Linux Sunucularda Uptime Kapatma

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Ubuntu 14.04 LTS	// Ana Makina
kali-linux-1.0.4-amd64.iso	// Kali (Eski) Sanal Makinası

Bu yazıda Ubuntu ana makinasından Kali (Eski) sanal makinasına (web sunucusuna) özel tcp paketleri yollanacaktır ve böylelikle hedef web sunucusunun uptime süresi öğrenilecektir. Ardından Kali (Eski) sanal makinası (web sunucusu) yapılandırılarak uptime bilgi ifşasının önü kesilecektir.

a. Uptime Süresini Öğrenme

Önce Kali'yi web sunucusu yapabilmek için Kali'de apache servisini başlatalım.

Kali:

> service apache2 start

Ardından Ubuntu ana makinasından Kali (Eski) sanal makinasına tcp paketini yollayalım.

Ubuntu Console

> hping3 -S --tcp-timestamp -p 80 -c 2 172.16.3.112 // Kali (Eski) IP'si

Output:

```
HPING 172.16.3.112 (eth0 172.16.3.112): S set, 40 headers + 0 data bytes

len=56 ip=172.16.3.112 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=14480 rtt=3.8
TCP timestamp: tcpts=4294938496

len=56 ip=172.16.3.112 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=14480 rtt=3.7
TCP timestamp: tcpts=4294938746
HZ seems hz=100
System uptime seems: 497 days, 2 hours, 23 minutes, 7 seconds

--- 172.16.3.112 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.7/3.7/3.8 ms
```

Görüldüğü üzere uptime süresi gelmiştir. Hedef web sunucusunun ne kadar süre açık durduğunu öğrenerek hedef web sunucusu son güncelleştirmeleri yapmış mı yapmamış mı sorusunun cevabını bulabiliriz.

b. Uptime Bilgi İfşasını Kapatma // İşe yaradı.

Hedef web sunucusunun Uptime bilgi ifşasını sonlandırmak için

/etc/sysctl.conf

dosyasına aşağıdaki satır eklenmelidir.

net.ipv4.tcp_timestamps = 0

Ardından Kali (Eski) sistemi yeniden başlatılmalıdır. Böylece tekrar Ubuntu ana makinasından Kali (Eski) sanal makinasına hping3 ile özel tcp paketini gönderdiğimizde uptime bilgisi gelmeyecektir.

Kali Console:

service apache2 start

Ubuntu Console:

> hping3 -S --tcp-timestamp -p 80 -c 2 172.16.3.112 // Kali (Eski) IP'si

Output:

HPING 172.16.3.112 (eth0 172.16.3.112): S set, 40 headers + 0 data bytes
len=46 ip=172.16.3.112 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=14600 rtt=3.8 ms
len=46 ip=172.16.3.112 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=14600 rtt=3.7 ms

--- 172.16.3.112 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.7/3.8/3.8 ms

Ekstra // Denenmemiştir

Uptime bilgi ifşasını linux sistemlerdeki varsayılan firewall olan iptables ile de engelleyebiliriz.

> iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
> iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROP

Ancak bu yöntem web sunucusunda performans kayıplarına yol açabilir.

[2021 Yılı] İlave Uygulama

[+] Birebir denendi ve başarıyla uygulandı.

Gereksinimler

Ubuntu 18.04 LTS // Ana Makina
Kali Linux 2021.2 // Kali Sanal Makinesi

[*] Bilgi:

Kali 1.0.4 amd x64'te uptime bilgisi alma işlemi 2021 yılında denendiğinde başarısız olmuştur. Bu nedenle güncel Kali 2021.2 sürümünde Kali 1.0.4 amd x64'e uygulanan uptime bilgisi alma ve sonra uptime bilgisini kapama adımları uygulanmıştır.

Bu başlıkta Ubuntu 18.04 ana makinasından Kali 2021.2 sanal makinasına (web sunucusuna) özel tcp paketleri yollanacaktır ve böylelikle hedef web sunucusunun uptime süresi öğrenilecektir. Ardından Kali 2021.2 sanal makinası (web sunucusu) yapılandırılarak uptime bilgi ifşasının önü kesilecektir.

a. Uptime Süresini Öğrenme

Önce Kali'yi web sunucusu yapabilmek için Kali'de apache servisini başlatalım.

Kali 2021.2:

> service apache2 start

Ardından Ubuntu ana makinasından Kali 2021.2 sanal makinasına tcp paketini yollayalım.

Ubuntu 18.04 LTS:

> hping3 -S --tcp-timestamp -p 80 -c 2 192.168.0.30 // Kali 2021.2 IP'si

Çıktı:

```
HPING 192.168.0.30 (wlp2s0 192.168.0.30): S set, 40 headers + 0 data bytes
len=56 ip=192.168.0.30 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=65160 rtt=7.8 ms
  TCP timestamp: tcpts=1582905626

len=56 ip=192.168.0.30 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=65160 rtt=3.3 ms
  TCP timestamp: tcpts=1582906631
  HZ seems hz=1000
  System uptime seems: 18 days, 7 hours, 41 minutes, 46 seconds

--- 192.168.0.30 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.3/5.6/7.8 ms
```

Görüldüğü üzere uptime süresi gelmiştir. Hedef web sunucusunun ne kadar süre açık durduğunu öğrenerek hedef web sunucusu son güncelleştirmeleri yapmış mı yapmamış mı sorusunun cevabını bulabiliriz.

b. Uptime Bilgi İfşasını Kapatma

Hedef web sunucusunun Uptime bilgi ifşasını sonlandırmak için

/etc/sysctl.conf

dosyasına aşağıdaki satır eklenmelidir.

net.ipv4.tcp_timestamps = 0

Ardından Kali 2021.2 sistemi yeniden başlatılmalıdır. Böylece tekrar Ubuntu ana makinasından Kali 2021.2 sanal makinasına hping3 ile özel tcp paketini gönderdiğimizde uptime bilgisi gelmeyecektir.

Kali Console:

service apache2 start

Ubuntu 18.04:

> hping3 -S --tcp-timestamp -p 80 -c 2 192.168.0.30 // Kali 2021.2 IP'si

Çıktı:

HPING 192.168.0.30 (wlp2s0 192.168.0.30): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.30 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=7.6 ms
len=46 ip=192.168.0.30 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=3.4 ms

--- 192.168.0.30 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.4/5.5/7.6 ms

Kaynak

http://www.tmltechnologies.com/2015/index.php/operating-systems/quick-picks/disable-tcp-timestamps-on-your-linux-system