Rigorous cyberspace defense expert training moves forward

By CW4 Ivery Torbert

As I write this, there are 12 Soldiers sitting in modular building 8C on Fort Gordon learning and practicing skills that will prepare them to be experts in gaining freedom of action in cyberspace.

Like the four that preceded it, the current class includes a mix of CW2's and CW3's. This is the fifth iteration of the course comprising active duty, National Guard, and Army Reserve Warrant Officers. Unlike classes of the past, this one has two senior non commissioned officers hopeful of becoming the first 25D enlisted cyberspace defender.

Military occupational specialty 255S, cybersecurity technician, is arguably the most challenging cyber professional military education and MOS qualification at the U.S. Army Signal Center of Excellence , if not across the Army and Department of Defense. To that end the SIGCoE created an accession process for those seeking to challenge this curriculum. A candidate must be a graduate of a Signal warrant officer basic course, be at least a senior CW2, possess a DOD 8570.1-M information assurance technical Level III certification, have documented cyberspace operations work experience, possess a current top secret-SCI security clearance, and be prepared for the most challenging course of their careers.

Warrant officers selected for training will gain access to an on-line security essentials course for 14 days and be required to take the GIAC security essentials certification on day 15. The GSEC certification is not a prerequisite, but serves as an entrance exam. Statistics indicate that candidates that do well on the GSEC have done well over the 25 weeks that make up the 255S curriculum. Failure of the GSEC certification does not disqualify candidates from seeking the 255S program, but it will place you at a disadvantage compared to candidates that meet all the perquisites and pass the GSEC.

The intent of course managers is to graduate a capable, fully trained officer from the 255S program. We are currently partnered with the SANS Institute and they provide approximately eight weeks of our resident training. The SANS instructors and course material are second-to-none. The classes are filled with the type of hands-on learning and validation that support the future Army Learning Concept. In addition to the resident course, students are given access to SANS on-demand portal with online access to the same material covered during that training week.

Students can also download audio files of the same lecture to mp3 players or DVD. Students have to complete exercises associated with all the SANS training created by 255S resident instructor. Most of the training is hands-on and meant to enforce and/or demonstrate learning from the previous week. The course has three Capstone events: Phase I, Phase II, and Capstone exercises. Students also compete in a minimum of three capture-the-flag type events that demonstrate their ability to gain access to and maintain access on a target system. In one CTF, PYWARS, students get to write and execute their own code.

The 255S course is professional military education. Graduates of the course are awarded Warrant Officer Advanced Course credit. It also serves as MOS qualification course when specific gates are met. It is possible for a Soldier to come to Fort Gordon to challenge the course and leave with WOAC credit only.

Beginning in January 2013, Soldiers will have to test and pass TRADOC exams before being allowed to take an industry certification. If the Soldier fails the TRADOC exam, they risk expulsion from the 255S WOAC and would possibly be slotted in the next available 255A/255N WOAC.

Soldiers that pass TRADOC exams will move on to challenge industry certifications. Soldiers will take the Global Information Assurance Certification, Certified Windows Administrator, GIAC Certified Intrusion Analyst, GIAC Certified Incident Handler, GIAC Certified Systems Auditor, GIAC Certified Forensic Analyst, and GIAC Certified Penetration Tester.

The tools and capabilities given to these Soldiers are difficult to learn, let alone master, so this makes the accession process extremely vital to the future success of the student. Candidates have to be scrutinized to protect the Soldier. This course requires tremendous dedication and focus.

Candidates should not take the course lightly. Under the current Course Management Plan, students have to pass four of six GIAC certifications offered and complete all WOAC requirements to graduate as a true 255S. Of the four GIAC certifications, GCIA and GCIH are mandatory. The skills

(Continued on page 32)

(Continued from page 31)

trained during these two courses and during the Basic Computer Network Operations Planners' Course make up the core foundation of what we believe 255S will do for commanders in the field. Failure of certifications will not get you removed from the course as long as the effort remains consistent.

A core component of the 255S course is the Basic Computer Network Operations Planners' Course. This course prepares planners to integrate computer network operations into the commander's operations down to the tactical edge. Aspects of CND by themselves are functions of all Signal skill-sets.

Protection is a key component of the Signal Warrant Officers' duty. Network technicians should never engineer networks without taking into account firewall placement and management, intrusion prevention systems, content filtering, IDS, encryption, remote access, and basic computer network defense.

Systems technicians cannot place automation systems onto that network without accounting for patches, anti-virus, firewall, backups, host IDS, host IPS, ports and protocols, encryption, remote access, or basic security and network defense. By taking from this force that is immersed with defensive talent, we can focus the training for 255S on more offensive tactics that can be used to better understand the threat and proactively find and fix vulnerabilities before any threats can exploit them.

One option offered to candidates who excel, is to take Global Information Assurance Certified Security Expert exam prior to graduation from the course. The GSE exam has two parts. The first is a multiple choice exam which may be taken at a proctored location just like any other GIAC exam. The current version of the GSE multiple choice exam has the passing score set at 75% and a time limit of 3 hours. Passing this exam qualifies a person to sit for the GSE hands-on lab. The first day of the two day GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. The second consists of a rigorous battery of hands-on exercises.

