November 15th CSF

Hacker Profiling Project: Looking into the Hacker's Mind

Aaron Grothe – CISSP

NEbraskaCERT

Overview

- “If you know your enemies and know yourself, you will not be imperiled in a hundred battles” - Sun Tzu
- “By knowing things that exist, you can know that which does not exist” - The Book of Void – Five Rings

Wouldn't it Be Great

- If you could figure out the level of sophistication of an attacker easily?
- E.g. Is it a disgruntled ex-employee, a script kiddie or a competitor
- “Let you know whether to use a rock or a cannon” - Dr. Burnham

Dream Scenario

- A company would send logs “exactly like in the TV Show C.S.I” - leading to a profile
- “By profile we mean, for example, his technical skills, his probable geographic location, an analysis of his modus operandi”
- Above from the Newsforge interview with Stefania Ducci

HPP

- The Hacker's Profile Project is an attempt to do this
- The HPP has 3 Phases
  - Open questionnaire
  - Select Hacker's get detailed questionnaire
  - Hacker's Profiling Grid

The Term Hacker

- Initially hacker was not a bad term
- Hacker has become associated with illegal activities
- Eric “I'm with those guys” Raymond has been attempting to popularize the term “Cracker” for bad people

How Phase 1 Works

- Anybody can submit an entry
- HPP will collate all the results and make them available to the public

What HPP is doing Right

- Multi-lingual (English, Greek, Italian, and Romanian)
- Voluntary
- Phase 2 will be weighted more heavily than Phase 1
- Being associated with the Open Source Testing Methodology folk

Potential HPP Issues

- Is this for Hackers or Crackers?
- What are we going to get out of Phase 1?
- Are the questions neutral or leading?
- Will pretty much get the N00Bs

Potential HPP Issues

- How do you get the next level of hacker skill?
- The world is shrinking trying to figure out that guys from Romania are using Metasploit are dubious

Misrating

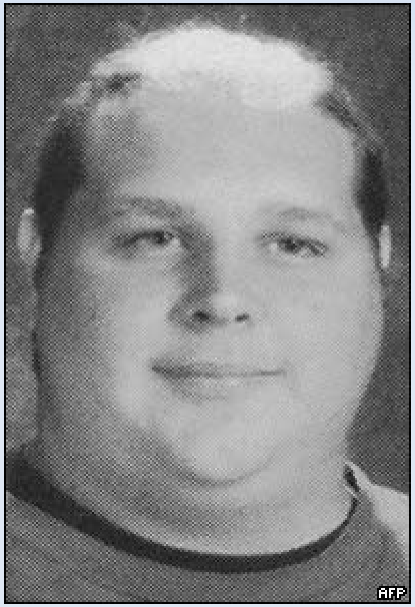
- One study found that 90% of the automobile drivers in Sweden rated themselves above-average drivers

Jeffery Lee Parsons

- Eighteen years old at the time
- Modified an already existing virus (Blaster)
- Put his NAME in the virus
- Code attempted to access his virus writing website
- got 18 months in Jail

Jeffery Lee Parsons

- Is this man l33t???



Phone Physic Example

- People say you're gullible
- You have money troubles

Interview is in 3 parts

- Personal Data
- Relational Data
- Technological and Criminilogical Data

A sampling of questions

- Lets take a look at some of the questions

A couple of the FAQs

- Q: Can I use a web anonymizer?
- A: Yes, you can use a web anonymizer (if you can find a working one) and fill-in the questionnaire

A couple of the FAQs

- Q: How can I be sure of the anonimity of the questionnaire?
- A: If you have a look at the credits and supporters, you should be certain about the ethics of the persons that manage the project. ... For this reason we suggest using a chain of proxy (we don't think you need instructions on it ;P), an anonymizer or TOR

Summary

- Is an interesting project
- How to get beyond the Script-kiddie/Wannabee lamer hacker?
- The hacker profiling grid sounds like it might be cool, how it stands out compared to the honeynet project still to be demonstrated

Resources

- Hackers Profile Project
  - hpp.recursiva.org
- Honeynet project
  - www.honeynet.org
- Cyber Adversary Characterization
  - Syngress Press
- Dr. Cohen's Work
  - all.net