Laboratory Assignment 3:
Vulnerability scanning with OpenVAS

1 Purpose

In this assignment you will use the OpenVAS vulnerability scanning tool to gather information about a system and to assess the security of a system. The purpose of the lab is threefold; 1) to get some hands-on experience with a common vulnerability assessment tool, 2) to learn common signs on insecure practices, and 3) to become a more security aware computer user.

2 Reporting

This assignment is reported by a written lab report that should be submitted through PingPong. The purpose of writing this report is to train your skills in technical writing by describing your task and results from this assignment. Use the report template provided on PingPong available for both LaTeXand Microsoft Word.

Work your way through the lab-pm. When you encounter a paragraph beginning with the text **Assignment** you should do the task. Some useful links to help you are also given in Section 5.

Keep in mind that a detailed description about the structure of the report and the peer-reviewing procedure can be found on PingPong `Content -> Assignments -> Assignment 3 - *`. For the final submission remember that you need to submit a discussion/reflection about your peer's comments including how you improved the report. In case you do not agree with your peer, justify your decision.

3 OpenVAS architecture and lab setup

Note: Before attempting to connect, be sure to read the entire paragraph 4.1.

OpenVAS is a vulnerability scanner. It performs port scans and is able to test a target computer system for more than 29000 vulnerabilities. The OpenVAS architecture consists of two parts; a set of backend services, and clients providing a graphical user interface for interaction with these backend services. The OpenVAS server runs on a separate host and can serve multiple clients simultaneously. More information on the architecture can be found at `http://openvas.org/software.html`.

To use the OpenVAS service, you will need a username and password for connecting to the server. *These will be given by the supervisor at the lab occasion.* The OpenVAS server runs at host `theoden.ce.chalmers.se`.

Figure 1 shows the lab setup. The OpenVAS client (Greenbone Security Assistant) is provided from a webserver. To perform a scan, you should connect to `https://theoden.ce.chalmers.se`. The Greenbone Security Assistant will then manage your requests and send them to the OpenVAS Manager residing on `theoden`, so that you can scan the hosts in the security network.

