Core Impact 6.2: Anatomy of an ethical penetration test

By Russ McRee

Prerequisites

CORE IMPACT is lean and can run on minimal systems with limited resources and requires either Windows 2000 Professional SP3 or greater or Windows XP Home or Professional SP1 or greater. It's largely written in Python, particularly the exploit code, but includes all the necessary libraries in the installation package.

Similar tools

Metasploit - http://www.metasploit.org

Canvas – http://www.immunitysec.com/

BiDiBlah – http://www.sensepost.com

Introduction

If you've been reading *toolsmith* from its inception, you know that we have typically focused on open source or inexpensive tools for your arsenal. After some reflection, it occurred to me that many organizations often put the onus on quality and ease of use in selecting security tools and thus, cost is sometimes a secondary consideration. To honor those organizations and shed light on a remarkable tool, allow me to describe CORE IMPACT in detail. IMPACT is certainly not inexpensive, but after testing it at length, with no influence from the vendor other than an initial, well-delivered demonstration, I can tell you with certainty that IMPACT will leave you extremely satisfied. Other respected security publications have reviewed earlier releases of this product, and all with very positive results. However, where their focus was largely a simple product review, we will walk through a complete penetration test scenario using version 6.2.

IMPACT is the first comprehensive penetration testing solution for assessing specific information security threats to your enterprise. IMPACT features the Rapid Penetration Test (RPT), an industry-first step-by-step automation of the penetration testing process. Now, any system, security, or network administrators can easily test the security of their networks, identify what resources are exposed, and determine if current security investments are actually detecting and preventing attacks.[1]

The developers at Core Security write exploits and update IMPACT as quickly as a worthy vulnerability is publicized. As an example, you are likely aware that a Microsoft patch was made available as of April 3rd for the Windows ANI vulnerability (MS07-017) that was rampant at the time of writing; but there was also an IMPACT exploit updated to licensed installations on the very same day.

In addition to Windows platforms, IMPACT also includes exploits for Linux, AIX, Solaris, BSD, and Mac OS X.

Anatomy of an ethical penetration test

Installation and setup

In my lab, I quickly installed IMPACT and set to work on a *victim*, specifically a vulnerable Windows XP virtual ma-

1 CORE IMPACT help files

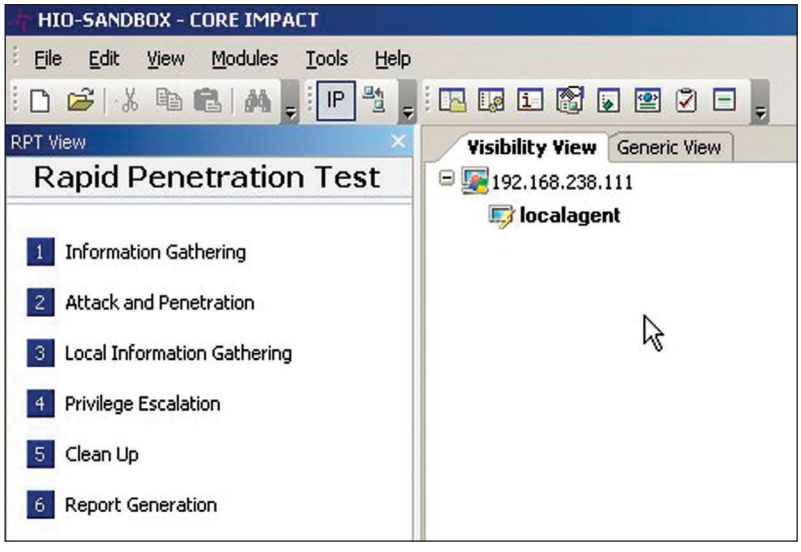

Figure 1 – RPT View

chine. IMPACT allows the convenience of defining individual work spaces for your penetration tests, useful if you are testing for multiple customers, or disparate networks within your environment. It will allow you to establish carefully guarded authentication per workspace, including generated key pairs, complete with mouse movement entropy generation. Your initial view will show you the RPT options. See Figure 1.

