Description:

This lab focuses on the use of active discovery tools and techniques that can be used to discover valuable information about a target organization. The VMs used in this lab are Kali Linux as the attack VM, and Metasploitable as the target VM.

Task One:

Metasploit login/pass: msfadmin

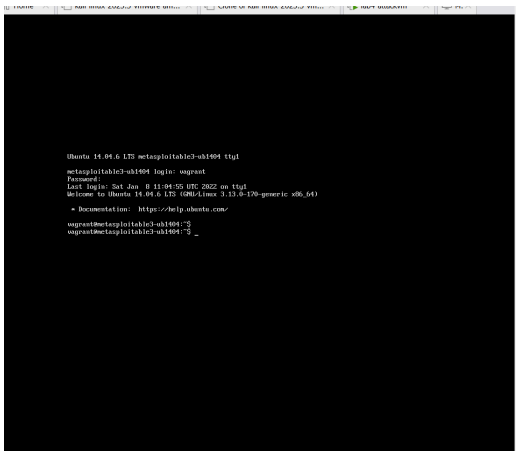
A)

1) Download Kali Linux (Attack VM)

Username: kali

Password:kali

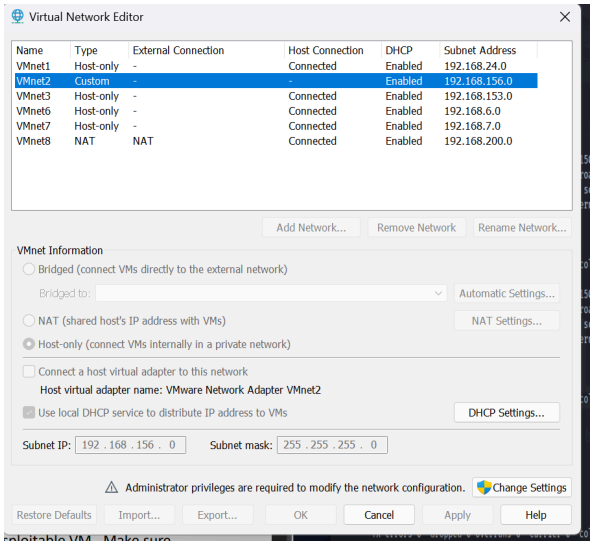
2) Download and Install Metasploitable (Target VM)

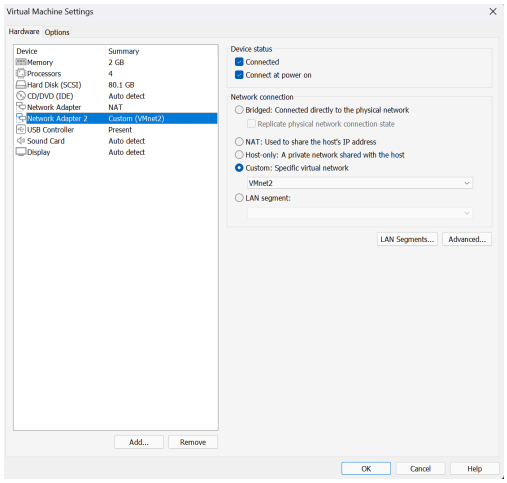


Username and passsword: msfadmin

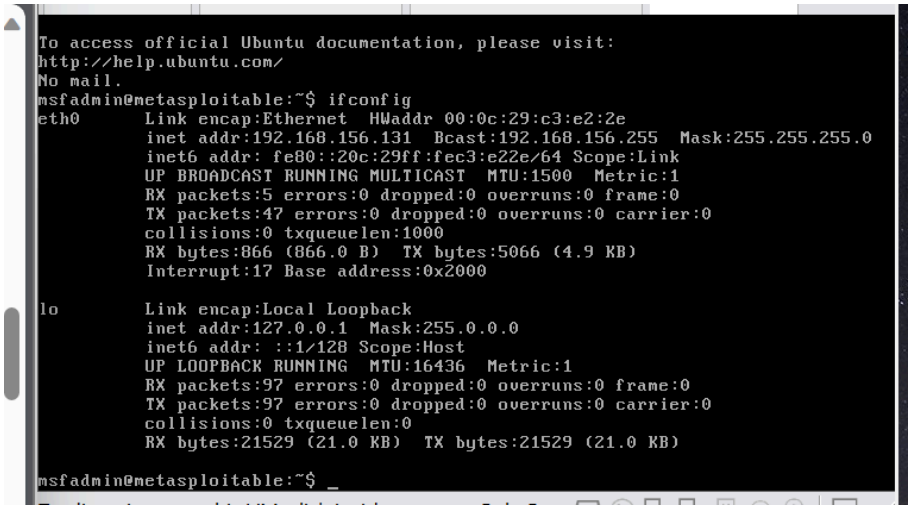
B)

