Actividad 04 – Mecanismos de defensa de red

Jorge Alejandro Cabrera Meza – 181591

CNO V – Seguridad informática

Ing. Tecnologías de la información

Mt Servando López Contreras

Regla	Comando Sugerido
Establecer una política restrictiva.	Iptables -p FORWARD DROP
Permitir el tráfico de conexiones ya establecidas	Iptables -A -m FORWARD state –state ESTABLISHED, RELATED -j ACCEPT
Aceptar tráfico DNS (TCP) saliente de la red local	Iptables -A INPUT -p tcp -s 192.1.2.11 – d 0.0.0.0 --dport 53 -m state --state NEW -j ACCEPT
Aceptar correo entrante proveniente de Internet en el servidor de correo	Iptable -A INPUT -p tcp -s 0.0.0.0 -d 192.1.2.10 --dport 25 -m state --state NEW -j ACCEPT
Permitir correo saliente a Internet desde el servidor de correo	Iptables -A FORWARD -p tcp -s 192.1.2.10 -d 0.0.0.0 --dport 25 -m state --state NEW -j ACCEPT
Aceptar conexiones HTTP desde Internet a nuestro servidor web	Iptables -A FORWARD -p tcp -s 0.0.0.0 -d 192.1.2.11 --dport 80 - m state --state NEW -j ACCEPT
Permitir tráfico HTTP desde la red local a Internet	Iptables -A FORWARD -p tcp -s 192.1.2.11 -d 0.0.0.0 --dport 80 -m state --state NEW -j ACCEPT