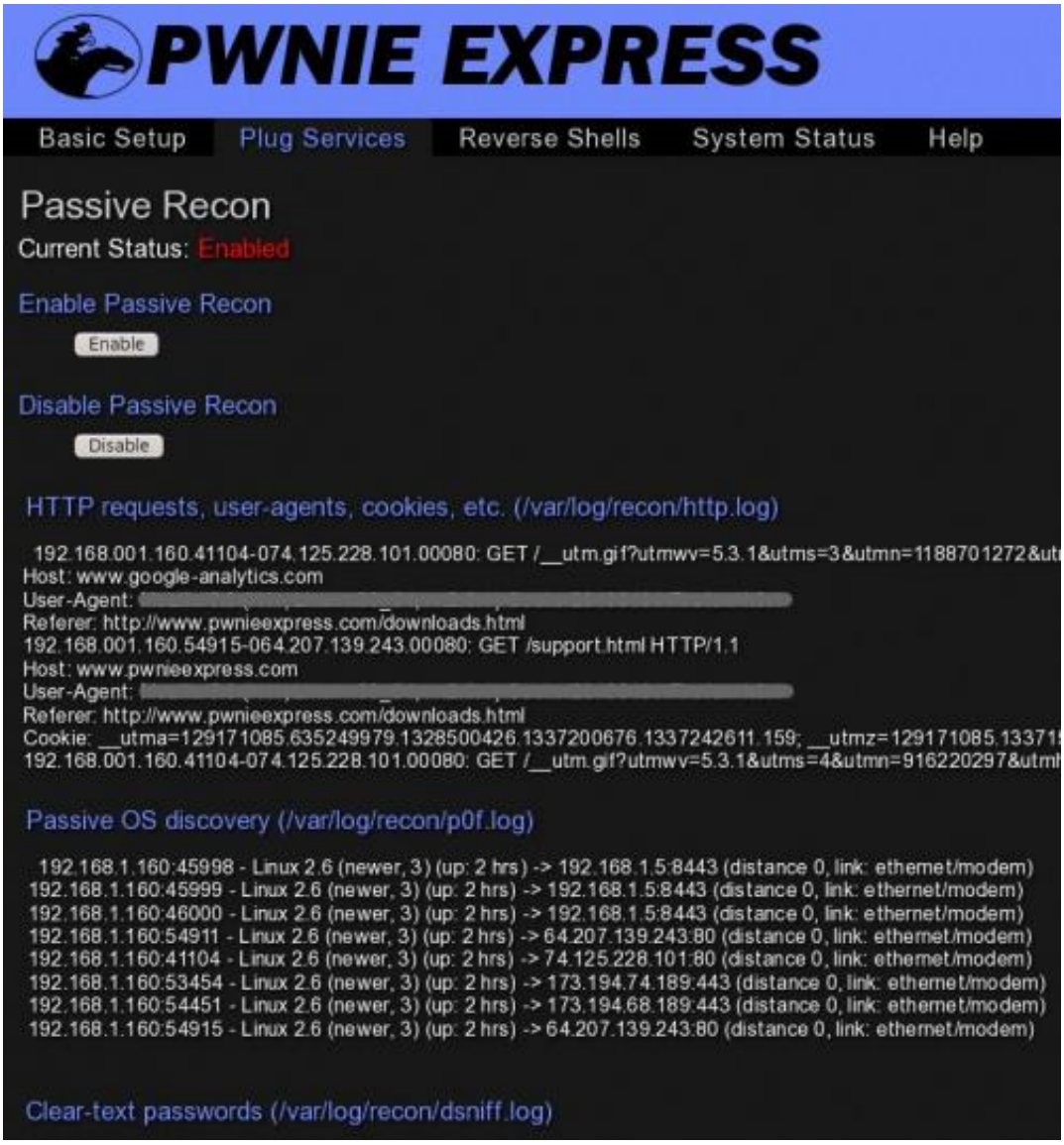
Power-strip lookalike hacks office networks

July 23 2012, by Nancy Owano

(Phys.org) -- Pwnie Express, the company specializing in cyber security products, calls its new device “ingenious.” Bloggers hearing about it are paying attention to the fact that it is a power-strip lookalike but with far more ambitious intentions, such as stealth-penetrating a corporate network. Power Pwn is the name of the little device for security testing on corporate networks. It looks like an under the office desk power strip. It is actually a testing platform where security can be put to the test, a self-hacking tool for launching remotely-activated Wi-Fi, Bluetooth, and Ethernet attacks.

The testing platform covers the range from physical to application layers. Pwnie Express is taking pre-orders for the device with a pricetag of $1295 and an estimated ship date of September 30.

The Pwnie Express product description says it is a first-to-market "commercial penetration testing drop box platform" for remote security testing of corporate facilities, including branch offices and retail locations.



The device has Bluetooth and Wi-Fi adapters, a cellular connection, dual Ethernet ports, and hacking and remote access tools that let security professionals test the network and call home to be remotely controlled via the cellular network. The device comes with easy-to-use scripts that cause it to boot up and then phone home for instructions.

A “text-to-bash” feature allows sending commands to the device using SMS messages. Power Pwn is preloaded with Debian 6, Metasploit, SET, Fast-Track, w3af, Kismet, Aircrack, SSLstrip, nmap, Hydra, dsniff, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools and. It really can function as a 120/240v AC outlet strip.

The Power Pwn has funding from a new Defense Advanced Research Projects Agency (DARPA) program called Cyber Fast Track (CFT), which is looking to advance new cyber-defense tools. The officially stated purpose of CFT is to fund research to be performed by boutique security companies, individuals, and hacker/maker-spaces, and allow them to keep the commercial intellectual property for what they create.

While the purpose is to place this in the right hands for identifying network weaknesses, Tony Bradley of *PCWorld* is asking what about the device landing in the wrong hands, as an attacker could communicate with the device from inside the network or around the world. The device can, after all, bypass Network Access Control and other security measures in place to keep unauthorized devices off the network. It can tunnel through firewalls, he notes, maintain an encrypted connection to the attacker, and operate in stealth mode.

“The fact is that any attacker with $1,300 can buy one and

surreptitiously plant it in your office," he said. His advice for those in business settings is to check out and mark their office surge protectors and strips and allow only approved power strips to be in the inventory.

More information: pwnieexpress.com/products/power-pwn