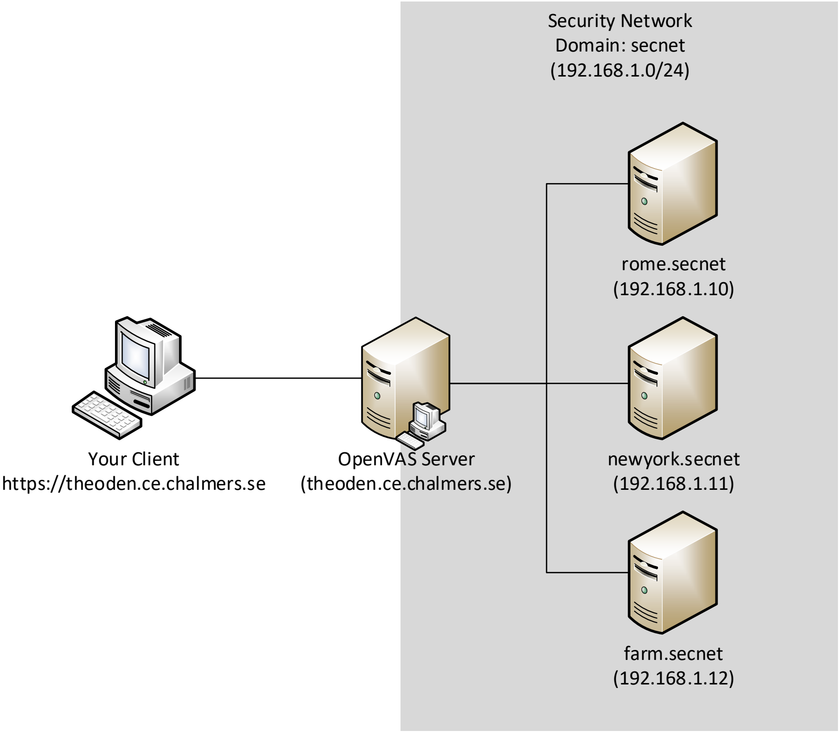


Figure 1: The laboratory network setup

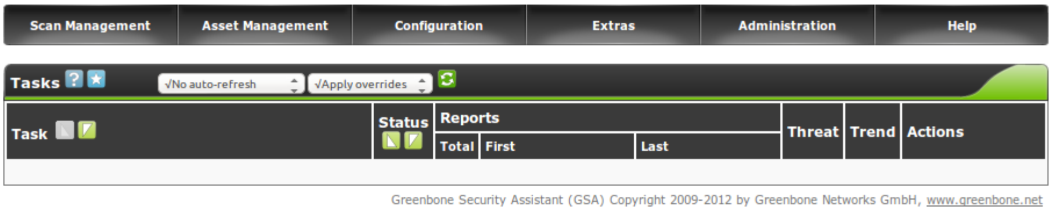
4 Lab assignment

In this lab, you will use the OpenVAS vulnerability scanner to scan a remote computer and assess its security. You will also use your findings to propose how the system can be made more secure. For instructions of how to report your findings, refer to Section 2.

4.1 Step 1: Get to know the OpenVAS client

To connect to the OpenVAS client (Greenbone Security Assistant) you need to open a web browser on the lab computer[1] and enter the server address (`https://theoden.ce.chalmers.se`). Confirm the security exception for the self-signed certificate and then use the credentials received from the lab supervisor to login. When done, the OpenVAS client web page will appear as shown in Figure 2.

[1] You can access the web client only from within the Chalmers network.



Scan Management | Asset Management | Configuration | Extras | Administration | Help

Tasks

√No auto-refresh

√Apply overrides

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			

Greenbone Security Assistant (GSA) Copyright 2009-2012 by Greenbone Networks GmbH, www.greenbone.net

Figure 2: The OpenVAS-Client graphical user interface as seen when the web page is loaded.

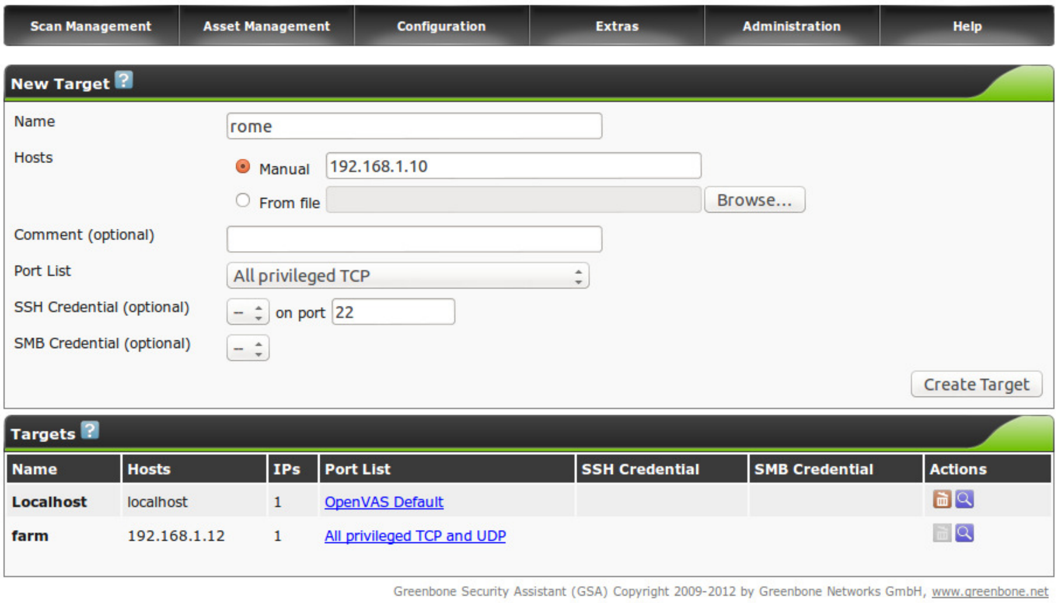
You should now get to know the OpenVAS client a little better. Take a moment and familiarize yourself with the OpenVAS client and its functionality. Refer to the Help section each time you are in doubt about a functionality. Also, each section has a small **blue question mark icons** next to the section name. You can click these icons to quickly check the help records for that specific section. To go back, you can click *Jump to dialog* in the top right side of the help page.

In order to see changes in the client you need to **refresh** it by clicking on the green refresh button on the Tasks pane or by pressing F5 on your keyboard. To set up an automatic refresh interval you can change "No auto-refresh" to "Refresh every N seconds." from the drop-down menu.

To create a new task you will need a target and a scan configuration. To **add a new target** go to Configuration->Targets. You will get a web page similar with the one in Figure 3 . Enter a name for the new target, an IP address in the "Manual" field and select a preconfigured port list from the drop down menu. When you are finished click on "Create Target" button and you will see your newly created target in the Targets list in the lower part of the page.

