ITIS 6010
Parag Mhatre
801073873

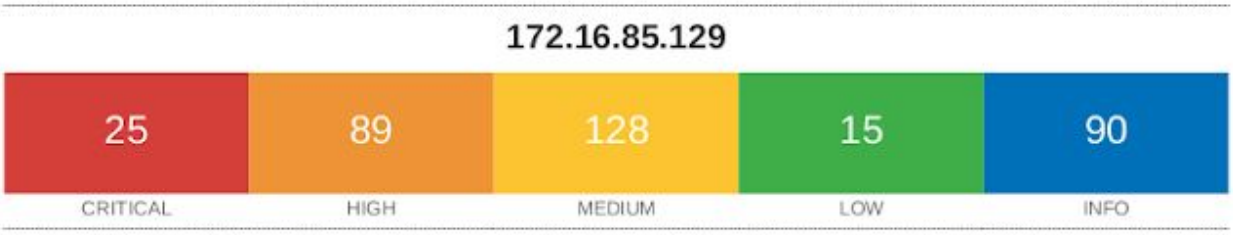
Vulnerability Scanning

1. Nessus

I used Nessus to perform the two mentioned scans, one without credentials and another with credentials. The results of both the scans are very different. The network scan got 98 vulnerabilities in total while the credentialed scan found 347 vulnerabilities as shown in the screenshot below.

1. Basic Network Scan

2. Basic Network Scan with root credentials



To perform the credentialed scan, I had to give the scanner a username and password which Nessus used to ssh into the machine that was being scanned. This tells us that more vulnerabilities can be found from the inside.

One more thing that I found was, if the credentials given to Nessus are of a unprivileged user, then Nessus manges to detect less vulnerabilities. The credentials that I used were “user” and “user”. Instead of Nessus detecting direct vulnerabilities, it detected more Information leakages when it didn’t have root access on the machine.

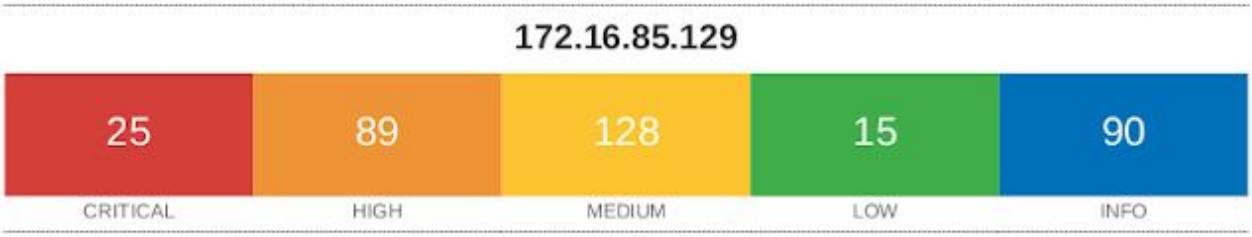
Thus, the Basic Network scan found out vulnerabilities like the “Debian OpenSSH/OpenSSL Package Random Number Generator Weakness” relating to a bug in random number generator of its OpenSSL libraries in Ubuntu and Debian machines.

It also found other vulnerabilities like Weak VNC password - “password”, etc. Nessus also assigns CVSS score to the vulnerabilities.

Vulnerabilities Total: 98

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	12085	Apache Tomcat Default Files
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	42256	NFS Shares World Readable

On the contrary, a scan with credentials enabled Nessus to find vulnerabilities like “Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)” which relates to one or more Security patches not being installed. Such information can usually be obtained from the inside.



Vulnerabilities Total: 347

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	78385	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)
CRITICAL	10.0	77823	Bash Remote Code Execution (Shellshock)
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	32432	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)
CRITICAL	10.0	37936	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)
CRITICAL	10.0	33531	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-625-1)
CRITICAL	10.0	36916	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerabilities (USN-673-1)
CRITICAL	10.0	36454	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linux vulnerabilities (USN-714-1)
CRITICAL	10.0	44399	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-894-1)
CRITICAL	10.0	39800	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)
CRITICAL	10.0	40576	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerabilities (USN-815-1)
CRITICAL	10.0	37762	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : apt vulnerabilities (USN-762-1)

