

Xuan(James) Zhai

CS3339 Lab

March 26<sup>th</sup>, 2021

## CS 3339 - Lab 5 - Lab Report

1: Use ifconfig to find the IP interface in Metasploitable2

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a2:a3:81
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea2:a381/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1252 (1.2 KB)  TX bytes:7423 (7.2 KB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56461 (55.1 KB)  TX bytes:56461 (55.1 KB)

msfadmin@metasploitable:~$ _
```

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

```
(student@kali)-[~]
$ sudo nmap -T4 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-20 22:48 CDT
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
```

### 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>

```

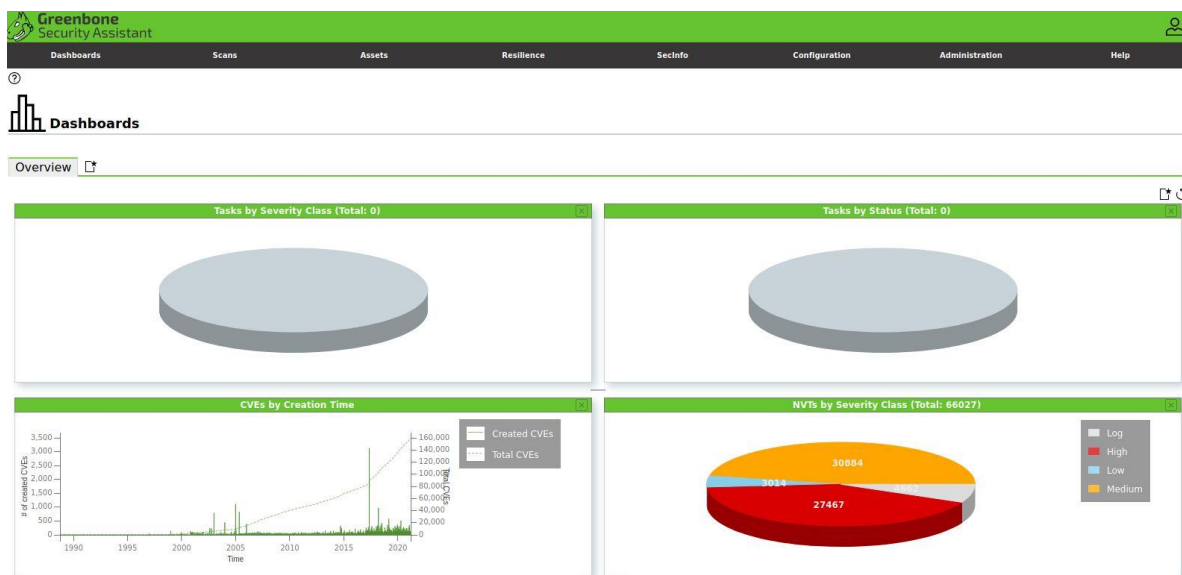
### 4: Use netstat -antp to check if the OpenVAS manager, and others are listening.

```

(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-8654-45ae50eed3e9

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	<div><div></div><div>Severity</div><div></div></div>	QoD	Host IP	Name	Location	Created
rlogin Passwordless Login	<div><div></div><div>10.0 (High)</div><div></div></div>	80 %	192.168.56.101		513/tcp	Sun, Mar 21, 2021 4:08 AM UTC
The rexec service is running	<div><div></div><div>10.0 (High)</div><div></div></div>	80 %	192.168.56.101		512/tcp	Sun, Mar 21, 2021 4:11 AM UTC
Possible Backdoor: Ingreslock	<div><div></div><div>10.0 (High)</div><div></div></div>	99 %	192.168.56.101		1524/tcp	Sun, Mar 21, 2021 4:16 AM UTC
OS End Of Life Detection	<div><div></div><div>10.0 (High)</div><div></div></div>	80 %	192.168.56.101		general/tcp	Sun, Mar 21, 2021 4:11 AM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	<div><div></div><div>10.0 (High)</div><div></div></div>	99 %	192.168.56.101		8787/tcp	Sun, Mar 21, 2021 4:14 AM UTC
Twiki XSS and Command Execution Vulnerabilities	<div><div></div><div>10.0 (High)</div><div></div></div>	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	<div><div></div><div>10.0 (High)</div><div></div></div>	95 %	192.168.56.101		1099/tcp	Sun, Mar 21, 2021 4:14 AM UTC
DistCC Remote Code Execution Vulnerability	<div><div></div><div>9.9 (High)</div><div></div></div>	99 %	192.168.56.101		3632/tcp	Sun, Mar 21, 2021 4:14 AM UTC
VNC Brute Force Login	<div><div></div><div>9.0 (High)</div><div></div></div>	95 %	192.168.56.101		5900/tcp	Sun, Mar 21, 2021 4:12 AM UTC
PostgreSQL weak password	<div><div></div><div>9.0 (High)</div><div></div></div>	99 %	192.168.56.101		5432/tcp	Sun, Mar 21, 2021 4:14 AM UTC
MySQL / MariaDB weak password	<div><div></div><div>9.0 (High)</div><div></div></div>	95 %	192.168.56.101		3306/tcp	Sun, Mar 21, 2021 4:14 AM UTC
