Laboratorní protokol cv. 5

Jméno: Mikhail Abramov
Datum: 26.11.2020
Login: xabram00

IP adresa rozhraní enp0s8 **cv5-master**: 192.168.56.5
IP adresa rozhraní enp0s8 **cv5-provider**: 192.168.56.6

Úkol 1, Netflow

1. Uveďte TOP 10 IP adres podle počtu přenesených bytů

[user@localhost ~]$ nfdump -R /home/user/nfdump-data/anon-2016-08-15 -s ip -n 10 -O bytes
Top 10 IP Addr ordered by flows:
Date first seen Duration Proto IP Addr Flows(%) Packets(%) Bytes(%) pps bps bpp
2016-08-14 17:26:30.976 88377.304 any 136.2.100.115 4.2 M(33.1) 4.7 M(1.0) 781.7 M(0.2) 52 70761 167
2016-06-26 01:08:02.008 4380711.968 any 136.2.58.138 2.3 M(18.0) 176.9 M(37.6) 159.1 G(38.7) 40 290599 899
2016-06-26 08:05:48.984 4355635.896 any 185.2.119.236 1.1 M(8.5) 52.7 M(11.2) 44.4 G(10.8) 12 81591 842
2016-08-14 18:00:01.768 86328.024 any 136.2.100.123 679456(5.3) 745386(0.2) 118.5 M(0.0) 8 10983 159
2016-08-14 17:58:01.680 86484.624 any 136.2.101.127 667260(5.2) 859986(0.2) 136.1 M(0.0) 9 12589 158
2016-06-26 08:27:51.984 4325041.808 any 36.122.83.223 333178(2.6) 13.4 M(2.8) 9.2 G(2.2) 3 17034 686
2016-06-26 17:13:42.984 4322745.296 any 122.153.198.41 290943(2.3) 2.3 M(0.5) 1.3 G(0.3) 0 2434 581
2016-08-14 18:00:00.792 86316.000 any 136.2.100.91 270182(2.1) 310471(0.1) 43.9 M(0.0) 3 4068 141
2016-08-14 17:59:31.280 86396.512 any 162.35.1.115 261118(2.0) 1.2 M(0.3) 73.2 M(0.0) 14 6775 59
2016-06-26 11:59:45.984 4341569.808 any 122.153.198.15 189779(1.5) 1.5 M(0.3) 1.1 G(0.3) 0 1996 728

2. Uveďte 3 datové protokoly s nejvyšším objemem přenesených bytů

[user@localhost ~]$ nfdump -R /home/user/nfdump-data/anon-2016-08-15 -s proto -n 3 -O bytes
Top 3 Protocol ordered by flows:
Date first seen Duration Proto Protocol Flows(%) Packets(%) Bytes(%) pps bps bpp
2016-06-26 01:35:24.984 4379071.992 UDP 17 7.1 M(55.7) 138.0 M(29.3) 102.7 G(25.0) 31 187604 744
2016-06-26 01:08:02.008 4380698.264 TCP 6 5.2 M(40.8) 325.2 M(69.1) 302.9 G(73.8) 74 553188 931
2016-08-14 17:58:02.168 86486.112 ICMP6 58 279625(2.2) 706485(0.2) 51.2 M(0.0) 8 4732 72

Úkol 2, Syslog

1. Uveďte pravidlo pro přeposílání všech syslog zpráv na **cv5-master**:

```
*.* @192.168.56.5:514
```

2. Uveďte pravidlo, které omezí zprávy přeposílané z **cv5-provider** na zprávy týkající se pouze autentizace

```
authpriv.info @192.168.56.5:514
```

3. Jakou zprávu odeslal **cv5-provider** při neúspěšném přihlášení? Stačí uvést pouze zkráceně

Nov 26 15:57:48 localhost sshd[5359]: Failed password for user from 192.168.56.6 port 34494 ssh2
Nov 26 15:57:48 localhost unix_chkpwd[5362]: password check failed for user (user)
Nov 26 15:57:51 localhost sshd[5359]: Failed password for user from 192.168.56.6 port 34494 ssh2
Nov 26 15:57:52 localhost unix_chkpwd[5363]: password check failed for user (user)
Nov 26 15:57:53 localhost sshd[5359]: Failed password for user from 192.168.56.6 port 34494 ssh2
Nov 26 15:57:53 localhost sshd[5359]: Connection closed by 192.168.56.6 port 34494 [preauth]
Nov 26 15:57:53 localhost sshd[5359]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.6 user=user

Úkol 3, Icinga

1. Jaký je časový interval mezi kontrolami pro HTTP službu?

```
check_interval=10m
```

2. Uveďte konfiguraci komunity pro SNMP ze stroje **cv5-provider**

```
rocommunity xabram00 192.168.56.0/24
```

3. Uveďte množství volné paměti zaslané ve zprávě SNMP

```
SNMP OK - 254136
```