## Name Services

**Security Policy Item**

Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

**Vulnerability**

Weaknesses in BIND (the most common DNS implementation) top the SANS top ten list of vulnerabilities. Packetstorm has nine BIND exploits available for easy download at <http://packetstorm.securify.com/exploits/apps/bind/>.

DNS also offers more than its share of security headaches in addition to the buffer overflow attacks that can give an attacker root access to a system.

Using DNS zone transfers, an attacker can download configuration information from your DNS server in bulk, giving them instant access to a remarkably complete and accurate picture of your network.

The IP addresses give a list of potential addresses to scan and attack, and if your host names are designed to be mnemonic (finance-1, proposal\_svr, payroll, etc) the information could help the attacker focus his efforts on the "juicy" targets.

Yet another vulnerability of DNS is cache poisoning. An attacker can send a DNS query that includes some answer records that would be cached at the resolving DNS server.

This can be exploited to redirect traffic from the target web server to the attacker's own web server.

According to CERT Advisory CA-97.22, "The mapping between host names and IP addresses may be changed. As a result, attackers can inspect, capture, or corrupt the information exchanged between hosts on a network."

**Filter Application**

Inappropriate uses of DNS should be stopped at the perimeter router. In this example, we will be applying the extended ACL to the inside interface of the perimeter router, as described earlier.

The syntax for an extended ACL is:

access-list {list name} permit/deny {protocol} {src} {mask} {operator} {port} {dest} {mask} {operator} {port} established

In the following block from the router's configuration file, we will block DNS queries to all machines except for the public DNS server on the screened services network, zone transfers to all machines except for the authorized secondary server at NNN.12.54.200, and LDAP.

!named ACL Packet Filter

ip access-list extended packet\_filter

!Allow DNS (UDP 53) to the DNS server

permit udp any host NNN.16.27.66 eq 53

!Allow DNS zone transfer (TCP 53) to the DNS secondary

!(BIND 4.x)

permit tcp host NNN.16.27.66 eq 53 host NNN.12.54.200 eq 53

!Block DNS to all others (UDP 53)

deny udp any any eq 53 log

!Block DNS host transfers to all others

deny tcp any any eq 53 log

!Block LDAP (TCP and UDP 389)

deny tcp any any eq 389 log

deny udp any any eq 389 log

!Allow other traffic

permit ip any any

The "packet\_filter" ACL is applied at the internal router interface for all incoming traffic, using the following command from interface configuration mode:

router# conf t

router(config)# int eth2/0

router(config-if)# ip access-group packet\_filter out

**Additional Actions**

Zone transfers can be disabled (or limited) in the configuration files of the DNS server. For BIND, this would be accomplished using the allow-transfer option in the named.conf.

Another common-sense method of limiting your exposure level is to make sure that a zone transfer yields no information that would be useful to an attacker.

A split DNS strategy that puts an internal DNS server on the protected network would leave the attacker with access only to an external DNS server that merely lists your public hosts (e.g.: web servers and FTP servers on your screened services network or DMZ).

**Filter Verification**

The DNS packet filters can be tested by attempting to use the blocked services from outside of the perimeter router.

Alternately, to test TCP protocol filters, one can simply use telnet to attempt to connect to the specific blocked ports, for example zone transfer blocking could be verified with: telnet NNN.16.27.66 53.

For UDP services, one can use a simple port scanner, such as NMAP to probe the relevant UDP ports.

The resulting log excerpt from the perimeter router shows that the connection attempts to the LDAP port 389, and the DNS zone transfer port 53 (via telnet) were stopped by the "packet\_filter" ACL on the router:

04:22:53: %SEC-6-IPACCESSLOGDP: list packet\_filter denied tcp NNN.16.11.5(18618) -> NNN.16.27.70(389), 1 packet

04:22:29: %SEC-6-IPACCESSLOGDP: list packet\_filter denied tcp NNN.16.11.5(36486) -> NNN.16.27.70(53), 1 packet