Quick Security TIP - 2

Fast configuration of OpenVAS on Kali Linux 1.5

On the market exist lot of good scanners and all of them are excellent, but unfortunately most of available scanners are paid and this relevant fact hinder some students of understanding how to analyze and invade remote machines. Nonetheless, a good free scanner exists and using it allow you find out any possible flaws: OpenVAS. In fact, OpenVAS is so good like Nessus, Retina or any other famous scanner, and learn it is an easy mission.

Whereas there’re some details about OpenVAS configuration, it follows a quick start procedure to configure OpenVAS and use it a.s.a.p. on Kali Linux 1.5.

Logged in Kali Linux as root user, type:

```
root@hacker:~# openvas-mkcrt -f
root@hacker:~# openvas-mkcrt-client -n om -i
```

(The next command is going to require you enter a password)

```
root@hacker:~# openvasad -c 'add_user' -n admin_linuxmagazine -r Admin
```

(These next two steps could take a long time)

```
root@hacker:~# openvas-nvt-sync
root@hacker:~# openvassd
```

(Onward)

```
root@hacker:~# openvasmd --rebuild
root@hacker:~# openvasmd -p 9390 -a 127.0.0.1
root@hacker:~# openvasad -a 127.0.0.1 -p 9393
root@hacker:~# gsad --http-only --listen=127.0.0.1 -p 5555
root@hacker:~# /etc/init.d/openvas-administrator restart
```

Restarting OpenVAS Administrator: openvasad.

```
root@hacker:~# /etc/init.d/openvas-manager restart
```

Restarting OpenVAS Manager: openvasmd.

Now, you must open a browser and go to: [http://localhost:5555](http://localhost:5555). If everything happens ok, you should see the following screen shown in the Figure 1:
This screen requires you enter an administrative user in username (**admin_linuxmagazine**) and the password that you’ve entered during the OpenVAS configuration steps. After you’ve logged, you should see the screen shown in the **Figure 2**:
At the right side of screen, there’s a textbox where you may to type the IP Address or hostname of the machine that you want to scan for finding vulnerabilities. This case I’ve typed **192.168.1.23** (my Windows XP SP2 machine) and I’ve clicked on **Start Scan**. You should see the screen shown in the **Figure 3**:
Under the **Name** column, the reader sees “Immediate scan of IP Address 192.168.1.23” which is a link to our scanning task. Clicking on this link bring us to next screen as shown in the **Figure 4**:
The Windows XP SP2 host was scanned by OpenVAS which has found several potential vulnerabilities, being five of them classified as High severity, four of them as Medium severity and 15 of them as Low severity. Clicking on magnifying glass at right of screen, you see the screen as shown in the Figure 5:
Finally we can analyze the results and use them for remote exploration through Metasploit framework. As the reader could notice, OpenVAS is an easy and powerful tool that we can use it in any penetration test. In future articles I going to explore the OpenVAS better.

Have a nice day.

Alexandre Borges.