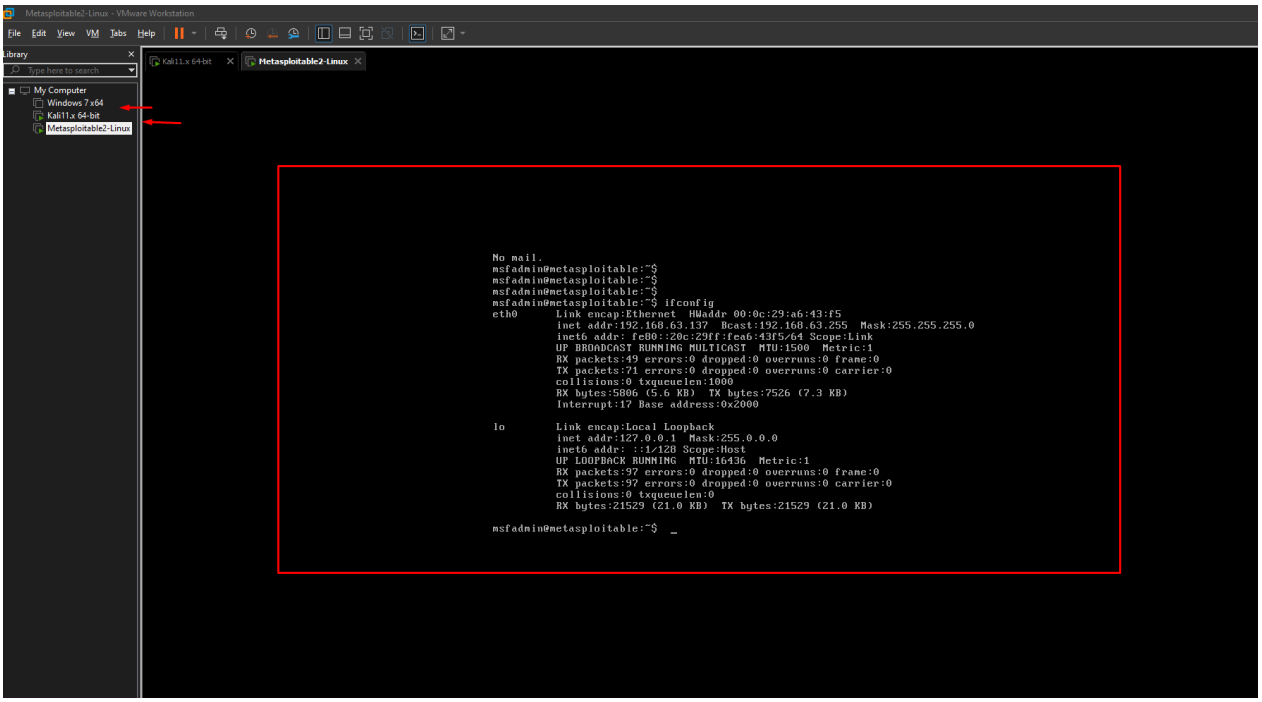
1 Metasploit2 zafiyetli makina kurulumu indirilecek.

