Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263/DAT641 Computer Security

Lluís Ripoll
Olle Svensson

Group 45

Version no: 1.0

February 19, 2017

Contents

1 Introduction

In this assignment we used the OpenVAS vulnerability scanning tool to gather information about and to assess the security of a system (remote computer) used for the identification and correction of security flaws. Vulnerability Assessment is a technique used to evaluate resources and assets present in a company. This type of audit is based on the identification of open ports, available services and from this the detection of possible failures present in the target systems. The purpose is to know what vulnerabilities exist in a company's systems and thereby develop an appropriate action plan. In this way, a security assessment can be carried out on the systems of an organisation in order to increase security in them. In addition to this activity, there are other concerns, so it is necessary to complement it with security solutions, such as those against malicious code, firewalls, intrusion detection tools and good security policies contribute to the protection of asset and the combination of different approaches to security. First of all we had to get familiar with how OpenVas works (interface as well) and try to understand the framework and it's different options and parameters. Then it comes the analysis part, because is really important to understand the different vulnerabilities that a system can has as well as find a way to solve them making the system more secure.

2 Description of OpenVAS Setup

OpenVAS Is a framework that offers services and tools that provide a complete and powerful solution for vulnerability scanning and vulnerability management as well as it allow us to identify different security risks in a system (not only scan ports). So the main aim of OpenVAS is to assert a system (vulnerability identification). At the same time it allows us to make several types of reports on detected vulnerabilities and to propose associated solutions. In relation with the architecture, OpenVAS consists in the client part (OpenVAS CLI command line/Greenbone assistant) that interacts with two services called OpenVAS scanner (core) and OpenVAS management (back-end part). The first one performs tasks related with classification/filtering of the scanned results, database control and user administration. On the other hand the OpenVAS scanner executes the NVT (Network Vulnerability Test) conformed by routines that check known vulnerabilities into the system.

In figure 1, the network setup is described as clients connecting to the OpenVAS server (*theoden.ce.chalmers.se* and in our case in a remote way SSH) via the client Greenbone that manages the requests and send them to the OpenVAS Manager in order to scan the hosts. In this case the network contains 3 hosts (this report is based on scans of *rome.secnet*).

Scanning methods allow to detection and handling of known security problems, can help identify rogue machines on the network and provide useful information about the devices that can be useful in security management and tracking. There are different types of vulnerability scanning such as network-based that scans a number of hosts on the network (port scanners, web application scanners) and host- based scanners where the same host is scanned.

The scanning results tell us the results of the prioritised vulnerabilities (high, medium, low) according to the impact on the system and the total amount for each category. In our case we made a scan against the target host *rome.secnet* and no vulnerabilities have been found. Once the scan has finished one vulnerability assessment report is available giving us useful information. It contains the results of the executed plugins associated with the corresponding subnet, host, port and severity.

To perform as scan using OpenVAS, a new target has to be created by clicking on Configuration/add a new target. Once there, some fields have to be filled (Name, host IP, port list). After, is it necessary to generate a new task clicking on scan management/new task for the execution of the analysis and evaluation. Finally the task must be executed and a report with the results is generated.

Depending on your needs and your budget there are a number of different well known vulnerability scanners available. Furthermore, multiple options are available depending on the type of system to be tested. For example scanning all ports in many cases takes too long. Many ports are normally not being used. For most scans it is often enough to scan the ports registered with the IANA.

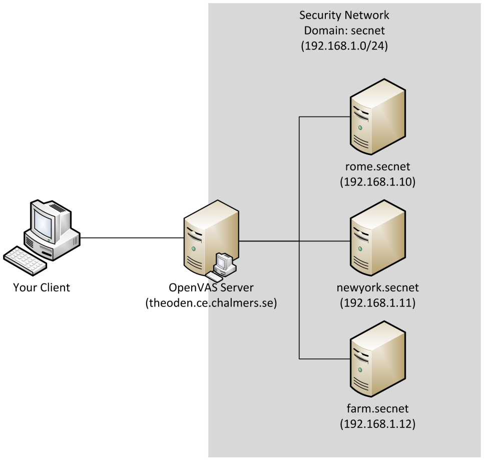

Figure 1: The laboratory network setup

3 Results

3.1 Port Scanning

A port is a logical construct that identifies a specific process or a type of network service. The port scan that we performed used the scan config port scanners. The ports mentioned in the report (open ports on the remote system) are known as well-known because they are used by system processes that provide widely used types of network services. Is really important to test all ports in order to achieve security verification and the main reason is that networks ports are the entry points to a machine that is connected to the Internet. A service that listens on a port is able to receive data from a client application, process it and send it back and consequently, malicious clients can take advantage of it.

