Linux Privilege Escalation Cheat Sheet [TR]

Fatih T. tarafından yayımlandı

Bu yazımda sizlere, CTF yarışmalarında veya sızdığınız Linux işletim sistemlerine "root" yetkilerine nasıl ulaşabileceğiniz hakkında detaylı bilgiler vermeye çalışacağım. Buradaki yöntemleri kullanarak ve sızdığınız makinelerde zafiyet keşfetmenize veya ipuçları yakalamanıza yardımcı olacak yöntemlerden bahsedeceğim. Linux işletim sistemlerinde yetki yükseltmek için yapılması gereken bazı yöntemler şunlardır:

1. İşletim sistemi hakkında bilgi toplamak
2. Uygulamalar veya servisler hakkında bilgi toplamak
3. İşletim sistemindeki ağ ve iletişim bilgilerini elde etmek
4. Kullanıcılar hakkında bilgi toplamak
5. Dosya sistemi hakkında bilgi toplamak

Kontrol Listesi:

Bu yöntemlere göre oluşturulabilecek en kapsamlı kontrol listesi aşağıdaki gibidir. Aşağıdaki listeye göre erişim sağladığınız Linux sistemde bu listeye göre kontroller yapabilirsiniz.

- ***Kernel ve Linux dağıtım sürüm ayrıntıları***
- ***Sistem bilgileri***
  - Hostname Bilgisi
  - IP Adresi Bilgisi
  - DNS Server Bilgileri
  - Genel Network Bilgisi
- ***Kullanıcı Bilgileri***
  - Kullanıcının Geçmiş Dosya Bilgileri(.bash_history)
  - Kullanıcı Hesabının Detayları
  - umask Değerinin Kontrolü
  - Basit SSH Kontrolü
  - Kısıtlanmış Dosyaları Okumaya çalışmak(/etc/shadow)
  - Root Kullanıcılarını Listelemek
- ***Ayrıcalıklı Erişim Sağlayacak Yöntemler***
  - "/etc/sudoers" dosyasını kontrolü
  - "root" kullanıcısının "home" dizini erişimi kontrolü
  - "/home" dizininin izinlerinin listelenmesi
- ***Çevresel Değerler***
  - "$PATH" değerinin görüntülenmesi
  - "Environment Information" değerlerinin görüntülenmesi
- ***Zamanlanmış Görevler***
  - "cron jobs" Listelemek
  - Herkes tarafından yazılan " cron jobs" ları bulmak
  - Aktif veya pasif "systemd timers" bulmak
- ***Servisler***
  - Network bağlantılarını listeleyin
  - Çalışan tüm "process" bilgilerini listeleyin
  - "init.d" binary izinlerini listeleyin
- ***Bazı Uygulamaların Versiyon bilgileri***
  - MySQL versiyonunu kontrol edin
  - PostgresSQL versiyonunu kontrol edin
  - Apache versiyonuna bakın
  - "www" dosyasına bakın

    - Apache için user config ayarlarına

- ***Default Bırakılmış Ayarlar***
    - MySQL veya PostgreSQl için default user denemesi yapın

- ***Dosya İzinleri, SUID ve GUID Biti araştırmaları***
    - SUID/GUID dosyalarını bulun
    - NFS server detaylarına bakın
    - "/etc" dizini altında "*.conf files" dosyalarını inceleyin
    - Yazma izni olan tüm dosyalarını görüntüleyin
    - POSIX özelliklere sahip tüm dosyalarını görüntüleyin

Yukarıdaki liste hemen hemen tüm CTF yarışmalarında sizlere yol gösterici bir rol üstlenebilir. Bu listede bulunan maddelerin çoğuna detaylı olarak aşağıda değineceğim.

Bu işler ile uğraşan arkadaşlar için de harika bir "cheet sheet" olması için de elimden geldiğince fazla kaynaktan yararlanmaya ve bilgiler toplamaya çalıştım.

İşletim Sistemi Hakkında Bilgi Toplama

1) Dağıtım Türü ve Versiyon Bilgileri

En önemli noktalardan biridir. Linux sistemin hangi versiyona ve hangi Linux dağıtımı olduğunu öğrenmeniz size "exploit" aramanız konusunda yardımcı olacaktır. Aşağıdaki komutlar ile bu bilgileri öğrenebilirsiniz.

```
1) cat /etc/issue

2) cat /etc/*-release

3) cat /etc/lsb-release # Debian based

4) cat /etc/redhat-release # Redhat based
```

---

2) Kernel Versiyonunu Öğrenmek

Eski versiyona sahip Linux işletim sistemlerinde mutlaka bir "kernel" zafiyeti bulunmaktadır. Aşağıdaki komutlar ile kernel versiyonunu öğrenebilirsiniz.

```
1) cat /proc/version

2) uname -a

3) uname -mrs

4) rpm -q kernel

5)dmesg | grep Linux

6) ls /boot | grep vmlinuz-
```

Çevresel Değişkenlerden Bilgi Toplama

Çevresel değişkenlerden aşağıdaki komutlar ile bilgi toplayabilirsiniz.

```
1) cat /etc/profile

2) cat /etc/bashrc

3) cat ~/.bash_profile

4) cat ~/.bashrc

5) cat ~/.bash_logout

6) env

7) lpstat -a #eger bir yazıcı var ise kullanılabilir
```

