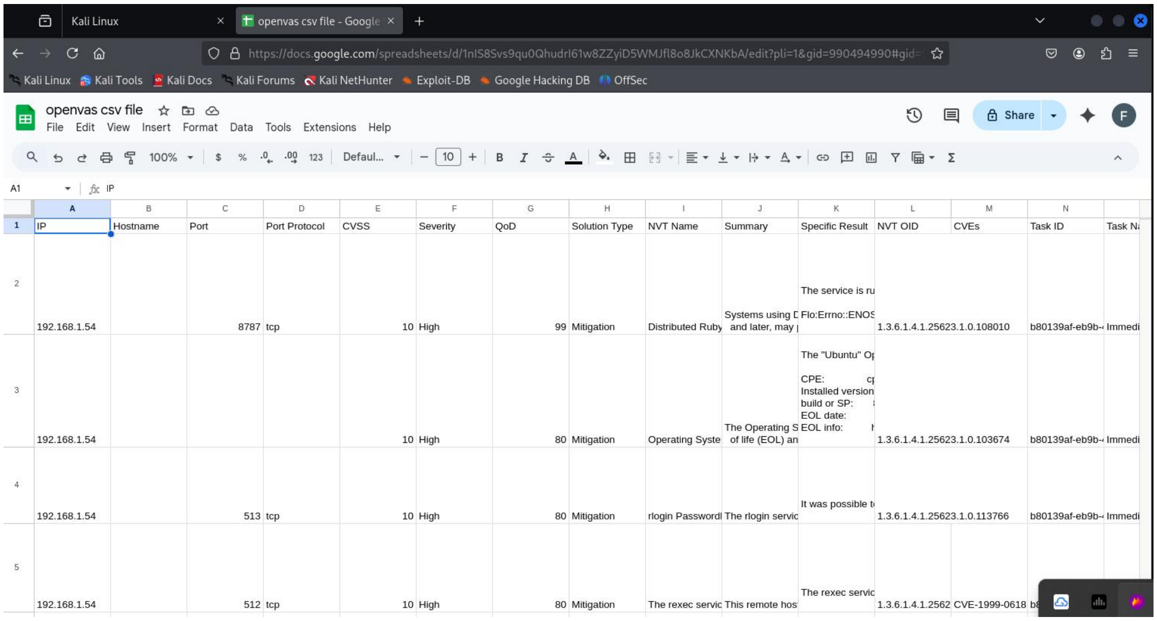
Build a Vulnerability Management Pipeline

1. Objective

Use OpenVAS to scan Metasploitable VM and import results into DefectDojo for vulnerability management.

2. Steps Performed

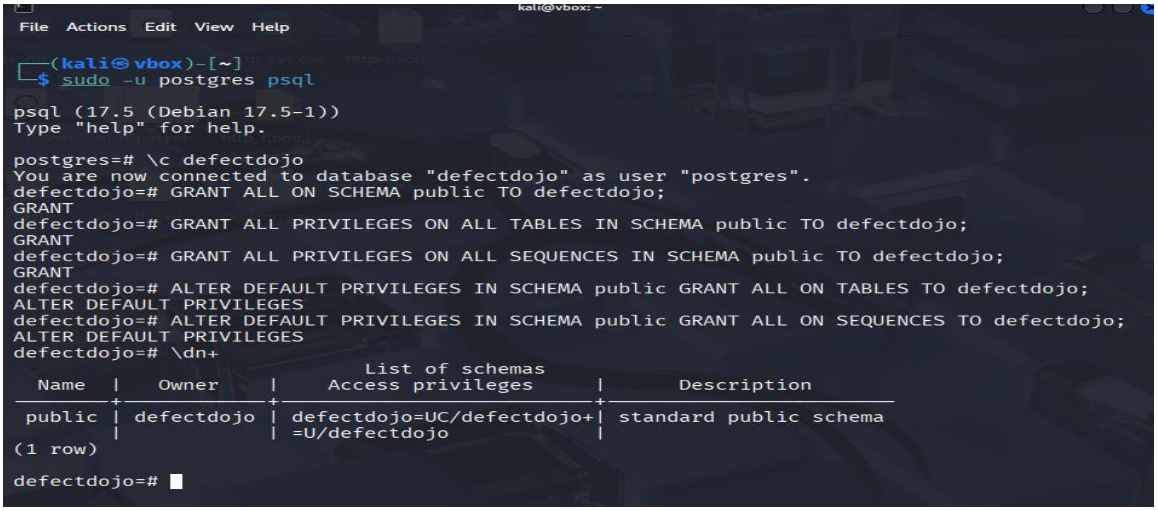
1. Configure and run OpenVAS against Metasploitable2 VM.
2. Export vulnerability results in XML/CSV format.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	IP	Hostname	Port	Port Protocol	CVSS	Severity	QoD	Solution Type	NVT Name	Summary	Specific Result	NVT OID	CVEs	Task ID	Task Na
2	192.168.1.54		8787	tcp	10	High	99	Mitigation	Distributed Ruby	Systems using D and later, may		The service is ru Flo:Errno::ENOS	1.3.6.1.4.1.25623.1.0.108010		b80139af-eb9b-	Immedi
3	192.168.1.54				10	High	80	Mitigation	Operating Syste	The Operating S of life (EOL) an	The "Ubuntu" Op CPE: cp Installed version build or SP: EOL date: EOL info: h	1.3.6.1.4.1.25623.1.0.103674		b80139af-eb9b-	Immedi
4	192.168.1.54		513	tcp	10	High	80	Mitigation	rlogin Password	The rlogin servic	It was possible t	1.3.6.1.4.1.25623.1.0.113766		b80139af-eb9b-	Immedi
5	192.168.1.54		512	tcp	10	High	80	Mitigation	The rexec servic	This remote hos	The rexec servic	1.3.6.1.4.1.2562	CVE-1999-0618	b8	

Figure 1 shows openvas csv file in google sheets

3. Import results into Defect Dojo.



```
┌──(kali㉿vbox)-[~]
└─$ sudo -u postgres psql

psql (17.5 (Debian 17.5-1))
Type "help" for help.

postgres=# \c defectdojo
You are now connected to database "defectdojo" as user "postgres".
defectdojo=# GRANT ALL ON SCHEMA public TO defectdojo;
GRANT
defectdojo=# GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO defectdojo;
GRANT
defectdojo=# GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA public TO defectdojo;
GRANT
defectdojo=# ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON TABLES TO defectdojo;
ALTER DEFAULT PRIVILEGES
defectdojo=# ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON SEQUENCES TO defectdojo;
ALTER DEFAULT PRIVILEGES
defectdojo=# \dn+
                              List of schemas
  Name  |   Owner    |      Access privileges       |      Description
--------+------------+------------------------------+------------------------
 public | defectdojo | defectdojo=UC/defectdojo+| standard public schema
        |            | =U/defectdojo              |
(1 row)

defectdojo=# 
```

Figure 2 shows defect dojo as the owner

4. Identify and prioritize top vulnerabilities.

Vulnerability	CVSS Score	Description
VSFTPD Backdoor	7.5	Backdoor version of VSFTPD 2.3.4 allows remote attackers to gain shell access
UnrealIRCd Backdoor	9.8	Malicious backdoor in UnrealIRCd 3.2.8.1 allows remote code execution
Samba smbd Buffer Overflow	9.3	Heap overflow in Samba (CVE-2007-2447) allows remote attackers to execute arbitrary code