Week 10
Packet Filtering Rule R2

Packet Filtering Rule R2 for Telnet

- Check the source port!
- Add a new column to R1 for the purpose

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

Attack A1 Against Rule R2

- External Attacker (5000) ➔ Internal Server (6000)
- A1 cannot satisfy the following rules:

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

★ The attack is failed!

Attack A2 Against Rule R2

- External Attacker (23) ➔ Internal Server (6000)
- The attacker satisfies R2

Packet direction	Source address	Dest. address	Protocol	Source port	Dest. port	Action
Incoming	External 10.1.2.2	Internal 172.16.1.2	TCP	23	6000	Permit (rule D)
Outgoing	Internal 172.16.1.2	External 10.1.2.2	TCP	6000	23	Permit (rule C)

★ The attack is successful!

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT