

Review: Advanced Penetration Testing (APT)

This year I had the opportunity to take a few stellar instructor-led training courses, one of which was Joe McCray's "Advanced Penetration Testing: Pentesting High Security Environments" course from his training entity LearnSecurityOnline.

Since I'm already doing pen testing full time I feel like it's a tremendous opportunity to see what techniques other testers use. I'm definitely not arrogant enough to think I know everything, but I do know Joe is tremendously skilled and has many more years "in the game" than I have. What an opportunity for me to learn from the best.

Joe's class is presented as higher level pen test course. There are no real introductions into pen testing theory, tools, or syntax. APT is largely comprised of labs and demos. The course also has a very unique structure. It comes from the mindset of attacking from the outside (web) and pivoting through the DMZ to the LAN. There is a lot of emphasis on stealth, persistence, and evasion. Even if your testing isn't scoped this way it is a powerful ability to be able to show your clients how one seemingly innocuous web flaw can lead to network disaster. Regardless, I found that this class was beneficial even to those that separated web and network scopes.

This review covers the course offered in conjunction with Black Hat Training at the venerable annual event in 2010 and will take a detailed look at the 2-day agenda, coverage of the 5-Day version of the course, thoughts on presentation and technical content, conclusions made as well as modest recommendations.

[del.icio.us](#)

[Discuss in Forums {mos_smf_discuss:Haddix}](#)

[Win a Free Seat in APT with Joe McCray](#)

[See EH-Net's Free Monthly Giveaway for September 2010 for Details](#)

[Day 1: Identifying Defenses, Stealth, and Attacking from the Web](#)

The first part of the day consisted of reviewing (quickly) the more intricate details of information gathering (passive recon, OSINT, etc.). Truth be told, this was the only part of the class that didn't have live examples, but it was only due to the Black Hat network not cooperating. Most of the class was hands-on, using pre-built VMs to attack servers Joe's interns managed up front. The OSINT material was current and up-to-date with what I've only seen a few pen testers cover.

Moving on, we went over techniques to identify virtual hosting, load balancing, WAFs, IPSs, etc. Joe carefully explained the types of devices and filtering he has come up against in real pen tests. The great benefit here is Joe's research into these devices' signatures and potential bypasses. Joe's next step involved setting up all of your standard web pen test tools to use tor, proxy lists, and other trickery to mask your attacks. This was especially interesting as Joe demonstrated some really sly ways to keep from being blacklisted.

This segued right into his module called "SQL Injection to Command Shell." Joe takes you through the ways to identify SQL injection (as well as LFI and RFI), and then through exploiting an ASP app first manually and then by using automated tools. Joe also provides some of his favorite tools/scripts that were custom patched for identifying and attacking these avenues. Besides some issues with VM installations, day one was refreshing, up-to-date, and an advanced glimpse of practical web hacking and stealth for enterprise pen testers.

**** Side note****

Joe's APT class is normally a five-day course. This incarnation of it only saw 1/5th of the total modules he trains at a full-length class. Fortunately for the students of the Black Hat training, Joe went over certain modules live and then provided the lab guides with a few additional modules that were not possible to demo at Black Hat. Even with the additional modules in the book, there was a good 75% more content to cover. In an attempt to fairly review all the content, Joe sat down with me personally to go over each additional section. I will try to cover this additional information at the end of the two-day description.

Day 2: Metasploit, Pivoting, Persistence, and Evasion

With the VM issues mostly resolved, the second day moved at a faster pace. To me, it provided a lot of insight on attacking more secure environments. Day 2 was filled with tons of Metasploit including tips and tricks on using incognito, getpriv, pass the hash, and more. What I liked about this day is that Joe pretty much tailored it around bypassing anti-virus solutions and evading IDS/IPS. It also was useful that for every function in Metasploit, there seemed to be a stand-alone script that he provided for performing similar functions. This way, if you didn't have a Meterpreter shell with the built in 'hotness,' you at least had some functionally equivalent code to use with your bind/reverse shells.

Since we were running low on time, Joe slightly touched on post exploitation and persistence. He then moved straight into attacking and bypassing AV + GPOs labs which were great. Joe goes over these sections both from an 'just popped a box' standpoint and an 'just sat down at this kiosk/locked down machine' avenue. This section was particularly impressive due to one of Joe's students actually modifying some tricks of Joe's and finding a previously undiscovered 'old-school' privilege escalation attack (alternate data stream) in the High Security

GPO VM we were attacking. The last part of the day covered some techniques to bypass port security and NAC solutions, which were very informative. All in all, Day 2 was my favorite.