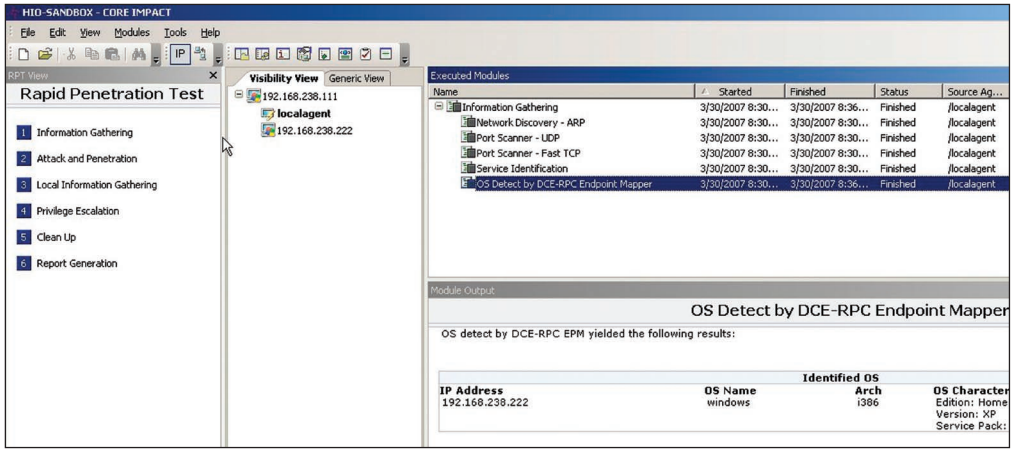

Figure 3 – Executed Modules

Information gathering

The initial phase, *information gathering*, includes port scanning, OS detection, network discovery, and service identification. With this fingerprinting complete, IMPACT then has all the information it needs to conduct a concise, accurate assessment, without executing unnecessary or irrelevant exploits (Sun Solaris `printd` against Windows XP). IMPACT also offers extensive import options from vulnerability scanners and patch management platforms including GFI LANguard, Qualys, nmap, Nessus, PatchLink STAT, and eEye Retina. Imagine the convenience, after running a weekly scan, of immediate false positive verification or severity level confirmation. Information gathering is as simple as defining your target, or target ranges, and then choosing from the *Fast* or *Custom* options. Fast offers the efficiency of identifying vulnerable hosts, noting them as available for attack, then quickly moving on rather take up additional time for more study. Custom, on the other hand, allows for additional advanced options. See Figure 2.

The results of your preliminary scan will show you a list of hosts available for testing along with the modules executed, including port scan findings, running services, and OS detection. See Figure 3.

Attack and penetration

Target selection for attack utilizes the *Attack and Penetration* wizard and only requires range or single target entries. You'll be offered the chance to deselect exploits that might leave a service unavailable. This step is vital in critical or production environments so as to avoid causing unintended harm or outage. The same window will ask you to decide on *every possible attack* or *stop at first deployed agent*. As I selected my settings for attack, for demonstrations sake, I unchecked the latter in order to illustrate how successfully (and successively for that matter) this tool will exploit an unpatched system. After the initial scan, the attack wizard selected sixteen exploits, four of which were successful. See Figure 4, next page.

Upon successful exploitation, IMPACT loads an agent useful for further exploration and penetration.

The agent

Agents run in memory, and leave no resident footprint on the system. This noninvasive methodology is ideal for corporate/enterprise environments where you seek to research and inform, rather than invade or permanently compromise.

Level0v2 agents are the default agent for all exploits. They have equivalent functionality to the level0 agent, but they can multi-task (run multiple modules), and they have a Secure Communication Channel. When part of an agent chain, they communicate more efficiently than level0 agents. Once deployed, they can provide all system calls and arbi-

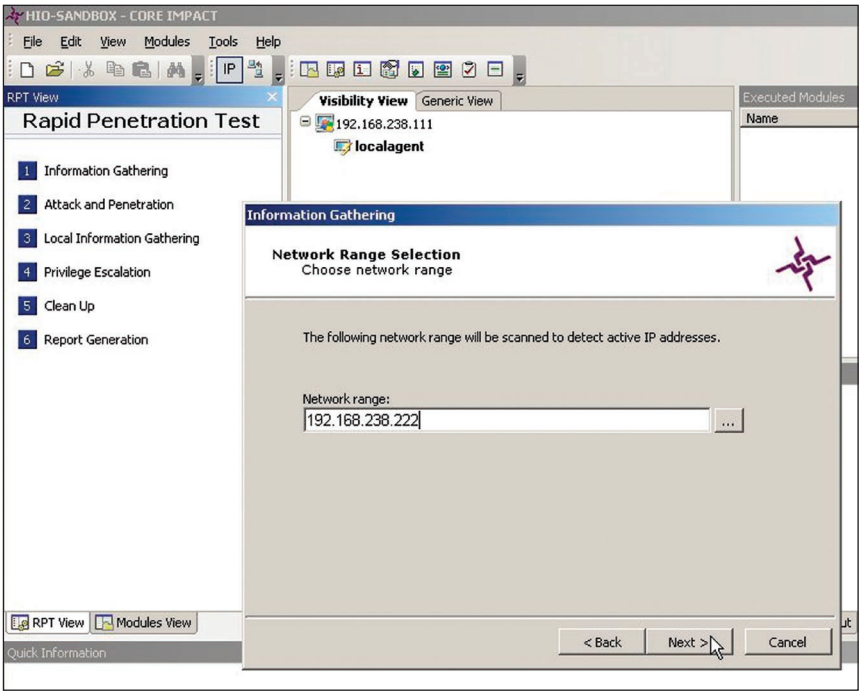

Figure 2 – Information Gathering

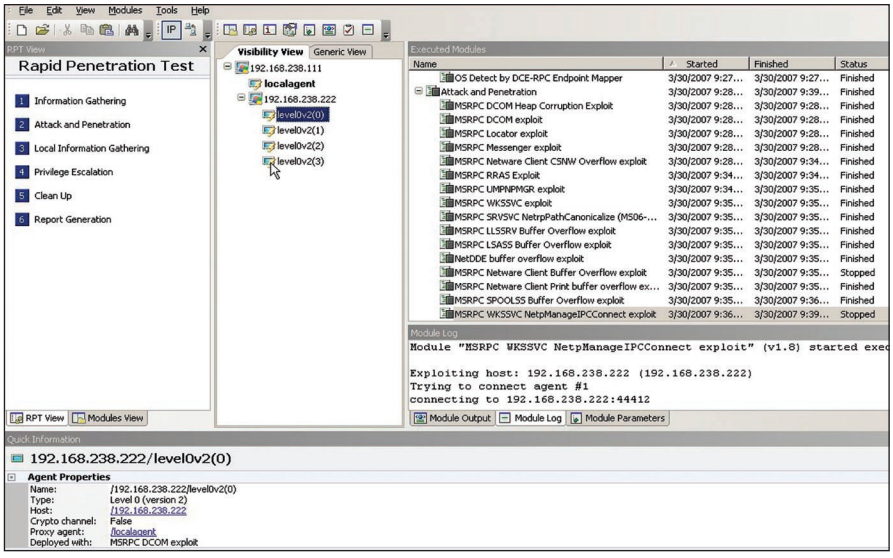

Figure 4 – Successful Exploits

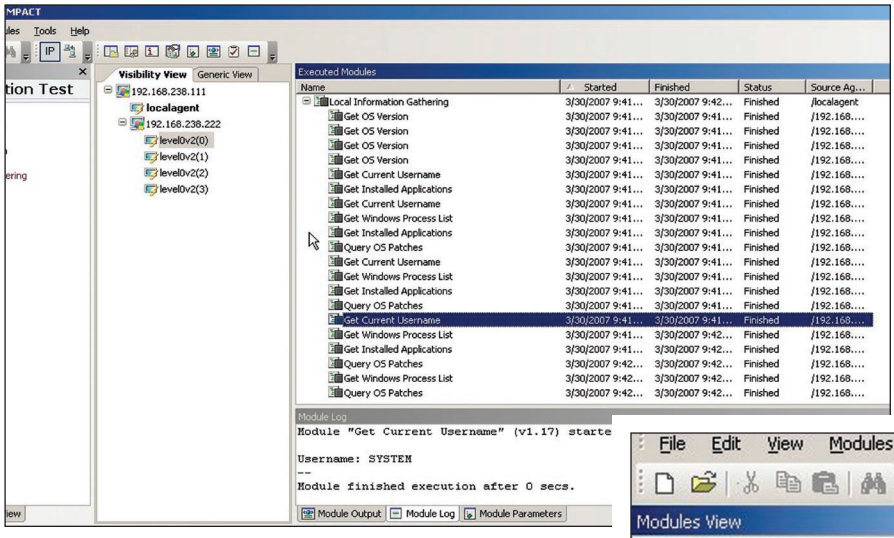

Figure 5 – Agents Deployed

trary code execution on platforms with built-in stack protection (such as Solaris).

