Week 10
Packet Filtering Rule R1

Packet Filtering Rule R1 for Telnet

- Inbound example
  - External Telnet Client ➔ Internal Telnet Server (23)
- Outbound example
  - Internal Telnet Client ➔ External Telnet Server (23)
- Rules

Service direction	Packet direction	Source address	Dest. address	Protocol	Dest. port	Action
Inbound	Incoming	External 192.168.3.5	Internal 172.16.1.2	TCP	23	Permit (rule A)
	Outgoing	Internal 172.16.1.2	External 192.168.3.5	TCP	>1023	Permit (rule B)
Outbound	Outgoing	Internal 172.16.1.2	External 192.168.3.5	TCP	23	Permit (rule C)
	Incoming	External 192.168.3.5	Internal 172.16.1.2	TCP	>1023	Permit (rule D)

Attack A1 Against Rule R1

- External Attacker (5000) ➔ Internal Server (6000)
- The attacker satisfies R1 with the following:

Packet direction	Source address	Dest. address	Protocol	Dest. port	Action
Incoming	External 10.1.2.2	Internal 172.16.1.2	TCP	6000	Permit (rule D)
Outgoing	Internal 172.16.1.2	External 10.1.2.2	TCP	5000	Permit (rule B)

★ The attack is successful!

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT