Cyber Space Security:

Dispelling the myth of Computer Network Defense by true Red Teaming the Marine Corps and Navy

Captain Scott S Buchanan

Expeditionary Warfare School

Conference Group #9

Major Ryan C. Leaman

5 January 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
05 JAN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Space Security: Dispelling the myth of Computer Network Defense by true Red Teaming the Marine Corps and Navy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Expeditionary Warfare School, , , ,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Public Release**	**9**	

Computer Network "defense" (CND) in the global information grid (GIG) is a myth. Yet, the Armed Forces, namely the United States Navy and Marine Corps, continue to operate as if our systems are secure. CND is a myth because it is retroactive and does not utilize the proactive ethical hacking teams that were designed to think, act, and operate like the multi-faceted adversaries we face in cyberspace. These teams, called Red Teams, continue to work hard to show where our network deficiencies lie, yet their reports are continually sidelined and never reach senior management until after a major incident occurs. So why is this important? Pose this question, can you go to work and perform your job without the use of the internet, whether for email, research, or applications such as sharepoint, regardless of the classification of the system? Cyber Space has infiltrated itself into every facet of our daily lives as well as our military command and control systems. Any briefing given by the President or the Chief of Naval Operations, Admiral Roughhead, will include CyberSpace and its far reaching implications for National Security "…cyberspace is real. And so are the risks that come with it" President Barack Obama, 29 May 2009[1]. The recent nation state-level network attacks in Estonia (2002) and Georgia and the hacking of the White House website (2009) have shown the defense of our networks and the information residing on them cannot be thought of as safe. As such, the Navy and Marine Corps network "defense" teams will continue to fail unless they fully utilize these Red Teams whose sole purpose for existence is to discover and assist in closing network associated vulnerabilities.

WHAT IS A RED TEAM?

---

[1] Remarks by President Barack Obama on Securing the Nation's Cyber Infrastructure. BC News. 29 May 2009.http://news .bbc.co.uk/2/shared/bsp/hi/pdfs/29_05_09_cyber.pdf

Department of Defense Manual 8570.01M is the Information Assurance Workforce Improvement Program. It defines a Red Team as "An independent and focused threat based effort by a multi-disciplinary, opposing force using active and passive capabilities; based on formal; time bounded tasking to expose and exploit information operations vulnerabilities of friendly forces as a means to improve readiness of U.S. units, organizations, and facilities." [2] Red teaming is an essential gauge of Computer Network Defense (CND). It is an independent, threat-based activity simulating an opposing force and is focused on improving readiness.

Red Teaming began in the late 1980's when former Navy Commander Richard Marcinko was mandated to create a team to emulate possible terrorist tactics against Naval (Navy and Marine) facilities worldwide. Marcinko and his team, which he writes about in his fictitious book *Rogue Warrior*, were highly successful and the Navy leadership of the time was not appreciative. This form of red teaming was abandoned for several years but returned in 1996 by order of Admiral Johnson, the Chief of Naval Operations(CNO). This mandate was stated in CNO Memorandum 3300 Ser N64/60335209: "Establish a Red Team to simulate attacks on DON systems. Include simulated attacks, contingency plans that would respond to them, and information warfare disaster recovery as a regular part of fleet and field exercises." [3]

Red Teams deploy to emulate the capabilities and methods of an adversarial force targeting Department of Defense information systems, including developmental systems. They do this by gathering target systems knowledge, approximating the adversary target threat

---

[2]Department of Defense Manual 8570.01M Information Assurance Workforce Improvement Program

[3] CNO MEMORANDUM, 19 Nov 1996 enclosure 2, para 7

environment, gathering appropriate attack tools, and training to affect the attack. Red Teams then deploy and launch the assault, documenting the vulnerabilities and suggest countermeasures. They may work closely with system owners demonstrating how the attacks were run and how owners can protect their systems. They then provide an accurate assessment on which system owners and developers can make coherent risk-management decisions concerning their information systems, networks, and supporting infrastructure. Doing this helps bolster their defenses by coordinating with those who patch entry points and monitor the networks, namely the Navy Cyber Defense Operations Command (NCDOC) and the Marine Corps Network Operations Security Center (MCNOSC). Red Teams are non-attribution organizations for the above reasons; the unit commanders should be comfortable using the above unique skill sets in order to improve network posture without fear of reprisals.

Red Teams employ an arsenal of open source equipment, all if it being readily available for purchase on the internet. In this manner, Red Teams cannot be said to have insider knowledge or an advantage by using exploits that have not been out in the public sector. The other aspect of red teaming is close access operations. Close access operations are used to gain access to installations and ultimately to secure facilities with the purpose of accessing their network resources; i.e. computers, servers, and attending classified briefings.

Each uniformed service has only one Red Team as well as one run by the National Security Agency (NSA). Red Teams are certified by a board at NSA and accredited through Strategic Command to ensure they are able to traffic the threads of cyberspace without doing harm to government systems. This stringent Certification and Accreditation (C&A) process is required every three years and teams which do not fall in compliance are not allowed to access the Global Information Grid (GIG). The C&A evaluation runs from the authorities that establish

the respective service Red Team, such as an annual Naval letter from the Navy or Marine Corps Designated Approval Authority (DAA), to tool development and usage.

THE "SO WHAT" FACTOR

All of the Command and Control Systems (C2) within the Navy and Marine Corps cannot function without using the internet whether it is across the Non-Secure Internet (NIPR) or the Secure Internet (SIPR). As such, Cyber Space is the one realm that is, and will remain, in a continual battle and one could argue a continual "shooting" war. Consequently, to share this vital information freely on all classifications of network safeguarding it from adversaries by adequate Computer Network Defense (CND) must be priority number one, something currently claimed to be done. Current network "defense" is reactive rather than proactive.

The Department of the Navy's Chief Information Officer Computer Network Roadmap[4] published in May 2009 lays out the vision for network defense of the GIG. Yet, in reality, it is far from hitting the mark. The Navy and Marine Corps' reactive approach relies completely on Prometheus, essentially an anomaly detector, to aggregate and analyze potential threats so signatures can be created for them. The problem here is that the anomaly has to have already occurred in order for a signature to be created for it, thus reactive, and not all anomalies can have a signature created for them thus creating gaps in security. The Host Based Security System (HBSS) is meant to be a proactive means of preventing intrusions yet has not been able to adequately and efficiently deploy it due to the lack of knowledge and training within our

---

[4]Department of the Navy Chief Information Officer Computer Network Defense Roadmap Version 1.1 May 2009.

Services as well as the installer, SPAWAR. Once the HBSS system is fully fielded it might have an impact but in its current configuration, it is just another piece of hardware that is collecting data that its operators do not know how to decipher. The main detractor for this system to work is ultimately the command. Our current policy is to allow the commander to "make the call" on the risk mitigation for his/her installation, facility, or vessel. This is the reason why so many security breaches occur. The author has served for three years as the Director of the Navy Red Team and seen first-hand how invaluable a tool they are in directing where we are deficient in protecting our systems. Yet, there are numerous problems facing the teams and the findings of their operations. Namely, their reports are seriously altered to paint a brighter picture before they are briefed to higher echelons, bad news does not travel well. As an example, Red Teams are used by their respective Service to gauge and evaluate the relative "health" of their internal systems. They also participate in annual Combatant Level Commander (COCOM) Tier 1 exercises such as Terminal Fury or Austere Challenge. These exercises are mandated by Congress and the findings are to assist the Joint Chiefs of Staff in whether or not to certify the COCOM as Joint Task Force capable. The goal of these exercises from the Red Team perspective is to portray a Nation-State level threat to our critical information systems. Yet, in the end, the findings of a Red Team are only a recommendation to the Commander, if they reach that level, on what to fix. Invariably, when the Red Teams return the following year, they find the exact same vulnerabilities to exploit. Simply put, current policies are not working. It is worth noting some Commanders are more proactive than others, Pacific Command in particular is far more conducive to findings than any other. Also, larger organizations such as a COCOM are more likely to be proactive in fixing issues than the Commander of a Naval warship.

