Guest Speaker: Eric Wedaa

Hudson Valley CyberSecurity Consortium Presents: LongTail Honeypot

Eric Wedaa has been involved with Unix System Administration since 1987 and Eric has been actively involved with Unix security since 1992 and has recently released Long Tail Log Analysis, an ssh brute force task analysis. This is the first publicly released tool that not only does basic analysis of ssh login attempts, but also can group them into botnets based on attack patterns.

Time: 6:00-8:00 p.m.

Date: October 27, 2015

Location: Marist College, 3399 North Road, Poughkeepsie, NY 12601, Donnelly Hall, Linux Lab (Rm 258A)

LongTail is both a honeypot and a set of programs that analyze ssh brute force login attempts. It performs not only the standard what passwords are being tried, it also analyzes them based on accounts tried. Where LongTail goes that nobody else currently does is that it groups them into attack patterns, and then provably groups attacking IP addresses into botnets that are controlled by a single person or group of people.

This talk contains light technical details on how this is done so it can be followed by non-technical staff, but is technical enough that the results can be reproduced by technical staff.