If you want to **create** your own **port list** for a specific host you can go to Configuration ->Port Lists and create a new port list by using a web form similar with the one for creating a new target.

In order to see the current **scan configuration profiles** or create a new one, go to Configuration->Scan Configs. To inspect a scan configuration profile, click the magnifying glass icon in the Actions tab in the right of its name. In the new window you will see the Network Vulnerabilities Test (NVT) families and the number of selected vulnerabilities from each family. You can also inspect the individual NVTs from each family by clicking the Details icon (magnifying glass icon) next to each.
Finally to **create a new task** go to Scan Management -> New task, enter a name for your scan, select a "Scan Config" from the drop-down list and a target for your task from the "Scan Targets" drop down menu. Click "Create Task" and you will return to the Tasks list page. Here you can see your newly created tasks and later on, your older ones. To start the new created task, click the green play button as shown in Figure 4. You can see the current task's status under the Status tab (don't forget to refresh the page or set the automatic refresh). After the task is completed, you can see the results



New Target

Name	rome
Hosts	● Manual 192.168.1.10 ○ From file
Comment (optional)	
Port List	All privileged TCP
SSH Credential (optional)	-- on port 22
SMB Credential (optional)	--

Targets

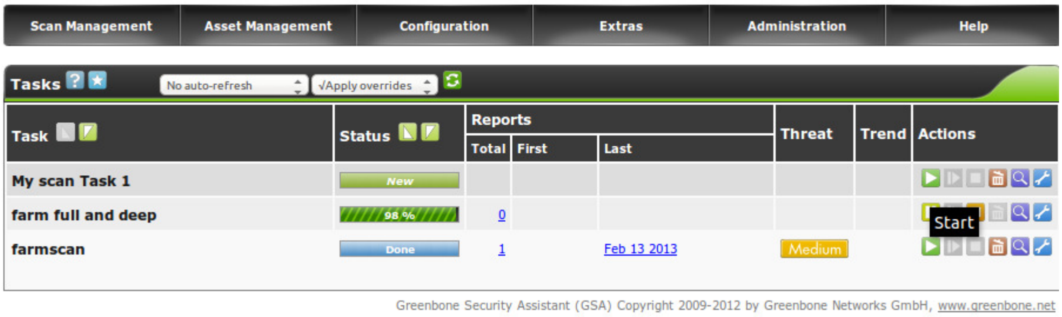
Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions
Localhost	localhost	1	OpenVAS Default			
farm	192.168.1.12	1	All privileged TCP and UDP			

Greenbone Security Assistant (GSA) Copyright 2009-2012 by Greenbone Networks GmbH, www.greenbone.net

Figure 3: The web page for creating a new target.

and/or download a report in different formats by clicking the `Details` icon (magnifying glass icon) and going to the `Report` section.

Note: Please refer to this section or to the help menu when doing the following tasks. If you get stuck, ask for help from one of the lab supervisors.



Tasks

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
My scan Task 1	New						
farm full and deep	98 %	0					
farmscan	Done	1		Feb 13 2013	Medium		

Greenbone Security Assistant (GSA) Copyright 2009-2012 by Greenbone Networks GmbH, www.greenbone.net

Figure 4: The Tasks list page.

4.2 Step 2. Port scanning

A running network service that serves incoming requests listens to a specific port. A port that a service listens to is considered as being *open*. A common first step in assessing the security of a computer host (as well as mounting an attack) is to figure out which network ports are open.

Prepare OpenVAS to perform a port scan **against one of the target host**, i.e., rome.secnet, newyork.secnet, or farm.secnet. (You will use this host throughout the rest of this lab.) First, you need to create a new target with the host you want to scan, and the port list. Then, you need to create a new scan config, **which uses only the "port scanners" NVT and set the configuration of "auto_enable_dependencies = no"**. Finally, you need to create a new task to perform the actual scan. When selecting the port list in the definition of the target, choose OpenVAS Default[2]. When you have finished the preparations you can perform the scan.

Note: Do not attempt to scan the full range of ports. Doing this takes a long time and slows down the other groups' scannings as well.

When the scan is complete, OpenVAS saves the report under Details of your Tasks. (The Details are found as a magnifier icon next to the start icon, see Figure 4.)

