

## Course Review: Hacking Dojo - Shodan Foundational Class

Review by Dan Kennedy

Over the past few years there has been a fairly steady increase in the amount of penetration testing classes available both in an online format as well as the classroom. Thomas Wilhelm is no stranger to the infosec community as he has written several books within the past few years in contribution such as "Professional Penetration Testing: Creating a Formal Hacking Lab" and "Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques"; as well as the initial offering into the certification realm with Heorot.net. He also has extensive experience within the information security field having worked in a penetration testing role as well as many others. Enter [Hackingdojo.com](http://Hackingdojo.com).

Tom's intent with the Hacking Dojo class platform was to follow a traditional form of learning martial arts, take material covered with his already present Heorot.net certification programs, and mold it into a virtual environment. He does so in a way that information sharing and direct cooperation between students and instructor(s) could take place, rather than Heorot.net's "learn on your own" style of learning.

[del.icio.us](http://del.icio.us)

Discuss in Forums {mos\_smf\_discuss:/root}

### The Course

This brings us to the (1D) Shodan (Foundational) class within the Hacking Dojo platform. It is the second tier of this six-tier program. It is meant as a foundational curriculum for its students and includes the following skills and knowledge to be learned during the enrollment of this class:

- ñ Penetration Testing Methodologies
- ñ Use and Selection of Hacking Tools
- ñ System Exploitation Fundamentals
- ñ Password Attacks (Remote and Local)
- ñ User Enumeration
- ñ Network Sweeping and Tracing
- ñ OS and Version Detection
- ñ Port Scanning Fundamentals

Students without the required skillsets needed to start at this level may begin their journey with the (1R) Mukyu (Novice) class on their way to quick and steady progression into further classes. For more information on the belts or levels of instruction, here's a quick excerpt from [hackingdojo.com](http://hackingdojo.com):

“Access to the material and live instruction on this site is limited to only 100 students, which are of different skill levels, all working their way towards an in-depth understanding of how to conduct computer and network attacks. Once enrolled in the Hacking Dojo, students journey through the following skill levels:

- (1R) Mukyu (Novice)
- (1D) Shodan (Foundational)
- (2D) Nidan (Intermediate)
- (3D) Sandan (Database / Web Hacking)
- (4D) Yondan (Network Hacking)
- (5D) Reverse Engineering

## The Experience

During my enrollment within the Shodan program, there was a great amount of information sharing that came to pass in this Skype-based learning environment. The classroom examples and real-time “show me” sessions from Tom are done within an info-sharing application. This approach gives the students a direct look at just what they are learning while Tom explains the contents of the lesson as he goes along with his demonstrations.

Student interaction is encouraged and Tom keeps a consistent pace with the material to be covered during the lesson. While inquiring with students about how to solve certain aspects of the class material being covered (if it's known by students), Tom is also querying students about any material that they do not understand or need to have reiterated for complete clarity of the concepts.

The course material is great and very closely follows Tom's book, "Professional Penetration Testing: Creating a Formal Hacking Lab." The homework assignments for each week's lesson are concise and easy, as long as the student understands the content within said lesson. These lessons and homework are all managed by a restricted student-only forum as well as a constantly evolving wiki of information for every student enrolled within any tier of the programs. Students are encouraged, nay required, to spin up a live distribution of their own such that they can do testing independently and complete their homework assignments. While this may seem intimidating to some, ideally this is a great concept as it gives the students a real hands-on feel for what they are learning. This also allows for endless trial and error on their own, as they cover material and complete their assignments.

To complete a class ranking (or belt in the Hacking Dojo terminology), a student must pass a two-part examination in which they complete a comprehensive written examination of the material covered during the duration of the course. This written exam is reviewed by Tom, and, if the student has achieved the required learning, they will then proceed onward to the technical part of the examination. Let the fun begin! This technical portion of the exam involves doing a penetration test against a live CD that is given to each student achieving this particular level of testing. The requirements are to "hack the disc" and report back findings in the proper methodology format during a 48-hour time frame. Here lies the greatest challenge: seeking great achievement while under a timetable of stress to ensure success!

Overall I enjoyed this course very much and have completed my achievements to earn my Shodan belt. I'm excited to continue my monthly membership in the dojo in moving onto the next level with the (2D) Nidan (Intermediate) program.

#### Areas for Improvement

This is a new project for Tom as mentioned earlier. It's loosely based on Heorot.net material and curriculum. That being said, he's done a stellar job thus far, and I foresee only greater things coming from this course. As with anything in this life there is room for improvement, so here are just some thoughts.

The content covered during the course of the Shodan program was very good, and Tom does an excellent job of performing the explanation of the curriculum at the same time as doing real-time examples. That being said, I think that a live lab for students with the means to revert the systems that they are testing against would be ideal. Given the cost of admission (a monthly subscription of \$145 per month or a yearly charge of \$1600), I think that students would benefit from an environment specifically tailored to Tom's needs. This would allow everyone to learn against exactly what Tom wants their focus to be in addition to facilitating their own testing with systems of their own.

I believe the only other recommendation that comes to mind at this time would be to encourage more interaction from students during live classes and within the forum, the IRC channel on Freenode and within the wiki by means of contributions to share with others. This would complete the martial arts format by having students of all belts learning and teaching each other based on the lead of their sensei.

