❤️

Linux Güvenlik Ayarları

GÜVENLİK AYARLARI

1. Kernel mesajlarının normal kullanıcılar tarafından okunabilmesini engelleyin.

```
sudo nano /proc/sys/kernel/dmesg_restrict
1
```

---

1. Buffer Overflow (Arabellek Taşırma) atağına karşı Kernel ExecProtection'ı açın. sysctl.conf dosyasına aşağıdaki değerleri ekleyin.

```
sudo nano /etc/sysctl.conf

kernel.exec-shield=1
kernel.randomize_va_space=2
```

---

1. Kernel'ın gelen paketler için kaynak adresi doğrulamasını açmak ve Reverse Path Filtering'i aktif etmek için sysctl.conf dosyası içindeki aşağıdaki satırları uncomment edin.

```
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
```

---

1. TCP'nin 3-Way-Handshake sırasındaki SYN-ACK özelliğinden yararlanarak bilgisayarın SYN Flood atağı almasını engellemek için sysctl.conf dosyasında aşağıdaki satırı uncomment edin. Ve ikincisini de altına ekleyin.

```
net.ipv4.tcp_syncookies=1
net.ipv4.tcp_synack_retries=5
```

---

1. Kernel dosya adlarının, süreç ID'leri (PID'leri) arasında görünmemesi için bu özelliği devre dışı bırakın.

```
sudo nano /proc/sys/kernel/core_uses_pid
0
```

---

1. Bilgisayar eğer bir router rolünde değilse, üzerinden IP yönlendirme işlemini devre dışı bırakmak için sysctl.conf dosyasında aşağıdaki satırları uncomment edin.

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
```

---

1. Durdurulmuş olan sahte veya yönlendirilemez olan paketlerin de log'unu alabilmek için sysctl.conf dosyası içinde aşağıdaki satırı uncomment edin.

```
net.ipv4.conf.all.log_martians = 1
```

---

1. Broadcast veya Multicast üzerinden gönderilen sahte ICMP paketlerine (Smurf Attack'a) cevap vermemek için sysctl.conf dosyası içine aşağıdaki satırı ekleyin.

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

1. Bilgisayarın ping'e cevap vermemesi için UFW'nin before.rules dosyasındaki aşağıdaki değişiklikleri yapın ve ufw reload komutuyla değişikliği uygulayın.

```
sudo nano /etc/ufw/before.rules

 A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type source-quench -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP

sudo ufw reload
```

1. Hedef dizin veya dosyada erişim izni olmayan saldırganın, sembolik ve katı link yaratma yönetmiyle hedefe ulaşma girişimini engellemek için sysctl.conf dosyası içinde aşağıdaki satırları uncomment edin.

```
fs.protected_hardlinks=1
fs.protected_symlinks=1
```