



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Defenders or Digilantes?

Christopher Loomis

December 14, 2000

The purpose of computer security is to protect the confidentiality, integrity and availability of data and the systems on which that data resides. That much we can agree on. However, there is a debate raging within security circles as to just how far one can go to protect that data. Specifically, is it acceptable to attack an attacker? When do you cross the line from defensive to offensive behavior? What are the dangers of doing so? This, not surprisingly, is a polarizing issue, with two major camps - the defenders and the digilantes (digital vigilantes). Defenders do not deviate from the incident response procedure as defined by their organization's written security policy. They will not undertake questionable actions because of the thorny legal and ethical implications. Digilantes, on the other hand, will take whatever measures are deemed necessary to protect their systems. They will not hesitate to strike back at whatever source is attacking them, in order to stop active attacks and to deter future ones.

I wondered what it would be like to put a prototypical defender and digilante together in a room to have it out. Perhaps it would go a little something like this . . .

MODERATOR: First off, I would like to thank both of you for coming tonight. This is a forum where you will be allowed to define and defend your respective positions regarding appropriate response and its limits. Hopefully, we can gain a better understanding of each side and perhaps find some common ground. Historically, vigilante behavior has emerged to fill a real or perceived void when conventional law enforcement efforts are considered to be ineffective. So, Digilante - where's a cyber cop when you need one?

DIGILANTE: Good question. I guess you should look for the guys reading those 'Internet for Dummies' books. Look, I have nothing against law enforcement per se, but it is becoming quite obvious that they are simply out of their league when it comes to technology-based crime. Agencies are overworked, understaffed, under funded and unable to attract individuals with the necessary expertise to combat cyber crime effectively.

DEFENDER: I think it's important that we acknowledge that cyber law enforcement efforts are only in their infancy. It takes a little time to get everyone up to speed. There was no way to predict the astronomical growth of the Internet and our almost-overnight transformation into an interconnected world. With the increasing backlog of cases, agencies will be able to justify the additional funding and personnel needed to do the job.

DIGILANTE: That's all well and good - for the future. But what about the cases that are

part of that increasing backlog? What's being done to solve those?

DEFENDER: Listen, I'm not here to defend law enforcement. What we really disagree on is deciding how to deal with the current situation. Just because we may not be able to rely on law enforcement doesn't mean that we are completely on our own. Instead, what we need are information-sharing partnerships between members of the Internet community that facilitate first, the prevention, and second, the investigation of security incidents. Think of it as a network neighborhood watch.

DIGILANTE: I feel a group hug coming on. Not that I disagree with your premise, its just that you shouldn't start a job you're not willing to finish.

MODERATOR: So when is the job finished? I'm sure that you are both aware of the Ready - Aim - Fire concept. My question is for Defender. Would you characterize digilantism as Fire - Aim - Ready?

DEFENDER: I think that's accurate. With the proliferation of spoofing, leapfrogging and the use of zombies by attackers these days, when you strike back, you really have no idea who you are hitting. Besides, when you retaliate, you become part of the problem, not part of the solution.

DIGILANTE: I agree that it's important to properly identify, as much as is practical, the true source of the attack. What you consider innocent bystanders, however, I call ignorant bystanders. If you are going to put a system on the Net without properly securing it, too bad if you get caught in the crossfire. As for the "part of the problem" argument, it's just an attempt to distract us from the real problem - that simple defense is not deterring attacks.

DEFENDER: Explain to me how digilantism is any better. All that you are accomplishing, say with a denial of service attack, is knocking the attacker off of the net temporarily. Why not complain to their ISP instead, which could get them knocked off permanently?

DIGILANTE: Because it takes them all of about 5 minutes to sign up with another ISP. Besides, ISPs are even less responsive than law enforcement.

DEFENDER: I just don't see the reward vs. the risk. Why expose yourself and your organization to the legal implications for such little benefit?