To date the SIGCoE has paid for nine candidates to take the GSE written exam and all passed. Students do not have enough time to attempt the lab prior to graduation. Upon certification as a GSE, Soldiers only have to recertify as GSE to update all previous GIAC certifications. All students who successfully complete the GSEC and the two core courses are eligible to challenge the GIAC GSE.

The 255S MOS is an accession MOS. It is comprised of former 251As, 254As, and 250Ns. Yes 250N.

A prevailing thought in the force is that we are graduating Warrant Officers who will go out and fill information assurance roles. However, that IS NOT the purpose of the training Soldiers are getting here.

Photo by Cotton Puryear, Virginia National Guard Public Affairs

Cyberspace network defense is a top priority throughout the Army. Here Soldiers from the Virginia National Guard Fairfax-based Data Processing Unit conduct a computer network defense exercise 15 Sept. in Fairfax. The exercise used different cyber-scenarios of varying difficulty in order to evaluate the proficiency levels of the unit's Soldiers in computer network defense and was also designed for senior leaders to evaluate the effectiveness of cyber-warfare training provided during the 2012 fiscal year. The 255S MOS Course is the U.S. Army Signal Center of Excellence training designed to provide the cyberspace defense experts the Army needs.

Having a "cybersecurity" expert in the force DOES NOT eliminate the inherent IA responsibilities of network/system administrators and users. We are pulling Soldiers with IA skills because they understand what is happening in computer network defense.

We want Soldiers who understand and comply with the standards technical implementation guidelines. We need Soldiers that are responsible for firewall management and access list creation on multiple tiers.

If you currently are an ePO administrator; write IDS/IPS signatures; work with RADIUS, VPN, IPSEC; perform scripting; or like playing with Linux in your spare time, then we are looking for you.

Remember this is an advance course with the focus on cyberspace operations and not IA compliance.

The 255S course has had four total graduating classes to date. The first class was considered a train-the-trainer which was followed by three pilot courses to validate our program of instruction. We have trained 38 active duty, 10 Army Reserves, and seven National Guard Signal warrant officers.

Much is made of the certification obtained in the course. Our primary focus is to graduate trained cybersecurity technicians capable of supporting operations throughout the cyberspace domain; however, until we have a cyber workforce, which by designation of MOS has the full respect and trust of Army leaders, one needs to have credentials.

The certifications serve to validate skills. Without knowing exactly at what echelon 255S will be placed in the force, we chose multiple disciplines for specialization. They are trained in areas such as: hacker techniques, incident handling, auditing of networks systems and perimeters, advanced computer forensics, intrusion analysis, network penetration and exploitation, Linux/Unix security, virtualization security, Windows security; cyber law and ethics, and even python scripting.

In January 2013, we are adding malware analysis and mobile forensics to the course. As mentioned earlier, students will take six total GIAC certifications during their stay at Fort Gordon; and they must pass four of six to graduate as a qualified 255S.

Who pays for recertification? With Soldiers obtaining so many certifications it will be a challenge to maintain them all. The hope is the Army will support future certification funding in order to maintain a highly skilled, operational cyber workforce. Until then, Soldiers may have to engage their units to stay current in their credentialing related to the mission of the unit. Ultimately, senior Army leaders will address this issue. Currently, educators at the SIGCoE are primarily charged with meeting individual training requirements that create Soldiers who can prevent, shape, and win in cyberspace.

The nature of threat and the Army's dependence on cyberspace to enhance operations has caused a change in the type of Soldier and training the Signal Regiment provides. With this second-to-none training, we are creating Soldiers who specialize in looking beyond the green, red, and amber status of the network. Graduates of this course will leave with a better appreciation of cyberspace by looking at it in a different fashion; and understanding what it will take in the future to prevent, shape, and win in a dynamic operational environment. As the Signal Regiment expands its role in cyberspace operations in order to meet the needs of the nation, 255S are leading the way. This rigorous course is well worth the effort.

CW4 Ivery Torbert *currently serves as the Computer Network Defense Branch Chief, 442nd Signal Battalion, Fort Gordon, Georgia, which is responsible for the 255S Information Protection Technician course, he is also a graduate of the first 255S class October 2010.*

Acronym QuickScan

CND - Computer network defense
CNO - Computer network operations
CTF - Capture-the-flag
DoD - Department of Defense
GCWN - Certified Windows Administrator
GCIA - Certified Intrusion Analyst
GCIH - Certified Incident Handler
GSNA - Certified Systems Auditor
GCFA - Certified Forensic Analyst
GPEN - Certified Penetration Tester
CMP - Course Management Plan
GIAC - Global Information Assurance Certification
GSEC - Security Essentials Certification
GSE -Global Information Assurance Certified Security Expert
IA -Information assurance
IPS -Intrusion prevention systems
MOS - Military Occupational Specialty
POI - Program of instruction
STIGS - Standards technical implementation guidelines
T3 - Train-the-trainer
TRADOC - U.S. Army Training and Doctrine Command
SIGCoE - U.S. Army Signal Center of Excellence
WOAC - Warrant Officer