Uygulama ve Servislerden Bilgi Toplama

Arka planda çalışan uygulamalar hakkında şu şekilde bilgi toplayabilirsiniz.

```
1) ps aux

2) ps -ef

3) top

4) cat /etc/services
```

Ayrıca bu çalışan servislerin veya "process" değerlerinin hangisini "root" kullanıcısının çalıştırdığını görüntülemek için aşağıdaki komutlar kullanılabilir.

```
1) ps aux | grep root

2) ps -ef | grep root
```

Bazı servislerin yapılandırma ayarları yanlış olabilir veya "default" değerde bırakılmış olabilir. Bu yüzden bazı "configuration" dosyalarına bakmanız gerekebilir.

```
1) cat /etc/syslog.conf

2) cat /etc/chttp.conf

3) cat /etc/lighttpd.conf

4) cat /etc/cups/cupsd.conf

5) cat /etc/inetd.conf

6) cat /etc/apache2/apache2.conf

7) cat /etc/my.conf

8) cat /etc/httpd/conf/httpd.conf

9) cat /opt/lampp/etc/httpd.conf

10) ls -aRl /etc/ | awk '$1 ~ /^.*r.*/
```

Zamanlanmış Görevler ve "crontab" Hakkında Bilgi Toplama

"crontab" veya "cronjob" işlemlerine bakarak arka planda görevlendirilmiş işlemler hakkında bilgi sahibi olabilir. Bu sayede bazen "root" erişim hakkına sahip olmada fikir sahibi olabiliriz.

```
1) crontab -l

2) ls -alh /var/spool/cron

3) ls -al /etc/ | grep cron

4) ls -al /etc/cron*

5) cat /etc/cron*

6) cat /etc/at.allow

7) cat /etc/at.deny

8) cat /etc/cron.allow

9) cat /etc/cron.deny

10) cat /etc/crontab

11) cat /etc/anacrontab

12) cat /var/spool/cron/crontabs/root
```

Network ve İletişim Sistemi Hakkında Bilgi Toplama

Sızdığınız bilgisayarın ağ ayarlarını öğrenmek bazen faydalı olabilir.

```
1) /sbin/ifconfig -a
```

```
2) cat /etc/network/interfaces

3) cat /etc/sysconfig/network
```

Network yapılandırma ayarlarına da aşağıdaki komutlar ile ulaşabilirsiniz. DNS adresi veya “iptables” gibi yerlerde önemli bilgiler elde edebiliriz.

```
1) cat /etc/resolv.conf

2) cat /etc/sysconfig/network

3) cat /etc/networks

4) iptables -L

5) hostname

6) dnsdomainname
```

Genelde unutulan bazı kontrol yerleri vardır. Sızdığınız sistem başka sistemler ile etkileşim halinde olabilir. Bunu öğrenmek sizlere büyük fayda sağlar. Dışarıdan başka hangi bilgisayarların sızdığınız bilgisayar ile etkileşim halinde olduğunu öğrenmek için aşağıdaki komutları kullanabilirsiniz.

```
1) lsof -i

2) lsof -i :80

3) grep 80 /etc/services

4) netstat -antup

5) netstat -antpx

6) netstat -tulpn

7) chkconfig – list

8) chkconfig – list | grep 3:on
```

ARP tablosuna da aşağıdaki komutlar ile ulaşabilirsiniz.

```
1) arp -e

2) route

3) /sbin/route -nee
```

Kullanıcılar ve Bazı Önemli Bilgilerin Toplanması

Şuanda **hangi kullanıcı olduğun, hangi kullanıcı ile giriş yaptığın gibi bilgileri** ve daha fazlasını aşağıdaki komutlar ile kontrol edebilirsin.

```
1) id

2) who

3) last

4) cat /etc/passwd | cut -d: -f1 # List of users

5) grep -v -E “^#” /etc/passwd | awk -F: ‘$3 == 0 { print $1}’
# List of super users

6) awk -F: ‘($3 == “0”) {print}’ /etc/passwd # List of super users

7) cat /etc/sudoers

8) sudo -l
```

Bakmamız gereken **bazı hassas dosyalardan bazıları** şunlardır.

```
1) cat /etc/passwd

2) cat /etc/group

3) cat /etc/shadow
```

```
4) ls -alh /var/mail/
```

Kullanıcının geçmiş işlemlerine bakmak çok önemli bir iştir. Lütfen burayı sürekli olarak aklınızda tutun. Bazı uygulamaların geçmişi, komut satırının geçmişi sizler için kritik önem taşımaktadır.

```
1) cat ~/.bash_history

2) cat ~/.nano_history

3) cat ~/.atftp_history

4) cat ~/.mysql_history

5) cat ~/.php_history
```

