Vulnerability Scanning with OpenVAS

Security Topics

Contents

1 Introduction

In this exercise we will show a popular open source vulnerability scanner called OpenVAS (Open Vulnerability Assessment System). OpenVAS is the evolution of a previous project called Nessus, which became a proprietary tool. The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 20,000 in total (as of January 2011).

2 Goals

- Install OpenVAS server and client packages on Ubuntu
- Update OpenVAS vulnerability tests
- Create a user for scanning
- Learn to run scans in batch mode from the command-line client

3 Notes

- Commands preceded with "$" imply that you should execute the command as a general user - not as root.
- Commands preceded with "#" imply that you should be working as root.
- Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

4 Installation

4.1 Install the server, client and plugin packages

```
$ sudo apt-get install openvas-server openvas-client openvas-plugins-base \
openvas-plugins-dfsg
```

4.2 Update the vulnerability database

```
$ sudo openvas-nvt-sync
```

4.3 Add a user to run the client

```
$ sudo openvas-adduser
Login: sysadm
Authentication (pass/cert) [pass]:  HIT ENTER
Login password: USE CLASS PASSWD
```

You will then be asked to add "User rules".

Ideally, you will want to only allow scanning on hosts that are under your control. To understand the syntax, check the openvas-adduser man page.

Let's allow this user to scan hosts in our lab network. Type:

```
accept 10.10.0./16
default deny
```

type ctrl-D to exit, and then accept.

5 Operation

5.1 Starting the server

```
$ sudo service openvas-server start
```

The server has to load thousands of vulnerability checks, which takes VERY LONG, especially on a machine that is not very powerful. Most likely, you will not be able to run this on the virtual NSRC lab.

On a production setup, you will need a machine with multiple processors/ cores and a quite a bit of RAM, especially if you will be scanning many hosts.

5.2 Running a scan

Create a text file with a list of hosts/networks to scan.

```
$ cd /home/sysadm
$ vi scanme.txt
```

Add one host, network per line, like this:

```
10.10.0.250
10.10.2.5
... etc.
```

Check the manual for the client to understand its parameters:

```
$ man openvas-client
```

Then, run the client like this:

```
$ sudo openvas-client -q 127.0.0.1 9390 sysadm nsrc+ws scanme.txt \
openvas-output-.html -T txt -V -x
```

Alternatively, you can export into prettier HTML format with:

```
$ sudo openvas-client -q 127.0.0.1 9390 sysadm nsrc+ws scanme.txt \
openvas-output.txt -T html -V -x
```

You might have to transfer that file to your laptop so that you can open it with a browser.

5.3 Keeping track of changes

You could take advantage of concurrent versioning systems like Subversion or Git to keep track of changes in the hosts you scan.

- Create a git repository
- Add a cron job to scan hosts periodically (e.g. once a month)
- Use -T txt or -T xml report format
- Update the repository after each run
- Add a post-commit hook on Git to generate e-mails with diffs

—End