Level1 agents can use plug-ins to add functionality to a deployed agent. Level1 plug-ins include PCAP, providing packet-capture capabilities for the agent. A level1 agent with the PCAP plug-in can execute modules that require packet capture including NMAP, a password sniffer or passive network discovery. There's also the TCP Proxy option allowing you to create TCP tunnels from IMPACT's Console to the level1 agent. Using this plug-in, you can redirect a local TCP port on the system running IMPACT to a remote TCP port on the other side of the level1 agent. See Figure 5.

Note in the *Agents Deployed* graphic that all information gathered was done so with *system* privilege thanks to the success of the exploit used to establish an agent.

With agents on board, you have options to utilize additional modules as seen in *Misc Modules*, including Dll Injection, Disable Firewall Capabilities, and Install Windows Driver. See Figure 6.

Privilege escalation

If need be, IMPACT offers you the opportunity to escalate privilege before gathering local information. In this attack scenario, we quickly achieved system level access, so no escalation was necessary. However, on a different system, you might seek to gain better access.

The *Privilege Escalation RPT* will conduct local privilege escalation attacks on connected agents not running as *root* or *admin*. This macro selects and runs exploits from the Exploits/Local module directory and some modules from the Exploits/Tools directory.[2] Thus, after the Attack and Penetration wizard completed, I ran the Local Information Gathering wizard, leading to further opportunities to explore.

The modules view

If you wish to conduct your test more interactively, switch from RPT view to Module, and work with those options

