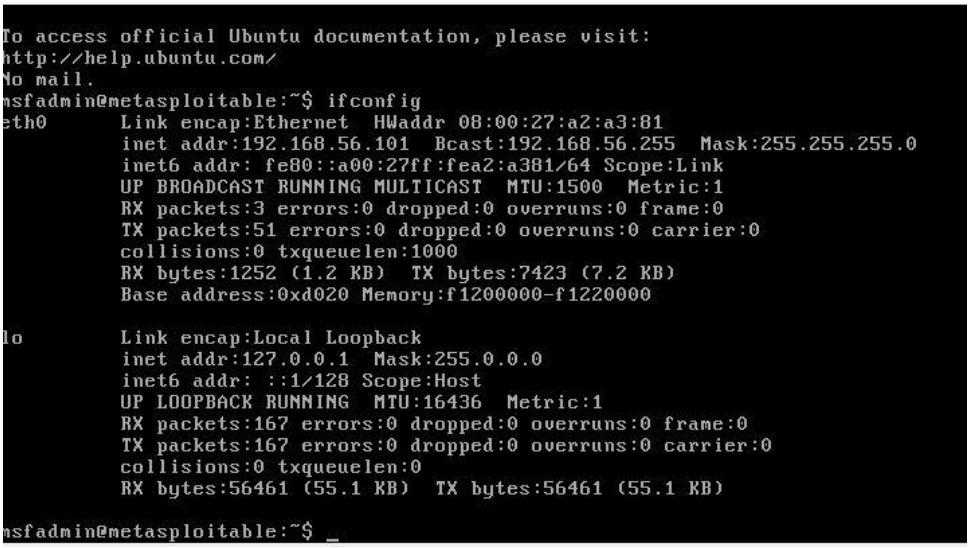
Xuan(James) Zhai

CS3339 Lab

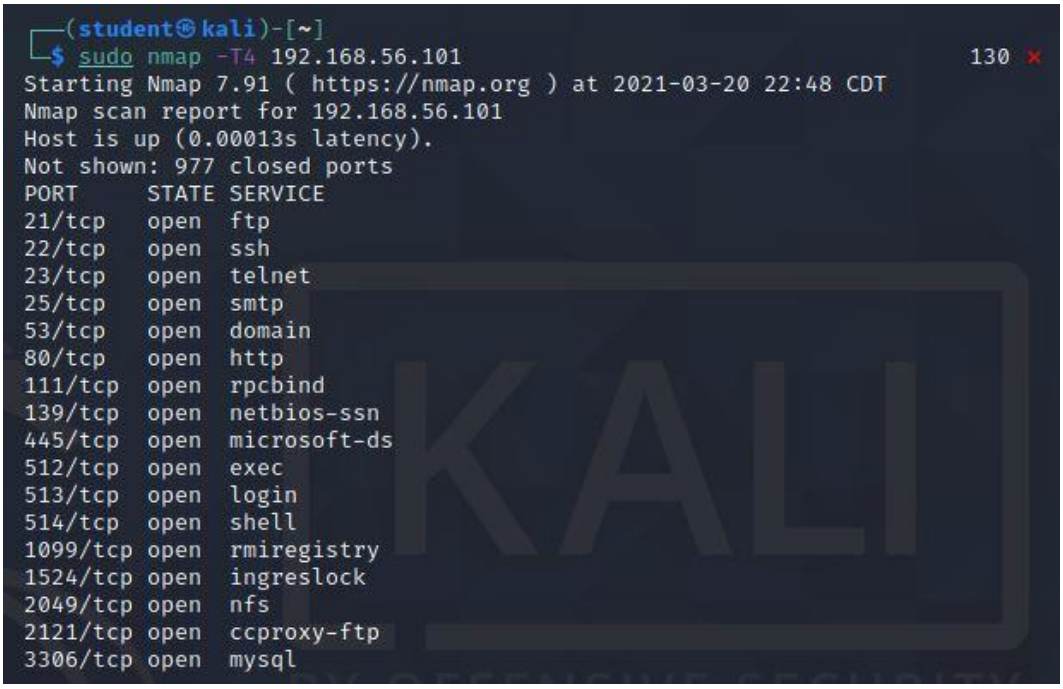
March 26th, 2021

CS 3339 - Lab 5 - Lab Report

1: Use ifconfig to find the IP interface in Metasploitable2



2: Use nmap to find the target machine on that IP interface.



