**Metasploitable 2 | Serverə sızma hesabatı**



Əməliyyat sistemi : Kali Linux

**Məzmun:**

1. Şəbəkə taraması
2. Qarşı tərəfin ip adressini seçirik
3. Serverin ip adressinin tamamilə taranması
4. Bizə uyğun açıq port və protokolun seçilməsi
5. Versiyası və s. Haqqında
6. Sızma prosesləri

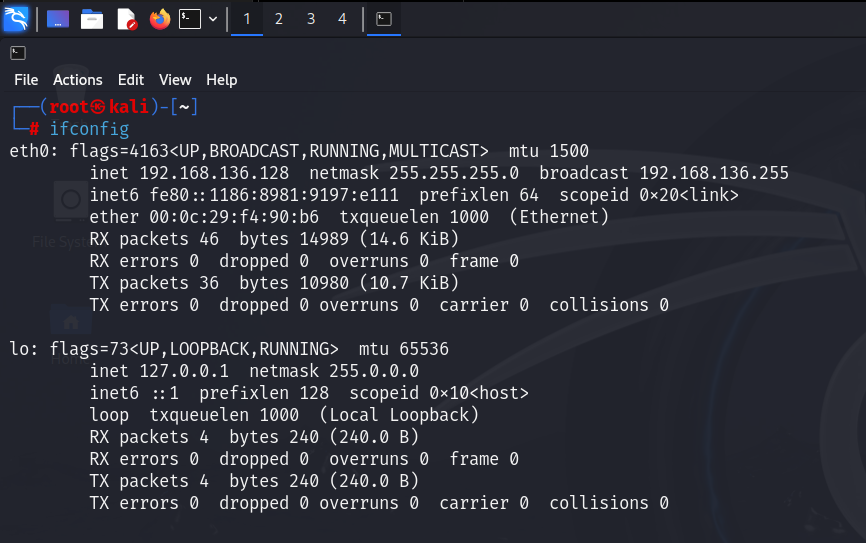
**Təşkilat: MilliSec**

**Hazırlayan:Cavanşir**

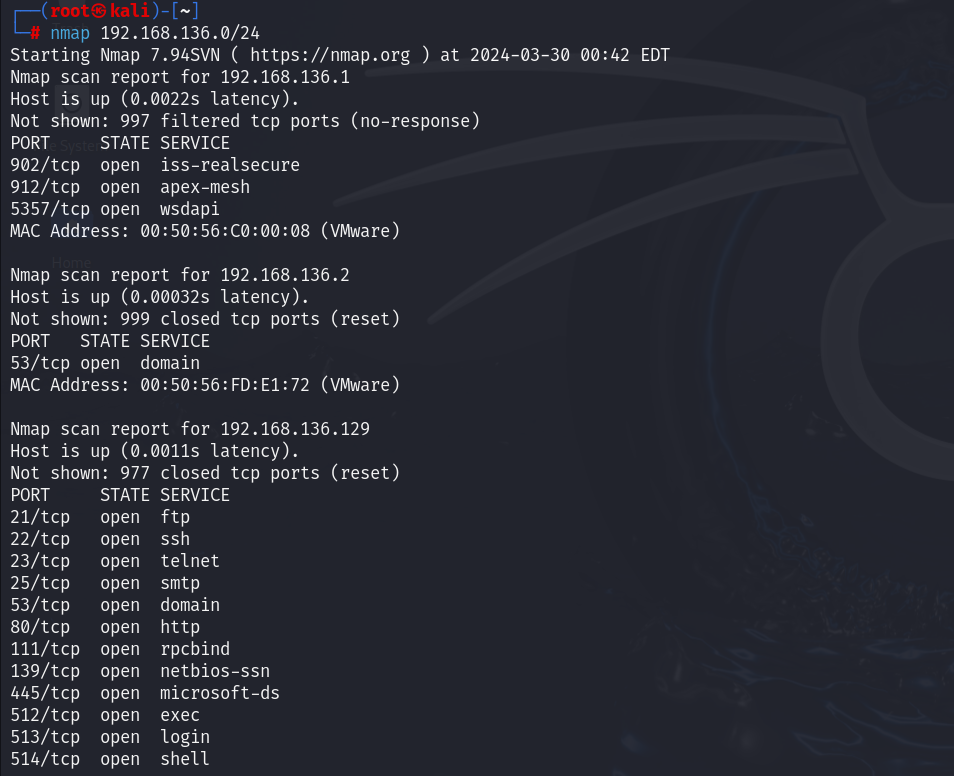
**21.02.2024**

1. Şəbəkə taraması

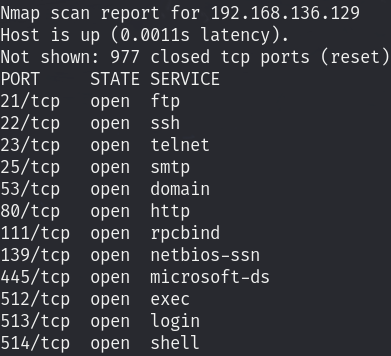
Şəbəkə taraması üçün “ifconfig” kommandı ilə ip ünvanımızı öyrənirik və daha sonra isə “nmap 192.168.136.129/24” yazıb başladırıq