Assignment 1: Gather information about open ports.
Make a list of <port number/service name> tuples for the ports that you see in the generated report. For each tuple in the list you should describe what the service most probably is used for. To find information you are free to use whatever resource available, such as man pages for the services and the Internet (some useful links are gathered in Section 5). Check particularly if any recommendations are issued against using a specific service or if there is already a more secure successor providing the same functionality. Limit your answers to a few sentences. Based on the information you find, suggest appropriate actions <keep, disable> for each tuple to make the system potentially more secure.

4.3 Step 3. Service fingerprinting

You have gathered information about what ports are open and what services you expect to find behind the ports. The next step is to find out a little bit more about each service.

Regularly performing checks of available resources is important to discover vulnerabilities in services. It is also important to know what resources are currently up and running and whether or not the services conforms to an established security policy. You should use a subset of the available NVTs to gather some more information, i.e. fingerprinting, about the services. Service fingerprinting NVTs in OpenVAS is located in the groups "service detection" and "general". Explore the groups to find appropriate NVTs to use. And remember, sometimes you need to use multiple NVTs to achieve your goal.

Assignment 2: Service fingerprinting.
Try to discover what *versions* of telnet, ftp, ssh, smtp and www that are running on the host you scanned in Assignment 1. Use NVTs from the *service detection* and the *general* groups.

Important: Make sure you set set **"auto_enable_dependencies = no"** in the Scan Config during preparation.

Note: As in real life, it is not certain that a service reveals its version. If you for any service do not find enough information to pinpoint the version of the service, try to

[2] By using the default, OpenVAS will scan a number of well known ports.

enable all NVTs in the general and service detection groups. If you still are unable to find the information, note this in the report.

In addition to vulnerable services, many attacks target certain versions of operating systems. An administrator need to be aware of what computers are active on the network as well as what operating system versions they run. Sometimes this information can be retrieved from the banners displayed by various services. Summing up banner information from different sources can reveal a lot about the host computer.

Assignment 3: Remote host fingerprinting.
Look again at the results from the service fingerprinting and try to gather as much information as possible about the remote computer. Document your findings.

4.4 Step 4: Vulnerability scanning

The next step is to scan the discovered services for potential vulnerabilities. Focus mainly on the telnet, ftp, ssh, smtp and www services for vulnerabilities. You can include other services for which you found vulnerabilities, if you consider them relevant and/or interesting.

Assignment 4: Service vulnerability scanning.
Scan the services for vulnerabilities using a full scan, i.e. enable all Network Vulnerabilities Tests available. Create a new task called "Full system vulnerability scan csecYYY" and enable all NVTs families. The result of the scan is a report containing all vulnerabilities that `OpenVAS` discovered on the scanned system.

Note: A full scan using all NVTs may take some time to finish. Be patient and do not stop the scan before it is finished. *If the scan still takes a painful long time, you may optimize the test by removing some NVTs families that you are quite sure will not hit your target system. For example, from the scans so far, we can conclude that the system is not a Cisco system.*

4.5 Step 5: Assessment and recommendations

Now when you have discovered the potential vulnerabilities you need to follow up your investigation by looking further into what can be done to mitigate or remove the problems. Focus your investigation on the `telnet, ftp, ssh, smtp` and `www` services. You can include also other vulnerabilities found if you consider them relevant and/or interesting. For the found vulnerabilities, OpenVAS provides recommendations as to what needs to be done.

Assignment 5: Assess and improve the security state.
Read the recommendations contained in the vulnerability scan report and give a detailed explanation to what needs to be done to improve the security. Do not forget to support your decisions with facts and recommendations from OpenVAS, such as severity of problem. Compare your recommendations to the recommendations you made in Assignment 1.

Note: If you find out that a service has several vulnerabilities of the same type, e.g.

several buffer overflow vulnerabilities, you should provide a general recommendation rather that doing one recommendation for each vulnerability.

4.6 Step 6: Assessment follow-up

Assignment 6: Propose a strategy for keeping the system secure.
A computer is constantly exposed to various threats. Propose a strategy for keeping a networked computer up to date with security. List a few actions that should be done regularly to keep the computer secure.

5 Useful links

Port numbers, services

- FILE: The file `/etc/services`. File is present on the lab computers.
- URL: `http://www.iana.org/assignments/port-numbers`
- URL: `http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers`
- URL: `http://www.unix.org.ua/orelly/networking/puis/ch17_03.htm`
- TIP: Use keywords like "tcp, port, <portno>" in a browser of your choice.

Vulnerabilities

- URL: `http://www.securityfocus.com`
- URL: `http://www.cve.mitre.org/cve`
- TIP: Browse service vendors' home pages