3: OS version detection

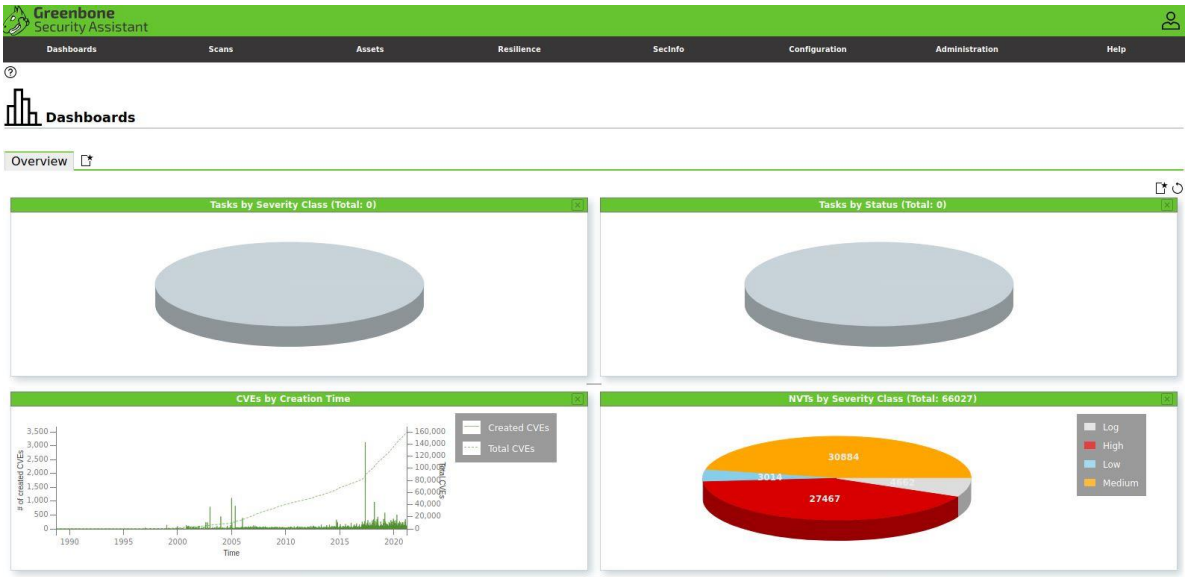
```
MAC Address: 08:00:27:A2:A3:81 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 59m58s, deviation: 2h00m00s, median: -2s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MA
C: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-03-21T00:48:43-04:00
| smb-security-mode:
|   account_used: <blank>
```

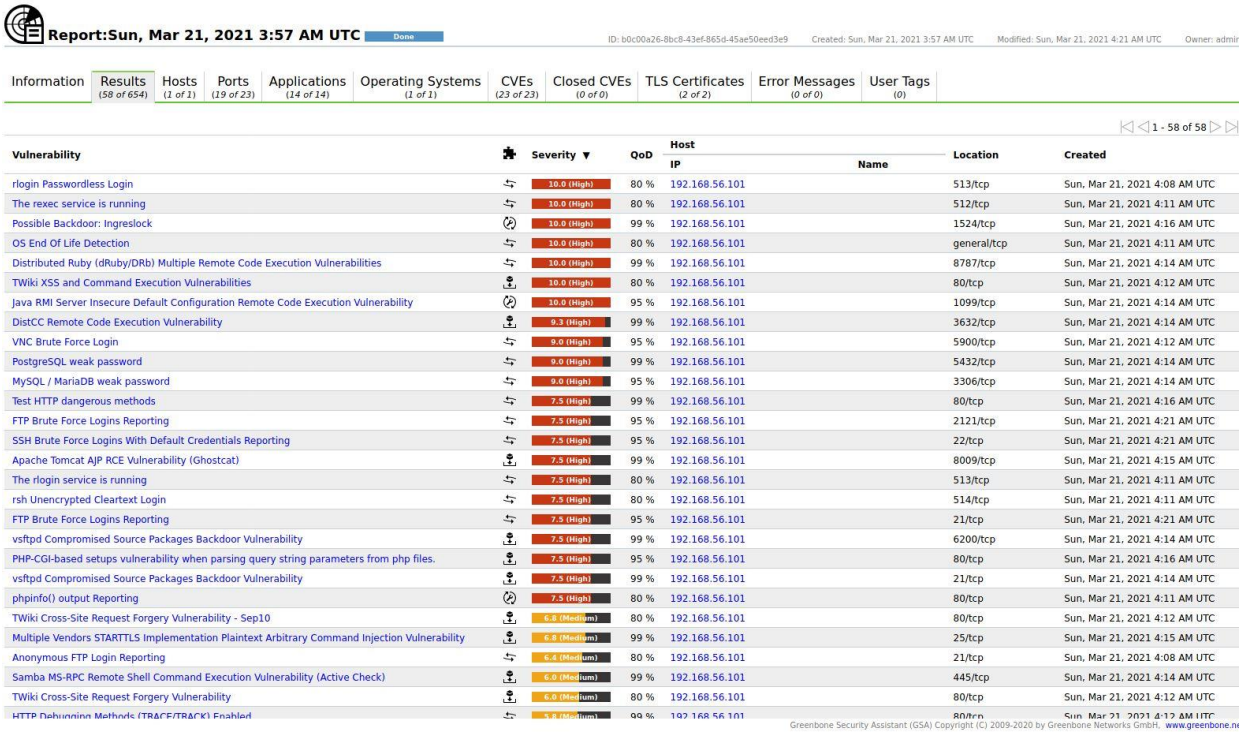
4: Use netstat -antp to check if the OpenVAS manager, and others are listening.

```
┌──(student㉿kali)-[~]
└─$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
      PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
      -
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN
      -
tcp6       0      0 ::1:5432                :::*                    LISTEN
      -
```

