Network Device Security

There are a number of configuration steps that one can take to ensure the proper operation of different network devices. These steps include applying patches as well as taking the time to configure the device for increased security.

- **Patching**: Patches and updates released by the product vendor should be applied in a timely manner. Quick identification of potential problems and installation of patches to address newly discovered security vulnerabilities can make the difference between a minor inconvenience and a major security incident. To ensure that timely notification of such vulnerabilities is received, vendor's e-mail notification services should be subscribed to, as well as to general security mailing lists.
- **Access Control Lists**: Routers have the ability to perform IP packet filtering. Access control lists (ACLs) can be configured to permit or deny TCP, UDP, or other types of traffic based on the source or destination address, or both, as well as on other criteria such as the TCP or UDP port numbers contained in a packet. While firewalls are capable of more in-depth payload inspection, strategically placed router ACLs can significantly increase network security.
- **Disabling Unused Services**: Routers run services that are not required for the process of routing packets. Taking steps to disable and protect such services can increase the overall security of the network.

  Proxy ARP allows one host to respond to ARP requests on behalf of the real host. This is commonly used on a firewall that is proxying traffic for protected hosts. Cisco routers have Proxy ARP enabled by default, and this may allow an attacker to mount an ARP poisoning attack against a host.

  There are several automatic discovery protocols, some of which are vendor specific, such as Cisco Discovery Protocol (CDP), others of which are open standard. In all cases, while these may provide some level of convenience for administering networks, they also present the opportunity for anyone sniffing the network to learn a significant amount of information about the network topology. If these protocols are not actively used, they should be disabled, and if they are used, careful attention should be paid to securing them as much as possible.

Most routers have a number of diagnostic services enabled for certain UDP and TCP services. These services should be disabled when not in use for troubleshooting or testing. Certain debug functions are particularly resource intensive, and an attacker could create a condition simply by accessing a compromised router and turning on a debug process that consumes all of the available resources on the device.

Many vendors provide a web server for making configuration changes. If the router will not be managed in this manner, the web server can be disabled.

- **Internet Control Message Protocol**: The Internet Control Message Protocol (ICMP) provides a mechanism for reporting TCP/ IP communication problems, as well as utilities for testing IP layer connectivity. It is an invaluable tool when troubleshooting network problems. However, ICMP can also be used to glean important information regarding network topologies and available host services.

  Echo requests and replies, more commonly known as pings, are used to determine if another host is available and reachable across the network. If one host can successfully ping another host, it can be concluded that the hosts have proper network operation. An attacker can use ping to scan publicly accessible networks to identify available hosts, though more experienced attackers avoid ping and use more stealthy methods of host identification.

  Traceroute is not itself an ICMP message type, but rather a method that frequently employs ICMP messages. It is also used to troubleshoot network-layer connectivity by mapping the network path between the source and destination hosts. Traceroute is useful in pinpointing where along the network path any connectivity troubles are occurring.