Vulnerability Scanning with OpenVAS

Laboratory report in
EDA263/DIT641 Computer Security

Arun Prakash Jothimani
Michel De Carvalho Folkemark

Group Number: 20

Chalmers University of Technology
Gothenburg, Sweden 2015
Version no.: 1.0

Table of Contents

1. Introduction

Today, the world is facing a technology revolution. The internet has reached nooks and corners of the country. It becomes very common for anyone to utilize the resources online and data is playing a crucial role in most of the business today. As the plenty of data are transferred over internet, there is always a risk factor of getting hacked. Nowadays success of any business depends upon the fact, how secure they provide the service to the consumers.

Irrespective of the size of the business, revenue, type of product, etc.. Its highly recommended to keep the system secure so that we can feel safe from the hands of intruders who may break in anytime and may do irreversible damage to the company's assets and reputation. With our powerful and more advanced security tools we have generated a vulnerability assessment report for Travel Biscuit AB, thus we want to make the system safe well in advance before any intruder find the loopholes. The vulnerability assessment exposed the potential pitfalls in the server system.

In this report the details of a vulnerability scan on the host farm(192.168.1.12) will be presented. The main purpose of this assessment is to expose the security pitfalls in the current system and to recommend the security measures to be undertaken to enable a highest possible security to the system.

The report structure is as follows:
Section 2 is all about the description of the OpenVAS in general and under some specific configuration. Section 3 holds all the results. Section 4 includes the discussion over the observed results. Section 5 is the conclusion for the report.

The report will really help Travel Biscuit AB to improve their security, thus enabling a better prospects for their business.

2. Description of OpenVAS setup

OpenVAS is a full-featured vulnerability scanner primarily used for vulnerability scanning and vulnerability management. It is also employed in penetration testing.

OpenVAS comprises of different components each in charge of different aspect of vulnerability scanning. OpenVAS manager receives tasks from the administrator through the client components and controls OpenVAS Scanner to performs actual vulnerability assessment against specified targets. The OpenVAS Administration component facilitates the admins in user creation, assigning privileges and NVTs feed management.

OpenVAS is installed on an intermediate server between the target and our client machine. Here, the scan in done against the target Farm. The network setup is represented below via Figure 1.

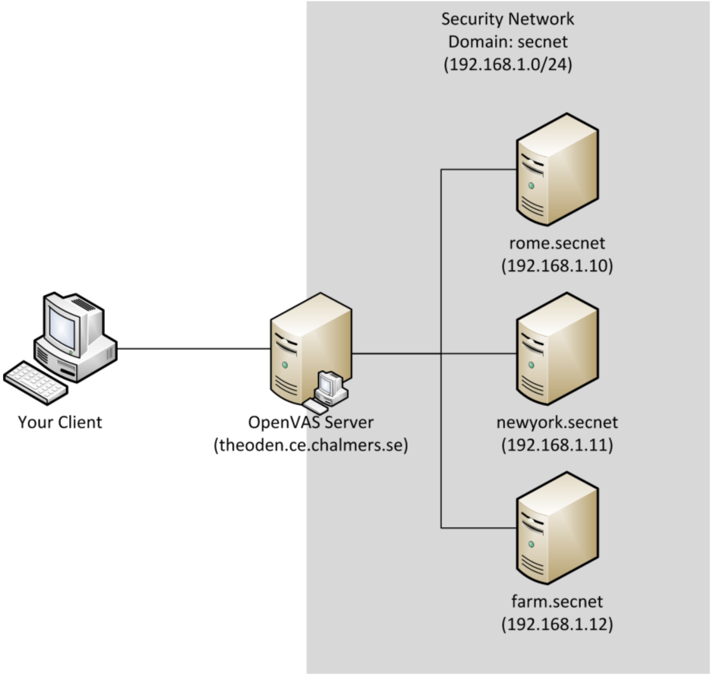


Figure 1: The laboratory network setup

The OpenVAS scan performs a comprehensive security testing over an IP address. Initially, the scan identifies the open services by performing a port scan. After identifying the listening services, the known vulnerabilities and the bad configurations are exposed. There are different types of vulnerability scanning and most significant types are Port Scanning, Network Vulnerability Scanning, Web Application Security Scanning.

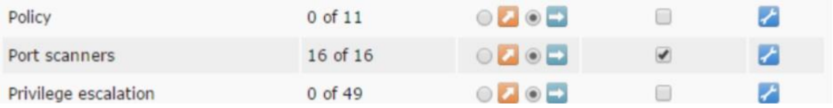
This report has the data based on the information retrieved by the port scan, service fingerprinting and network vulnerability scan. The port scan list the open ports in the host, if any. The fingerprint scan will progress through these open ports and generate a report about the type of services that are behind these ports along with their names and version. The service fingerprinting NVTs are located in the groups “service detection” and “general”, thus they must be checked before running fingerprinting scan. The scan report comprises of information like open ports, services behind the open ports along with the observed security risk behind the ports and services.

To perform different scans in OpenVAS, the user should configure the type of NVTs to be performed via the interface. The user also expected to provide the port range and the targeted network to be scanned. Custom list of ports can be added by navigating to Port Lists page under Configuration

Menu. Sometimes, to have quick results, user could prioritize to scan the most popular ports where the possibility of vulnerability is highly suspected.

2.1 Port scanning

The port scanners are used to generate the report containing the details of open ports on the target. To achieve this, we have to choose the port scanner NVTs during our scan configuration as represented in the figure 2. We can identify the list of open ports that listening the services via the generated report.



Policy	0 of 11	○ ●	☐
Port scanners	16 of 16	○ ●	☑
Privilege escalation	0 of 49	○ ●	☐

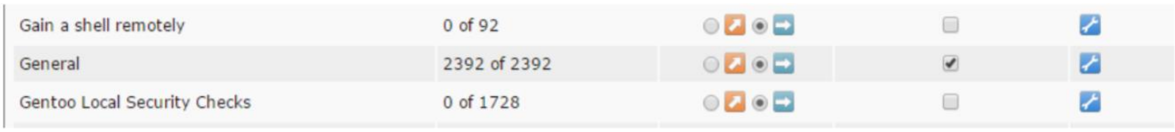
Figure 2 : Port Scanner NVT

2.2 Service fingerprinting

It is always important to audit what services are currently running and to ensure that they comply to the security policy. More detailed data is presented below

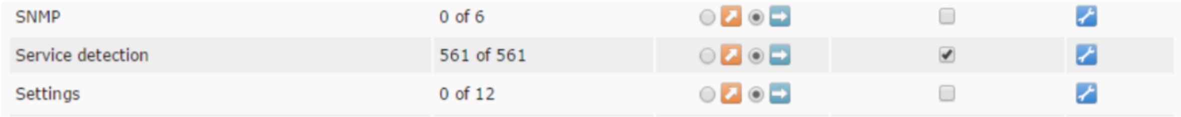
2.2.1 Service fingerprinting

The fingerprint scan will progress through the open ports and generate a report about the type of services that are behind these ports along with their names and version. The service fingerprinting NVTs are in the groups “service detection” and “general”, thus they must be checked before running fingerprinting scan. Sometimes there is requirement to use multiple NVTs to achieve the expected goal.



Gain a shell remotely	0 of 92	○ ●	☐
General	2392 of 2392	○ ●	☑
Gentoo Local Security Checks	0 of 1728	○ ●	☐

Figure 3: General NVT



SNMP	0 of 6	○ ●	☐
Service detection	561 of 561	○ ●	☑
Settings	0 of 12	○ ●	☐

Figure 4: Service Detection NVT

2.2.2 Remote host fingerprinting

Maximum details about the remote host are accumulated from the fingerprinting scan report. The server running in the remote host, time stamp responses and possibility of attacks over the remote host will be generated in the report

2.3 Vulnerability scanning

All the Network Vulnerability Tests were enabled as a part of scan configuration. The scanning task is created with this complete NVT enabled scan configuration against the target and the vulnerability scan is executed

3. Results

Table 1 shows the open ports that were found during the vulnerability scan performed by OpenVAS. There is no vulnerabilities reported on these ports and the services detected are presented in the Table2.

3.1 Port scanning results

The open ports identified during the can are listed in the Table 1. No threats witnessed

Table 1: Information about open ports

Port number	Service name	Service task	Suggestions
53	DNS	Domain Name System	Keep
21	FTP	Data Transfer	Keep
80	HTTP	Web Traffic	Keep
445	Microsoft - DS	Network Access	Keep
139	NetBIOS Session Service	Heavy Data Traffic	Keep
1099	RMI Registry Port	Object Lookup	Keep
514	Shell	Handle Syslog Event Notification	Keep
25	SMTP	Mail Communication	Keep
22	SSH	Secure Data Communication	Keep
23	Telnet	Bidirectional interactive text-oriented communications	Keep

3.2 Fingerprinting results

3.2.1 Service fingerprinting

During fingerprint scan Domain Name System server called bind with the version number 9.4.2 . Apart from that vsftpd server version was noted as 2.3.4. The vsftpd is prone to a backdoor vulnerability thus its recommended to download the repaired package from https://security.appspot.com/vsftpd.html . A number of known default credentials is tried for log in via SSH protocol , its recommended to change the password soon.

