ECS DMZ Network Report

# Scan Results

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | No. of Servers running services | Port(s) | Service description |
| Admdog | 509 | 5101 | Port used for Yahoo Messenger communication |
| Airport-admin | 509 | 5009 | Airport wireless network admin utility |
| H323q931 | 510 | 1720 | H.323 (Microsoft NetMeeting) call setup protocol |
| http | 44 | 80/443 | World Wide Web HTTP/HTTPS |
| https | 2 | 443 | HTTPS |
| Ida-agent | 510 | 5051 | Symantec Intruder Alert |
| ldap | 505 | 389 | Lightweight Directory Access Protocol, used by Microsoft NetMeeting |
| Printer | 509 | 515 | Used by printers for listening to incoming connections |
| Sip | 500 | 5060 | Session initation protocol, used for VoIP |
| ssh | 1 | 22 | Secure Shell remote access |
| upnp | 490 | 5000 | Universal Plug and Play |
|  |  |  |  |

# Analysis

The majority of the ports used by services in this section of the network are filtered, making it hard to find any vulnerabilities within it, which is probably a good thing.

Most of the servers are running OpenBSD, with a few on FREEBSD or something other Linux distribution, the servers running the “other” variant of Linux all seem to have an open HTTP port, in fact, all but 5 of the http ports are reported as open, presumably they’re web servers so it’s understandable. In any case, an open port is still more vulnerable than a filtered one, and considering the huge amount of Trojans that gain access using port 80 (HTTP), you would have to hope that the server running these open ports have some kind of adequate intrusion prevention and/or security software running.

Following on from this, some of these servers are also running an open HTTPS port (443), which seems a bit troubling as HTTPS should be a secure protocol, and leaving its access port unprotected seems like a vulnerability that should be investigated.

These web servers are the most vulnerable hosts in the network, with an average of 3-4 open ports. None of the hosts on the network are completely locked down, as they all have at least one open port (1720), and this is due to the strangely named h323q931 service. While there is a thin amount of information about this service online, I have managed to work out that it is used for VoIP set-up functionality by Microsoft NetMeeting. The fact that this port is open might allow an attacker to perform a man-in-the-middle hijacking of a VoIP conversation, which could be potentially a huge vulnerability. As every single host in the network has this open port, there is the possibility that an attacked could perform a DDOS on this port on every single host in the network, which would be pretty damaging.

There is one server with an open SSH port, which could be open to the same sort of vulnerabilities at the HTTP port; however, as SSH is usually used for remote access, hijacking this port might allow control of the machine itself, which is a serious vulnerability.

# Network Penetration Limitations