Kali Linux:

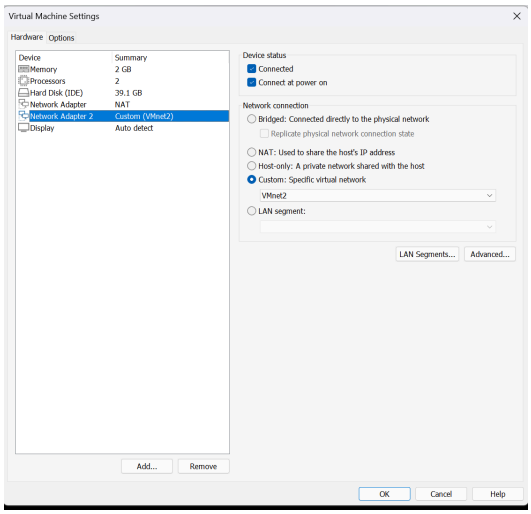

Virtual Network Editor
Name Type External Connection Host Connection DHCP Subnet Address
VMnet1 Host-only - Connected Enabled 192.168.24.0
VMnet2 Custom - - Enabled 192.168.156.0
VMnet3 Host-only - Connected Enabled 192.168.153.0
VMnet6 Host-only - Connected Enabled 192.168.6.0
VMnet7 Host-only - Connected Enabled 192.168.7.0
VMnet8 NAT NAT Connected Enabled 192.168.200.0
Add Network...
Remove Network
Rename Network...
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to:
Automatic Settings...
NAT (shared host's IP address with VMs)
NAT Settings...
Host-only (connect VMs internally in a private network)
Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet2
Use local DHCP service to distribute IP address to VMs
DHCP Settings...
Subnet IP: 192 . 168 . 156 . 0
Subnet mask: 255 . 255 . 255 . 0
Administrator privileges are required to modify the network configuration.
Change Settings
Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help


Virtual Machine Settings
Hardware
Options
Device Summary
Memory 2 GB
Processors 4
Hard Disk (SCSI) 80.1 GB
CD/DVD (IDE) Auto detect
Network Adapter NAT
Network Adapter 2 Custom (VMnet2)
USB Controller Present
Sound Card Auto detect
Display Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet2
LAN segment:
LAN Segments...
Advanced...
OK
Cancel
Help

Metasploit:

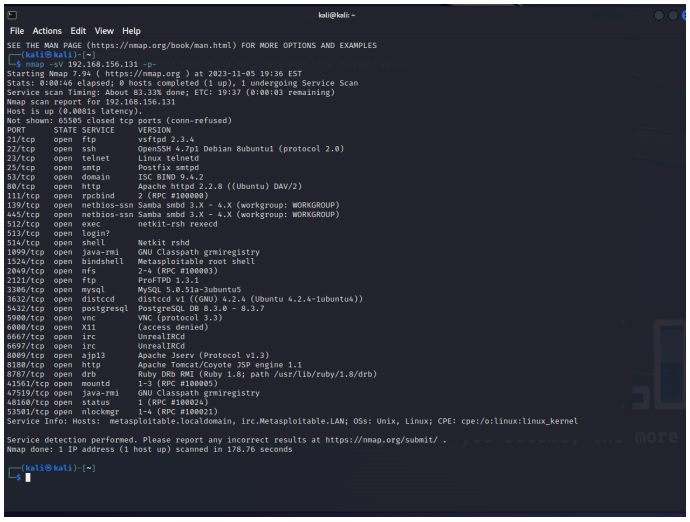


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c3:e2:2e
          inet addr:192.168.156.131  Bcast:192.168.156.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec3:e22e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:866 (866.0 B)  TX bytes:5066 (4.9 KB)
          Interrupt:17 Base address:0x2000

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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$ _
```



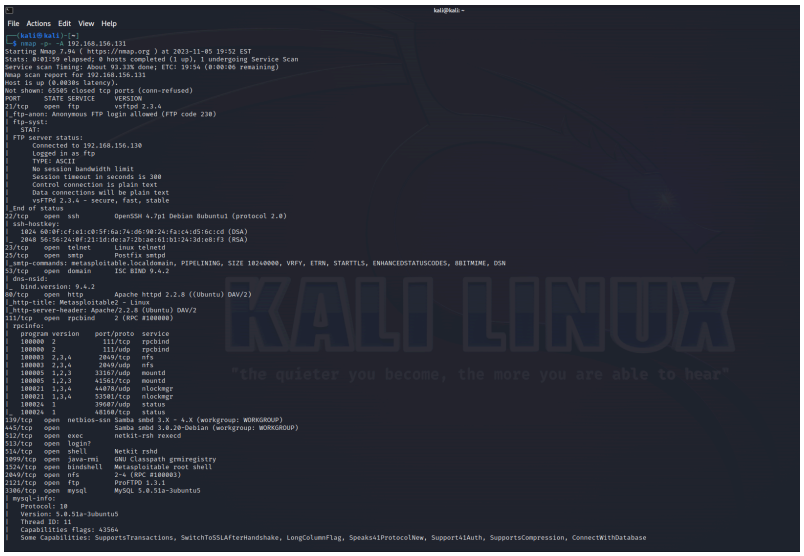
C)

1. NMap:



```
kali@kali: ~
File  Actions  Edit  View  Help
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.156.131 -p-
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 19:36 EST
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 19:37 (0:00:03 remaining)
Nmap scan report for 192.168.156.131
Host is up (0.0081s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (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 ((Ubuntu) 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?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41561/tcp open  mountd     1-3 (RPC #100005)
47519/tcp open  java-rmi   GNU Classpath grmiregistry
48160/tcp open  status     1 (RPC #100024)
53501/tcp open  nlockmgr   1-4 (RPC #100021)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.76 seconds

┌──(kali㉿kali)-[~]
└─$
```

These are the results of running an nmap scan, the port numbers, their state, service ad version are all listed.
Then I ran a scan retrieving information about the ports using nmap -p- -A 192.168.156.131



This scan returns detailed information about the different ports in the target vm,
I then ran a command that would make nmap run all of its vulnerability detection scripts, this gave me a lot of results, and also a lot of useful information like possible sqli injection, possible vulnerabilities, CSRF vulnerabilities and other possible vulnerabilities that can be exploited.

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -p- 192.168.156.131
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-05 20:14 EST
Stats: 0:04:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
SSL Ping|: About 99.60% done; ETC: 20:19 (0:00:01 remaining)
Nmap scan report for 192.168.156.131
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|     vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeasts.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vulns: STARTTLS not supported
|_The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.156.131:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=large-log.html%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.156.131:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=reset-administrator-pages.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=text-file-viewer.php
|     http://192.168.156.131:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.156.131:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|     http://192.168.156.131:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=documentation%27how-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=view-profile-1.php%27%20OR%20sqlspider
|     http://192.168.156.131:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
```

```
target-lab4   lab4-attackvm   Metasploitable2-Linux
1  2  3  4
File  Actions  Edit  View  Help
kali@kali: ~
    http://192.168.156.131:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
    http://192.168.156.131:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
    http://192.168.156.131:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
    http://192.168.156.131:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
    http://192.168.156.131:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
    http://192.168.156.131:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
  Possible sqli for forms:
    Form at path: /mutillidae/index.php, form's action: index.php. Fields that might be vulnerable:
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      choice
      initials
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-trace: TRACE is enabled
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.156.131
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.156.131:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|
|     Path: http://192.168.156.131:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.156.131:80/mutillidae/index.php?page=user-poll.php
|     Form id: idpollform
|_    Form action: index.php
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
```

```
File  Actions  Edit  View  Help
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-trace: TRACE is enabled
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.156.131
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.156.131:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://192.168.156.131:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|
|     Path: http://192.168.156.131:80/dvwa/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.156.131:80/mutillidae/index.php?page=user-poll.php
|     Form id: idpollform
|_    Form action: index.php
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
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
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
```

```
File  Actions  Edit  View  Help
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.securityfocus.com/bid/70574
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
```

```
kali@kali: ~
File  Actions  Edit  View  Help
|     References:
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
| irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.jsp:
|     JSESSIONID:
```

```
File  Actions  Edit  View  Help
|   /admin/controlpanel.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 331.65 seconds

┌──(kali㉿kali)-[~]
└─$ ssssssssss
```

These are all the possible vulnerabilities that can be exploited through different means like and sql injunction, SSL vulnerabilitiec and others.

Enumeration:

1. Web Services (HTTP/HTTPS): Web servers are often a prime target for testing because they are commonly exposed to the internet and can contain various vulnerabilities. Nmap can be used to identify the web server software and version, discover open ports, and conduct further testing for common web application vulnerabilities using additional tools or scripts.

2. Database Services (e.g., MySQL, PostgreSQL, MSSQL): Databases can store sensitive information, making them attractive targets. Nmap can be used to identify open database ports and their respective services. Further testing can be performed using database-specific tools or scripts.

3. SSH and Remote Administration Services: SSH and remote administration services like RDP (Remote Desktop Protocol) may provide access to the system. Identifying open SSH ports and their versions can help determine if secure remote access is possible.

4. File Transfer Services (FTP, SFTP): Services like FTP and SFTP can expose files and directories that may contain sensitive information or configuration files. Nmap can be used to identify open ports and services related to file transfer.

5. Mail Services (SMTP, POP3, IMAP): Email services are valuable targets because they often contain sensitive communication and attachments. Nmap can be used to identify open mail ports and their respective services. Further email-specific testing can be conducted with other tools.

