PLEASE NOTE: The Government of the United States of America does not endorse ANY commercial product. As such the following information should not be construed as anything more than student reviews for Government and Military Customers.

Government & Military Couse Reviews

www.mile2.com

From: XXXXXXXXXXXXXXXXXXXXXX .mil
Sent: Monday, September 18, 2006 11:42 AM
To: 'XXXXXXXXXXXXX.mil'
Subject: DoD8570.1 - Mile2 CPTS consideration

XXXXX,

The Workforce Certification Matrix located in DoD8570.1 Appendix 4T.1, the DoD IA Approved Baseline Certifications, is lacking a comprehensive list of certifications that revolve around the IA (Information Assurance) discipline. Since this email is targeted towards the Mile2 Certified Penetration Testing Specialist (CPTS) curriculum, I will only mention the lack of penetration testing certifications in the certification matrix. Penetration Testing, also known as "Red Team[ing]", is a crucial part of the IA lifecycle because it employs hacker-like vulnerability assessments of an information system(s) to improve the readiness and defensive capabilities of the operational information assets within the service being tested. Additionally, penetration testing helps provide a targeted understanding of the risks involved with a particular asset, and how to mitigate the risk in question.

Appendix 1.24 (Red Team Function) is described in the 8570.1 as an "Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of (IS)." Based on the description in Appendix 1.24, it is clear that CPTS should be added into the certification matrix as either a Level II or Level III certification. Traditionally, IA personnel are gleaned from experienced System Administrators and/or Network Engineers/Operators that already have the underlying expertise of a system or set of systems in order to perform effective penetration tests in addition to feedback on understanding the vulnerability and the risk mitigation.

I attended the CPTS course in XXXXXX without any expectations assuming that the instructor, XXXXX, would have been someone that had memorized the tool-set and briefed off of the slides. To my surprise, XXXXX was extremely knowledgeable with demonstrated real-world experience in the Penetration Testing arena. The course started off with an introduction to the Open Source Security Testing Methodology, and Rules of Engagement for a professional penetration tester, followed by the theory behind an attack, performing an actual attack, and ending with mitigations for the attack...this structure went on throughout all of the 15-or-so course modules. The modules ranged anywhere from "google hacking" by using advanced operators, to constructing an actual exploit and running the exploit on a vulnerable machine. The CPTS certification should be considered for either Level II or Level III certification based on the idea that CISSP is used as a high-level understanding of security across many different areas, and CPTS is applying the understanding of security by performing the actual task that the CISSP course theorizes about.

V/R

XXXXXXX, SSgt, USAF

XXXXXXXXXXXXXXXXXXX

PLEASE NOTE: The Government of the United States of America does not endorse ANY commercial product. As such the following information should not be construed as anything more than student reviews for Government and Military Customers.

Government & Military Couse Reviews

www.mile2.com

Subject: In regards to the 8570
Date :Mon, 31 Jul 2006 13:44:00 -0500
From:XXXXXXXX.mil
To:XXXXXXXX.mil

Dear XXXXXXXX,

After speaking with Mile2, about the government trying to add more certifications to 8570, I thought this was an outstanding idea since it was sort of limited at this time and not job specific. At this time the 8570 can get my personnel up to the standards needed to basically do the job, but not to the skill level needed for their task. By adding some of the specialized certifications into the 8570 at different level this would make people work harder to become more focused in their task, such as Blue team members or Red team members for the Marine Corps Information Assurance Assessment Team.

In XXXXXX 2006 the CPTS course was taught to the Marine Corps Information Assurance Assessment Team and it was found to be a value-added skill set needed to accomplish our mission. The Marine Corps' current schools for Information Assurance Technician MOS 0689 does not offer any training like the CPTS course, so this would reinforce the need for this certification to be added to the DoDD 8570.1- M as Technical Level II and the CPTE as Technical Level III. We are already seeing the effects of commands using the 8570 as a tool to ensure properly trained personnel are assessing their networks. But we are also seeing contracting agencies and government agencies only training to what is written in the 8570.1-M and nothing else. This is going to hurt the IT sections that have specialized traits such as Information Assurances that do penetration testing and threat analysts work.