2 CORE IMPACT help files

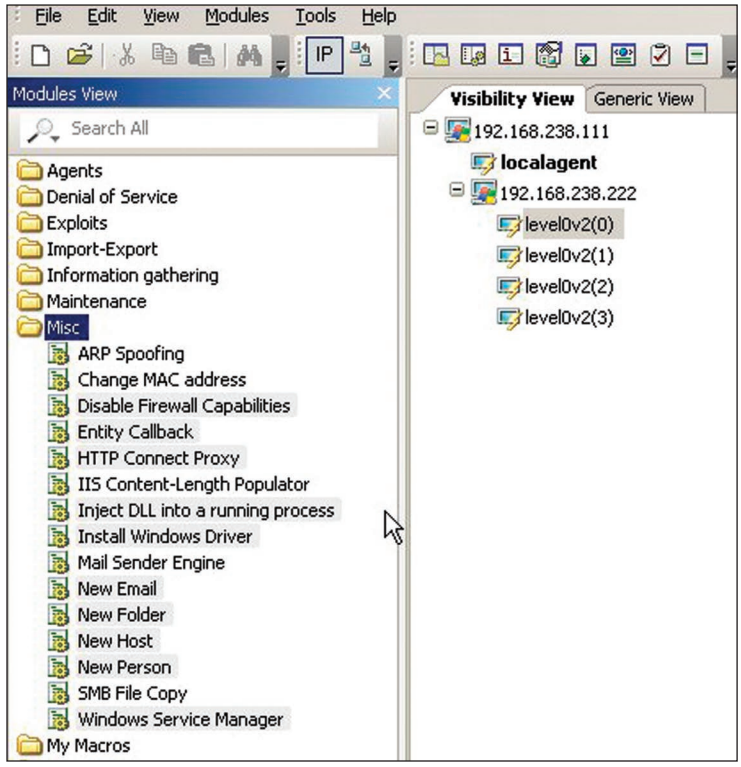

Figure 6 – Miscellaneous Modules

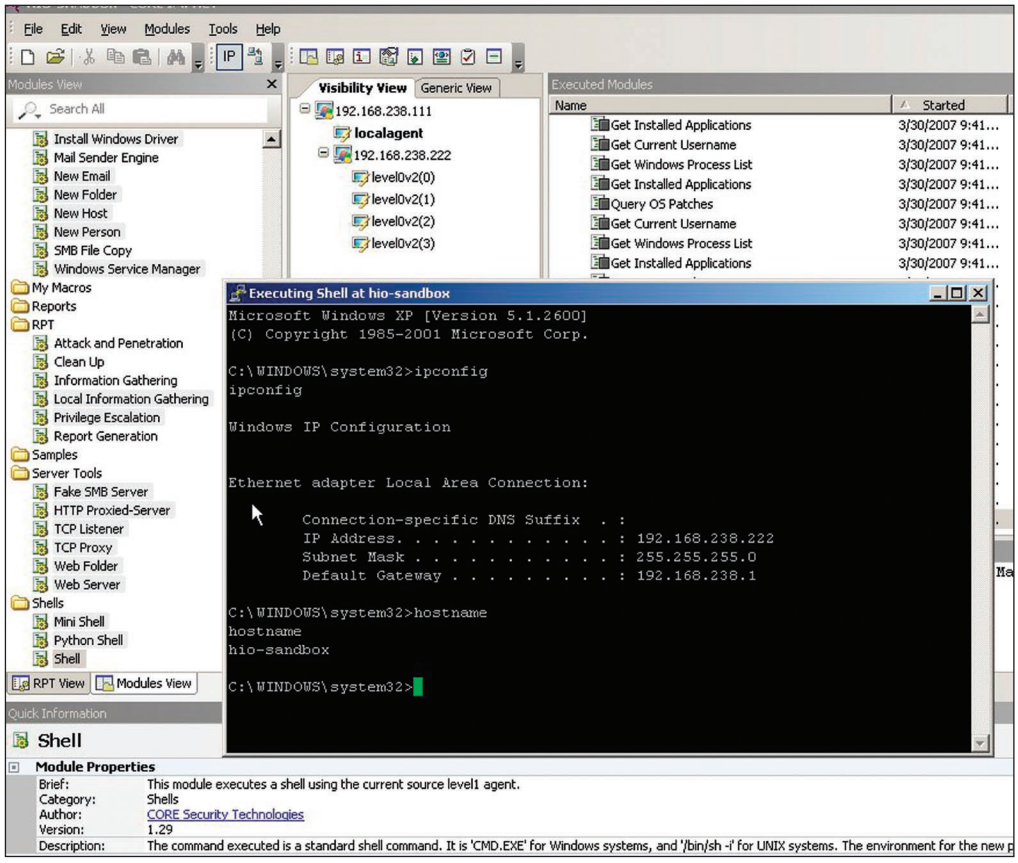

Figure 7 – Shell access

that are highlighted for you. In this case I literally dragged *Shell* from the Shells directory and dropped it on one of the four deployed agents. See Figure 7 next page.

Perhaps you wish to prove that current admin passwords are weak. Under Information Gathering/Local, you can drag Password Dump from SAM, to the agent of choice, then refer to the Module Log for the resulting hashes. Copy the hashes to a text file and import them into your cracker of choice (Cain & Abel from Oxid works nicely). Note: Don't bother with those you see in *Grab the SAM*, they're empty). See Figure 8 below.

Agent chaining

Agent chaining is an excellent feature that allows you to connect to a newly-installed agent behind a firewall using an existing connected agent's communication channel. As you deploy successive agents, chaining allows the Console to maintain a single connection versus many. This feature would obviously be useful if you're exploiting hosts in a DMZ and seek to drill further into the internal network. See Figure 9 next page.

Clean up and report generation

Enough fun, let's clean up and generate a report. Yes, there are RPT macros for that also. Remember, the agents are running in memory, so backing out is easy.

The *Clean Up* wizard will allow you to remove all deployed agents after confirming that you wish to uninstall every connected agent. See Figure 10.

Reports Generation includes Executive, Activity, Host, and Vulnerability reports, depending on your intended audience, and includes the all important charts and visual enhancements. Remember, IMACT logs absolutely every step it takes, so detailed findings reports are just that. Check out sample reports here: http://www.coresecurity.com/?module=ContentMod&action=item&id=1474

Benefits and drawbacks

CORE IMPACT will aid you in meeting any compliance framework you might face, including PCI, SOX, HIPAA, GLBA, as well as general vulnerability management.

You will find no challenges installing and deploying IMPACT, and after a bit of use and some vendor training, you will find it an extremely easy tool to use. It takes mere minutes to install and I was comfortable with the interface in minutes.

This is a tool that, while expensive by some standards, will pay for itself almost immediately in larger, compliance-bound organizations.

I truly tried to find a drawback to this tool, and unable to come by one on my own, asked one of their engineers how

Figure 8 – Grab the SAM

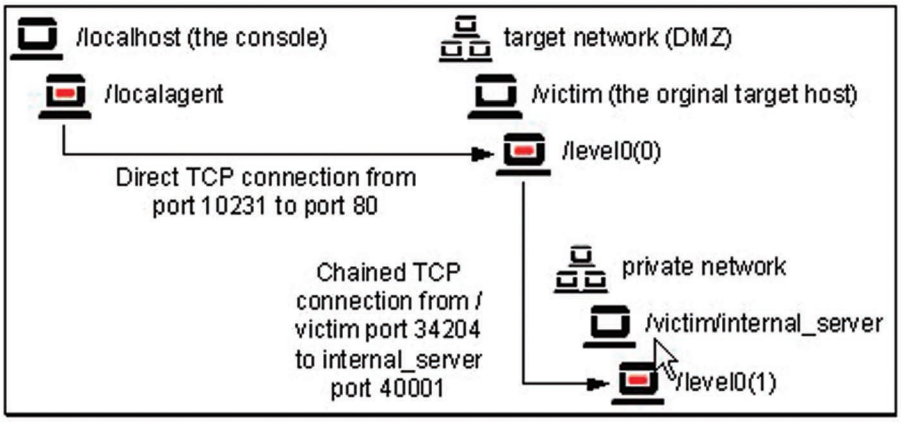

Figure 9 – Agent Chaining

he thought they might further improve their product. He responded by indicating Core's desire to improve automation of client-side exploits via RPT wizards, a goal which Core Security developers are actively pursuing.

Conclusion

CORE IMPACT was a blast to test and a product I am certain would benefit organizations that choose to engage it. My findings were consistent with other reviews of IMPACT, and I heartily recommend contacting Core Security for a live demo. IMPACT has all the convenience of fast food with the quality better suited to a five-star restaurant. Bon appetite, pen testers!

Cheers…until next month.

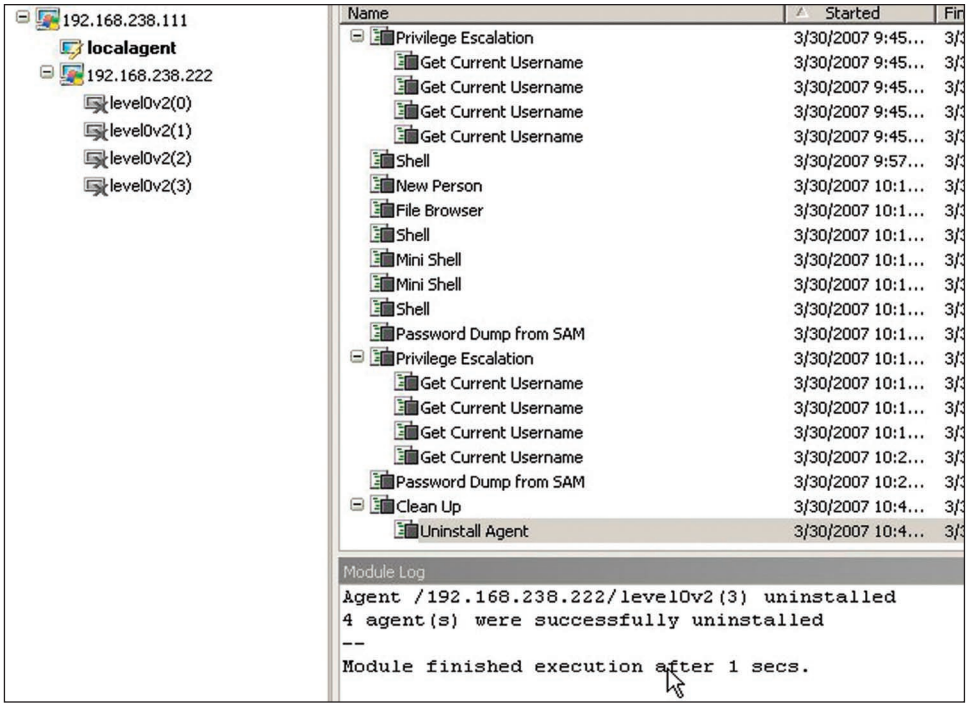

Figure 10 – Clean Up

About the Author

Russ McRee, GCIH, CISSP, is a security analyst working for Expedia. He is a member of numerous security organizations and maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.