Results: There wasn’t anything I was surprised about, it was all pretty standard for this type of scan, but this tool was very fun to use, and a lot of different type of data was able to be extracted using this tool.
Nikto

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.156.131
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.156.131
+ Target Hostname:    192.168.156.131
+ Target Port:        80
+ Start Time:         2023-11-05 21:08:13 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X
-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differen
t fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The followin
g alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibm
cloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_
Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain
 specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain
 specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain
 specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain
 specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540
, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: C
WE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hos
ts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: htt
ps://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2023-11-05 21:09:10 (GMT-5) (57 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
```

This is the result of the Nikto scan, checking the web server to identify issues like outdated software, site tracing, and other security issues.
Result: Nothing here was too surprising, but this is a more simple scan. I liked how easy this tool was to use. This is a useful tool for checking outdated software, and more basic vulnerabilities like site tracing.
Enumeration:
1. Web Server (HTTP):
   - Nikto can scan the web server (e.g., Apache, Nginx, IIS) to identify misconfigurations, known vulnerabilities, and other issues related to the web server's configuration.

2. Content Management Systems (CMS):
   - Many websites and web applications use popular content management systems (e.g., WordPress, Joomla, Drupal). Nikto can target these CMS platforms to detect outdated plugins, themes, or common vulnerabilities associated with them.

