



# Sicurezza delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica e Comunicazione  
Università degli Studi di Milano, Italia

[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2010/11



Sicurezza delle  
reti

Monga

Esercizi  
riassuntivi

# Lezione XX: Esercizi riassuntivi



- Connettersi alla porta tcp:80 del server `www.unimi.it`
- Scrivere una regola Snort che impedisca e abbatta tale connessione



- il worm apre un ftp server 6666/tcp
  - il worm cerca host che ospitano un servizio vulnerabile su 0.0.0.0/8 192.168.0.0/16, porta 513
- ① Scrivere regole Snort per fermare il worm.
  - ② Scrivere regole Iptables che impediscano il traffico collegato alle attività del worm.



Esaminare il traffico in `evidence.pcap`

- 1 Identificare e descrivere le interazioni avvenute
- 2 Identificare potenziali interazioni anomale
- 3 Utilizzare snort per ottenere allarmi



## Spiegare l'effetto delle seguenti regole

- 1 Chain PREROUTING (policy ACCEPT 33 packets, 1604 bytes)
- 2 pkts bytes target prot opt in out source destination
- 3 33 1604 sshuttle-12300 all -- \* \* 0.0.0.0/0 0.0.0.0/0
- 4
- 5 Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
- 6 pkts bytes target prot opt in out source destination
- 7
- 8 Chain OUTPUT (policy ACCEPT 24 packets, 1568 bytes)
- 9 pkts bytes target prot opt in out source destination
- 10 48 3008 sshuttle-12300 all -- \* \* 0.0.0.0/0 0.0.0.0/0
- 11
- 12 Chain POSTROUTING (policy ACCEPT 48 packets, 3008 bytes)
- 13 pkts bytes target prot opt in out source destination
- 14
- 15 Chain sshuttle-12300 (2 references)
- 16 pkts bytes target prot opt in out source destination
- 17 0 0 RETURN tcp -- \* \* 0.0.0.0/0 127.0.0.0/8
- 18 24 1440 REDIRECT tcp -- \* \* 0.0.0.0/0 0.0.0.0/0 TTL match TTL != 42 redir ports 12300