



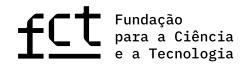


NETFLOW

Carlos Friaças RCTS CERT







PREPARAÇÃO



Login (sistema Linux), 193.136.2.x

username: ...

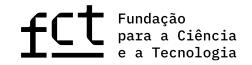
password: ...

cd /opt/traffic

Usar a ferramenta "nfdump"







PROBLEMA #1: DDOS



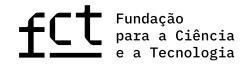
Há um IP da nossa rede (193.136.0.0/15) a ser atacado. Temos metadados do período em que o ataque ocorreu, no ficheiro nfcapd-problema1

- 1) Qual é o IP em concreto que está a sofrer o DDoS?
- 2) Que switches da ferramenta nfdump podemos usar para determinar o top de comunicações?



Hint: man nfdump





PROBLEMA #2: PORTSCAN



Aconteceu um portscan a um dos nossos servidores (193.136.2.58).

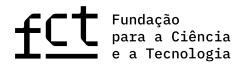
Temos metadados do período em que este scan ocorreu, no ficheiro nfcapd-problema2

1) Qual o IP a partir de onde o portscan foi realizado?

2) Quantos flows ficaram registados nesta amostra relativos a este portscan?







PROBLEMA #3: MALWARE



80.92.65.188 e 34.98.99.30 são IPs de C2 conhecidos usados pelo malware dircrypt

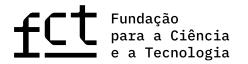
No ficheiro nfcapd-problema3 temos metadados que nos permitem verificar se houve comunicações com esses C2

183-

1) Que IPs estão potencialmente infectados, uma vez que estão a comunicar com um dos C2?

2) O C2 recebe as comunicações em que porto?





PROBLEMA #4: ANOMALIA ICMP



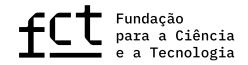
No ficheiro nfcapd-problema2 temos também uma anomalia detectada.

1) Qual a % de flows existentes nesta amostra relativos ao IP que mais usou o protocolo ICMP (IPv4)?

183-

2) Qual é o IP em causa?





SOLUÇÕES

Problema 1: 193.136.6.51

(usando /usr/bin/nfdump -r nfcapd.problem1 -s dstip -O flows)

Problema 2: 79.168.241.195

(usando /usr/bin/nfdump -r nfcapd.problem2 | grep 193.136.2.58)

Ficaram registados 78 flows

(adicionar "| grep 79.168.241.195 | wc -| ao comando)

Problema 3: 193.236.86.49; porto 80

(usando /usr/bin/nfdump -r nfcapd.problem3 | grep <IP C2>)

Problema 4: 3.7%; 194.210.238.72

(usando /usr/bin/nfdump -r nfcapd.problem2 -s srcip 'proto icmp')









Obrigado!