Extras and 5-Day Content

With some students having had VM troubles Joe really wanted them to head home satisfied with the course. Towards the end of Day 1, Joe took a class survey to assess what the majority of the class was interested in (IE, attack vectors, methodologies, tools, etc.). Later on Day 2 he actually provided us his personal Web Application attack methodology, Nessus policy files for specific Metasploit exploits, his AV Disable tricks module, his exploits by OS cheat sheet, his privilege escalation cheat sheet, and more. These are all tremendously useful resources.

As mentioned, I had the opportunity to check out the full 5-day content. Obviously with the instructors and labs not present, you'd expect to be underwhelmed, but that was not the case. Represented within the 5-day material there was a module for almost every advanced attack type or tool I have seen blogged or presented in the last year. This includes advanced attacks for XSS using BeEF and XSS shell, bypassing flash logins, attacks and useful payloads in SET, using metaphish for more fun and profit, web payloads, MiTM with ettercap + SSLstrip, Custom MSF trojans, karmetasploit, tons of post exploitation tricks, and just really too much to be listed here. All in all 36 modules, a handful of custom patched tools, and several cheat sheets will clearly make for a jam-packed 5-day course.

The Skinny

Presentation and Delivery: 9/10

Technical Content: 9/10

Value: 9/10

Presentation and Delivery Notes

Joe is a unique instructor. He teaches with a certain enthusiasm that is infectious. As mentioned he also tailors the class dynamically to what his students want to learn. In addition he had some great teaching aides, Jason Vaan and James Fitts, who kept the network running and assisted with all the labs. All the teaching staff was available for questions regarding anything related to pen testing, which included staying after the allotted Black Hat hours and lunches to have a drink and swap tricks of the trade. On several occasions students would come up with good ideas that went along with the courseware to which Joe would immediately take notes and offer to help code up the attacks or ideas they had. When hard times arose with the VMs, Joe's team worked into the late hours of the morning to re-burn the images and make the class flow smoothly the next day. All of this, in addition to the fact that the class is lab driven, would have rated a 10/10, but the VM situation, which I have been assured after this course will be remedied, deducted a point.

Technical Content Notes

A lot of people say there isn't any magic left in pen testing; that it's all been documented. But this class gave me more than enough hacks to take home and drop some shells. It focused on exactly what it advertised and with great quality. Every module covered was both step-by-step and also contained the technical details of the attacks. The tools and techniques were very current, and, since Joe knows almost everyone in the pen test social circle, you could see that he worked hard on incorporating the newer ideas and concepts into the methodologies. As a course reviewer I've been lucky to see some really good classes (as well as some horrible ones), and APT is the closest I've come to yet to wanting to award a 10/10 score on content. Alas, I'm one of those guys who is always under the impression that there is more fu out there and therefore will be hard pressed to actually give up a 10/10.

Areas for Improvement

Two days was not enough for the class. Although this was hardly the APT team's fault, after seeing the whole of the content, you could tell that there was so much more that the course offers in its five-day version. The VM situation was a real difficulty the first day, and frustrated some students. After talking with Joe post course, he has assured me that they have rebuilt the VM images, and started to move to USB as a delivery media as opposed to CD/DVDs. On the true content side of things, I have no criticisms. The course was technically solid. I did hear a student complain that the course did not have an intro to developing exploits, but that's not what the course is really about. It focused on practical pen testing against current, high security environments. If you want this type of course, hold your horses a bit until Joe and his team release some details on their actual reverse engineering and exploit dev class. Another point, not necessarily a criticism, is that I'd love to see this course offered online. Although Joe and the APT crew fly the hacker con circuit pretty extensively offering this course to the masses, an online version would really challenge some of the lackluster training programs out there.

I'll keep the closing quote simple:

“If you have any remote chance to take this class... make it happen. You won't regret it.”

**** Another Side Note ****

After finishing this review I have been informed that Joe is giving an APT class on Dec 13 – 17, 2010 in Maryland. It will be the full 5-day course and even have updates to the content listed here. Don't miss it.

at <http://www.securityaegis.com>. Jason has been working in information technology for many years doing everything from admin work, component bench technician, and identity theft researcher. He has been a lead on projects in the Fortune 100 space including companies such as Comcast and has experience with numerous infrastructure and web application security assessment projects. Jason actively participates in research and discussions regarding (E)hacking, Social Engineering, the security-con community, et cetera. Jason's current projects include numerous reviews of current pen-testing and incident handling teaching curriculum as well as being a creator/contributor/columnist to SecurityAegis.com, PentesterScripting.com, Ethicalhacker.net, and Hakin9 magazine. He also serves on the advisory board for all GIAC Penetration Testing curriculum as well is GSEC, GPEN, and eCPPT certified.