

1)



Siber saldırılar açısından hedef sistemdeki /etc ve /home dizinleri değerlidirler. Çünkü /etc dizini konfigürasyon dosyaları içeren bir dizindir. /home dizini ise kişisel dosyalar içeren bir dizindir.

2)

Siber saldırılar açısından hedef sistemdeki bazı önemli dosyalar ise şunlardır:



Some important files

File	Contents and Reason
/etc/resolv.conf	Contains the current name servers for the system.
/etc/issue	Current version of distro
/etc/passwd	List of local users. Likely to trigger IDS alerts
/etc/shadow	List of users' passwords' hashes (requires root privileges)
/etc/sudoers	Rules that users have to follow when using sudo.
/home/xxx/.bash_history	Will give some directory context
/home/*/.ssh/id*	SSH keys, often passwordless
/home/*/.vnc	VNC remote access information

3)

resolv.conf dosyası hedef sistemde tanımlı DNS adresini tutar.

Information about name servers to be queried is specified in /etc/resolv.conf

```
#cat /etc/resolv.conf
search mydomain.com
nameserver 8.8.8.8 dns
nameserver 9.9.9.9 just another dns
```

Hedef sistemdeki bu dosya kendi DNS sunucumuz ile manipüle edilirse kurbanı oluşturduğumuz klon web sitelerine götürebiliriz. Domain'den IP'ye dönüşümde domain adresi adres çubuğunda olduğu gibi kalırken IP adresi klon web sitesinin IP'si olacağından kurban farkı anlamayacaktır ve örneğin login bilgilerini girerek bilgilerini saldırgana verecektir.

4)

/etc/issue dosyası hedef sistemin işletim sistemi ismi ve versiyonu bilgisini tutar:

```
root@SGEDHSIMSEK03: /home/hasan
root@SGEDHSIMSEK03:/home/hasan# cat /etc/issue
Ubuntu 14.04.5 LTS \n \l
root@SGEDHSIMSEK03:/home/hasan#
```