Björn Geirsson

From: Stefán S. Stefánsson
Sent: 13. febrúar 2012 11:46
To: Hrafnkell V. Gíslason; Björn Geirsson
Subject: NetFlow útskýring

Sælir,

Í framhaldi af umræðu okkar í morgun vil ég benda á nánari eiginleika NetFlow upplýsinga um umferðarflæði.

Á vefsíðunni hér að neðan kemur fram greinargóð lýsing á NetFlow og margt sem á ekki við og er þar af leiðandi ekki skilgreint í búnaði að eigi að safna saman. En þeir í Example 2 sýna þeir eftirfarandi dæmi,

In this example, we are reporting the following 3 Flow records:

Src IP addr.	Dst IP addr.	Next Hop addr.	Packet	Bytes	Number	Number
198.168.1.12	10.5.12.254	192.168.1.1	5009	5344385		
192.168.1.27	10.5.12.23	192.168.1.1	748	388934		
192.168.1.56	10.5.12.65	192.168.1.1	5	6534		

Í tilfelli netárása er í þessu einfalda dæmi gagnlegast fyrir okkur að sjá að mest umferðin (534485 Bytes) er frá 192.168.1.12 og er beint á 10.5.12.254. Sú vitneskja getur gagnast okkur að sjá hvaðan árásin kemur og að hvaða marki henni er beint. Nú, ef árásin kemur dreifð frá Botneti, þ.e. frá hinum ýmsu vélum Botnetins, þá gagnast okkur mest að sjá hvert umferðinni er beint. Þ.e. í okkar búnaði að lesa Netflow yfirlitsgögn fjarskiptafyrirtækjanna yfir stutt tímabil (t.d. 1 – 5 mín.) og nýta það í þeirri greiningu.

Ef ástæða þykir til, má síðan skoða aðra tæknilega eiginleika, svo sem á hvaða port fórnarlamsins er verið að herja á, eru pakkarnir TCP, UDP eða ICMP pakkar, o.s.frv.

Ég vona að þetta skýri málið eitthvað, annars ræði það við mig ef óljóst þykir.

http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html

Kv. SSS

Stefán Snorri Stefánsson
Hópstjóri CERT-ÍS / Head of CERT-IS
Tæknideild / Technical Division
Sími / Tel. (+354) 510 1500
Fax (+354) 510 1509
email: stefan@pfs.is
Post- & Telecom Administration of Iceland
Suðurlandsbraut 4 • 108 Reykjavik • Iceland
www.pfs.is