As the Director of the Navy Red Team, the author has participated in, developed, and led network exploitations at every COCOM, to exclude the newly formed AFRICOM, and at Naval installations world-wide. At one point, the author was chastised by an O-6 level commander to the effect "I take offense to the fact that you feel that a commander would "game" the exercise." Yet, that is exactly what is done daily by falling into a false sense of security with the systems in use. This particular Commander, like numerous others, wanted advance notification of Red Team intrusions. It sure would be nice if the adversary divulged where and when he was entering systems, but that is a pipe dream.

The other main issue is that the Red Teams are not located at the proper level to get the attention deserved and required to be effective. The Marine Corps Red Team is owned by the Marine Corps Network Operations and Security Center (MCNOSC), the Corps' computer network defense provider (CNDSP). Essentially, this set-up is a self-licking ice-cream cone. When the CNDSP owns a Red Team, they can regulate what the Red Team looks at as well as the reports they generate with no accountability or requirement to report outside of the command. So who knows about deficiency's aside from the CNDSP? This author contends Red Teams should be seen as "the Right hand of God" and owned by a non-vested party such as Marine Corps Combat Development Command or even Headquarters Marine Corps C4I (although C4I would have to report on itself). In this manner, the reports reach the highest level where they will elicit a response as well as to be in the position to leverage monetary funds towards a fix, if necessary. The Navy is in a similar situation with at least four levels between the Red Team and the N3 at Naval Network Warfare Command (being renamed Navy Cyber Command). The best place for the Navy Red Team to call home would be as a direct agency working for the NNWC Deputy Commander, or better yet, directly for OPNAV. One option that

should not be adopted is to turn Red Teaming into an Inspector General tool as they will lose all relevancy and be imposed with strict guidelines on how to operate, which is counter-intuitive to how a Red Team should operate. They cannot be placed with unchanging "guidebooks" to follow.

THE OTHER SIDE OF THE COIN DISAVOWED

Proponents of Computer Network Defense myth would say that Red Teams do more harm than good. In fact, Red Teaming takes away valuable resources and time chasing false leads trying to determine whether they are adversarial or our own "internal affairs" version of network checks and balances. To this the answer is simple, de-confliction of exercise and real-world events has been successful in countless exercises and non-cooperative assessments. The bottom line is that looking bad after a Red Team has shown your weaknesses does not allow aspiring officers to have their "stars" aligned so the O-6 to O-6 pipeline kicks in and agreements are made to announce when and where Red Teaming will occur. This defeats the purpose of having a Red Team but does succeed in getting said officers promoted to flag rank and is the true definition of "gaming" an exercise. Thus, we move one step forward and ten years back with this analog thinking.

REPORT THE FINDINGS UP

Until the Navy and Marine Corps Red Team's findings are read by those in the upper echelons of the network warfare hierarchy, unaltered or doctored, or they are moved to more conducive environments; effective countermeasures to adversarial hacking will not be employed. Simply put, it takes one to know one. Those whose tenant is to hack can better tell you how they did it and how to fix it than those who maintain and monitor. Sidelining the findings and

ignoring the facts will keep our Services in the "passive" maintainer role and we allow adversaries to exploit networks at will. Better yet, move operational control of the Service Red Teams to the newly forming Cyber Command, or at least place Cyber Command in the reporting chain for reports. Hopefully, this COCOM will not be another 'dead beat dad" in Cyber Space as Computer Network "Defense" Service Providers have been. Much like the recent discovery of how unmanned aerial vehicles camera feeds are being hacked with a $26 application[5], Red Teams can find these vulnerabilities faster, cheaper, and before they become public knowledge

[5]Gorman, Siobhan; Dreazen Yochi J.; Cole, August. "Insurgents Hack U.S. Drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected." Wall Street Journal, 17 December, 2009.