Cyber Security - Firewall Port Analysis
TwinSPIN
April 8, 2010
University of Minnesota

Ports to Watch

- Port 21 - File Transfer Control
- Port 22 - Used for SSH, Secure Shell and old versions of PC Anywhere
- Port 23 - Telnet - New Zealand (multiple)
- Port 53 - DNS Service (Exploited by various Trojans and Worms. Also used by X-Box)
- Port 135 - Remote Procedure Call (RPC) Used by to set up VPNs and SPAM Pop Up Windows
- Port 139 - Critical Windows RPC vulnerability affecting ports 135,139 and 445. Also used by many Worms and Trojans
- Port 443 - Used by HTTPS and Encrypted Responses from Compromised Computers to Bot Net Handlers
- Port 445 - TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer (Most common port attacked. Represents most attacks.)
- Port 455 - Used by the tcp/udp protocol for service type creativepartnr and trojans
- Port 889 - Server FTP Listening Port
- Port 1026 - Calendar Access Protocol Port
- Port 1080 - Socks Proxy is an Internet proxy service, potential spam relay point. Common programs using this port: Wingate. Trojans and Worms also use this port.
- Port 1433 - SQL Data Base Access (European Origin Most Common)
- Port 1521 - Oracle Server Communications (TNS) Access (Hefei China)
- Port 1755 - Windows Media Services
- Port 1935 - Adobe Flash Streaming Media
- Port 2967 - Symantic Download Access (China)
- Port 3306 - Used by mySQL database server
- Port 3389 - Microsoft Terminal Server (RDP) officially registered as
Ports to Watch

- Windows Based Terminal (WBT)
- Port 3128 - squid-http3128/tcp#Proxy Server MastersParadise3129/tcp#[trojan]
- Port 4899 - Remote Administration Radmin (Remote Administrator) by Famatech, Remote Administrator default port (China, Spain)
- Port 5038 - Asterisk Open Source VOIP Call Set Up
- Port 5900 - VNC - the original cross-platform remote control solution - Brampton Canada & others plus “Back Orifice” and numerous trojans
- Port 6029 - #X Window System
- Port 7212 Used by GhostSurf™ open proxy also has been used for streaming audio and video - (Mostly Chinese IP Addresses)
- Port 8000 - iRDMI (Intel Remote Desktop Management Interface) (Mostly Chinese IP Addresses)
- Port 8009- Used by Apache Server “Behind the Firewall”
- Port 8443 - PCSync SSL (Hurth Germany)
- Port 8080 - HTTP alternate (http_alt)—commonly used for Web proxy and caching server, or for running a Web server as a non-root user (China)
- Port 8880 - Port 8880 may be used for several services including CDDBP-- and more.
- Port 9043 IBM WebSphere Secure Administration Console
- Port 9165 (one address above “NetLOCK”)
- Port 9415 - Appears to be a Trojan Command Link
- Port 9659 CGI Script?
- Port 10000 - Webmin—Web-based Linux admin tool (Unofficial) BackupExec (Unofficial) Ericsson Account Manager (avim)
- Port 10001 - Lantronix UDS-10/UDS100[43] RS-485 to Ethernet Converter default
- Port 18338 - Private Port? - (Turin, Italy)
- Port 20267- Used for “Bad Company” Multi-player “Electronic Game”
Ports to Watch

- Port 21086 - Multicast Voice (Cisco?)
- Port 28881 - “Call Duty 2: Modern Warfare Multiplayer” Electronic Game
- Port 28148 - “Call of Duty 4: Modern Warfare Multiplayer” Electronic Game
- Port 32000 - Merak WebMail server, Artisoft XtraMail DoS vulnerability
- Port 32768 - Trojan “Hacker’s Paradise” and Filenet TMS (Moscow, Russia)
- Port 37893 Norton Anti-Virus host discovery China
- Port 41166 “Brothers In Arms” Electronic Games and Trojan “Reboot Tool”
- Port 41486 - Likely Trojan
- Port 47092 - Likely Trojan
- Port 60641 - Likely Trojan
- Port 62599 SSHd Hack