The Mile2 CPTS and CPTE surpasses the level of training provided by other certifications similar to it such as Foundstone and CEH (CNDA which they call it now), due to extensive hands on training that you receive. The CPTS / CPTE also teaches the methodology of how to perform an assessment from a penetration tester's standpoint. The CEH is out to training only to teach how to pass a test and how to use dangerous tools. I have taken both courses and have found this (CPTS) to be one of the most professional certification courses I have been to, comparable only to CISSP.

Being a former Marine Corps Data Chief and now a part of the Marine Corps Information Assurance Assessment Team I think that these two certifications would take vital role in training of our IA workforce. As Sun Tzu stated "Know your enemy".

Thank you for your time on this matter and I hope this information helps you in your studies of the 8570.

XXXXXXXX

Technical Lead

Marine Corps Information Assurance Assessment Team (MCIAAT)

PLEASE NOTE: The Government of the United States of America does not endorse ANY commercial product. As such the following information should not be construed as anything more than student reviews for Government and Military Customers.

Government & Military Couse Reviews

www.mile2.com

Subject : recommendation
Date : Wed, 20 Sep 2006 10:26:00 -0500
From : xxxx@faa.gov
To : <roberts06@mile2.com>

Michael,

Having attended both the CPTS and CPTE security training classes presented by Mile2, I will definitely recommend this training for IS security analysts within the FAA (Federal Aviation Administration).

As you may know, our certification and authorization packages performed on various critical infrastructure assets are directed by FISMA guidelines, as well as other Federal directives and orders. FISMA guidelines state that"periodic testing and evaluation of the effectiveness of information security policies, procedures and practices, to be performed with a frequency depending on risk,.. which shall include testing of management, operational, and technical controls of every information system identified in the inventory..."

The only way for an organization to know the effectiveness of the security controls already in place is to think like an attacker, and be knowledgeable about, and skilled with, the cyber attack tools that are readily available to anyone. This is not any different than securing a house or other structure. You must know all of the entry points in order to make sure those are secure. This is where the value of the Mile2 CPTS/E classes lie. Mile2 instructors do not just teach theory of information system attacks. They have real world penetration testing experience that they professionally convey in a hands-on environment. I have attended a similar course offered through SANS which taught volumes about tools and theory, but with 300 other individuals in the class, and no hands-on until the last day of class, the learning experience was disappointing, to say the least. All Mile2 classes I have attended have had no more than 15 students, which allows substantial one-on-one time with the instructor.

All of the modules include hands-on labs that allow the student to gain an understanding of the attack tools, which is paramount in mitigating attacks.

All in all, Mile2 training far surpasses that of SANS for the following reasons:

1) Small class size ensures that all questions from students are discussed and answered, either as a group, or one-on-one with the instructor. This is not possible in a large class setting typical of SANS training.
2) Hands-on experience with attack tools on a daily basis.
3) Lower cost than SANS training, usually by at least $500.00.

Thank you for presenting the penetration testing material in such a way that was very conducive to really absorbing the knowledge needed to better help me protect the critical information infrastructure of our nation.

Best Regards,
XXXXXXX M.S. IA, CISSP
Senior Information Systems Security Analyst
Federal Aviation Administration / MMAC

PLEASE NOTE: The Government of the United States of America does not endorse ANY commercial product. As such the following information should not be construed as anything more than student reviews for Government and Military Customers.

Government & Military Couse Reviews

www.mile2.com

Subject : RE: 8570
Date : Sun, 25 Jun 2006 11:17:00 -0500
Linked to : xxxxxxx
From : "xxxxx, xxxxxx LTC xxxxx" <xxxxx.xxxx@xxxxx.army.mil>
To : xxxxxxxxxxx

xxxxxxxxx,

The current table of certifications which meet DoD IA requirements per 8570.1-M is lacking in training focused on meeting threats to the DoD computer network operations environment.

The CPTS course as taught in xxxxxxxxx 2005 is relevant to DoD Computer Network Defense efforts at Technical Level II and should be considered for inclusion in the matrix. The CPTS provides excellent awareness of the hacker threat to DoD AIS and the Tactics, Techniques and Procedures used by the hacker community.

In light of the recent cancellation of the military Computer Network Defense level III course at Fort Gordon due to interpretation of DoD Dir 8570, I would support adding the CPTS to the matrix to fill this void.

xx
-
xxxxx
LTC, AV, xxxxxxx
CISSP, MCSA, MCSE, IANM
xxxxxx-DCSIM Information Assurance / Network Operations
xxxxxxxx
xxxxxxxx