Misbehavior in the Face of the Enemy

By
Beau Beeson

Introduction

Article 99 of the Uniform Code of Military Justice defines misbehavior in the face of the enemy as:

> Any person who before or in the presence of the enemy
> 1. Runs away;
> 2. Shamefully abandons, surrenders, or delivers up any command, unit, place, or military property which it is his duty to defend;
> 3. Through disobedience, neglect, or intentional misconduct endangers the safety of any such command, unit, place, or military property;
> 4. Casts away his arms or ammunition;
> 5. Is guilty of cowardly conduct;
> 6. Quits his place of duty to plunder or pillage;
> 7. Causes false alarms in any command, unit, or place under control of the armed forces;
> 8. Willfully fails to do his utmost to encounter, engage, capture, or destroy any enemy troops, combatants, vessels, aircraft, or other thing, which it is his duty to encounter, engage, capture, or destroy; or
> 9. Does not affect all practical relief and assistance to any troops, combatants, vessels, or aircraft of the armed forces belonging to the United States or their allies when engaged in battle;
>
> Shall be punished by death or such punishment, as a court-martial shall direct.[i]

Now I'm sure that your wondering what this has to do with network security or your self since you are not at war. Let me assure you that it does apply to network security, to you, and you most certainly are at war. Every day, someone from a subculture other than our own is waging a battle against us, and our systems. We as network professionals are the propagators of our own doom. We are guilty of misbehavior in front of the enemy by not admitting our own fallibility, by not passing critical information to our own team, and from our sheer arrogance in thinking that we can't be bested by some punk kid.

Misbehavior

Imagine if you will, you are the MIS Director of wonderfulnewstoreonline.com, this years e-commerce superstar that is getting ready to leave the market reeling in the wake of its impending red-hot IPO. Life is good. Suddenly your system administrator bursts into your office, "we have a problem ", he breathlessly gasps. It seems that after applying the latest and greatest service pack to your commercial web server software last week, it caused a little hole in your credit card database security. Life isn't so good any more. When you post the days transactions at midnight, a little hole is created and lasts for the 2 to 3 hours it takes to batch and process the credit card orders. Now this little glitch causes customers who try to make an order during this time receive an error and get thrown into a table that contains all of the credit card numbers and names from the previous days orders. Let us say that amounts to about 1000 customers a day. Nope, life sucks. What to do, what to Do? Unfortunately, most companies will reinstall the previous service pack, notify the commercial software vendor that their updates stink, and if they are very conscientious, they will notify the credit card companies that X number of cards may have been compromised.

After the hole has been fixed, the software vendor will post and update to their update and might say something that sounds like this," this update resolves an issue that may or may not have happened and might or might not have happened to you." The Credit Card company will probably wait until someone disputes any charges on one of the compromised cards and may respond with a line like this one, " since you shop on-line, it is possible that you may have compromised it, we suggest that you request a new one." Then one day, maybe, the whole incident might come out and wonderfulnewstoreonline.com along with the credit card Company will say it's highly unlikely that any cards were compromised, we notified the software vendor and patched the patch, what more could we do? The reason that we didn't publicly announce it at the time was because while there was a hole we fixed it and didn't see the need to upset any of our customers unnecessarily and that would be that. Sound far-fetched? It could be, ask Western Union.[ii]

Great, Fine, Dandy. Leave the rest of us running the same commercial software open and exposed for the X amount of days it took to patch the patch and then don't advertise it. They (our team, our brother administrators) compromise the rest of us in order to save face. The sheer arrogance of it all! Complete and utter misbehavior in the face of the enemy. You can bet that if a hacker had discovered the hole in the beginning, it would be common hacker knowledge in 10 minutes. They would post the vulnerability, exploit, and list of every site that runs that software to every enemy (hacker) site, bulletin board, and news group that they ever thought about visiting.

Communication

Communication, or failure to communicate, rather is the system administrator's main charge in misbehavior before the enemy. There is a subculture that hackers belong to that fosters the exchange of information and trading of knowledge. In this subculture or underground of several layers, there exist some extremely polished Internet sites. They post exploits, tools, and even tests that explain how to increase your hacking skills. Willingly and happily they share their victories and defeats among their community. A prime example of this is www.portwolf.com. This site is run by a very intelligent and creative young man who posts texts, tools, and exploits to be freely used by any and all.[iii] There are also several sites that call for a greater proliferation of unity among the hacker subculture.[iv]

Maybe the time has come for the "professionals" within our industry (subculture) to foster greater unity and cooperation among security managers and network administrators. I recently caught a "hacker" who was trying to gain access to our FTP server. I traced the offending IP address to a company across the country and called to talk to their system administrator. I could tell he was embarrassed by the situation and was quite polite and sincere on the phone. He promised to investigate the matter. Towards the end of the week I called back to see how his investigation went partially to satisfy my own curiosity and to write a definite conclusion to my after action report. I have yet to be able to get him on the phone or have him return any of my phone calls or emails. While he certainly does not owe me any explanation or return phone call, I considered it an insult. I could have been the one to alert him that some one was using his IP as a launching pad for these attacks. Unfortunately, this is not an isolated incident. Several of our comrades have displayed this same unprofessional behavior. I know that it was probably embarrassing to receive the phone call saying that I was getting hacked from his IP range, but a little professional courtesy could have gone a long way in drawing the whole incident to a close.

Summary

There are other things besides communication that we as professionals can do to aid ourselves and our 'team". We all need to utilized Bug Traq. Stay up to date on the patches that you need to apply to your own software. This not only helps you out; it also prevents the hacker in using you as a launching pad to disguise attacks against other systems. We need to aid groups like SANS GIAC and send them the results of our scans and intrusion detection analysis. After all, they are asking for our help.[v] They use this information to help keep all of us up-to-date on the latest and greatest security issues. We have to pass on the information of our defeats and victories. Even when we have egg on our face compliments of some 17 year-old in his/her parents basement who just brought our mega-dollar security system to its knees with a simple 486 box.

Remember; misbehavior in the face of the enemy. True, it is not life or death and they aren't really our enemy, but the concept is the same. In neglecting to raise the alarm and warn the others, we are guilty of this cowardly act. Open communication is their greatest advantage and our greatest weakness.

References

[i] Uniform Code of Military Justice (UCMJ) Article 99
http://jaglink.jag.af.mil/ucmj.htm

[ii] Fox News.com Hackers invade Westernunion.com
http://www.foxnews.com/vtech/090900/westernunion.sml

[iii] Cavern of the Wolf The Truth
http://www.portwolf.com/texts/truth.txt

[iv] SoldierX Revelation #1
http://soldierx.com/revelation1.html

[v] SANS Institute (GIAC) Welcome
http://sans.org/giac.htm