IP Adress: 192.168.136.128



1. Qarşı tərəfin ip adressini seçirik

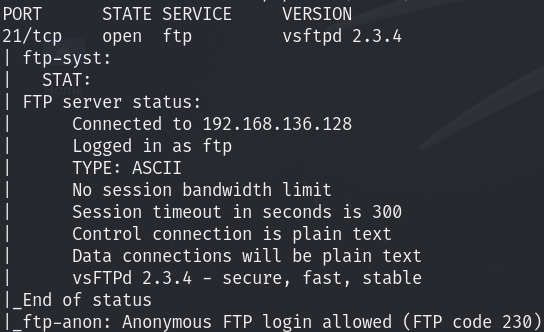


1. Serverin ip adressinin tamamilə taranması

Kommand: “nmap -p- -A 192.168.136.129”



1. Bizə uyğun açıq port və protokolun seçilməsi
2. Versiyası və s. Haqqında



FTP protokolu, 21ci port, versiya: vsftpd 2.3.4

1. Sızma prosesləri

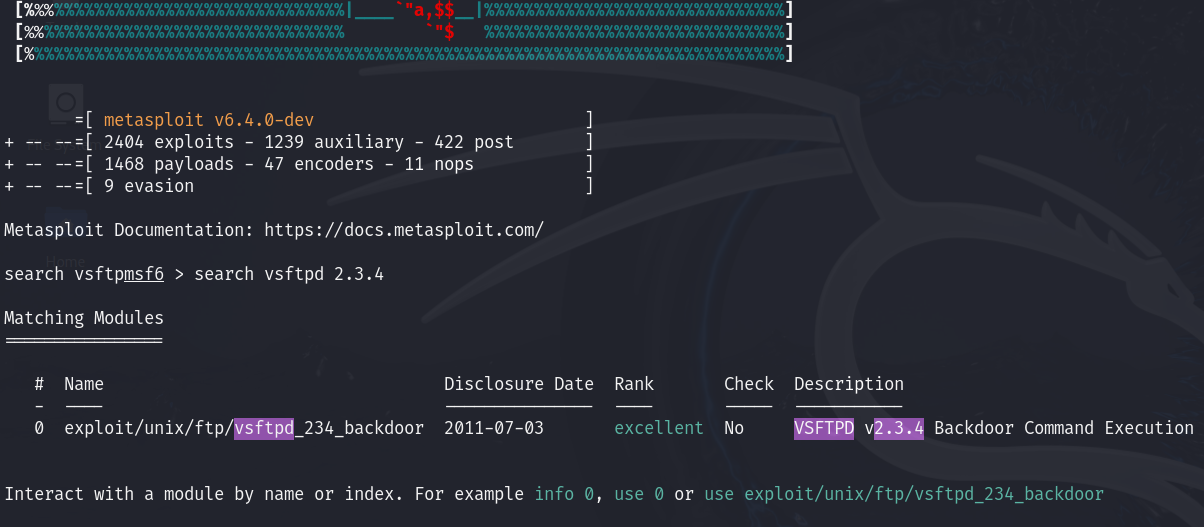
5-ci hissədə sonda gördük ki, “Anonymous FTP login allowed” yazısı var, yəni anonymous şəkildə parolsuz və ya anonymous parolu ilə daxil ola bilərik. Yoxlayaq!

