Windows Security Cheat Sheet

Defensive Tools

- Windows Update http://windowsupdate.microsoft.com
- MS Security Baseline Analyzer http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp
- IIS Lockdown Tool http://www.microsoft.com/technet/security/tools/tools/locktool.asp
- URL Scan http://www.microsoft.com/technet/security/tools/tools/urlscan.asp

Offensive Tools (kinda)

- Start with WinPcap http://winpcap.polito.it/
- Ethereal http://www.ethereal.com/ (Yes it works on windows too)
- Nmapwin http://www.nmapwin.org/

A few words about Terminal Services

- Provides a new remote user session, not a mirror of console
- Installed in “Remote Administration” mode, its free, restricted to 2 sessions
- Encrypted RC4 with 56bit key (default) – Change using the TS Configuration MMC Snapin
- Runs on port 3389, this can not be easily changed

Quick and Easy IP Filtering

- TCP/IP Properties -> Advanced -> Options
- Set IPSec Policies
- Filter TCP, UDP ports here

System Configuration

- System Properties -> Advanced ->Startup and Recovery
    - Small Memory Dumps mean Quick Reboots
    - Make sure it reboots and doesn’t hang looking for feedback
- Default Shares
    - C$, ADMIN$ - be careful
- Enabled Auditing, Perfmon
    - Watch failed logins, etc
- Default File Permissions are weak, but change them at your own risk

Some Services Available in a default installation

- Web (static and dynamic), FTP, SMTP
- Telnet

General Notes

- IIS is not on by default (at least not in the RTM version)
- Prove that this product is secure “Out of the Box”