Global Information Assurance Certification Paper

Should You Counter-Attack when Network Attackers Strike?

Robert Wildt

12/13/00

Most IT security administrators have been (or will be) in the following situation-- Your firewall or intrusion detection system is alarming. You are on the receiving end of a portscan, a denial-of-service (DOS) attack or an actual computer break-in.

"Oh, if only I could blast that attacker and make him stop!" you exclaim. Perhaps you can. But should you? This paper discusses some of the issues surrounding network vigilantism-- responding to a network attack with a counter-attack of your own.

Taking your systems offline in defense of an attack is a safe move, but what is the price of unavailability to your company? Wouldn't you just love to retaliate? Imagine how great it would feel to charge in, attack tools blazing, and bring that perpetrator's system to its knees? It's the stuff that heroes and great movies are made of.

On a more serious note, network counter-attacking, also known as strikeback, is indeed possible. Network defenders have access to the same tools as network attackers. Should the counter-attack be one of the tools of the well-armed IT security specialist?

A Counter-Attack Example: The Pentagon Strikes Back.

In September, 1998, a group of activists called the "Electronic Disturbance Theater" (EDT) mounted a denial-of-service attack called Floodnet against a Pentagon web site. The attack had been pre-announced, so the Pentagon was prepared to meet the attack with an counter-attack of its own. The Pentagon website redirected the incoming http requests to a Java applet called "hostileapplet". According to Ricardo Dominguez, a member of the EDT, this applet fired a "series of rapidly appearing Java coffee cups across the bottom of the browser screen coupled with the phrase 'ACK.' [1] The applet caused the attacking browsers to crash.

Meanwhile, back at the Pentagon, lawyers went ballistic as soon as they found out about the counter-attack. The lawyers pointed out that the Pentagon technical staff had committed federal felonies for which other hackers had been sent to jail. Additionally, they had broken a military prime directive, "posse comitatus", which forbids the military from taking unilateral actions within the United States and against U.S. Citizens.[2]

Pitfalls of Counter-Attacking.

As demonstrated in the story above, there are numerous pitfalls to network counter-attacks. The problems encountered range from questionable ethics to international law.

Here are some of the problems.

Over-reaction.

Over-reaction to a perceived attack can cause problems. In 1997, one of the Big Six accounting firms used scanning tools from Internet Security Systems (ISS) to assess the security of Internet service provider Sprint. A Sprint network administrator noticed a thousand simultaneous connections to his firewall. Panicking over a perceived network attack, he quickly shut down several routers. "His manual reaction took down 75% of the Internet," says Tom Noonan, president of ISS. Anyone using Sprint at that time was in a world of hurt." [3] Although the accounting firm was ultimately at fault for running network scanners without announcing it to the technical staff, the knee-jerk reaction of a staff member caused a major Internet outage.

How can you be sure who the attacker is?

The possibility of mistaken identity is one of the biggest arguments against the use of counter-attack. If your home were broken into, the law allows you to use self-defense to preserve your safety and protect your home. You are allowed steps to disarm or disable the attacker. This analogy does not translate well in the case of a cyber-attack. In a physical attack, you may not know who the attacker is, but he is physically there and you can be sure that the knife-wielding man in front of you is certainly the person who is meaning to do you harm.

The current mode of operation for most network attackers is that they never attack from their own hosts. IP addresses can be spoofed in network packets, thus masking the true source of the packet. Denial-of-service attacks also tend to launch attacks from a distributed group of previously compromised third party hosts. Using these "zombie" hosts, the attacker gains anonymity and economy of scale. Also, an attacker who does attack from his own hosts can easily configure his system to return false information when queried with ident, finger or netbios, thus deflecting a counter-attack to an innocent party.

In a cyber-attack, you cannot know for sure who the attacker is. In retaliation to the perceived attacking host, you may in fact be attacking and possibly harming an innocent third party. Imagine your future legal problems when your counter-attack knocks an Internet stock-trading site offline for 2 hours.

Counter-attacks can backfire.

You have determined that you will strikeback to any network attacks against you. In the middle of an attack, you point your strikeback weapons at the perceived perpetrator. However, your target is not the original source of the attack. What happens if an intrusion-detection system on the counter-attacked network is tripped and the administrators of that network report you as an attacker? You are now the hacker! Here come troubles by the boatload. Your ISP drops you for unethical behavior. The FBI launches a probe against

you. Criminal charges and damage lawsuits are brought against you.

Here is an example of a counter-attack that was redirected back to the counter-attacker: [4] A security expert configured his system to respond to attempted telnet connections. If you were to attempt a telnet connection, his system posted a nasty message-of-the-day accusing you of hacking his system. He automatically emailed complaints to you. He emailed complaints to the root, postmaster and abuse accounts of your domain. He emailed the admin of your parent domain and the Point Of Contacts for your domain and network address. Someone found out about this and created a web page with lots of links to click on. These links referenced several URLs that resulted in connection attempts to port 23 on the booby-trapped system. They posted the web page to a search engine and waited for people to begin connecting. Soon the security expert's system was being flooded with telnet attempts and it responded by spewing emails all over the place. The results were that he created a denial-of service for himself by sending out a flood of emails. He also earned the wrath of the administrators of all the systems and domains he flooded.