Table 2: Service fingerprint

Service	Version
DNS	9.4.2
telnet	Not Found
ftp	vsftpd 2.3.4
ssh	Not Found
smtp	Unknown
www	Not Found

When vulnerability scan is performed, the versions of HTTP,Microsoft-ds, MySQL and PostgreSQL are recorded and displayed in the table 3.

Table 3: Vulnerability Scan Fingerprint

Service	Version
HTTP	Apache 2.2.15
Microsoft-ds	Samba 3.4.5
MySQL	4.0.0
PostgreSQL	8.3.6

The HTTP version is not up to date. Latest HTTP Server version is 2.4.41. Samba is used for Linux interoperability with windows and its version is pretty old dates back to 2010. Samba is prone to a remote denial-of-service vulnerability. Samba 3.4.5 and earlier are vulnerable. Latest Samba version is 4.11.6. MySQL is prone to Multiple format string vulnerabilities and there is a possibility for Denial of Service attack. It is suggested to upgrade MySQL version 5.1.36 or later. PostgreSQL 8.3.6 is prone to an information-disclosure vulnerability. The version must be revisited.

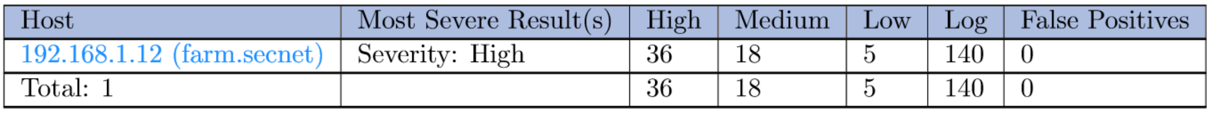
3.2.2 Remote host fingerprinting

Based on the scan report, the operating system of the system is found to be the Linux distribution Ubuntu (Debian 8). The remote host has TFTP server running. In case if not required, its advised to disable it. The remote host responded to an ICMP timestamp request which gives a probability of using this information to exploit weak random number generators in other service.

3.3 Vulnerability scanning results

As reported in 3.2.1, The report has recorded the possibility for few backdoor vulnerabilities, Denial of Service Attack, Multiple format string vulnerabilities, brute force attack, etc and Various recommendations like version upgrade, version repair, password change , etc were briefly suggested in the attached report .

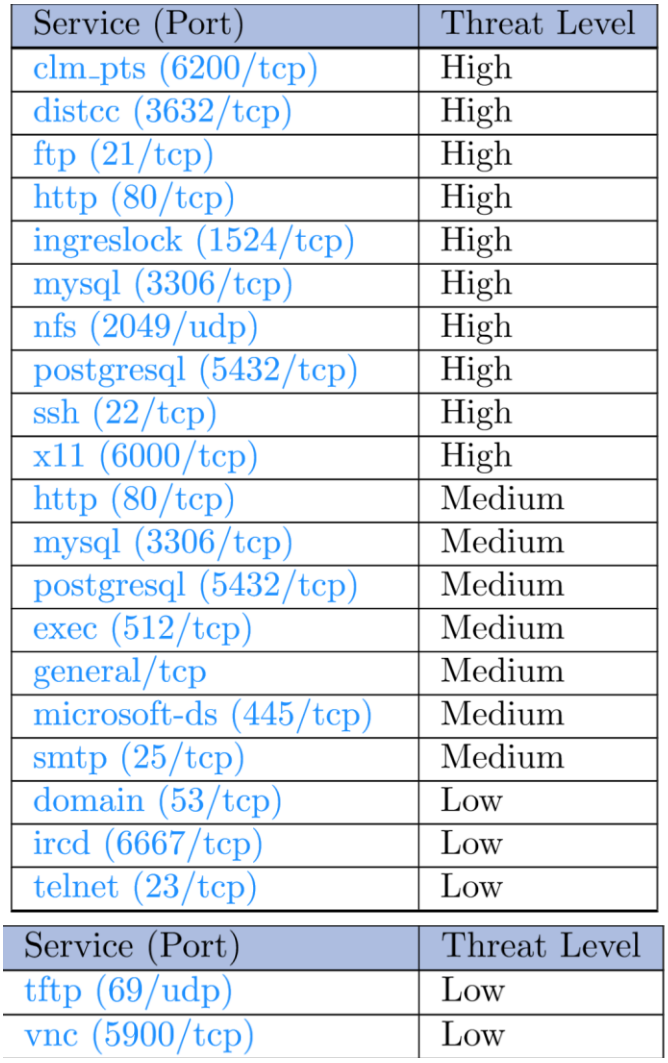
The OpenVAS report has the scan report with threats classified under the categories of High Risk, Medium Risk and Low Risk. To be very specific, total of 36 High Risks, 18 Medium Risks and 5 Low Risks were recorded during the vulnerability scan as represented in the Figure 5



Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.12 (farm.secnet)	Severity: High	36	18	5	140	0
Total: 1		36	18	5	140	0

Figure 5

The OpenSSL, which is used for secure email retrieval were found to be in danger of getting exposed to Man in the Middle Security Bypass Vulnerability. FTP Server allows anonymous logins. If there is no requirement to share files, its recommended to disable anonymous logins. High x11 server does not allow any client to connect to it however it is recommended to filter incoming connections to this port as attacker may send garbage data and slow down the session or even kill the server. The risks associated with ftp, http ,MySQL , PostgreSQL are pretty high as represented in the Figure 6



Service (Port)	Threat Level
clm_pts (6200/tcp)	High
distcc (3632/tcp)	High
ftp (21/tcp)	High
http (80/tcp)	High
ingreslock (1524/tcp)	High
mysql (3306/tcp)	High
nfs (2049/udp)	High
postgresql (5432/tcp)	High
ssh (22/tcp)	High
x11 (6000/tcp)	High
http (80/tcp)	Medium
mysql (3306/tcp)	Medium
postgresql (5432/tcp)	Medium
exec (512/tcp)	Medium
general/tcp	Medium
microsoft-ds (445/tcp)	Medium
smtp (25/tcp)	Medium
domain (53/tcp)	Low
ircd (6667/tcp)	Low
telnet (23/tcp)	Low
tftp (69/udp)	Low
vnc (5900/tcp)	Low

Figure 6 : Full Vulnerability Scan Report

4. Discussion

The port scan and finger printing scan yielded very minimal results which shows the low probability of risk in the scanned areas. The basic entry points are safe, and no major actions required there. It portrays the fact that, no uncommon ports are in use.

During fingerprint scan, only the issue observed was with DNS server version and its great to have a minimal vulnerability here.

The full vulnerability scan reported too many risks which exposed the greatest risks of the system. Total of 36 High Risks, 18 Medium Risks and 5 Low Risks were recorded during this scan. The report has recorded the possibility for backdoor vulnerabilities, Denial of Service Attack, Multiple format string vulnerabilities, brute force attack and Various recommendations like version upgrade, version repair, password change, etc. were given to overcome the risks.

Table 3: Summary of vulnerability scan recommendations

Service name	**Problems**	**Suggestions**
HTTP	Outdated	Software Update
Microsoft-ds	Outdated	Software Update
MySQL	Outdated	Software Update
PostgreSQL	Outdated	Software Update
Samba 3.4.5	Outdated	Software Update

5. Conclusions

OpenVAS exposed the vulnerabilities of the system and based on the report we received we conclude that the host farm is not sure. The major security issues are due to the outdated software.

Our first recommendation is to keep the software of the system updated and create a regular routine to audit the same. Avoid using default credentials. If there is no requirement for file sharing, disable anonymous logins. Filter the data coming to x11 server to avoid any garbage input. Final recommendation is to keep the Operating system updated as and when the upgrades are released.

References

[1] OpenVAS. *About OpenVAS*. URL:https://www.openvas.org/

[2] Wikipedia. *Vulnerability Scanner*. URL: https://en.wikipedia.org/wiki/Vulnerability_scanner

[3] Apache. *Apache HTTP Server project*. URL: https://httpd.apache.org/download.cgi

[4]Samba. *Samba Versions*. URL: https://www.samba.org/samba/history/

Appendix: OpenVAS Vulnerability scan report