PDF

Specific
Recommendations: Router Access 1. Shut down unneeded services
on the router. Servers that are not running cannot break. Also, more
memory and processor slots are available. Start by running the show
proc command on the router, then turn off clearly unneeded
facilities and services. Some servers that should almost always be
turned off and the corresponding commands to disable them are
listed below. Small services (echo, discard, chargen, etc.) no service
tcp-small-servers no service udp-small-servers BOOTP - no ip
bootp server Finger - no service finger HTTP - no ip http server
SNMP - no snmp-server 2. Shut down unneeded services on the
routers. These services allow certain packets to pass through the
router, or send special packets, or are used for remote router
configuration. Some services that should almost always be turned off
and the corresponding commands to disable them are listed below.
CDP - no cdp run Remote config. - no service config Source routing
- no ip source-route 3. The interfaces on the router can be made
more secure by using certain commands in the Configure Interface
mode. These commands should be applied to every interface.
Unused interfaces - shutdown No Smurf attacks - no ip
directed-broadcast Mask replies - no ip mask-reply Ad-hoc routing
- no ip proxy-arp 4. The console line, the auxiliary line and the
virtual terminal lines on the router can be made more secure in the

Configure Line mode. The console line and the virtual terminal lines should be secured as shown below. The Aux line should be disabled, as shown below, if it is not being used. Console Line - line con 0 exec-timeout 5 0 login Auxiliary Line - line aux 0 no exec exec-timeout 0 10 transport input none VTY lines - line vty 0 4 exec-timeout 5 0 login transport input telnet ssh 5. Passwords can be configured more securely as well. Configure the Enable Secret password, which is protected with an MD5-based algorithm. Also, configure passwords for the console line, the auxiliary line and the virtual terminal lines. Provide basic protection for the user and line passwords using the service passwordencryption command. See examples below. Enable secret - enable secret 0 2manyRt3s Console Line - line con 0 password Soda-4-jimmY Auxiliary Line - line aux 0 password Popcorn-4-sara VTY Lines - line vty 0 4 password Dots-4-georg3 Basic protection - service password-encryption 6. Consider adopting SSH, if your router supports it, for all remote administration. 7. Protect your router configuration file from unauthorized disclosure. 100Test

www.100test.com