4: Start OpenVAS



5: Scan the vulnerability



Report:Sun, Mar 21, 2021 3:57 AM UTC — Done

ID: b0c00a26-8bc8-43ef-865d-45ae50eed3e9 Created: Sun, Mar 21, 2021 3:57 AM UTC Modified: Sun, Mar 21, 2021 4:21 AM UTC Owner: admin

Information | Results (58 of 654) | Hosts (1 of 1) | Ports (19 of 23) | Applications (14 of 14) | Operating Systems (1 of 1) | CVEs (23 of 23) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (0 of 0) | User Tags (0)

1 - 58 of 58

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
rlogin Passwordless Login	10.0 (High)	80 %	192.168.56.101		513/tcp	Sun, Mar 21, 2021 4:08 AM UTC
The rexec service is running	10.0 (High)	80 %	192.168.56.101		512/tcp	Sun, Mar 21, 2021 4:11 AM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.56.101		1524/tcp	Sun, Mar 21, 2021 4:16 AM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.56.101		general/tcp	Sun, Mar 21, 2021 4:11 AM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.56.101		8787/tcp	Sun, Mar 21, 2021 4:14 AM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.56.101		1099/tcp	Sun, Mar 21, 2021 4:14 AM UTC
DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.56.101		3632/tcp	Sun, Mar 21, 2021 4:14 AM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.56.101		5900/tcp	Sun, Mar 21, 2021 4:12 AM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.56.101		5432/tcp	Sun, Mar 21, 2021 4:14 AM UTC
MySQL / MariaDB weak password	9.0 (High)	95 %	192.168.56.101		3306/tcp	Sun, Mar 21, 2021 4:14 AM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:16 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.56.101		2121/tcp	Sun, Mar 21, 2021 4:21 AM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.56.101		22/tcp	Sun, Mar 21, 2021 4:21 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	192.168.56.101		8009/tcp	Sun, Mar 21, 2021 4:15 AM UTC
The rlogin service is running	7.5 (High)	80 %	192.168.56.101		513/tcp	Sun, Mar 21, 2021 4:11 AM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	192.168.56.101		514/tcp	Sun, Mar 21, 2021 4:11 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.56.101		21/tcp	Sun, Mar 21, 2021 4:21 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.56.101		6200/tcp	Sun, Mar 21, 2021 4:14 AM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:16 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.56.101		21/tcp	Sun, Mar 21, 2021 4:14 AM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:11 AM UTC
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99 %	192.168.56.101		25/tcp	Sun, Mar 21, 2021 4:15 AM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.56.101		21/tcp	Sun, Mar 21, 2021 4:08 AM UTC
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0 (Medium)	99 %	192.168.56.101		445/tcp	Sun, Mar 21, 2021 4:14 AM UTC
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC

6: Analysis

There are many vulnerabilities are identified after scanning; the first one is “rlogin Passwordless Login.” The rlogin, or remote login, program was a tool for remotely using a computer over a network. Without a password, an attacker can easily get a remote access to the machine.

There’s another vulnerability called “Possible Backdoor: Ingreslock.” According to the article from Cyber Security Associates, Ingres database is a SQL database that is commonly used to support very large commercial and government applications. As applications become larger there are additional services are added and in the process of developing the Ingres application, it was decided to have port 1524 open. This port links to a service called ingreslock which is meant to lockdown specific areas of the database application. Inadvertently, ingreslock has a backdoor associated with it that automatically binds when a connection is made with this port.

(https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c1cc92588251b338fea2d12/1545390373629/Ingreslock+Vulnerability.pdf) In a word, an attacker can access the locked area of the Ingres database using the backdoor and steal information they need.