

Linux Hardening

1) Sistem veya Sanal Makine Başına Bir Ağ Hizmeti

Ayrı sunucularda veya sanal makine örneğinde farklı ağ hizmetleri çalıştırın. Böylece, tehlikede olabilecek diğer hizmetlerin sayısını sınırlar. Örneğin, bir saldırgan Apache akışı gibi bir yazılımdan başarıyla yararlanabiliyorsa, MySQL/MariaDB/PGSql, e-posta sunucusu vb. gibi diğer hizmetler de dahil olmak üzere tüm sunucuya erişim elde eder. Semanage, linux politikalarında değişiklik veya yeniden derleme gerektirmeden belirli öğelerini yapılandırmak için kullanılır. Aşağıdaki örnekte sorunumuz için gerekli sıkılaştırma adımları gerçekleştirilmektedir.

```
# mkdir /vm
# semanage fcontext -a -t xen_image_t "/vm(/.*)?"
# restorecon -R /vm
# ls -dZ /vm
# virt-install \
--paravirt \
--name webserver01 \
--ram 512 \
--file /vm/webserver.nixcraft.com.img \
--file-size 10 \
--nographics \
--location http://mirrors.kernel.org/centos/5.3/os/x86_64/
```

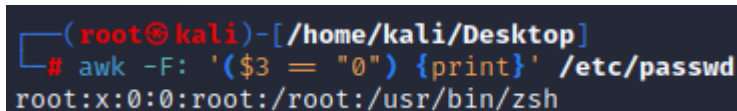
2) Kök Olmayan Hesapların UID'sinin 0 Olarak Ayarlanmadığından Emin Olun

Yalnızca kök hesap, sisteme erişmek için tam izinlere sahip UID 0'a sahiptir. UID'si 0'a ayarlanmış tüm hesapları görüntülemek için aşağıdaki komutu yazın:

```
# awk -F: '($3 == "0") {print}' /etc/passwd
```

Aşağıdaki gibi yalnızca bir satır görmelisiniz:

```
root:x:0:0:root:/root:/bin/bash
```



```
(root@kali)-[/home/kali/Desktop]
# awk -F: '($3 == "0") {print}' /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
```

Başka satırlar görürseniz, bunları silin veya diğer hesapların UID 0'ı kullanmak için sizin tarafınızdan yetkilendirildiğinden emin olun.

3) Dinleme Ağı Bağlantı Noktalarını Bul

Tüm açık bağlantı noktalarını ve ilişkili programları listelemek için aşağıdaki iki komut kullanılabilir:

```
netstat -tulpn
```

```
ss -tulpn
```

Aşağıdaki port benim docker containerıma ait olduğu için ellemiyorum.

```
(root@kali)-[/home/kali/Desktop]
# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:35451         0.0.0.0:*               LISTEN      609/containerd

(root@kali)-[/home/kali/Desktop]
# ss -tulpn
Netid            State            Recv-Q           Send-Q
tcp              LISTEN          0                4096
609,fd=12))
```

Kullanılmayan portların kapatılması gerekir. Kullanılan portların varsa en güncel ve güvenli servis versiyonlarının kullanılması gerekir.

4) IPv6'yı yalnızca Linux'ta KULLANMIYORSANIZ Kapatın

İnternet Protokolü sürüm 6 (IPv6), İnternet Protokolü sürüm 4'ün (IPv4) yerini alan ve birçok fayda sağlayan TCP/IP protokol paketinin yeni bir İnternet katmanını sağlar. IPv6 kullanmıyorsanız devre dışı bırakın.

```
# cat /sys/module/ipv6/parameters/disable
```

Yukarıdaki komut sonucunda "0" çıktısı alınırsa ipv6 "enabled" durumdadır. "1" çıktısı alınırsa ipv6 "disabled" durumdadır.

```
# ip a | grep inet6
```

Yukarıdaki komut ile var olan ipv6 adreslerini listeleyebilirsiniz.

```
(root@kali)-[/home/kali]
# ip a | grep inet6
inet6 ::1/128 scope host
inet6 fe80::20c:29ff:fe63:9c82/64 scope link noprefixroute
```

```
$ sudo mousepad /etc/sysctl.conf
```

Sysctl.conf dosyasının sonuna aşağıdaki satırları ekliyoruz.

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

Daha sonra reboot ile yeniden başlatıyoruz.

```
# sudo reboot
```

```
(root@kali)-[/home/kali]
# ip a | grep inet6
inet6 fe80::20c:29ff:fe63:9c82/64 scope link noprefixroute
```

5) İstenmeyen SUID ve SGID İkili Dosyalarını Devre Dışı Bırakın

SUID/SGID yürütülebilir dosyasında bir güvenlik sorunu veya hatası olduğunda, tüm SUID/SGID bitleri etkinleştirilmiş dosya kötüye kullanılabilir. Tüm yerel veya uzak kullanıcılar bu dosyayı kullanabilir. Bu tür dosyaların tümünü bulmak iyi bir fikirdir. Find komutunu aşağıdaki gibi kullanın:

#See all set user id files:

```
find / -perm +4000
```

See all group id files

```
find / -perm +2000
```

Or combine both in a single command

```
find / \( -perm -4000 -o -perm -2000 \) -print
```

```
find / -path -prune -o -type f -perm +6000 -ls
```

Bildirilen her dosyayı araştırmanız gerekir. Eğer dosya önemli değilse veya SUID, SGID olmadan da aynı işlevi yerine getirebiliyorsa devre dışı bırakın.

Faruk Ulutaş