

Laboratorní protokol cv. 5

Jméno: Tomáš Ďuriš

Datum: 5.12.2020

Login: xduris05

IP adresa rozhraní enp0s8 **cv5-master**: 192.168.56.102

IP adresa rozhraní enp0s8 **cv5-provider**: 192.168.56.101

Úkol 1, Netflow

1. Uveďte TOP 10 IP adres podle počtu přenesených bytů

136.2.58.138

185.2.119.236

136.2.24.237

136.2.24.236

136.2.24.239

136.2.24.238

122.153.220.92

42.208.57.175

124.106.137.204

36.122.83.223

2. Uveďte 3 datové protokoly s nejvyšším objemem přenesených bytů

TCP

UDP

GRE

Úkol 2, Syslog

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

. @192.168.56.102:514

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

authpriv.info @192.168.56.102:514

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

Dec 5 06:05:26 localhost sshd[6749]: Failed password for root from 192.168.56.102 port 44238 ssh2

Úkol 3, Icinga

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

10min

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

rocommunity xduris05 192.168.56.0/24

3. Uveďte množství volné paměti zaslané ve zprávě SNMP

1683508 KB