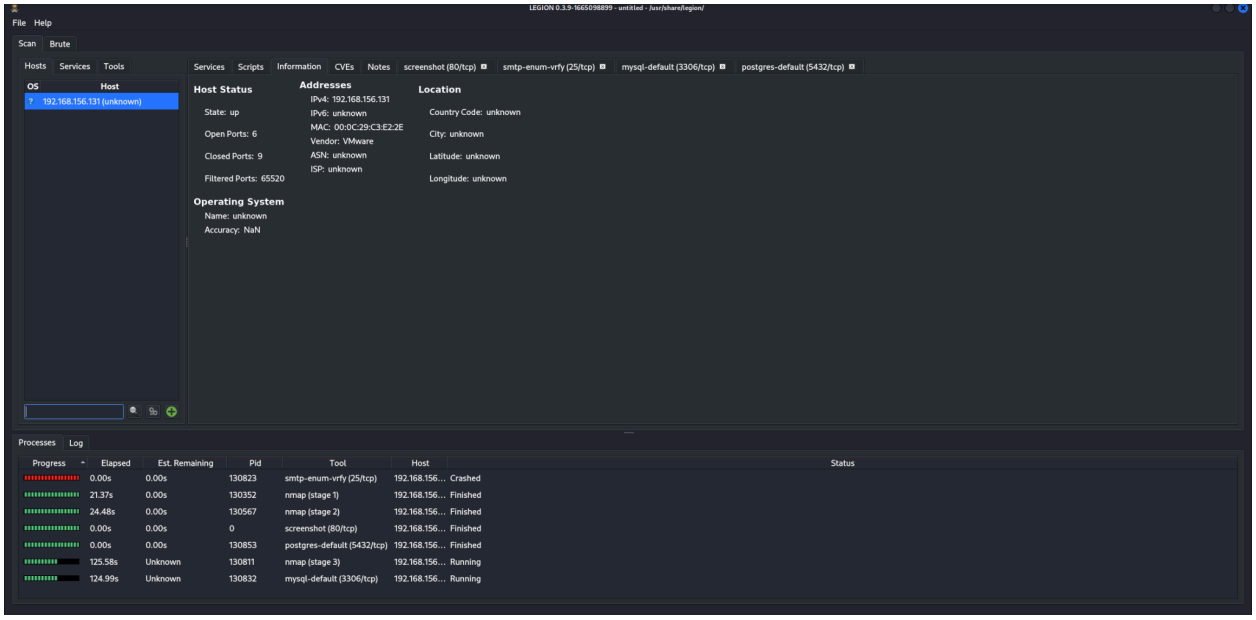
3. Web Applications:
   - Web applications are a common target for security assessments. Nikto can be used to scan the web application for vulnerabilities like SQL injection, cross-site scripting (XSS), directory traversal, and other web application-specific issues.

4. Databases:

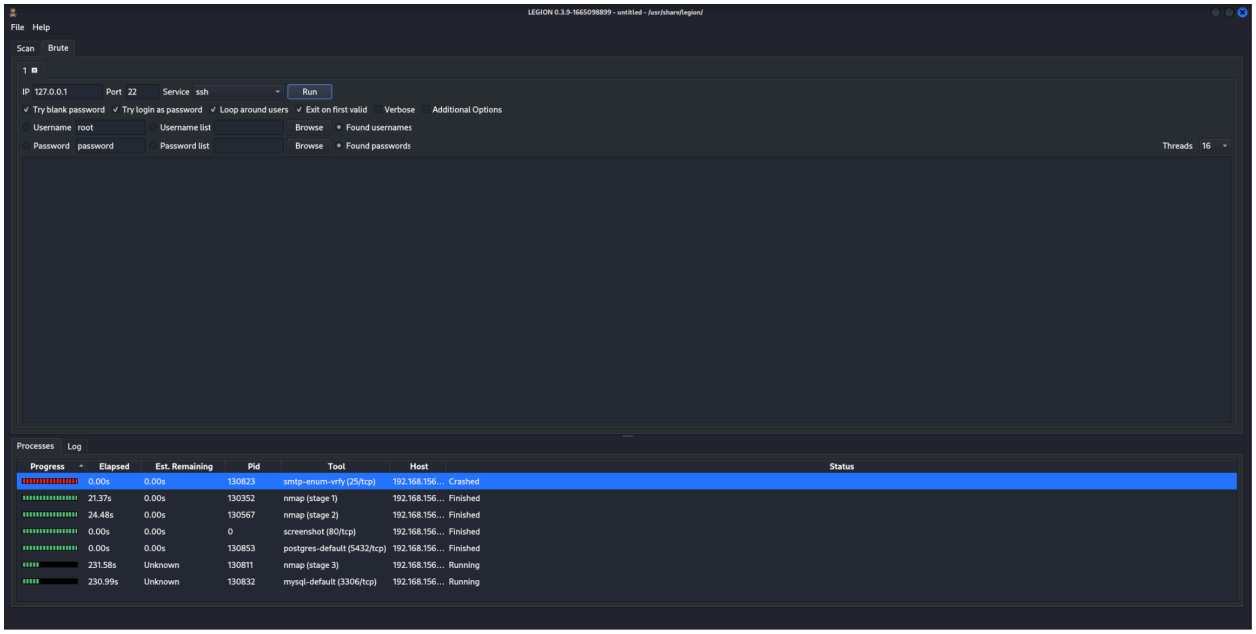
- Nikto can be used to identify potential database-related vulnerabilities, such as misconfigured database servers or known vulnerabilities in the database software itself.

5. APIs:
   - Modern web applications often have APIs (Application Programming Interfaces) that expose functionality and data. Nikto can target these APIs to check for authentication issues, insecure API endpoints, and other security concerns.

Legion



This tool checks the IP address that the user inputs and retrieves information like the host statistics, operating system, addresses, location, the scripts, services and other possible vulnerabilities.



This service also is useful for password and username cracking through brute force.

Results: This tool is one of the most useful out of the tools i used in this lab, along with testing and scanning for vulnerabilities and producing those results, this tool also checks username and password strength, scripts, and more.

Enumeration:

1. Web Applications: Web applications are often a prime target for penetration testing. Issues such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure configurations can lead to serious security vulnerabilities.

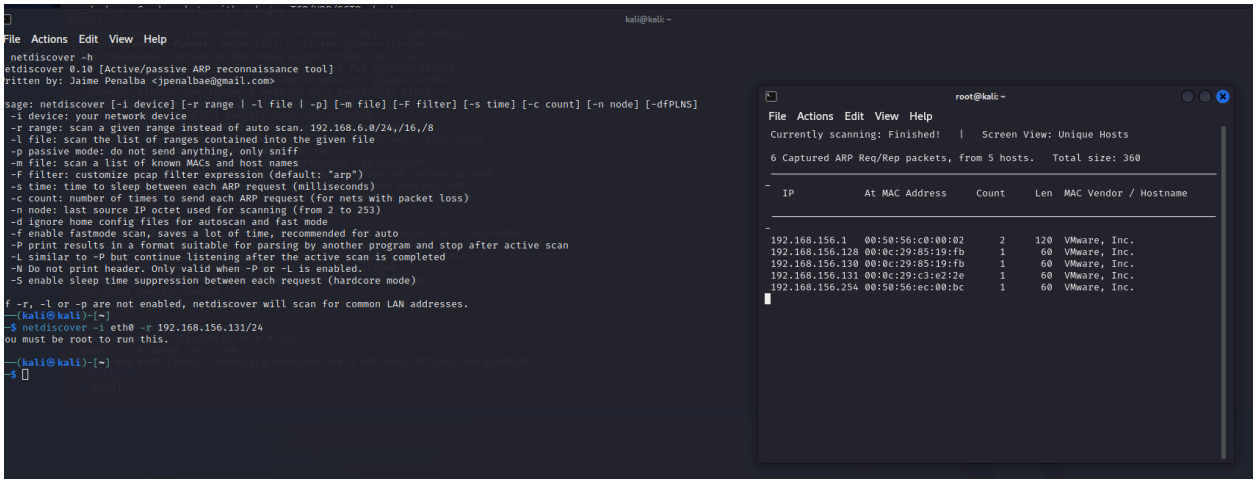
2. Databases: Databases, especially those containing sensitive data, are high-value targets. Testing for database vulnerabilities like SQL injection and weak access controls is essential.

3. File Services (e.g., SMB, FTP): Services that involve file sharing, such as Server Message Block (SMB) and FTP, are often targeted to identify misconfigurations or access control issues that could lead to unauthorized access.