DIGILANTE: Because you can't negotiate with cyber-bullies. Do you really think that the Electrohippies would have stopped their assault on the WTO web site if the WTO had just politely asked them to?

MODERATOR: I'm going to need a little background here.

DIGILANTE: Sure. Conxion, a web hosting service, noticed a denial of service attack

against one of its client's websites - the World Trade Organization. Conxion traced the attack back to a lone server run by a group calling themselves the Electrohippies. Conxion configured their own machines to 'return to sender' the massive number of page requests directed at the WTO site back to the source, which crashed the Electrohippies' server.

DEFENDER: I have to admit that I am a little torn about this one, since returning requests is a legitimate server function and the action was taken to repel an active attack. However, if Conxion had gone beyond that, such as sending a flood of crafted offensive applets or sending a group of thugs to rough up the Electrohippies, than they would definitely be breaking the law.

MODERATOR: Let's talk about the law. How can we expect to have any legal clarification on what constitutes an appropriate response when computer security law has yet to achieve consensus on many of the key issues?

DIGILANTE: I'm afraid that we're going to be lost in the fog until a body of case law gets established. Progress has been hindered in this area because lawmakers have been turned off by the technical complexity of these issues. Today, there are many more questions than answers. I really would like to know what the legal ramifications are if a company, acting in good faith, happens to make a mistake.

DEFENDER: Also, should there be minimum security requirements to have a system on the Net? I know that there are some voluntary efforts being made to establish what constitutes a reasonable security baseline. What is the threshold that an organization must cross in order to avoid a charge of contributory negligence?

DIGILANTE: Who will make the determination whether or not a system is secure? Please don't tell me that this will be on the honor system. Is that a herd of lawyers I hear coming down the hall?

DEFENDER: I think a lot of the due diligence questions will be addressed, as companies will be required to quantify their security postures for insurance purposes.

DIGILANTE: Oh great. The insurance industry and lawyers. We're doomed.

MODERATOR: I'd like to get your thoughts on the recent Microsoft break-in.

DIGILANTE: That case raises a couple of issues. Microsoft claimed, at least in their latest version of events, that they monitored the intruder while he was on their system instead of immediately kicking him out. It is unclear if this action would affect their legal standing as it pertains to any damage the intruder may have caused after they first became aware of his presence. Would Microsoft be held partially responsible if the intruder used their network as a launching pad for more attacks? The other issue involves the poor Microsoft employee whose home system was allegedly compromised

and used as a conduit into the main network. Is he negligent?

DEFENDER: That raises the general issue - with the rapidly increasing number of employees working from home - how do you extend and enforce your company's security policy to those systems?

DIGILANTE: As much as I hate to say it, it's going to take some legal action in order to get some clarity for these questions. In the meantime, I will take whatever measures necessary to protect my systems.

DEFENDER: What you should be concerned about is protecting your own backside. I know of no organization that has articulated in its written security policy an authorization for vigilante behavior. Therefore, I am assuming that Digilante receives his marching orders from the higher-ups with a wink and a nod, as they say.

DIGILANTE: Just don't get caught.

DEFENDER: That's my point. While I don't doubt Digilante's skills, it is just a matter of time before he does get caught. Guess what happens then. Those higher-ups who used to be his best buddies will invariably go running to the written policy and exclaim, "We never authorized that!"

DIGILANTE: I am just a patsy!

DEFENDER: Well, you can joke about it, but I don't think that it's a wise career move to set yourself up for what could potentially be some serious personal liability.

MODERATOR: Defender, you've told us what not to do - do you have any recommendations for what we should do?

DEFENDER: While this topic could take up an entire forum on its own, I will just hit upon a few key points that apply to our discussion. First - make sure that you have a written security policy. This is your 'get out of jail free' card. All procedures should follow from this policy. Second - make sure that the legal department is represented when the policy is drafted to insure that it is defensible and enforceable. Third - develop an incident severity scale to categorize incidents and define, based on the severity, exactly what actions should be taken. Fourth - make sure that all incident response team members are aware of and have practiced proper evidence collection procedures. Lastly - set up lists of internal and external contacts to be notified during an investigation, which vary depending on the severity of the incident. There is a lot of information on the Internet that fully explains the incident response cycle - I know that the SANS site has some excellent resources.

