# Pen Testing with Pwn Plug

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Join the Discussion
Connect

## Prerequisites

Sheevaplug[1]

4GB SD card (needed for installation)

**Dedicated to the memory of Tareq Saade 1983-2012:**

*This flesh and bone*
*Is just the way that we are tied in*
*But there's no one home*
*I grieve for you –Peter Gabriel*

As you likely know by now given *toolsmith's* position at the back of the *ISSA Journal*, March's theme is Advanced Threat Concepts and Cyberwarfare. Well, dear reader, for your pwntastic reading pleasure I have just the topic for you. The Pwn Plug can be considered an advanced threat and useful in tactics that certainly resemble cyberwarfare methodology. Of course, those of us in the penetration testing discipline would only ever use such a device to the benefit of our legally engaged targets.

A half year ago I read about the Pwn Plug when it was offered in partnership with SANS for students taking vLive versions of SEC560: Network Penetration Testing and Ethical Hacking or SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. It seemed very intriguing, but I'd already taken the 560 track and was immersed in other course work. Then a couple of months ago I read that Pwnie Express had released the Pwn Plug Community Edition and was even more intrigued, but I had a few things I planned to purchase for the lab before adding a Sheevaplug to the collection.

But alas, the small world clause kicked in, and Dave Porcello (grep) and Mark Hughes from Pwnie Express,[2] along with Peter LaPlante, emailed to ask if I'd like to review a Pwn Plug.

The answer to that, which you, dear readers, know to be a rhetorical question, goes without saying.

Here's the caveat. For *toolsmith* I'll only discuss offerings that are free and/or open source. Pwn Plug Community Edition meets that standard, but the Pwnie Express team provided me with a Pwn Plug Elite for testing. As such, for this article, I will discuss only the features freely available in the CE to anyone who owns a Sheevaplug: "Pwn Plug Community Edition does not include the web-based Plug UI, 3G/GSM support, NAC/802.1x bypass."

For those of you interested in a review of the remaining features exclusive to commercial versions, I'll post it to my blog on the heels of this column's publishing.

Dave provided me with a few insights including the Pwn Plug's most common use cases:

- Remote, low-cost pen testing: penetration test customers save on travel expenses; service providers save on travel time.
- Penetration tests with a focus on physical security and social engineering.
- Data leakage/exfiltration testing: using a variety of covert channels, the Pwn Plug is able to tunnel through many IDS/IPS solutions and application-aware firewalls undetected.
- Information security training: the Pwn Plug touches on many facets of information security (physical, social, and employee awareness, data leakage, etc.), thus making it a comprehensive (and fun!) learning tool.

One of Pwnie Express' favorite success stories comes from Jayson Street (The Forbidden Network) who was hired by a large bank to conduct a physical/social penetration test on ten bank branch offices. Armed with a Pwn Plug and a bit of social engineering finesse, Jayson was able to deploy a Pwn Plug to four out of four branch offices attempted against before the client decided to cut their losses and end the test early. In one instance, a branch manager actually directed Jayson to connect the Pwn Plug underneath his desk. Pwnie Express hopes the Pwn Plug helps illustrate how critical physical security and employee awareness are and Jayson's efforts delivered exactly that to his enterprise client.

Adrian Crenshaw (Irongeek) has Jayson's Derbycon 2011 presentation video posted on his site. It's well worth your time to watch it.[3]

In addition to the Pwn Plug there is also the Pwn Phone which is also capable of full-scale wireless penetration testing. Penetration testers and service providers often utilize the Pwn Phone for proposal meetings and demonstrations as the

1 http://www.globalscaletechnologies.com/p-22-sheevaplug-dev-kit-us.aspx.

2 http://pwnieexpress.com/.

3 http://www.irongeek.com/i.php?page=videos/derbycon1/jayson-e-street-steal-everything-kill-everyone-cause-total-financial-ruin-or-how-i-walked-in-and-misbehaved.

"wow factor" is high. As with Pwn Plug, if you already own or can acquire a Nokia N900 you can download the community edition of Pwn Phone and get after it right away.

PwnPlug compatibility is currently limited to Sheevaplug devices. There has been little demand so far for the Guruplug/Dreamplug form factors and the Guruplug hardware has a history of overheating while the Dreamplug is quite bulky and flashy. Bulky and flashy do not equate to good resources for physical and social testing. The development team is working on a trimmed down Pwn Plug for the $25 Pogoplug. Even though it only offers about half the performance and capacity of the Sheeva, with a larger board, it is only $25.


Figure 1 – Who, me?

Figure 2 – The Pwn Plug looking so innocent

Figure 1 is a picture taken of the Pwn Plug I was sent for testing. You can see what we mean by the importance of form factor. It's barely bigger that a common wall wart and you can use the included cord or plug it in straight to the wall. Pwnie Express included a couple of sticker options for the Sheeva. I chose what looks to be a very typical bar code and manufacturer sticker that even has a PX part number. I chuckle every time I look at it (figure 1).

With Sheevaplugs typically sporting a 1.2Ghz ARM processor, 512M SDRAM, and 512M NAND Flash configuration, it's recommended that you don't treat the device like a work horse (no Fastttack, Autopwn, or password cracking), but it's crazy good for maintaining access in stealth mode, reconnaissance, sniffing, exploitation, and pivoting off to other victim hosts. Figure you'll find the 512M storage at about 70% of capacity after installation but adding SD storage means you can add software within reason. Pwn Plug is Ubuntu underneath so `apt-get` is still your friend.

The tool list for a device this small is impressive. Expect to find MSF3, dsniff, fasttrack, kismet, nikto, ptunnel, scapy and many others at you command, most of which can be called right from the prompt without changing directories.

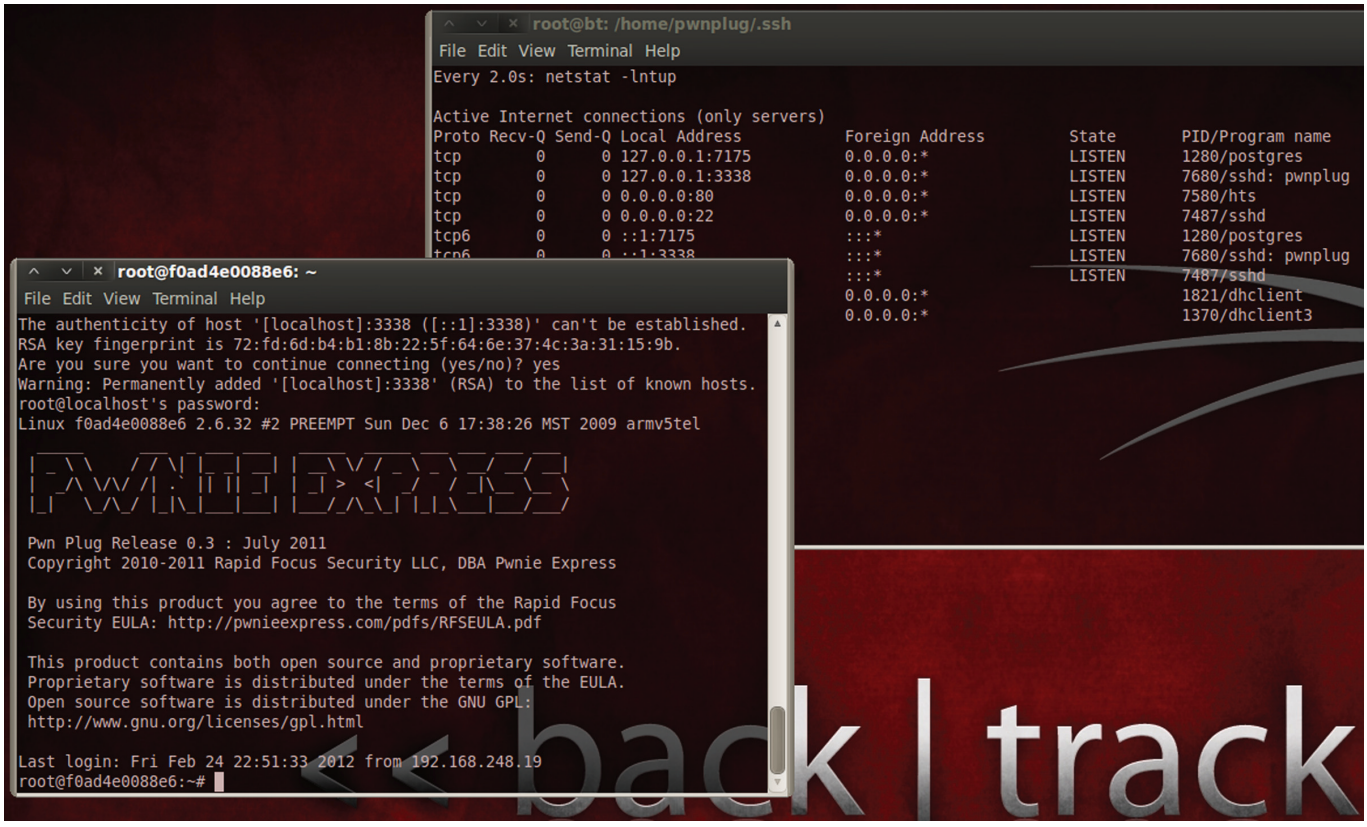



Figure 3 – Have shell, will pwn

## Installation

To install Pwn Plug CE to a stock Sheevaplug, download the JFFS2[4] and follow the instructions.[5] No need to reinvent the wheel here.

## Pwning with PwnPlug

First, imagine the Pwn Plug hidden at the target site, lurking amongst all the other items usually plugged in to a power strip, hiding behind a desk in so innocuous a fashion so as to go easily undetected. Figure 2 will send you scurrying about your workplace to ensure there are none in hiding as we speak.

I'll walk through an extremely fun example with Pwn Plug but first you'll need to ensure access. Commercial Pwn Plug users benefit from the Plug UI but those rolling their own with Pwn Plug CE can still phone home. Have a favorite flavor of reverse shell pwnzorship? Plain old reverse SSH is available or shell over DNS, HTTP, ICMP, SSL, or via 3G if you have the likes of an O2 E160.

The supporting scripts for reverse shell on the Pwn Plug are found in `/var/pwnplug/scripts`.

On your SSH receiver (Backtrack 5 recommended - figure 3) I suggest checking out the PwnieScripts for Pwnie Express from Security Generation.[6] @securitygen even has a method for setting up reverse SSH over Tor.[7] I configured the Pwn Plug for HTTP because who doesn't allow HTTP traffic outbound? ☺

Access established, time to pwn. One of my all-time favorite collections of mayhem is the Social Engineer Toolkit (SET). You will find SET at `/var/pwnplug/set`. Change directories appropriately via your established shell and run `./set`. You will be presented with the *SET* menu. I chose *2. Website Attack Vectors*, then *3. Credential Harvester Attack Method* followed by *2. Site Cloner* (SET supports both HTTP and HTTPS). In an entirely intentional twist of irony I submitted `http://mail.ccnt.com/igenus/login.php` to SET as the URL to clone. Mind you, this is not a hack of the actual site being cloned so much as it is harvesting credentials via an extremely accurate replica wherein usernames and passwords are posted back to the Pwn Plug.

The test Pwn Plug was set up in the HolisticInfoSec Lab with an IP address of `192.168.248.23`.

Imagine I've sent the victim a URL with `http://192.168.248.23` hyperlinked as opposed to `http://mail.ccnt.com/igenus/login.php` and enticed them into clicking. Now don't blink or you'll miss it; I froze it for you in Figure 4.

4 http://pwnieexpress.com/communitydownloads.html.

5 http://pwnieexpress.com/support/pwnplug_community_install.txt.

6 http://www.securitygeneration.com/security/pwniescripts-for-pwnie-express/.

7 http://www.securitygeneration.com/security/reverse-ssh-over-tor-on-the-pwnie-express/.

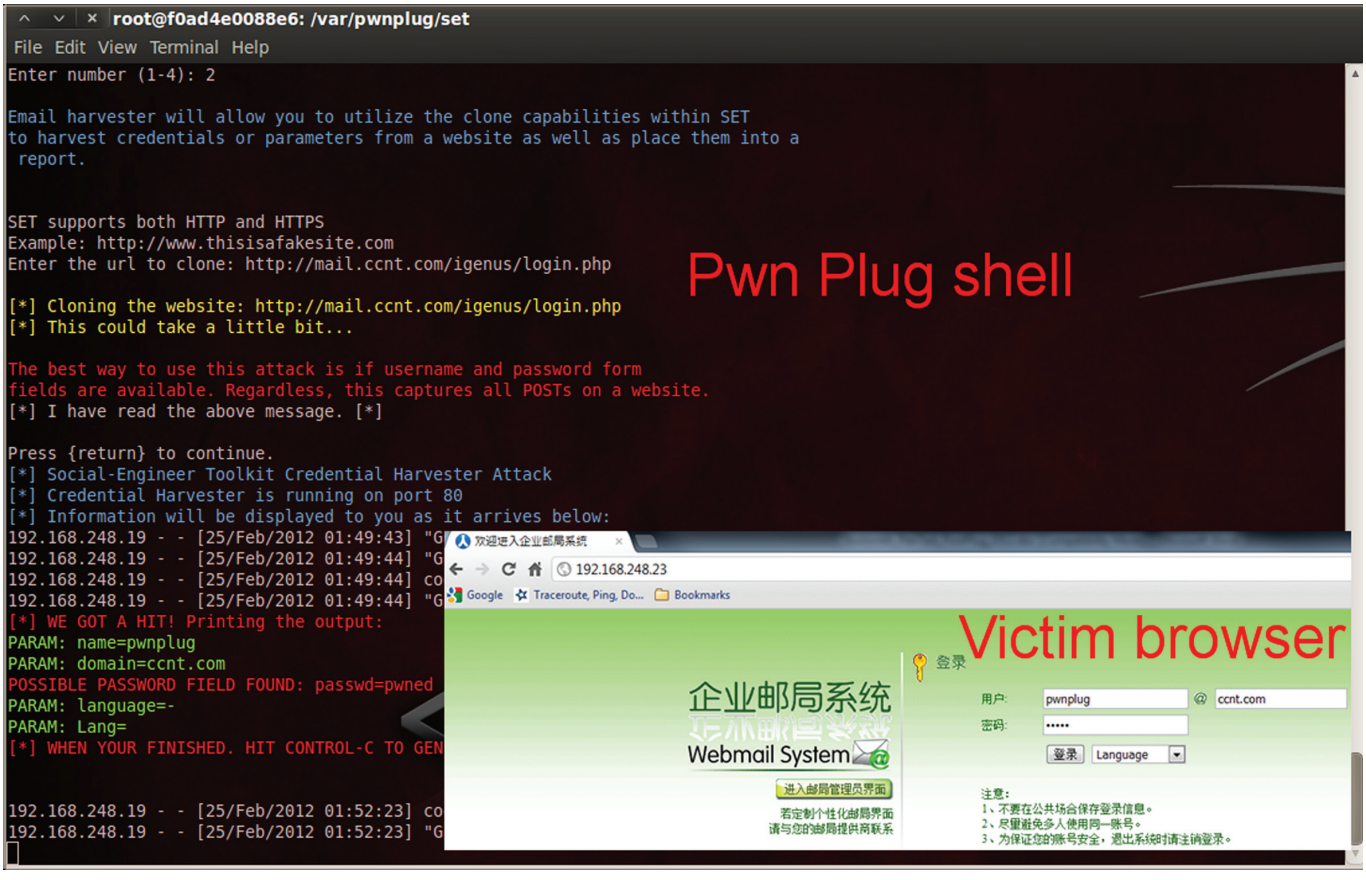
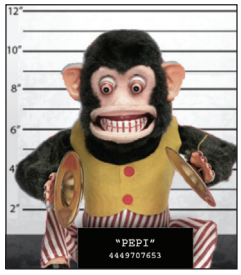



Figure 4 – SET harvesting from Pwn Plug

After passing credentials, the victim is then redirected back to the legitimate site none the wiser.

This is the tip of the iceberg for SET, and a mere fraction of the chaos you can unleash in whisper quiet mode via Pwn Plug. There are simply too many options to do it much justice in such short word space so as mentioned earlier I'll continue the conversation on the HolisticInfoSec blog.




## In conclusion

I had a blast testing Pwn Plug. This is me after spending days doing so.

If you make your living as penetration tester or need a really capable demonstration tool for social engineering awareness and prevention training, Pwn Plug is for you. Grab yourself a Sheevaplug, download Pwn Plug CE and enjoy yourself (with permission)!

Ping me via email if you have questions (russ at holisticinfosec dot org). Cheers…until next month.

## Acknowledgements

—Dave Porcello, CEO and Technical Lead, Pwnie Express

## About the Author

*Russ McRee leads the incident management and penetration testing functions for Microsoft's Online Services Security team. He advocates a holistic approach to information security via holisticinfosec.org and volunteers as a handler for the SANS Internet Storm Center. Reach him at russ at holisticinfosec dot org or @holisticinfosec.*