

Interview: Daniel Martin of Dradisframework.org

Review by Todd Kendall

A few years ago, I had completed a Report on Compliance (ROC) as a Qualified Security Assessor (QSA) based on the Payment Card Industry Data Security Standard (PCI-DSS) and was performing a final read out for a customer, when they showed me a framed copy of the cover letter of my report on the wall. The Chief Compliance Officer told me that this single piece of paper had cost the organization over a million dollars and thousands of man hours. Of course, the engagement was nowhere near the cost he quoted, but, after thinking about it a bit, I realized the preparation, project plans, hardware, software, implementation, testing, segmentation, scope definition, and everything else the customer had done to comply with the standard had led to that moment and that one document.

While I had always felt my documentation was up to par, it wasn't until that moment that I truly realized the gravity of my reporting. It is necessary to capture not only the efforts I go through to assess the organization appropriately, but also illustrate a consistency and thoroughness that ensures I have captured the efforts the organization had gone through to prove their overall compliance. But, let's face it, who truly enjoys documentation and how do we ensure consistent, efficient, and repeatable results that can withstand multiple and various types of reviews without the need to completely re-write the report?

I've seen many approaches over the years as an Information Security professional ranging from the copy-and-paste from old reports approach (probably still the most prevalent), word templates, and when I was lucky an in-house developed PHP or AJAX report deliverable generators. The problem with these approaches varied. Lack of sanitation when copying and pasting can lead to embarrassment or even lawsuits, word templates aren't as efficient as we'd like, and code changes to the in-house application are either infrequent or it becomes obsolete over a short period of time because of numerous reporting requirements. Taking these factors into account I began to wonder if there was a solution out there that could address what I had seen over the years and remain flexible enough to keep up with the changing reporting requirements I had, from one engagement to the next? While still relatively young in its maturity, I have hope for the Dradis Framework and wanted to find out more. This interview is the result.

Discuss in Forums {mos_smf_discuss:/root}

The Dradis Framework is an open-source project designed to enable effective information sharing especially during security assessments. Dradis Professional Edition leverages the advanced features of the Dradis Framework and extends it to enable multiple teams to work concurrently. In addition to a web application that provides a centralised repository of information to keep track of what has been done during an assessment, Dradis's features include the ability to create methodologies, create custom plugins, tool-to-company mapping modules, and even the ability to integrate with vulnerability databases. And lest we forget, the ability to automatically generate a consistent professional report at the end of your assessment efforts.

Daniel Martin is member of the Dradis Framework Core Team and founder of Security Roots Ltd. I have had the opportunity to work with Daniel in the past and wanted to take an opportunity to talk to him about his experience with reporting, the impetus for the Dradis Framework, some of the recent development efforts in the newly released 1.6 version of pro, and what we can expect/hope to see in the near future.

Todd Kendall (TK): Daniel, many of our readers don't know much about you, your site dradisframework.org or securityroots.com. Why don't you provide us with a brief background about the sites including your own history?

Daniel Martin (DM): Todd, thanks for having me around. I've been in the security industry for the last nine years and I love it. However, from the very beginning I realised there was something wrong with the way most companies deal with collaboration and reporting. Security specialists thrive when attacking (or defending) systems, everything else (e.g. sharing findings, reporting, project planning) is overhead. I started the open-source Dradis Framework in 2007 to let people working together share and present their findings. Three years and 20,000 downloads later Security Roots (the company) was started to provide professional services to the very same user base. A year later it became obvious that businesses were seriously using Dradis as part of their delivery workflow, and some key features were missing. That's when we decided to release Dradis Professional edition.

TK: You support both an open-source project as well as a professional product. Can you describe the main differences, and why it might make sense to use one versus the other?

DM: On the one hand, the open-source version (dubbed 'community edition') contains the core collaboration functionality plus all the tool plugins (14 right now). It's great to work on one project at a time and for

smaller teams. Once the project is over, you reset the environment and start with a blank slate.

Dradis Pro on the other hand, is for those taking a longer-term approach: you can define clients and create projects associated to those clients. Multiple teams can be working in different projects at the same time. On top of that, Pro ships with a few additional extras like a tool-to-company mapper, very advanced (and easy to customise) Word 2010 reporting, support for things like testing methodologies and the ability to create note templates. Users of Pro fall in two groups: more mature security consultancies (and freelancers) that realise the importance of delivering consistent results every time and internal security teams on larger organisations.

TK: We've mentioned some of the capabilities the Dradis Framework provides to its users, can you comment on how/why creating or utilizing a methodology as part of your process helps the overall reporting effort?

DM: No matter how experienced you are, if you don't play close attention, you might miss something. There are just too many things to take into account when doing a security assessment and so many different technologies exist that oversights can happen, which can be pretty serious.

If you are serious about your testing methodology and ensure you follow it every time, you will produce higher quality results and deliverables and you will be perceived as consistent by your clients. Of course you need to ensure your methodology is easy to maintain and update, otherwise it's not going to be very useful in practical terms.

In addition, having a testing methodology is a great way to bring less experienced members of your team up to speed fast. If all the steps and checks are documented anyone can follow and ask questions when they get stuck.

TK: Can you help our readers better understand what you mean by plugins? In addition, the framework supports a number of commercial and open source tools via these plugins, can you comment on the decision to support or develop a plugin for one tool versus another?

DM: Plugins are small extensions to the framework. For instance, we have plugins that parse the output generated by other tools like Burp or SureCheck and others that import findings from external sources like OSVDB or VulnDB HQ and yet others that let you extract the information out from Dradis into a number of formats like HTML or Word.

