Alexander boyd

Sean Kerrigan

Daniel Musalim

Matt Wyant

12/8/19

OpenVas Testing Lab Documentation

This document explains the test plan of the testing lab that our client has asked us to set up. Since our project is mostly setting up a system (not just a piece of software), we have different types of tests. This document will go over the possible tests that can be done on our system.

**System tests:**

**Testing DHCP Server**

To test if the DHCP server is working, we'll use a BASH script that checks the ip address of host machine. The host machine should get an IP from the DHCP server and can be checked with ifconfig. Output of ifconfig will be sent to a text file on the desktop.

**Testing Isolated local network**

To test if the local network is isolated we will use a BASH script that attempts to ping different networks. You should get a reply from internal network but no reply from networks outside of the LAN. Output of these pings will be sent to a text file on the desktop.

**Testing switch**

Testing if the switch can work is pretty straight forward. First check if there link lights on the switch for the port you are connected to. Using ifconfig or ‘ip -a’, you should see an ip address that starts with 192.168. and can ping 192.168.1.1 successfully.

**Testing OpenVas**

This will be a system test that starts out rather shallow but can be made deeper later on. The first part of testing to see if it is working would be to run a scan on the machine that openvas is running on. While it will probably not find anything this will allow you to test if the scan can be run.To test that is able to find vulnerabilities you will need a locally hosted vulnerable website such as OWASP Mutillidae II which can be found here <https://github.com/webpwnized/mutillidae>.

After you install the vulnerable site on a machine plug the machine into the switch and run a scan on it this will test if openvas can see things on the network and see if it can find vulnerabilities.

**Testing maintenance scripts**

-Does the crontab automatically run the scripts?

-Do the scripts work as they are intended to?

**Usability Testing**

User will be able follow the readme file that will be placed on the desktop of the virtual machine. The readme will contain detailed instructions for how to scan your target device. To test this we will have some sample users follow the readme and make sure they can run the system without any other resources. We plan to get both CS students and non-CS students to test as well as the client.

**Stories:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Story | Time required | Risk 0-10(low-High) | Percent comp | Actual time | Notes |
| Student will be able to plug their host device into a switch to join the network | 4 hours | 4 | 90% | 6 hours | Need switch |
| Standards will be set in place that will guide the maintainer in addition of other documentation | 2 hours | 3 | 100% | 1 hour |  |
| Student will be able to follow Documentation to use the tools independently should the CLI fail |  |  |  |  |  |
| Student will be able to use a command line interface to interact with tools and get report | 18 hours | 8 | 0% |  |  |
| Student will be able to print a report to a PDF which will show results of each scan |  | 8 |  |  |  |
| Maintainer will be able to follow documentation to setup a new switch if it fails | 2 hours |  |  |  |  |
| Maintainer will be able to setup Ubuntu server on attack device by following documentation should a hardware failure occur | 4 hours | 3 | 75% |  |  |
| Maintainer will be able to setup the Virtual machine from appliance file by following documentation should a failure occur | 4 hours | 3 | 0% |  |  |
| Maintainer will be able to follow documentation to add a new tool to the suite and CLI |  | 3 |  |  |  |
| Maintainer will be able to follow documentation to update tools / operating system to current version | 3 hours | 3 | 75% |  |  |
| Machine will be hidden from outside networks except for updating | 1 hour | 3 | 90% |  |  |
| Student will be able to join a wireless network via wifi with host machine | 2 hours | 8 | 0% |  | Low priority |

**What can be scanned by OpenVas**

OpenVas can scan a target device on a network for vulnerabilities. This link contains a list of all the network vulnerability tests that openVas can test for <https://secinfo.greenbone.net/nvts> This is a live document and updated by the community regularly.

**Command line interface**

The CLI will be written in python and allow the end user to select their device to scan. If any other tools other than OpenVas are added they will be listed in the CLI as an option to run on target device.