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Digər bir üsul isə “msfconsole” işlədərək versiyaya uyğun exploit tapıb və o exploit ilə sistemə shell açmaqdır. Yoxlayaq!

Terminala msfconcole yazaraq daxil oluruq və “search vsftpd 2.3.4” yazırıq

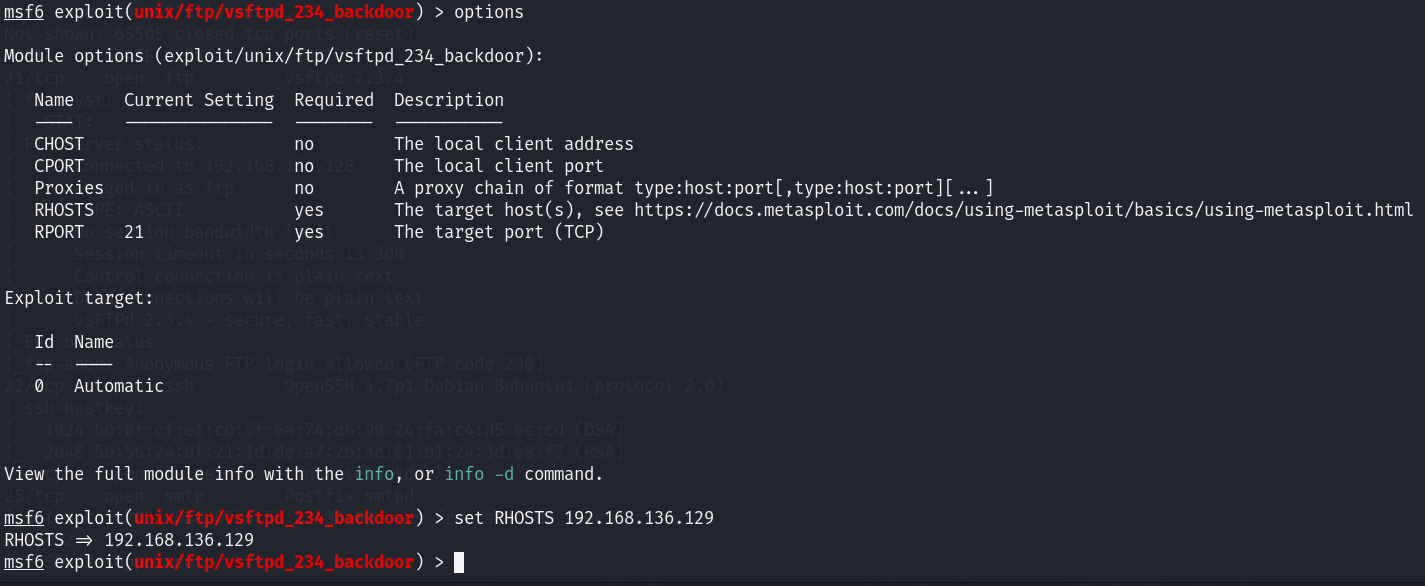


“options” yazırıq

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

RHOSTS tələb olunduğundan və qarşısı boş olduğundan “set RHOSTS 192.168.136.129” yazırıq



metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

VƏ hazırdır, başladıla bilər “run” və ya “exploit” yazıb başladırıq

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu