The Webbones Hacker System

By Bill Sommerville

A hacker can be like a bad family member or neighbor. You have made it clear to them that you do not want their company. Yet they keep knocking at the door or calling on the phone. You know they are up to no good and the funny thing about it is they know you know. No matter how much you lock the doors and use different tools to screen your calls, they keep trying to get to you.

What you need is some type of security agent that recognizes them and stops them from ever getting to you. In the analog world they are called body or perimeter guards. In the world of the Internet, they are called firewalls. Like a bodyguard who learns who can have access to you or not, firewalls can learn who can attempt to have to access to your system. The bodyguard gets his access information from the person he protects. The firewall gets it's information from the windows of knowledge in the computer world called logs.

There is not a operating system, application, program, tool, or server that does not have some type of logs of what is going on. If there are any that does not use logs, then I highly recommend that you do not use them. Logs can provide the information you need to fix a problem, figure out a situation, or with some idea and initiative, make improvements. They can reveal the smoking gun and can claim the title that if it was not for them, the problem may not have been fixed. No matter what system you are using, there are logs that recorded when you turned the system on, login, open an application, went on the internet, and of course, who tries to accessed your system as well.

Now before you get all excited, let me clarify that the particular log files being mentioned will not tell you whom a hacker is. They can tell you where the person is with the help of IP addresses. Yet this may be limited due to the technique of remote access and zombies. In truth you do not need to know the person's name nor where they are located. You have all the information you need. Like the family member or neighbor, you know a hacker is up to no good and when they attempt to access and fail, that failure can be recorded and the IP address they used to access be blocked. For a hacker to access a system on the first attempt is rare and if accomplished, means there was some other type of hacking/spying prior to accomplish the goal. Many out there are "wanna be" hackers who leave a trail of information. A true professional hacker will be able to enter a system and do or get what they want leaving very little evidence if any at all.

True even a legitimate person can fail when trying to login to a system. Most organizations have the three time rule and this can be applied as well, but you have to be a little bit like a detective to determine is the person knocking at your gateway is a hacker or not.

In my case, I use other information that makes the determination and the script I wrote looks at the same information from the log files.

Looking at the logs (see Fig1) the section in red tells me this may be a hacker. First notice the time, each attempt takes a second. Manual attempts takes a little longer than a second

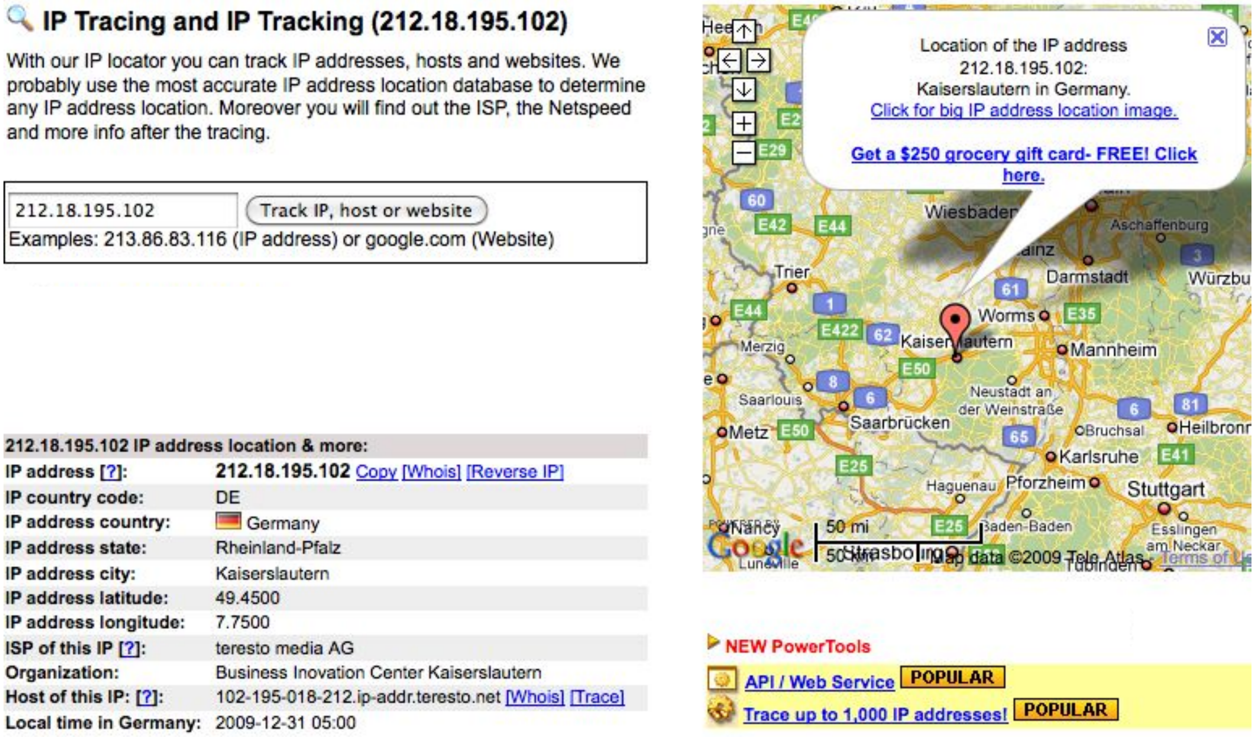
so this bit of information tells me that this person may be using a cracker program, and is looking for the password for root (last red line) which it attempts to login based upon its previous scans. The cracker program did an analyst after 07:42:22 time. The hacker did another scan at 10:56:18, then based upon the cracker program recommendation, the hacker makes a legitimate attempt to login using the account root. The cracker program recommendation on the password to use failed and that is the smoking gun that this is a hacker. If a person is able to login a system across SSH using the account root, then they will have full access to that systems and can do anything they wish. This is like letting your bad family member or neighbor come into your house and do what ever they wish, NOT GOOD.

```
Dec 27 07:42:12 webbones sshd[3887]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:13 webbones sshd[3889]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:14 webbones sshd[3891]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:15 webbones sshd[3893]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:16 webbones sshd[3895]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:17 webbones sshd[3897]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:18 webbones sshd[3899]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:20 webbones sshd[3901]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:21 webbones sshd[3903]: Could not reverse map address 212.18.195.102.
Dec 27 07:42:22 webbones sshd[3905]: Could not reverse map address 212.18.195.102.
Dec 27 10:56:18 webbones sshd[3928]: Could not reverse map address 212.18.195.102.
Dec 27 10:56:21 webbones sshd[3928]: Failed password for root from 212.18.195.102 port 34009 ssh2
Dec 27 18:11:43 webbones sshd[3984]: Accepted password for wiskey from 192.168.77.18 port 53977 ssh2
Dec 27 18:13:09 webbones xinetd[27806]: START: ftp pid=4025 from=192.168.77.15
Dec 27 18:23:47 webbones xinetd[27806]: START: ftp pid=4050 from=192.168.77.18
Dec 27 18:41:49 webbones sshd[4056]: Did not receive identification string from 201.227.228.35
Dec 27 18:45:07 webbones sshd[4057]: Could not reverse map address 201.227.228.35.
Dec 27 18:45:10 webbones sshd[4057]: Failed password for root from 201.227.228.35 port 52752 ssh2
Dec 27 21:05:55 webbones sshd[4078]: Could not reverse map address 212.18.195.102.
Dec 27 21:05:56 webbones sshd[4080]: Could not reverse map address 212.18.195.102.
Dec 27 21:05:57 webbones sshd[4082]: Could not reverse map address 212.18.195.102.
```

Fig 1

Fortunately for Webbones, root access across the network is not available so no matter what the cracker program comes up with, with that feature not available, there will always be a Failed attempt in the logs when a hacker tries to login. So in a wrap when a person tries to login using the account root, I know they are a hacker no matter how many times they have performed a scan.

Technology can be a wonderful thing. Out of curiosity, I decided to try and find out where this person may be. Going to http://www.ip-adress.com/ip_tracer/212.18.195.102 I discovered that this person is located in Kaiserslautern, Germany. See Fig 2



IP Tracing and IP Tracking (212.18.195.102)

With our IP locator you can track IP addresses, hosts and websites. We probably use the most accurate IP address location database to determine any IP address location. Moreover you will find out the ISP, the Netspeed and more info after the tracing.

212.18.195.102 | Track IP, host or website

Examples: 213.86.83.116 (IP address) or google.com (Website)

212.18.195.102 IP address location & more:

IP address [?]:	**212.18.195.102** Copy [Whois] [Reverse IP]
IP country code:	DE
IP address country:	Germany
IP address state:	Rheinland-Pfalz
IP address city:	Kaiserslautern
IP address latitude:	49.4500
IP address longitude:	7.7500
ISP of this IP [?]:	teresto media AG
Organization:	Business Inovation Center Kaiserslautern
Host of this IP: [?]:	102-195-018-212.ip-addr.teresto.net [Whois] [Trace]
Local time in Germany:	2009-12-31 05:00

Location of the IP address 212.18.195.102: Kaiserslautern in Germany.
Click for big IP address location image.

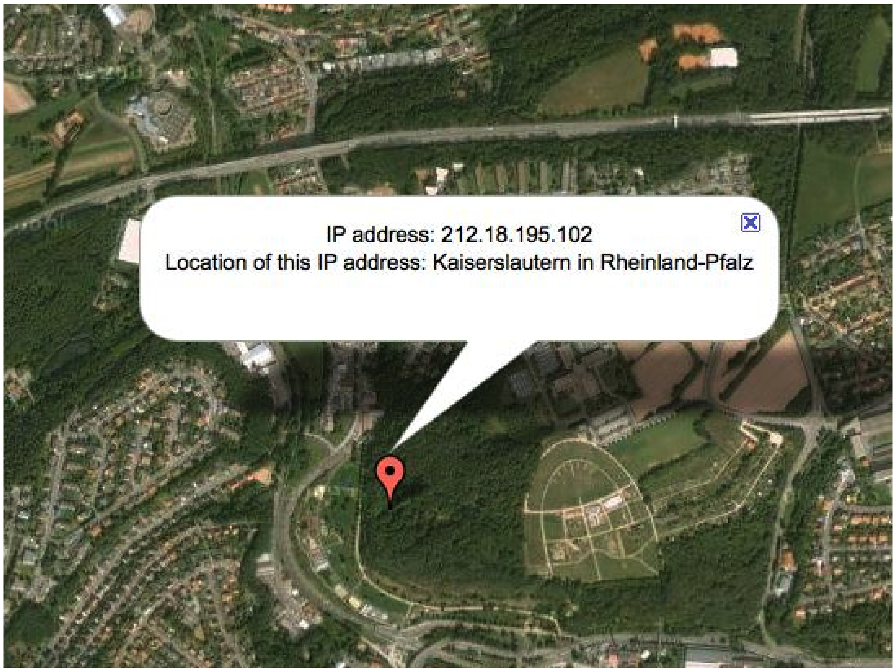
Get a $250 grocery gift card- FREE! Click here.

NEW PowerTools

API / Web Service POPULAR

Trace up to 1,000 IP addresses! POPULAR

Fig 2



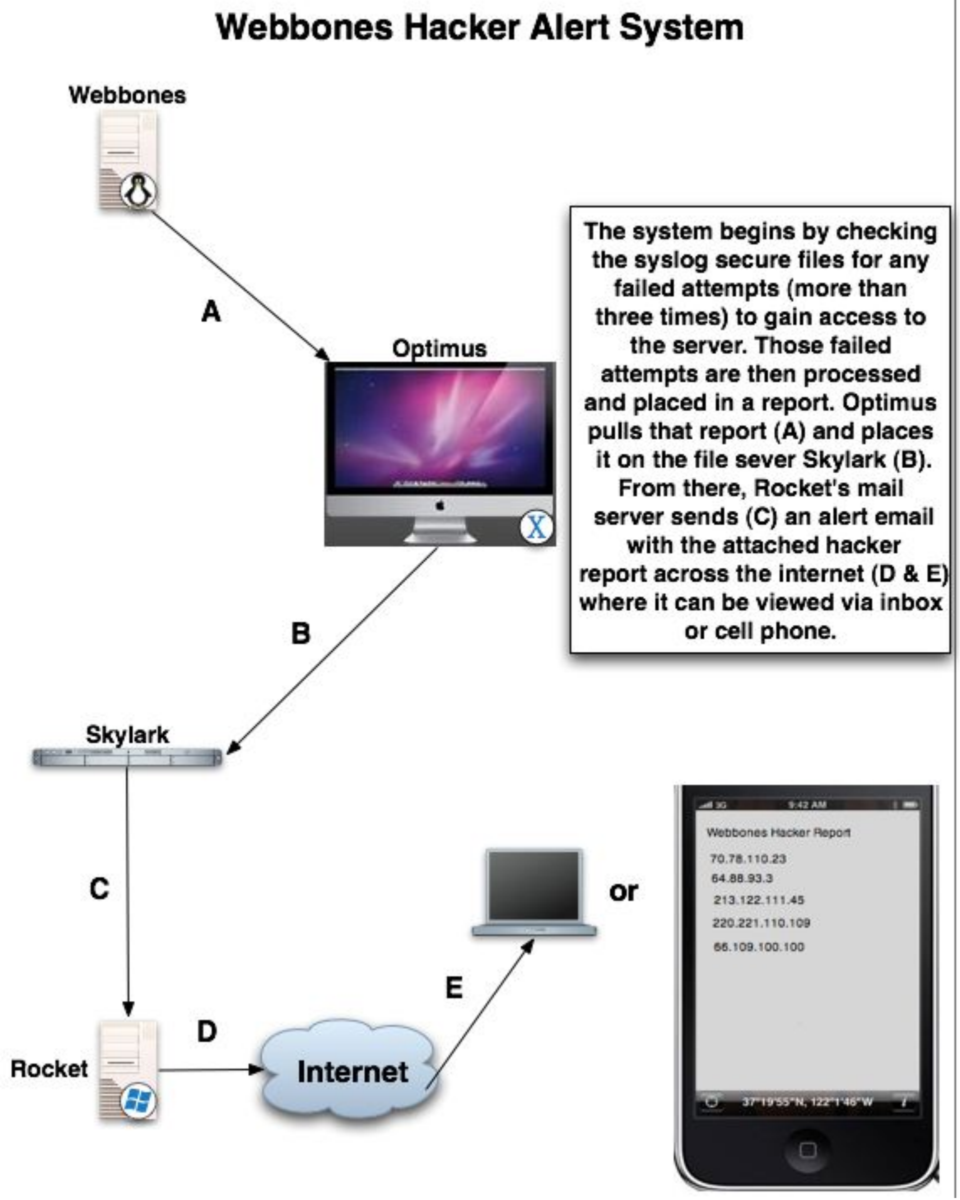
IP address: 212.18.195.102
Location of this IP address: Kaiserslautern in Rheinland-Pfalz

Fig 3

Since I do not know anyone there, it is safe to determine this is a hacker. I did this as an example of what you can do. I have heard of tools that will even get you the physical address. Why go through all of that when you can just put them in your firewall. Again like our bad neighbor, we do not care where they live, as long as they are not knocking on our door anymore.

This is where the Webbones Hacker System (See Fig 4) comes in. Scanning the log file it makes many of the same determinations I do of the possibility of a hacker.

Once it does this, then a report is generated containing a list of the possible hackers and is sent to my email address alerting me of the offenders by ipaddress. At this point even though I have been alerted, it does not do much good until they are placed in the firewall. This can be a manual or an automated process. Presently it is a manual process, but an automated process is in the works



The system begins by checking the syslog secure files for any failed attempts (more than three times) to gain access to the server. Those failed attempts are then processed and placed in a report. Optimus pulls that report (A) and places it on the file sever Skylark (B). From there, Rocket's mail server sends (C) an alert email with the attached hacker report across the internet (D & E) where it can be viewed via inbox or cell phone.

```
Webbones Hacker Report
70.78.110.23
64.88.93.3
213.122.111.45
220.221.110.109
66.109.100.100
```

Fig 4

Many out there have what I call the friendly firewall system. These are mostly integrated into routers where a few settings stops most intruders. This information is for server type firewall systems where files are used to address the strength of the protection.

Bill Sommerville is a long time IT professional that has worked for some of the largest organization in the country. His knowledge, skill, and experience has put forth many successful projects that are still in use today. A 20 year veteran and a graduate of Henry Ford College and Capella University, Bill has written many papers and reports covering a vast amount of IT subjects, processes, and procedures. For more information, please go to
Bill Sommerville.com
12/30/2009