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

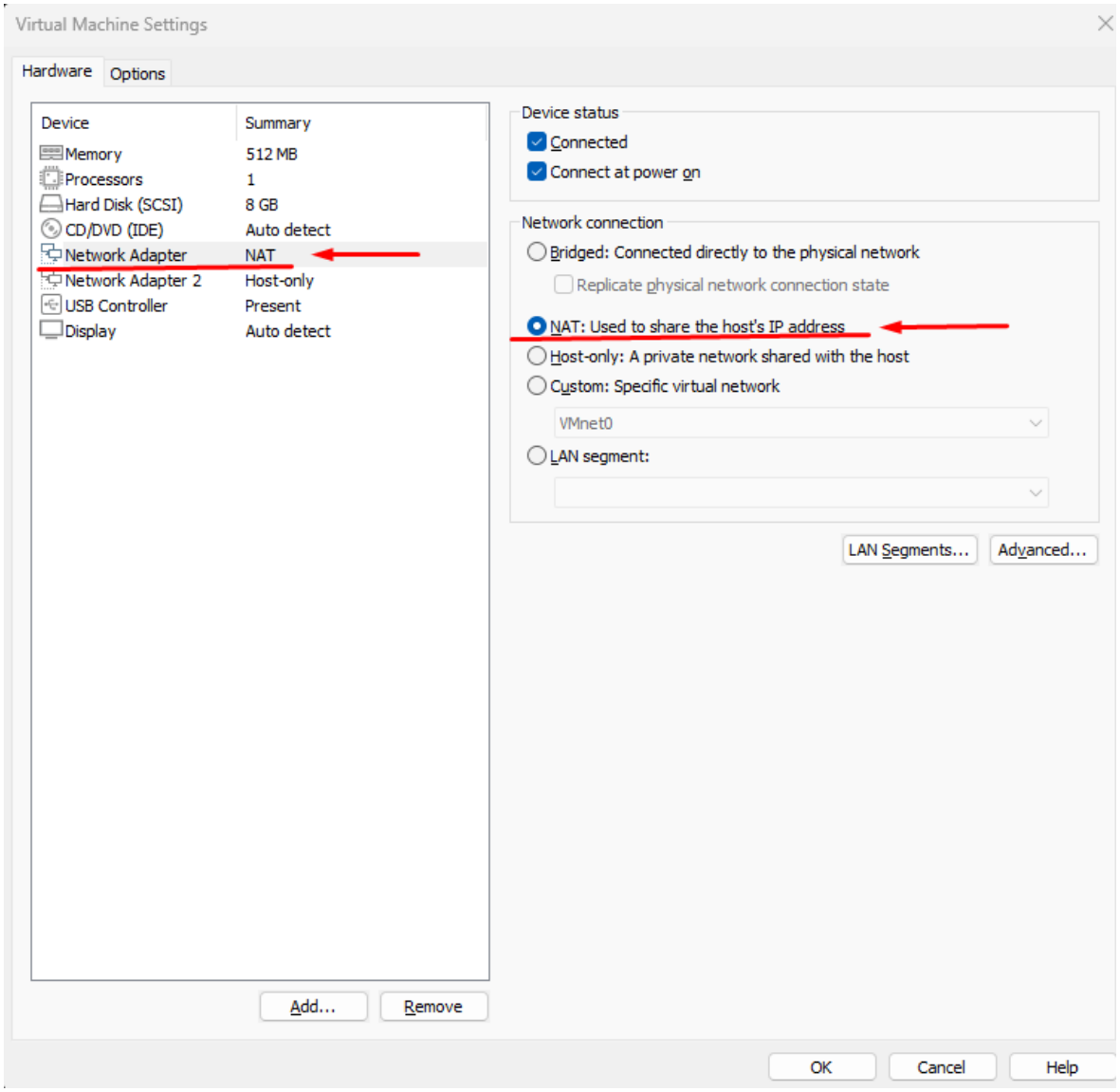
İlgi zafiyet makinesini indirdim, VMware üzerinde sanal makine olarak kurdum.



Ayrıca, VMware üzerindeki makinelerin network ayarlarını NAT'a almamız gerekiyor ki bu sayede cihazlar aynı network üzerinde olsun ve nmap taramalarına cevap alabilelim. Yani hem sanal makine üzerindeki kali hem de Metasploit 2 zafiyetli makinesi aynı ağ üzerinde olmalı. Bu yüzden network ayarlarından ikisini de NAT' almamız gerekiyor.

Tabii, gerçek hayattaki sızma testlerinde hedef makine local'de değilse ya da aynı network üzerinde değilse bu tarz uğraşlara gerek yok. Sadece kali'nin çalıştığı sanal makineyi internete çıkarmamız gerekli. NAT ya da bridged mode kullanılabilir.

Network ayarı aşağıdaki şekildeki gibi olmalıdır;



2- Zafiyetli makinada port taraması yapılacak.

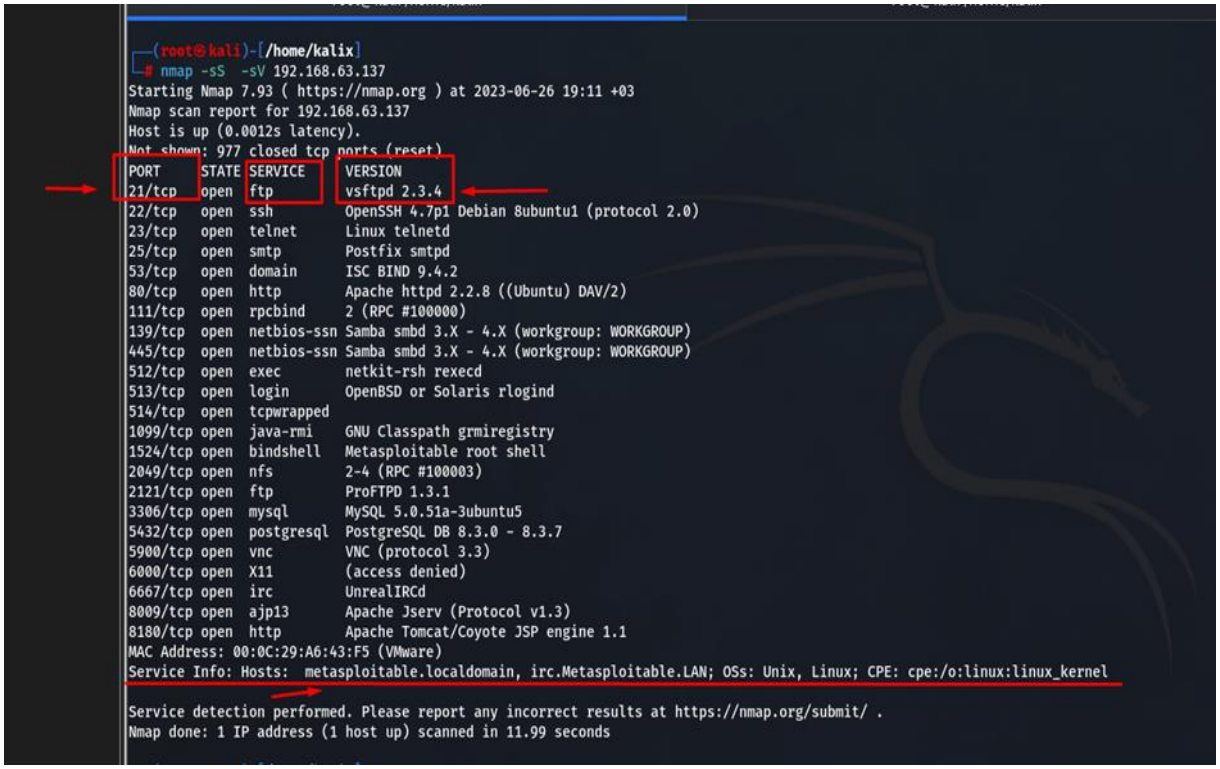
Zafiyetli makinenin ip'sini öğreniyoruz, daha sonra bu ip adresini nmap ile tarıyoruz.

