Sicurezza delle reti[1]

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

Lezione XVI: Snort

Snort

- snort −−help man snort
- snort −r traffico.pcap −c rules −l .
- Regole: `action protocol address port direction address port (rule option)`
- alert icmp any any −> 192.168.10.2 any (itype: 8; msg: "ping detected"; sid:42)

Esercizi

Nel traffico fornito (da Christopher Misra, `http://courses.umass.edu/cs415`) ci sono 30 pacchetti, di 8 tipi diversi.

1. Provare a vedere l'effetto di un cambiamento nella regola icmp (p.es. itype)
2. Scrivere 7 regole come quella d'esempio per identificare gli altri 7 tipi (bilanciando generalità e specificità)
3. Esaminare `/etc/snort/rules`

Ferma il worm sasser

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Search.aspx?query=sasser

- il worm apre un ftp server 5554/tcp
- il worm cerca host vulnerabili su 0.0.0.0/8 192.168.0.0/16
- Considerate l'efficacia di queste regole

```
1 alert tcp $HOME_NET any -> any 9996 ( msg:"Sasser ftp script to transfer up.exe"
2 content:"|5F75702E657865|"; depth:250; flags:A+; classtype: misc-activity; sid:1000
3 rev:3;)
4 alert tcp any any -> $HOME_NET 5554 ( msg:"Sasser binary transfer get up.exe";
5 content:"|5F75702E657865|"; depth:250; flags:A+; classtype: misc-activity; sid:1000
6 rev:1;)
```

- Valutare l'introduzione di altre regole