Malware and Persistence: Supplement

Exercises

1. Malware can be included in Microsoft Office Documents. Consider the Metasploit module MS12-027 MSCOMCTL ActiveX Buffer Overflow. This exploits CVE 2012-0158, which is a vulnerability in Microsoft Office 2007 and 2010 that can be triggered by a malicious .rtf file. Use it to obtain a shell on a target.
2. Use the MS15-100 Microsoft Windows Media Center MCL Vulnerability to attack a Windows 7 SP1 system through Windows Media Center.
3. (Advanced) The source code for ls is available as part of the GNU coreutils package (<http://www.gnu.org/software/coreutils/coreutils.html>). Download the package and compile it using configure, make, and make install. Use the --prefix option to configure to choose the installation directory. Run the newly compiled ls. Modify the source code for ls (src/ls.c) to include return a shell to an attacker. Compile and test the result.
4. The at command is a deprecated but still available alternative to schtasks. Use it to build persistence on a compromised Windows system.
5. Use a MOF to prevent tools (e.g. Sysinternals defensive tools) from running.
6. Read <https://room362.com/post/2016/wpad-persistence/>. Implement the WPAD persistence mechanism it describes.
7. Use the at command on a Linux system to set up a persistence mechanism. What are the differences between using cron and at? Try the module <https://www.rapid7.com/db/modules/exploit/unix/local/at_persistence>
8. Bash provides the command Prompt\_Command, which will execute a Bash command before displaying a prompt. Use it as a persistence mechanism.