Kod: **nmap -sS -sV 192.168.63.137**

Çıktı olarak hedef ip üzerindeki portlar hakkında çeşitli bilgiler ediniyoruz. Girdiğimiz komut bize sadece açık portları listeliyor ki bizim işimize yarayacak olan portlar da bunlar. Ayrıca her port üzerinde çalışan servisleri ve o servislerin sürümleri hakkında da çeşitli bilgiler veriyor.

Riskli portlar sırasıyla 21. Portta çalışan ftp servisi, 80. ve 8180. porttaki çalışan http servisi (paketler şifrelenmiyor) ve 23. Porttaki telnet (paketler şifrelenmiyor) riskli portlar. Ayrıca açık olan sql portları da fakat bu servisler local'de çalışıyor. Eğer bu portlar (yani aslında servisler) internete açık olursa çok büyük zafiyete sebep olur. Fakat burada bizden istenen ftp servisi üzerinden hedef makineye sızmamız. Bu yüzden bizi ilgilendiren sadece 21. Porttaki çalışan servis ve onun versiyonu.

```
┌──(root㉿kali)-[/home/kalix]
└─# nmap -sS  -sV 192.168.63.137
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 19:11 +03
Nmap scan report for 192.168.63.137
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
```

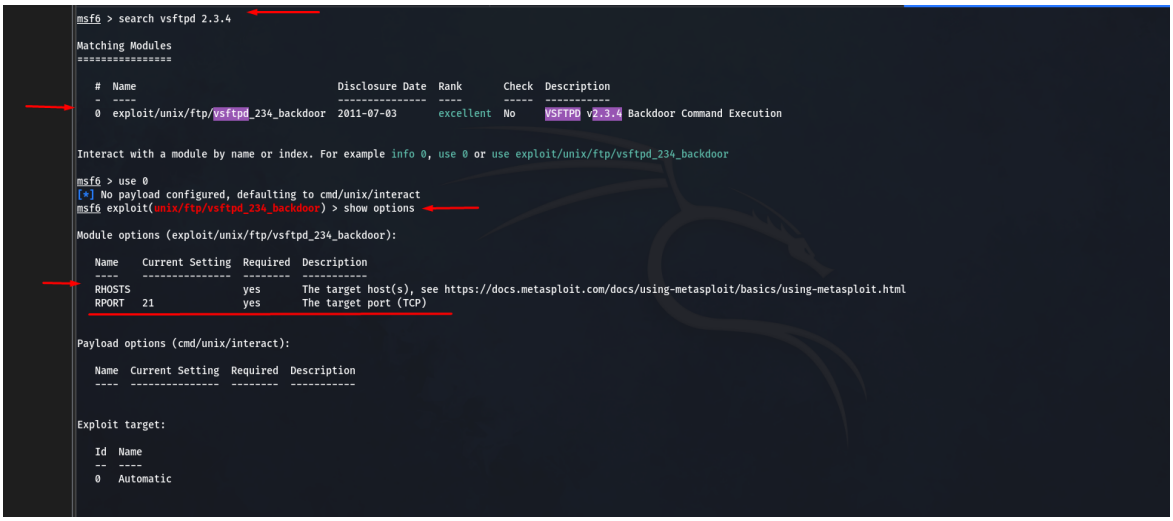


Zafiyetli makine üzerindeki açık portları ve versiyonlarını tespit ettik. Biz ftp servisi üzerinden zafiyet sömüreceğiz bu yüzden port 21'de çalışan ftp versiyonunu kullanacağız.