Plugins can end in the framework in two different ways, either by a user contribution through our GitHub page (thanks guys!) or via a "sponsored development" by one of our Dradis Pro clients. For instance, if one of our clients needs to use a particular tool that we don't support, they usually approach us to create a plugin for them. We suggest the sponsored development route: we would develop the plugin and include it in the result and give them a discount over our standard consulting rates. People love this, it is a win-win, the company gets what they want, we add a new plugin to our solution (which we will maintain with the rest of the product) and they give back to the community.

TK: What exactly is a tool-to-company mapping module?

DM: Not every organisation uses the same names and labels in their deliverables: some people use Name, other use Title, some use Recommendation others use Mitigation, etc. And the same goes with tools: some give you a list of Findings, others call them Issues, others have Plugin which Names. There is a lot of heterogeneity.

The tool-to-company mapping module is a pretty smart piece of code that we have in Dradis Pro that lets you create a mapping between whatever fields the tool provides to the names and labels your organisation uses. You spend a few minutes creating those mappings and from that point on all the information you import from different tools is using the nomenclature you need for your report.

TK: You also support VulnDB HQ. Can you tell us a little bit about this and how it may or may not be connected to Dradis?

DM: VulnDB HQ is a service that lets you manage the information that you already know but that you were not managing as efficiently as you should: testing methodologies and issue templates.

We haven't discussed this yet, but one of the things that involve the greatest amount of wasted time during reporting is repetition. We spend our lives writing the same boilerplate stuff again and again. What the issue is, what effective mitigation strategies are available, what references our clients should consult to get further information, etc. The truth is that a very small amount of the information for the issue in the report is specific to the instance at hand (i.e. the "evidence"). With VulnDB HQ you can manage all the boilerplate: issue descriptions, standard recommendations, CVSSv2 numbers, everything. Then when you need to create a report, you just copy your issue template from VulnDB, add the case-specific evidence and you are done. Our users have told us they now create their reports in less than half of the time they used to. And remember that nobody likes report-writing, so that's a big win.

We've talked about the importance of having a comprehensive testing methodology. In a fast-moving field such as ours, a testing methodology is of very little use if it is a static document. You need to be able to update it and improve it, if not after every test, certainly after every few months. VulnDB also lets you manage testing methodologies in a convenient way.

Of course VulnDB HQ and Dradis work really well together, however they are independent and one can be used without the other. In VulnDB HQ we have a RESTful API that lets you integrate your information with virtually any tool.

TK: Obviously one of the greatest features of the Dradis Framework is the ability to efficiently generate consistent results. You have recently released a new version of the Dradis Pro, 1.6. What are the new, improved reporting capabilities we can expect in this version and what can we hope for in the future?

DM: You are spot on there, reporting is a huge pain point for our clients. That's why we work so hard at it. In the latest release we've added some cool features, for example, the styles and screenshots that you have in your

Dradis notes are now maintained when generating your Word report. In addition, it is now possible to group and filter your issues in the report: you can have a section that lists only the High-impact findings, or the notes associated with a given phase of the engagement (e.g. application testing vs. infrastructure testing).

In terms of what the future holds, I can assure you we are not running out of ideas any time soon. There are two main forces driving the development of Dradis these days: first, we are going to continue improving the reporting capabilities, making it ever easier to create more complex report structures; second, we want to tap on the potential of having information about multiple projects. We want to enable our clients to provide better service to their clients with things like an historic view of their security profile across projects and over time and better tools to understand and address their security issues.

There is plenty to be excited about what the future will hold, and most definitely are!

TK: Thanks Daniel. To get a better appreciation for what Dradis might do for you, here is a real world example that I've dealt with, working with securityroots.com.

Dradis Pro Report Plugin Customization

The goal of this development effort was to develop a plugin that enabled team members the ability to add notes to the final report from within the framework, which would then be added to a table in our report. In a real world scenario team members often complete automated vulnerability scanning activities during an assessment and then begin manual verification efforts. The bulk of our "high-risk findings come from this manual effort and entails creation of a new key vulnerability within our report.

This first screen shot is an import of an automated scan into Dradis, which then gets mapped to the customized plugin we created.

Figure 1 - Initial Scan Findings

The second screenshot is an example of a manual effort that was mapped to the plugin.

Figure 2 - Adding a note to the findings using the template

The third step is exporting to a Word XML file.

Figure 3 - Exporting to a word template

The final step is an updated table, in the report, in our standard template. The nice thing about this effort was that as we completed our analysis, we could weed out false-positives by simply ensuring they weren't assigned to the report we wanted to generate, yet maintain accurate information based off of the automate vulnerability scan that was performed. The generation of the report by the time the analysis was complete, was a simple point and click effort.

Figure 4 - Final report

Hopefully this interview, small tutorial and the tools itself are helpful to all of you EH-Netters. I now it has been extremely useful in my own professional work.

Todd Kendall is an experienced security consultant in the commercial security world as well as within the highly secure networks for the Department of Defense (DOD). He provides expert consulting and consulting management for tasks that include security policy development, network security design and review, vulnerability assessments, penetration testing, intrusion detection, analysis and incident response. Todd is responsible for performing vulnerability assessments on operational networks within the finance, healthcare, and utility industries as well as wireless infrastructures. Todd has been heavily involved in incident response and management as a Security Engineering Lead within Symantec Managed Security Services and as a Consulting and Forensic lead within Symantec Business Advisory Services. Todd is currently working as an advisory consultant within the airline industry supporting third-party risk assessments including risk assessments for migration of Cloud activities.