Test HTTP dangerous methods	<div><div></div><div>7.5 (High)</div><div></div></div>	99 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:16 AM UTC
FTP Brute Force Logins Reporting	<div><div></div><div>7.5 (High)</div><div></div></div>	95 %	192.168.56.101		2121/tcp	Sun, Mar 21, 2021 4:21 AM UTC
SSH Brute Force Logins With Default Credentials Reporting	<div><div></div><div>7.5 (High)</div><div></div></div>	95 %	192.168.56.101		22/tcp	Sun, Mar 21, 2021 4:21 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	<div><div></div><div>7.5 (High)</div><div></div></div>	99 %	192.168.56.101		8009/tcp	Sun, Mar 21, 2021 4:15 AM UTC
The rlogin service is running	<div><div></div><div>7.5 (High)</div><div></div></div>	80 %	192.168.56.101		513/tcp	Sun, Mar 21, 2021 4:11 AM UTC
rsh Unencrypted Cleartext Login	<div><div></div><div>7.5 (High)</div><div></div></div>	80 %	192.168.56.101		514/tcp	Sun, Mar 21, 2021 4:11 AM UTC
FTP Brute Force Logins Reporting	<div><div></div><div>7.5 (High)</div><div></div></div>	95 %	192.168.56.101		21/tcp	Sun, Mar 21, 2021 4:21 AM UTC
vstftpd Compromised Source Packages Backdoor Vulnerability	<div><div></div><div>7.5 (High)</div><div></div></div>	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.	<div><div></div><div>7.5 (High)</div><div></div></div>	95 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:16 AM UTC
vstftpd Compromised Source Packages Backdoor Vulnerability	<div><div></div><div>7.5 (High)</div><div></div></div>	99 %	192.168.56.101		21/tcp	Sun, Mar 21, 2021 4:14 AM UTC
phpinfo() output Reporting	<div><div></div><div>7.5 (High)</div><div></div></div>	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:11 AM UTC
Twiki Cross-Site Request Forgery Vulnerability - Sep10	<div><div></div><div>6.8 (Medium)</div><div></div></div>	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	<div><div></div><div>6.8 (Medium)</div><div></div></div>	99 %	192.168.56.101		25/tcp	Sun, Mar 21, 2021 4:15 AM UTC
Anonymous FTP Login Reporting	<div><div></div><div>6.8 (Medium)</div><div></div></div>	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)	<div><div></div><div>6.0 (Medium)</div><div></div></div>	99 %	192.168.56.101		445/tcp	Sun, Mar 21, 2021 4:14 AM UTC
Twiki Cross-Site Request Forgery Vulnerability	<div><div></div><div>6.0 (Medium)</div><div></div></div>	80 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:12 AM UTC
HTTP Authentication Methods (TRACE/TRACK) Enabled	<div><div></div><div>5.9 (Medium)</div><div></div></div>	99 %	192.168.56.101		80/tcp	Sun, Mar 21, 2021 4:17 AM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, [www.greenbone.net](#)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH. [www.greenbone.net](https://www.greenbone.net)

## 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.