(S//SI) Exploiting Terrorists' Passwords

FROM: Mike O'Hara
Research Pod 31 (under S3T)
Run Date: 04/08/2004

FROM: Mike O'Hara
Research Pod 31 (under S3T)

(S//SI) When government agencies seize computer media (hard drives, CDs, floppies, etc.) used by terrorists, they send the materials to the SIGINT Forensics Lab to be analyzed for potential actionable intelligence leads. (See the previous article on SIGINT forensics .) Researchers in Pod 31 realized that data in these computers are a rich source of passwords and related information, and set about finding ways to exploit this information.

(S//SI) The Pod's suite of tools automatically scans text documents, e-mails, web pages and other files to identify passwords. In this manner they harvested hundreds of thousands of occurrences of passwords, some accompanied by collateral account information, all of which can be used to support SIGINT exploitation in various ways.

(TS//SI) For example, these passwords can be used to aid in password-guessing against encrypted files found on the hard drives. Not only might passwords be re-used by targets, but they may also fall into a pattern that SID can use to tailor our password guesses. Preliminary results are promising: in a couple of instances the pod researchers collaborated with the SIGINT Forensics Lab and the JUMBLEDPET password-guessing team to break very hard passwords with little work.

(TS//SI) Passwords can also be used to aid in computer network operations, and to link individuals who use common passwords. In one instance, intelligence analysts were able to relate caches of documents which might not have otherwise been discovered. Together with the Forensics Lab, the CNE Technical Development branch, and the JUMBLEDPET team, the researchers continue to pursue ways to exploit this novel collection of data.

(U//FOUO) This work was done in SID Research Pod 31: Information Diagnosis Evaluation and Assessment (IDEA), which has been investigating ways to better exploit computer media data using prioritization algorithms and other approaches. Research pods are run under the auspices of the Technical Advocate Office in Data Acquisition.

(U//FOUO) Questions can be directed to Mike O'Hara ([redacted] nsa) or [redacted] nsa).