Week 10
Packet Filtering Rule R3

Packet Filtering Rule R3 for Telnet

- Check the initiator (ACK bit)!
- Add a new column to R2 for the purpose

Service direction	Packet direction	Source address	Dest. address	Protocol	Source port	Dest. port	ACK = 1	Action
Inbound	Incoming	External	Internal	TCP	>1023	23	Any	Permit (rule A)
	Outgoing	Internal	External	TCP	23	>1023	Yes	Permit (rule B)
Outbound	Outgoing	Internal	External	TCP	>1023	23	Any	Permit (rule C)
	Incoming	External	Internal	TCP	23	>1023	Yes	Permit (rule D)
Default	Either	Any	Any	Any	Any	Any	Any	Deny (rule E)

Attack A2 Against Rule R3

- External Attacker (23) ➔ Internal Server (6000)
- A2 cannot satisfy the following rule:

Packet direction	Source address	Dest. address	Protocol	Source port	Dest. port	ACK = 1	Action
Incoming	External 10.1.2.2	Internal 172.16.1.2	TCP	23	6000	No	Deny (rule E)

★ The attack is failed!

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT