Honeypots: The Wasp Trap

By Zainab Ebrahimi

**What is a Honeypot?**

Honeypots are a really fascinating and flexible security technique. Many tend to agree on the complexity of defining honeypots because of its versatility. A honeypot is not necessarily a static tool or software. It is more of a combination of techniques along with a strategic infrastructure and goal that can be implemented in a variety of ways. As a resource it gains its value by its unauthorized or illicit use. This is the fascinating part; a honeypot is of no use if it’s not somehow manipulated maliciously. Basically, it’s a trap. It captures malicious/unauthorized network traffic but unlike a packet sniffer the technique deceives attackers by mimicking vulnerable services and opening a large range of listening sockets. It doesn’t solve a problem or prevent them, although, in the long run it might. The main purpose of its implementation is to learn how intruders probe and attempt to gain access to your system (Even). “Collect raw data and throw away what is expected. What remains challenge your theories” (Stoll). With honeypots you can expect the unexpected.

The concept of Honeypots is almost a decade old, but it’s not until recently that more papers have been published and more commercial products have been developed (Spitzner, Honeypots: Tracking Hackers). Good references on the early beginning of this technique are Cliff Stoll’s book “The Cuckoo’s Egg” and Bill Cheswick’s paper “An Evening with Berferd”.

Honeypots haven’t been massively implemented because of little knowledge in the matter. Many organizations find little use in them and it has been tagged as a technique oriented to research. Honeypots have great security value. For example, one of honeypots biggest trait is that they may be detected. Upon detection an attacker will be aware of which systems to avoid or feed the honeypot with wrong information or bring the attackers attention to other systems in your network outside of the DMZ. But there is potential in an exposed honeypot. This might deter attacker from probing your network. Also, it can prevent against automated attacks, such as worms or auto-rooters, which are based on randomly scanning entire networks looking for vulnerable systems. A honeypots can slow their scanning down, potentially even stopping them. Called sticky honeypots, these solutions monitor unused IP space. They do this using a variety of TCP tricks, such as a Windows size of zero, putting the attacker into a holding pattern. (Spitzner, Honeypots: Definitions and Value of Honeypots). Also, by using honeypots administrators can watch an intruder exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned or the hacker can be caught and stopped while trying to obtain root access to the system. These are just a few examples of the potential of honeypots. Unlike any other security technique, honeypots have been exposed to many ethical concerns. Many researchers in the field expect the growth of this technique in the next couple of years.

**Building a basic Honeypot**

Now, how do you implement a honeypot? As mentioned, honeypots have different forms and flavors, but they all share some common characteristic. There are low-interation honeypots and high interaction ones, defined by the amount of data that can be collected. Honeypots can be setup inside, outside or in the DMZ of a firewall design. Most of the time they are used behind a firewall, for control purposes (Even). A honeypot has to be setup as an easy prey for intrusion. A basic application of a honeypot may well just consist of a workstation with some kind of sniffer and log tracker exposed publically to the Internet.

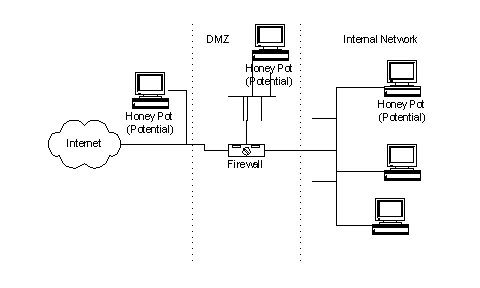
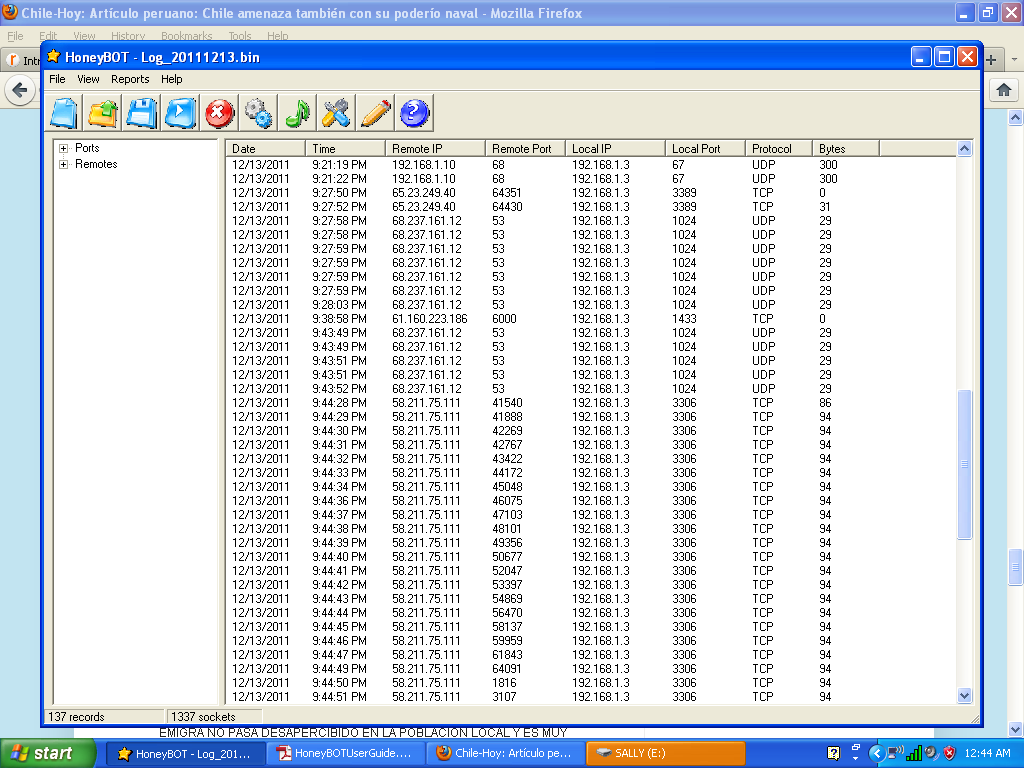


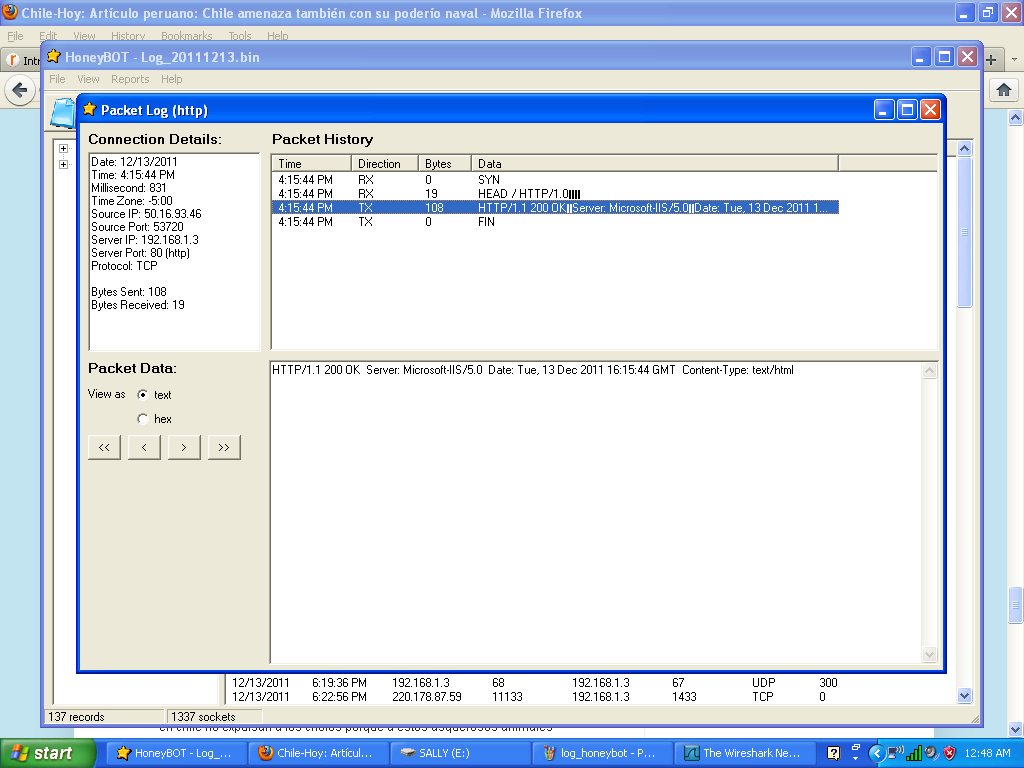
Image above display different implementation of a Honeypot. <http://www.sans.org/security-resources/idfaq/honeypot3.php>

I built a basic honeypot on an old Dell Latitude D520 that had been retired a while ago. I did a clean install of Windows XP service pack 3. Then I installed HoneyBot, a free Windows based prepackage honeypot. This software opens a large range of listening sockets on your computer from which a selection of these sockets are designed to mimic vulnerable services. The honeypot safely captures all communications with the attacker and logs these results. Should an attacker attempt an exploit or upload a rootkit or trojan to the server the honeypot environment can safely store these files on your computer for malware collection and analysis purposes ([HoneyBOT](http://www.atomicsoftwaresolutions.com/honeybot.php)). I also installed [Wireshark](http://www.wireshark.org/). Before launching either software I disabled Windows services that were not crucial to the PC. HoneyBOT cannot listen on ports that are already in use by Windows services, so I disabled FTP Publishing, SMTP, SNMP, TCP/IP NetBIOS Helper and SMB. Then I checked how many port were still in use. In command line:

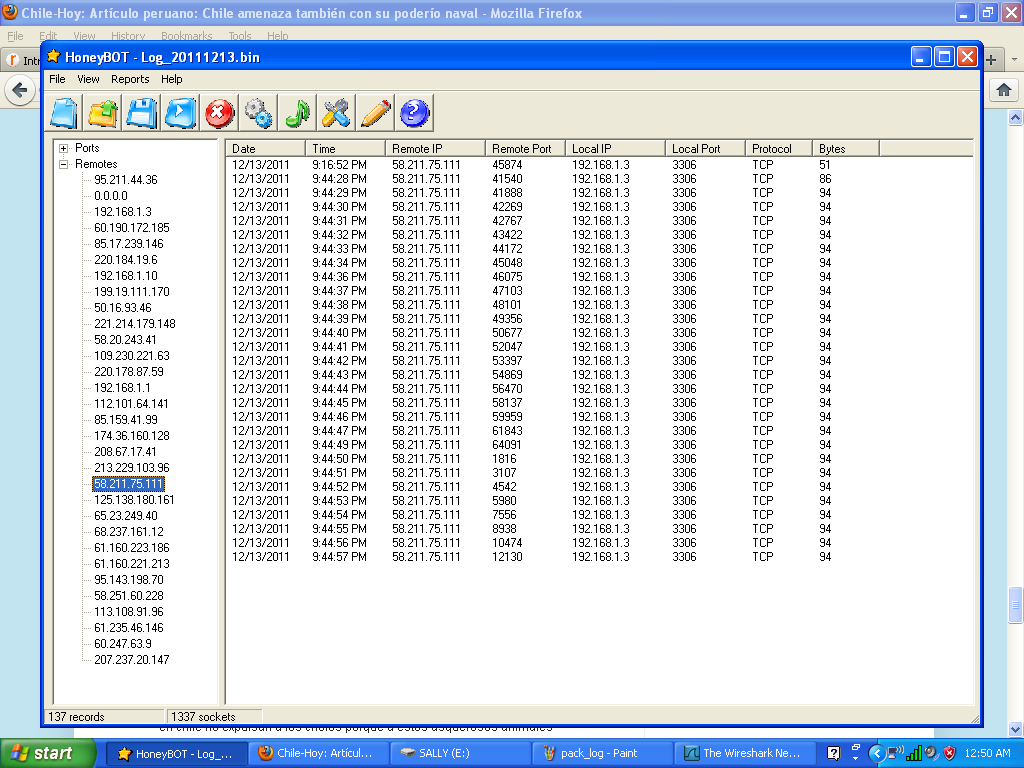
C:\>netstat -ano  
Active Connections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proto | Local Address | Foreign Address | State | PID |
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING | 1104 |
| TCP | 127.0.0.1:1028 | 0.0.0.0:0 | LISTENING | 1052 |
| UDP | 127.0.0.1:123 | \*..\* |  | 1144 |
| UDP | 127.0.0.1:1900 | \*..\* |  | 1704 |

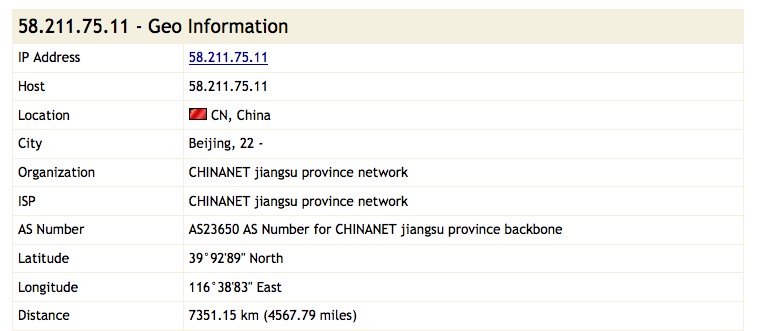
Once determined my baseline. I had to configure the router to determine the DMZ. The router in use was a FIOS router. I didn’t know the user/pass and the default wasn’t working. I did a hard reset, which reset the default settings and also reset user/pass to default. Once the router was configured, I launched HoneyBOT. The software in a matter of 15 minutes collected a considerable amount of logs.