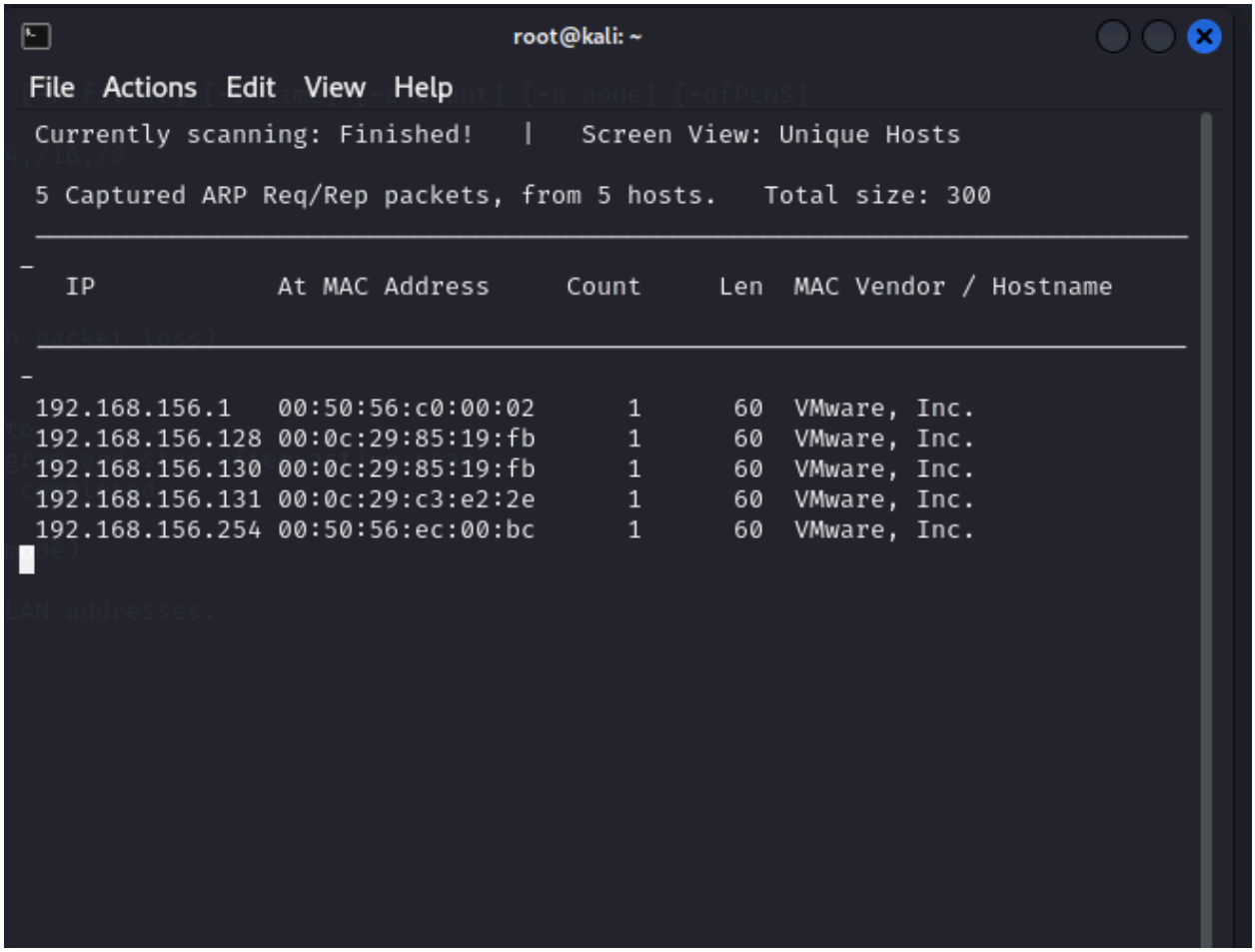
4. Email Services: Email servers and services are targeted to identify issues such as open relays, misconfigured spam filters, and phishing vulnerabilities.

5. Remote Desktop Services (e.g., RDP, SSH): Services that allow remote access to systems, like Remote Desktop Protocol (RDP) and Secure Shell (SSH), are scrutinized for weak passwords, insecure configurations, and other potential entry points.

Netdiscover :



This command needed to be run in root command line, when i did i got the results displaying the IP addresses in the range, their mac addresses, the count, MAC vendor and hostname.



Results: These results weren't surprising, but i did have a little trouble at first getting it to run, but once i tried it in the root terminal, it worked. This is a great tool for checking active ip addresses on a server.

Enumeration:

1. Port 22 (SSH): SSH (Secure Shell) is a common service used for secure remote administration and access to Linux and Unix-based systems. It's a prime target because vulnerabilities in SSH can lead to unauthorized access.

2. Port 80 (HTTP): Port 80 is the default port for HTTP (Hypertext Transfer Protocol), which is used for web services. It's a potential target for web application vulnerabilities and can be used to gather information about the web server and any web applications running on it.

3. Port 443 (HTTPS): Port 443 is used for secure HTTP (HTTPS) communication, typically associated with websites that use SSL/TLS encryption. It's important to assess the security of SSL/TLS configurations and the web applications behind HTTPS.

4. Port 445 (SMB): Port 445 is commonly associated with the Server Message Block (SMB) protocol used by Windows systems for file and printer sharing. Vulnerabilities in SMB can lead to unauthorized access, data exfiltration, and lateral movement within the network.

5. Port 3389 (RDP): Port 3389 is used for the Remote Desktop Protocol (RDP), which is often targeted because it provides remote access to Windows machines. Exploiting RDP vulnerabilities can result in unauthorized access to the targeted systems.

Dmitry:

