CCDC Inject

INJECT NAME	Reject Firewall Rule Probing
INJECT ID	NETW02A

INJECT DESCRIPTION:

The Security Operations team has learned that a hacker group has been probing the firewalls of organization, delineating what they might be using a tool like Firewalk.

Construct a security policy on the perimeter firewall that will drop packets that appear to be coming from a tool like Firewalk.

INJECT DELIVERABLE

Respond with a business memo that explains how an attacker might probe a firewall for rule delineation. Explain how the knowledge of how these tools work have lead to the specific firewall policy or router ACL that was developed. Show evidence of the rule or ACL implemented and functioning.