3- Ftp servisinin güvenlik açığından yararlanarak zafiyetli bilgisayara giriş yapılacak.



sudo su komu ile yönetici yetkisi alıyoruz ve msfconsole yazarak metasploit'in ilgili framework'ünü açıyoruz.



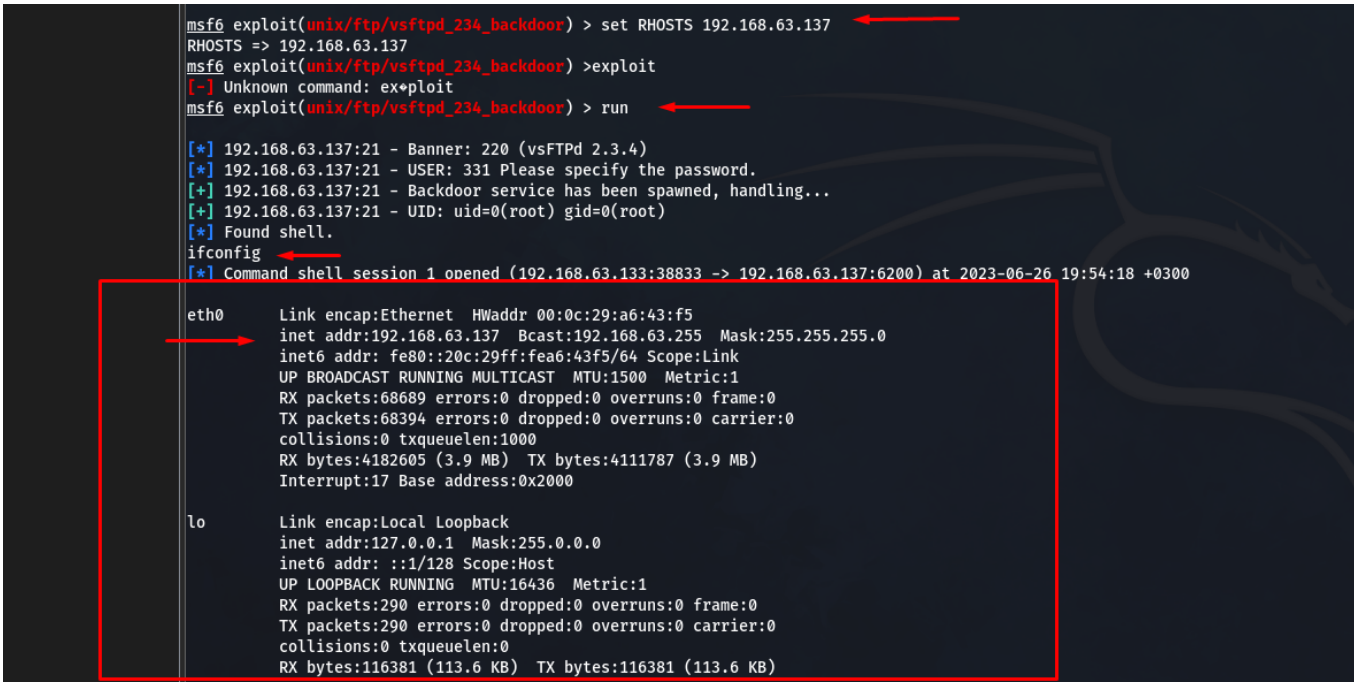
search komutu ile çalışan ftp servisinin versiyonuna göre modül buluyoruz.

use 0 (id'sine göre seçiyoruz) diyerek ilgili modülü seçiyoruz.

show options diyerek girmemiz gereken eksik parametreleri görüntülüyoruz

set RHOST parametresinin eksik olduğunu tespit ediyoruz. Bu parametreye hedef makinenin ip adresini giriyoruz, yani 192.168.63.137.

Başka eksik parametremiz yok, o yüzden run ya da exploit diyerek çalıştırabiliriz.



4- Giriş yapılınca ifconfig komutu çalışıtılacak.

Sisteme girdik ve Shell açıldı. Yazdığımız her komut şu an hedef bilgisayarın shell'inde çalışabilir.

ifconfig diyerek hedef bilgisayarın ip adresini kontrol edebiliriz. Gördüğünüz üzere 192.168.63.137 ip adresini çıktı olarak aldık. Yani başarı ile karşı tarafa sızdık ve shell'de komut çalıştırabildik.

whoami komutu ile de sisteme ne olarak sızdığımızı görüntüleyebiliyoruz. Biz şu an sistemde root yetkisi ile sızmışız ki bu sistemdeki en üst yetkidir.