```
┌──(kali㉿kali)-[~]
└─$ cd desktop
cd: no such file or directory: desktop

┌──(kali㉿kali)-[~]
└─$ dmitry 192.168.156.131
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.156.131
Continuing with limited modules
HostIP:192.168.156.131
HostName:

Gathered Inet-whois information for 192.168.156.131
---------------------------------

Error: Unable to connect - Invalid Host
ERROR: Connection to InetWhois Server whois.ripe.net failed
Error: Unable to connect - Invalid Host
ERROR: Connection to InetWhois Server whois.arin.net failed
close error
Error: Unable to connect - Invalid Host
ERROR: Connection to InetWhois Server whois.lacnic.net failed
close error
Error: Unable to connect - Invalid Host
ERROR: Connection to InetWhois Server whois.apnic.net failed
close error

Gathered TCP Port information for 192.168.156.131
---------------------------------

 Port            State
21/tcp           open
22/tcp           open
23/tcp           open
25/tcp           open
53/tcp           open
80/tcp           open
111/tcp          open
139/tcp          open

Portscan Finished: Scanned 150 ports, 141 ports were in state closed

All scans completed, exiting

┌──(kali㉿kali)-[~]
└─$
```

That command gathers TCP port information for the specified ip address, if the port is open or net, and it displayed the ports that are open.