DIGILANTE: From my perspective, for obvious reasons we like to keep things in house. All of these "proper procedures" that Defender highlighted seem like a lot of work to

me - why let the attackers have all the fun?

MODERATOR: Are the attackers having all the fun?

DEFENDER: Well, I would hope that security professionals who are truly professional would get some measure of satisfaction from doing their jobs properly. However, there is a class of advanced, yet legal, measures that we haven't yet talked about. I refer to them as active defense, for they go beyond the standard hardening techniques which we are all familiar with.

DIGILANTE: Finally, we agree on something! The greatest asset for a majority of attackers, especially those pesky script kiddies, is time. What active defense aims to do is to use deception and trickery to waste as much of their time as possible.

DEFENDER: I want to make it clear that these are considered advanced techniques because it is assumed that you have already taken all of the basic hardening steps at your site. Skipping over those to get to this stuff won't do you much good.

DIGILANTE: The basic premise here is to make components of your system, or even the entire system itself, appear to be something it isn't. Some examples include setting up bogus accounts with very difficult passwords that take forever to crack, or modifying the functionality of standard commands and programs in order to confuse and frustrate that attacker. Use your imagination - I know that security professionals are pretty twisted. Just don't get too cute with this, for you may end up making the system unusable for everybody.

DEFENDER: Another option is to set up a honeypot, which is a decoy server loaded with mock info that attackers get routed to. While they spend time perusing this useless data, you silently gather evidence that can be used to help track down and prosecute them.

MODERATOR: Those are all interesting ideas. Well, gentlemen, we are nearly out of time. How about a final word from both of you.

DIGILANTE: Whether you are aware of it or not, there is a war going on in cyberspace. I'm just a mercenary, determined to protect my employer's systems by any means necessary. Until we get some clarification on many of the issues we discussed here tonight, understand that frustrated and fearful companies will continue to consider digilantism a viable option.

DEFENDER: I, too, am waiting for clarification. While we wait for legal guidance, however, we should be steered by moral and ethical principles. Right now the Internet community is a target-rich environment. It's time for the members of this community to come together and work together to try to prevent the attacks from succeeding in the first place, making this whole appropriate response debate moot. I call upon

industry leaders, security experts, lawmakers, vendors and law enforcement officials to take a seat at the table and try to hash these things out. They have to, for in order to solve systemic problems you must have systemic solutions.

MODERATOR: Well, that's it then. Thank you both for coming. Goodnight.

Sites of interest:

<http://www.sans.org>
<http://project.honeynet.org/>
<http://www.infowar.com/>

References:

Bridis, Ted. Buckman, Rebecca .Fields, Gary. "MS Claims Hacker was Watched." eWeek. 30 October, 2000.

URL: <http://www.zdnet.com/eweek/stories/general/0,11011,2646430,00.html>

CERT Coordination Center. "How the FBI Investigates Computer Crime." 27 July, 2000.

URL: http://www.cert.org/tech_tips/FBI_investigates_crime.html

Koch, Lewis Z. "Beware the Security Zealot." Inter@ctive Week. 23 May, 2000.

URL: <http://www.zdnet.com/zdnn/stories/comment/0,5859,2573856,00.html>

Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook. New Riders Publishing. 1999.

Radcliff, Deborah. "Can You Hack Back?" 1 June, 2000.

URL: <http://www.cnn.com/2000/TECH/computing/06/01/hack.back.idg/index.html>

Schwartau, Winn. "An effective way to disarm online muggers." Network World. 3 April, 2000.

URL: <http://www.nwfusion.com/columnists/2000/0403schwartau.html>

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event