiz ederek bilgiler elde edebiliriz.Veya **autopsy** aracı ile yeni bir dava oluşturup yine imaj üzerinde inceleme- ler gerçekleştirebiliriz.



# 12-)Reporting Tools

Raporlama işlemleri ile ilgili tüm araçlar bu menüde yer almakta- dır.Yapılan herhangi bir analiz veya tarama sonucunda analizlerimizi rapor haline getirip bu araçlar üzerinde barındırmak , analiz etmek , incelemek için kullanırız.Örnek olarak dradis aracı ile test sonuçları- mızı buarad barındırıp daha sonra tüm kullanıcılar için tek bir noktada toplayabiliriz.



# 13-)Social Engineering tools

Burada sosyal mühendislik ile ilgili tüma araçlar yer almaktadır.sosyal mühendislik bölümü daha çok kullanıcıları birtakım uydurmalarla kandırıp ve aldatıp sahte link,e-posta veya sahve site gibi gibi yöntem- lerle bilgilerini ele geçirme işlemleri ele alınır.