The scan found 10 open TCP ports in total from the OpenVAS default range of ports. The open ports are used for standard services like mail, web browsing and file and printer sharing. No significant threats, a few minor issues regarding the services *domain*, *microsoft-ds* and *ssh* that could be evaluated further if needed.

3.2 Fingerprinting

3.2.1 Services

The scan was unable to retrieve any version information from the targeted services even when extending the range of ports and selecting all available NVT's in the categories General and Service Detection.

The only service information retrieved was from the DNS server which is an open-source variant called BIND 'NAMED' running on version 9.7.0-P1.

3.2.2 Remote Host

As with services, the scan was unable to retrieve any information regarding the host operating system or architecture.

3.3 Vulnerability Scan

The scan found a total of 7 high threats and 14 medium threats. All high threats are related to outdated versions of Apache and OpenSSL applications. The majority of the medium threats are related to outdated versions as well. Remaining errors consists of two configuration issues and a expired certificate.

Table 1: Information about open ports

Port Number	Service Name	Service Task	Suggestions
53	domain	Used for DNS services.	Could expose a list of all computers connected to the internal network through a *zone transfer* request. If this is considered sensitive information, incoming TCP requests on this port should be blocked.
80	http	Used for sending and receiving HTTP-requests.	Should remain open if the network is to support the usage of web browsers.
8080	http-alt	Alternative port for offering web services through HTTP.	Mostly used for hosting web services when port 80 is unavailable. The port could be closed if it is not used for this purpose.
143	imap	Used to retrieve mail from remote mail servers.	Should be kept open if the network wishes to support mail clients.
993	imaps	IMAP over SSL.	Should be kept open if the network wishes to support mail clients.
445	mircosoft-ds	Used for Windows file sharing and numerous other services.	Used by the SMB protocol which has had multiple vulnerabilities in the past. Should be closed if not needed. If needed, make sure that the services using it support secure authentication protocols.
139	netbios-ssn	A protocol used for file and print sharing under all current versions of Windows.	Should remain open if the network wants to support file and print sharing.
110	pop3	Used by mail clients for retrieval of mail from designated mail servers.	Keep open to support mail clients or servers.
995	pop3s	POP3 over SSL.	Keep open to support mail clients or servers.
22	ssh	Used for the SSH remote login protocol.	SSH has contained vulnerabilities in the past. Close if SSH access is not needed.

Table 2: Service fingerprint

Service	**Version**
Telnet	*unknown*
FTP	*unknown*
SSH	*unknown*
SMTP	*unknown*
WWW	*unknown*

4 Discussion

The scanning of ports did not reveal anything out of the order. However the applications using the open ports and services contain multiple security issues. As mentioned in Table 1, if these services are not needed, they should be closed to avoid the issues altogether. If the applications and services are to remain, the common solution for the majority of them is to update the software to the latest version. Since multiple vulnerabilities were considered as high risk, whatever decision the company decides to make should be done as soon as possible.

Table 3: Summary of vulnerability scan recommendations

Service Name	**Problems**	**Suggestions**
http, http-alt	Outdated versions of Apache, Apache HTTP Server and Apache Tomcat. Enables multiple security vulnerabilities. Existing example files could expose version information.	Update to latest version and remove example files.
imap, imaps, pop3, pop3s	Outdated version of OpenSSL. Enables man in the middle security bypass.	Updated to latest version.
tcp	TCP timestamps could possibly expose system uptime.	Disable TCP timestamps.
netbio-ssn	Outaded version of Samba which enables denial-of-service vulnerabilities.	Update to latest version.
imaps, pop3s	The SSL certificate has expired.	Renew the certificate.
ssh	Outdated version.	Update to latest version.

5 Conclusion

Even though the current system contains multiple security threats, these could be easily fixed and avoided by applying a basic security policy. Most importantly, the company should introduce regular checks to ensure that the software running on their server is up to date. Second, they should introduce a regular task to renew their SSL certificate to make sure that it does not expire. If possible, the company should perform regular vulnerability checks as well to find any new threats that might be introduced when making new configurations on the server.

By applying this simple policy, the company should retain decent protection against common vulnerabilities and attacks.