When double clicking on a specific entry, a window pops showing detailed information on the intrusion attempt. It shows packet details and data in text or hex format.

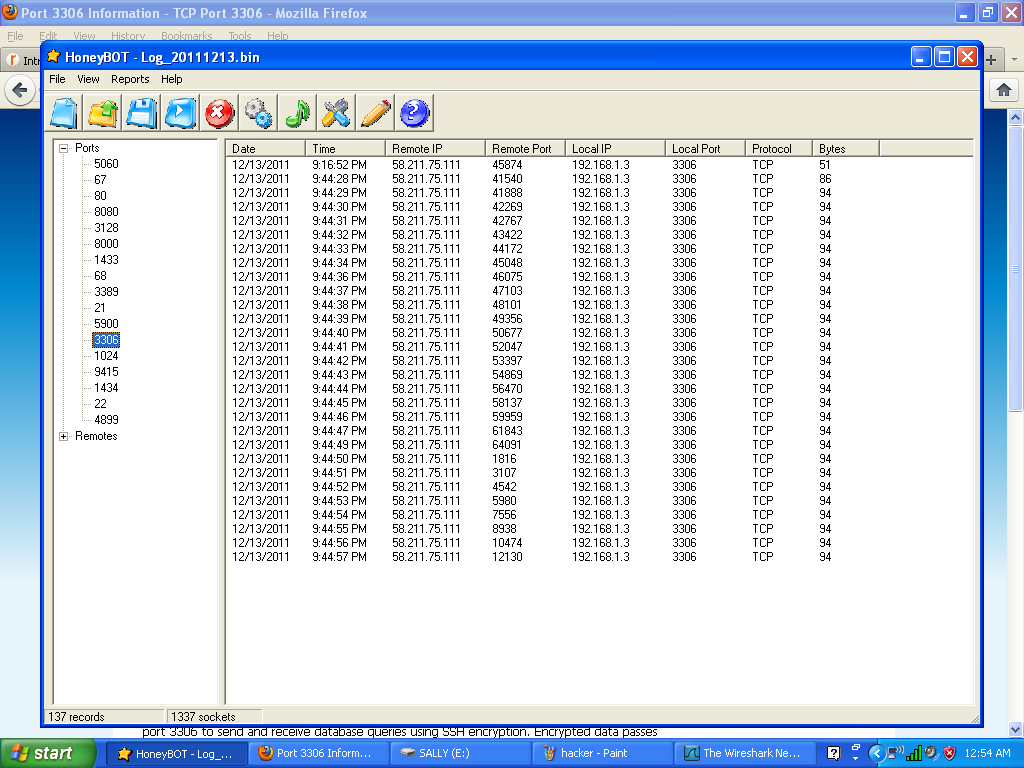
When filtering by remote address. I realized ip address 58.211.75.111 had a longer list of attempts.



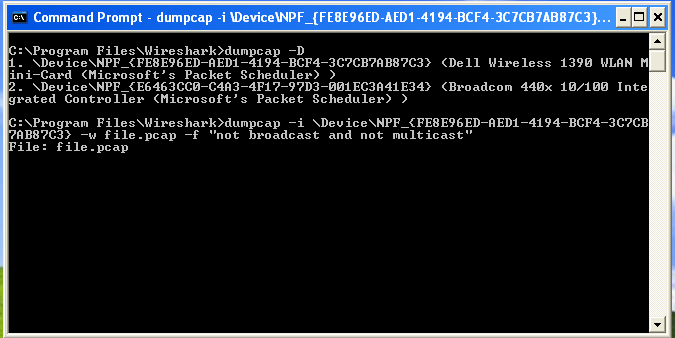
I looked up the ip in whois:



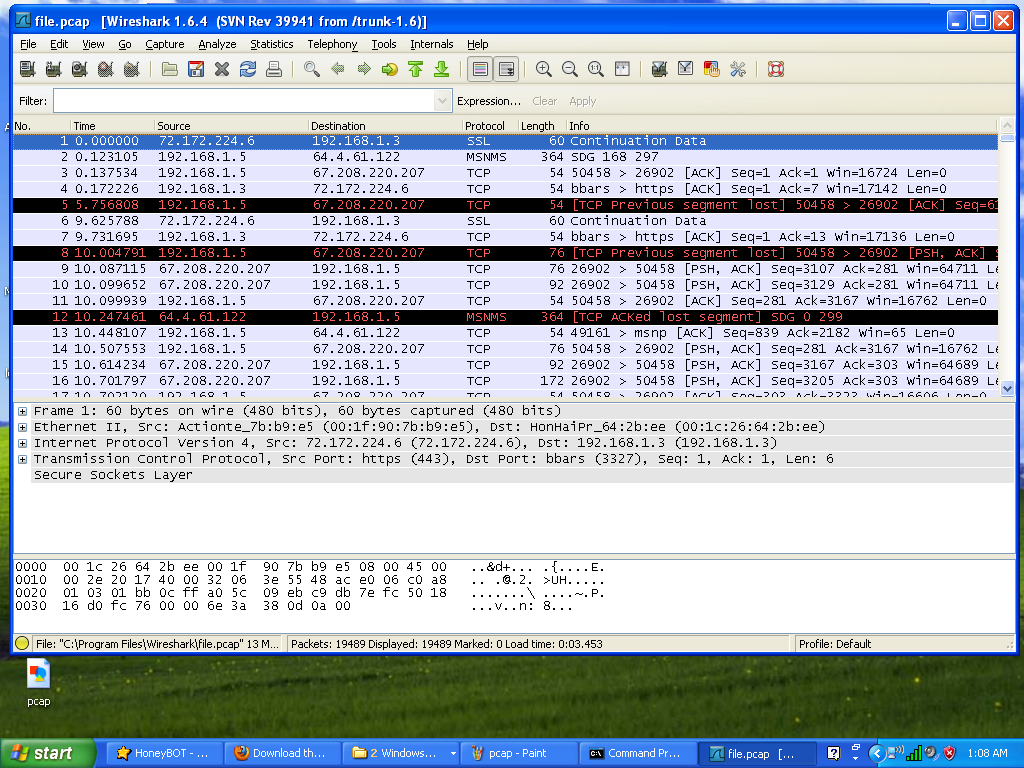
I also realized when filtering by port, that port 3306 was highly solicited. Port 3306 is considered as an unsecured port that is easily exploited by malware to gain access to a computer system to initiate DoS or backdoor-creation attacks. Port 3306 is configured on MySQL application for SSH Tunnel. (PC-Library).



I wanted to gain a little more insight on the data received. I decided to use a

****program called dumpcap that comes with Wireshark. I checked the interface it uses to sniff and created a pcap file.

Then I opened the .pcap file using wireshark. Wireshark displayed much more detailed information on the packets received. Many turned out to be flagged as malicious.



Seeing all that information collected was exciting, but what to do with it? And here is the dilemma with Honeypots. In order to give it a practical use there must be a plan for all that interaction. Honeypots are not only the technique, but also the strategy.

**Concluding …**

We live in an Internet driven society and the risks of security breaches are growing as our dependency grows. The need for a more secure environment is pressing. Honeynets have been proposed as a solution to it (Kleiner). Honeypots are fascinating and should be developed further, despite the ethical controversy built up. The argument is that since it is both unethical and illegal to lure someone into stealing an object, why is it legal or ethical to lure an individual into committing a computer crime? (M. E. Kabay) . This argument is completely valid and states a really good point, but Honeypots can’t be tagged as unethical given the obvious advantages it provides. Honeynet.org is an organization committed to raising awareness of the vulnerabilities that exist on the Internet today and putting the advantages of honeypots into use. Completely needed. Let’s see if we can trap the wasp.

# Bibliography

PC-Library. <http://www.pc-library.com/ports/tcp-udp-port/3306/>.

Even, Loras R. "Intrusion Detection: What is a Honeypot?" 12 July 2000. SANS. 13 December 2011 <http://www.sans.org/security-resources/idfaq/honeypot3.php>.

Kleiner, Kurt. "Viral cure could 'immunise' the internet ." 01 December 2005. New Scientist. 2011 <http://www.newscientist.com/article/dn8403>.

M. E. Kabay. 22 May 2003. Network World. 2011 <http://www.networkworld.com/newsletters/sec/2003/0519sec2.html>.

Spitzner, Lance. "Honeypots: Definitions and Value of Honeypots." 29 May 2003. Tracking Hackers. 2011 <http://www.tracking-hackers.com/papers/honeypots.html> --. Honeypots: Tracking Hackers. Addison-Wesley Professional, 2002.

Stoll, Cliff. The Cuckoo's Egg. New York, 1989.