Bazı **"private key"** değerlerinin bulunabileceği yerler aşağıdaki gibidir. Buralara bakmak da sizlere önemli bilgiler sağlayabilir.

```
1) cat ~/.ssh/authorized_keys

2) cat ~/.ssh/identity.pub

3) cat ~/.ssh/identity

4) cat ~/.ssh/id_rsa.pub

5) cat ~/.ssh/id_rsa

6) cat ~/.ssh/id_dsa.pub

7) cat ~/.ssh/id_dsa

8) cat /etc/ssh/ssh_config

9) cat /etc/ssh/sshd_config

10) cat /etc/ssh/ssh_host_dsa_key.pub

11) cat /etc/ssh/ssh_host_dsa_key

12) cat /etc/ssh/ssh_host_rsa_key.pub

13) cat /etc/ssh/ssh_host_rsa_key

14) cat /etc/ssh/ssh_host_key.pub

15) cat /etc/ssh/ssh_host_key
```

Sistemde bulunan dosyalardan hangisine sizin yetkiniz olduğunu görmek sisteme sızmak için anahtar rol oynar. Buradaki komutları gerekirse ezberlemenizi tavsiye ediyorum. Bunları iki kısım olarak grupladım. Eğer bir grup çalışmazsa diğer grupla işlemlerinize devam edebilirsiniz.

Birinci grup:

```
1) ls -aRl /etc/ | awk '$1 ~ /^.*w.*/' 2>/dev/null # Anyone

2) ls -aRl /etc/ | awk '$1 ~ /^..w/' 2>/dev/null # Owner

3) ls -aRl /etc/ | awk '$1 ~ /^…..w/' 2>/dev/null # Group

4) ls -aRl /etc/ | awk '$1 ~ /w.$/' 2>/dev/null # Other

5) find /etc/ -readable -type f 2>/dev/null # Anyone

6) find /etc/ -readable -type f -maxdepth 1 2>/dev/null # Anyone
```

İkinci grupda ise hangi dosyaların sizin tarafınızdan tekrar yazılabildiğini bulmak için kullanabilirsiniz.

```
1) find / -writable -type d 2>/dev/null #world-writeable folders

2) find / -perm -222 -type d 2>/dev/null #world-writeable folders

3) find / -perm -o w -type d 2>/dev/null #world-writeable folders

4) find / -perm -o x -type d 2>/dev/null #world-executable folders

5) find / \( -perm -o w -perm -o x \) -type d 2>/dev/null #world-writeable & executable folders
```

Daha öncede bahsettiğim SUID/GUID bitlerine sahip dosyaları bulmak önemlidir.

Bu dosyaları aşağıdaki komutlar ile

```
1) find / -perm -1000 -type d 2>/dev/null
2) find / -perm -g=s -type f 2>/dev/null
3) find / -perm -u=s -type f 2>/dev/null
4) find / -perm -g=s -o -perm -u=s -type f 2>/dev/null
5) for i in `locate -r "bin$"`; do find $i \( -perm -4000 -o -perm -2000 \) -type f 2>/dev/null; done
6) find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null
```

****Bazı Faydalı Yollar:

Buradaki bazı komutlar yukarıda geçmiş olabilir. Elimden geldiğince en genellerini burada toplamaya çalıştım.

1) Bazen bazı dosyalarda "kullanıcı adı" ve "şifre" aramanız gerekebilir. Bunu yapmanın en basit yollarında biri aşağıdaki gibidir.

```
1) grep -i user [filename]
2) grep -i pass [filename]
3) grep -C 5 "password" [filename]
4) find . -name "*.php" -print0 | xargs -0 grep -i -n "var $password"
```

---

2) Sistemde bazen "shell" almanız gerekebilir. Muhtemelen bağlandığınız "meterpreter" shell sizin için uygun olmayabilir. Bu yüzden aşağıdaki komutlar ile kendinize "shell" almanız gerekebilir.

```
1) python -c 'import pty;pty.spawn("/bin/bash")'
2) echo os.system('/bin/bash')
3) /bin/sh -i
```

---

3) Sistemde en son düzenlenen dosyayı aşağıdaki komut ile bulabiliriz.

```
1) find / -mmin -10 2>/dev/null | grep -Ev "^/proc"
```

---

4) "Password" kelimesi içeren dosyaları şu şekilde bulabiliriz.

```
1) grep — color=auto -rnw '/' -ie "PASSWORD" — color=always 2>/dev/null
2) find . -type f -exec grep -i -I "PASSWORD" {} /dev/null \;
```

---

5) SUID binaries dosyalarına şu şekilde listeleyebiliriz.

```
1) find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
2) find / -uid 0 -perm -4000 -type f 2>/dev/null
```

---

6) Yazılabilir tüm dosyaları şu şekilde görüntüleyebiliriz.

```
1) find / -writable ! -user `whoami` -type f ! -path "/proc/*" ! -path "/sys/*" -exec ls -al {} \; 2>/dev/null
2) find / -perm -2 -type f 2>/dev/null
3) find / ! -path "*/proc/*" -perm -2 -type f -print 2>/dev/null
```

Buraya kadar olan her detayı en ince ayrıntısına kadar anlatmaya çalıştım. Herkesin kullanabileceği bir "cheet sheet" oluşturmayı denedim. Umarım sizler için faydalı olmuştur. Bir sonraki yazımda görüşmek üzere...