This article is the fourth in a short series examining vulnerability assessment systems (VAS) and intrusion detection systems (IDS). In the preceding article, I looked at some aspects of responding to IDS alerts. In this article, I summarize some of arguments against retaliation when your computer systems are attacked.

* * *

There’s a long-standing debate, mostly underground and informal, about how satisfying it would be to strike back at criminal hackers, industrial spies, saboteurs and other baddies who have the nerve to attack our systems. People have speculated about counter-flooding, using buffer-overflow attacks, sending “explosive” HTML code that could cause system freezes, and so on. Much of this talk is really just good-natured fun – more along the lines of “wouldn’t it be nice if” than actually serious proposals for corporate responses. But to be absolutely sure that all of the readers of this column, at least, have a chance to think about it, let me flatly state that any such counterattacks are to be formally forbidden by corporate policy.

Firstly, although I am not a lawyer and this is not legal advice (for legal advice, consult an attorney with appropriate expertise), as far as I know, there is absolutely no waiver in US law which would exculpate anyone who gains unauthorized access to other people’s computer systems. In particular, the Computer Fraud and Abuse Act of 1986 (18 USC §1030), the Unlawful Access to Stored Communications Act (18 USC §2701), and the Electronic Communications Privacy Act of 1986 (18 USC §§1367, 2232, 2510 and several other sections) do not make any allowance for revenge attacks. Investigation of such crimes (the revenge attacks) could involve seizure of equipment as evidence.

Secondly, because IPv4 provides inadequate authentication of packets, it is difficult or impossible to prove the exact origin of denial-of-service attack packets or even of packet streams used in attack sessions. Attacking the wrong target would be an unmitigated disaster.

Thirdly, many attackers subvert poorly-secured intermediary systems to launch their attacks; attacking these hosts would damage other victims but cause no direct harm to the real attackers.

Fourthly, unauthorized penetration of anyone’s computer systems and networks can lead to civil lawsuits for damages; even if the lawsuits are unsuccessful, they can rack up expensive attorneys’ fees and also cause expensive computer equipment to be seized as evidence under subpoena.

No, although it might seem like a satisfying tactic that would be the geek equivalent of innumerable Steven Seagal and Jean-Claude Van Damme movies, trying to strike back at attackers through illegal means is a thoroughly bad idea.
In the next short contribution on this subject, I’ll look at how you can prepare for an effective response IDS alarms.

For further reading:

http://www4.law.cornell.edu/uscode/18/1030.html

18 USC 2701 Unlawful Access to Stored Communications Act.  
http://www4.law.cornell.edu/uscode/18/2701.html


NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay.  All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.