2. OpenVAS

The OpenVAS website defines OpenVAS as

“OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low level Internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner is accompanied by a vulnerability tests feed with a long history and daily updates. This Greenbone Community Feed includes more than 50,000 vulnerability tests.
The scanner is developed and maintained by Greenbone Networks since 2009. The works are contributed as Open Source to the community under the GNU General Public License (GNU GPL).
Greenbone develops OpenVAS as part of their commercial vulnerability management product family "Greenbone Security Manager" (GSM). OpenVAS is one element in a larger architecture. In combination with additional Open Source modules, it forms the Greenbone Vulnerability Management solution. Based on this, the GSM appliances use a more extensive feed covering enterprise needs, a GVM with adnal features, appliance management and a service level agreement.”

OpenVAS is a fork of the Nessus project. But unlike Nessus, OpenVAS is open source and completely free of charge and is standard in Kali Linux. In my opinion, Nessus has a more professional feel to it and along with showing vulnerabilities, and the reports The scanning results in both the scanners are somewhat different than each other.

I scanned the same system with OpenVAS to get the following results without any vulnerabilities.

Host	High	Medium	Low	Log	False Positive
172.16.85.129	15	34	2	0	0
Total: 1	15	34	2	0	0

This scan was performed without providing any credentials. I can say that at least in this scenario, OpenVAS found more vulnerabilities than Nessus could find. A detailed Screenshot of the report is shown on the page below.

One of the big differences that I saw is that OpenVAC tried brute forcing SSH connections and found out the username and password as “user” and “user”. Nessus didn’t find the credentials which are pretty easy to bruteforce, meaning it didn’t try brute forcing the system.

... (continued) ...

Service (Port)	Threat Level
8787/tcp	High
2121/tcp	Medium
22/tcp	Medium
5900/tcp	Medium
21/tcp	Medium
80/tcp	Medium
6667/tcp	Medium
5432/tcp	Medium
25/tcp	Medium
22/tcp	Low
80/tcp	Low

2.1.1 High 22/tcp

High (CVSS: 7.5)

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
It was possible to login with the following credentials <User>:<Password>
user:user

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via the SSH protocol.
Details: SSH Brute Force Logins With Default Credentials Reporting
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: $Revision: 13568 $

[return to 172.16.85.129]

Nessus VS OpenVAS:

Parameter	Nessus	OpenVAS
Open source	No (Proprietary)	Yes
Free	No	Yes
Network Monitoring	Yes	No
Asset Discovery	Yes	Yes
Asset Tagging	No	Yes
Network Scanning	Yes	Yes
Policy Management	Yes	No
Risk Management	No	Yes
Support	Available	No
Platforms	Win, Mac, Linux, BSD	Windows, Linux
Report Export	Yes	Yes
Solutions to vulnerabilities	Yes	Yes
Official documentation	Yes	No
Would I use this?	Yes, I would use both	Yes, I would use both

3. Other tools

1. Nmap

Nmap is a open source network scanner that started for Linux and was later ported to other operating systems that is primarily used to discover hosts and services on a computer network. Nmap does this by sending various types of specially crafted packets and analyzing the responses.
Primary features of Nmap include Host discovery and port scanning. Nmap can do some additional tasks like OS fingerprinting and version detection.

In contrast with Nessus and OpenVAS, the functionality of Nmap is a subset of the functionality of Nessus/OpenVAS. Nessus/OpenVAS already does network scanning as a part of vulnerability analysis.

2. SQL Map

SQLmap, just like nmap for network scanning is a tool used to automate detection and exploiting SQL injection flaws. It is a open source tool and is very handy for a penetration tester. It also performs tasks like database fingerprinting, data fetching from the database, access the underlying file system and execute commands on the operating system via out-of-band connections.

The functionality of detection of SQL injection flaws is a subset of Nessus and OpenVAS. The advantage of SQL Map is that it is a exploitation tool, which the previously discussed scanners are not.

3. Oscanner

Oscanner is a tool developed in Java. It is a Oracle based assessment framework and supports plugins with functionality like Sid Enumeration, Password tests, Enumeration of account roles, privileges, hashes, database links, password policies.
The output of Oscanner is shown in a graphical java tree.

In contrast, Nessus and OpenVAS are scanners and can only detect vulnerabilities which can then be exploited or patched while Oscanner is a active exploitation tool used for Enumeration depending on the plugin used for it.