Attack escalation: one giant food fight.

What would happen if everyone had intrusion detection and counter-attack capability? SystemA detects a denial-of-service attack from SystemB. SystemA is programmed to respond with a denial-of-service of its own and begins counter-attacking SystemB. More attacks, more response, spiraling up into a meltdown on both sides.

A counter-attack could embroil you in a "holy war" with a determined group of crackers. Jay Dyson was part of a NASA team charged with intrusion detection. After discovering break-ins by a hacker group calling themselves Hagis, he bashed the group by posting a written attack on his website, where he called the group "just a bunch of lame kids." For the next two years, two members of Hagis, u4ea (Euphoria) and tr0ut, stalked Jay. According to Jay, they hacked two Internet service providers to get him. They cracked his home business and harassed his wife, which he says cost him his marriage. [5]

Counter-response can invite further probes.

Responding to a probe by querying back to the alleged sender is like attempting to unsubscribe to an email spammer. The final result is that the other party now has real evidence that there is something at the other end. The attacker may now become further interested in you.

"Hmmm," the attacker asks. "Why does this box respond to my probe? Why did they go to the trouble to make it respond? This could be an important server. What other server processes might it be running? This looks like a challenge! I must probe this host further."

You do not want to attract attention. You do not want to look attractive. You do not want to invite further investigation of your host.

An example of this problem can be seen in Back Officer Friendly (BOF), a small "burglar alarm" application offered by Network Flight Recorder, Inc (NFR). [6] This application was originally designed to alert a Windows user that another host was attempting a network connection on the network port used by the trojan remote control program Back Orifice. Although BOF is a useful program, one of its features can turn your PC into a possible attack magnet. The BOF program can also be configured listen on other well-known ports such as FTP, Telnet, SMTP, HTTP, POP3 and IMAP2. Not only can it listen and alarm on these ports, but it can be further configured to respond back. Generally the response looks like an error message, but it gives the impression that your PC is hosting a number of attractive, hackable services. NFR defaults to stealth (invisible) mode, and mentions that by providing replies, makes it is easier to determine that the host is running BOF.

The question of liability.

One of the largest pitfalls of launching a crippling counter-attack is the question of liability for equipment and/or business loss in such an attack. The liability waters become even more murky if the damaged party was not the real attacker who originated but simply owned the "zombie" platforms that were used as part of the attack.

"Fighting back is a bad idea. I wouldn't do it," says Al Potter, manager of network security labs at ICSA Labs in Carlisle, Pa. "If it's illegal for them to attack you, then it's also illegal to attack them. And then we have this whole problem of crossing state and national boundaries. I don't even want to go there." [7]

Attacking computers is illegal.

A company crosses the line when it responds to intrusion attempts by unleashing a denial-of-service attack against the intruder, as the Pentagon did. Current computer law does not concern itself with why a computer attack is made. A counter-attack makes use of the same toolbox that offensive attacks do-- hostile applets, denial-of-service tools and software vulnerabilities. The net effect is that both the attacker and the counter-attacker are breaking the law.

Don't do it

The future will surely provide better relief against network attacks. Examples might be: industry-approved response tools; better mechanisms for trace-backs; internet-based Caller ID providing less anonymity [2]; more responsibility on the part of ISP's; better trained and equipped law enforcement agencies. At this time, however, overwhelming issues over the legality and liability of counter-attacking would counsel us not to become

cybervigilantes. The risks aren't worth the rewards.

An effective defense is the number one priority in repelling network attacks. Harden your computing platforms. Use perimeter defense (firewalls) and intrusion detection systems. As new vulnerabilities are discovered, be timely in the installation of security patches. Have an effective user access/password strategy. Promote security awareness in all employees. Make your defense so complete that your attackers will soon move on, looking for an easier target.

Finally, have procedures in place for reporting attacks to law enforcement agencies.

"Although ultimately the FBI is essential if you want to prosecute criminals, your 'due diligence' in documenting everything, preserving all evidence, and management of the crisis is going to be more important than playing Rambo." [8]

References

1 Schwartau, Winn. "Cyber-Civil Disobedience." 1/11/99. URL: http://www.idg.net/go.cgi?id=45544

2 Schwartau, Winn. "Can You Counter-Attack Hackers?" 4/7/00. URL: http://www.cnn.com/2000/TECH/computing/04/07/self-defense.idg

3 Schwartau, Winn. "Cyber-Vigilantes Hunt Down Hackers." 1/12/99. URL: http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/index.html

4 Warfield, Michael H. "The Risk of Counter-Attack Tactics." 3/30/00. URL: http://webokay.com/news/security/0031.html

5 Penenberg, Adam L. "A Private Little Cyberwar." 2/21/00. URL: http://www.forbes.com/forbes/2000/0221/6504068a.html

6 Network Flight Recorder, Inc. BackOfficer Friendly documentation. URL: http://www.nfr.com/products/bof/docs/

7 Radcliff, Deborah. "Can You Hack Back?" 6/1/00. URL: http://www.cnn.com/2000/TECH/computing/0601/hack.back.idg

8 Peck, Greggory. "Should You Fight Back When Computer Criminals Strike?" URL: http://www.happyhacker.org/defend/help1.shtml

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event