Results: This tool is good for capturing port information about ip addresses, ad the port status. This tool also checks for vulnerabilities. There wasn't anything surprising about this tool, or its results.

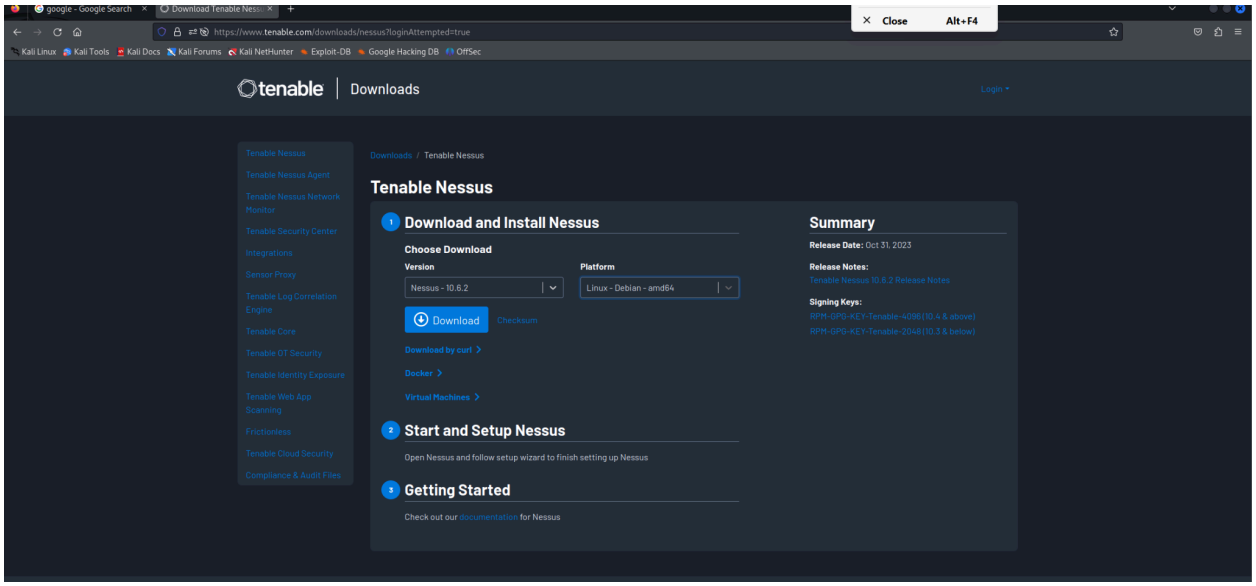
The service that I would target using this tool is

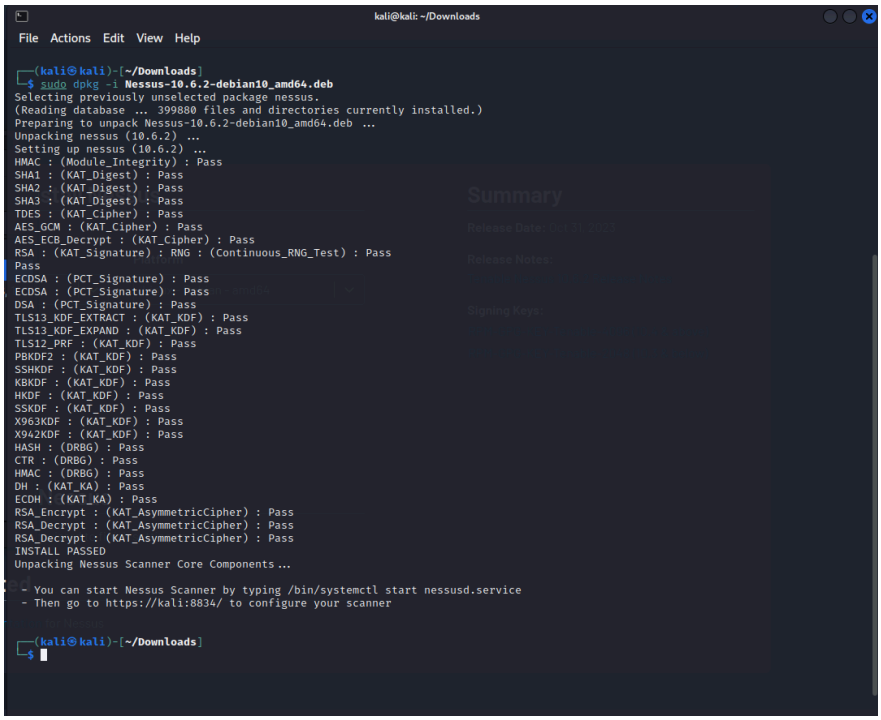
- HTTP: enumerating information about the target's web server is crucial for pen tests. Dmitry helps gather details like the web server version, available virtual hosts, etc
- SMTP Service: if the target as an SMTP service running, this tool can provide information about the server.
- DNS: revealing information about the target's DNS infrastructure
- SNMP ServiceL if the target exposes SNMP services, this tool can be used to gather information about the snmp configuration, like community strings, device descriptions, and potentially sensitive system data

- Whois informationL this tool can retrieve whois information about the target, providing details about the domain, ip address, and contact information

Nessus:

The installation:





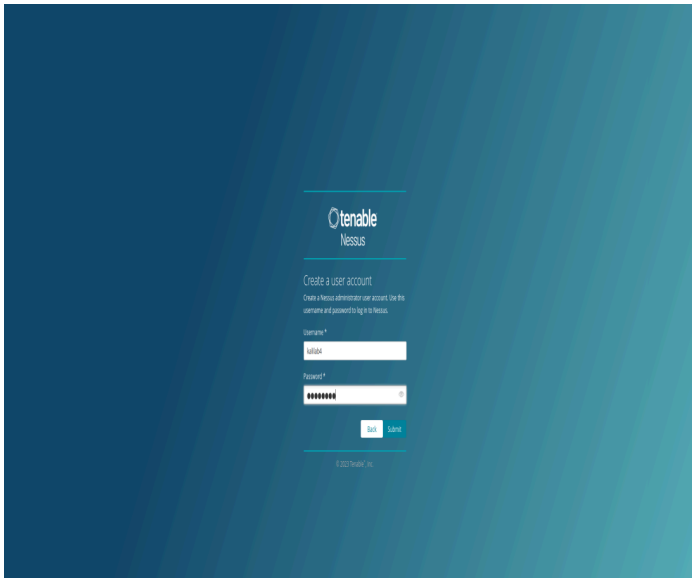
This is the installation of Nessus on my kali VM,

```
kali@kali: ~/Downloads
File  Actions  Edit  View  Help
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(kali㉿kali)-[~/Downloads]
└─$ sude systemctl start nessusd
Command 'sude' not found, did you mean:
  command 'sure' from deb python3-sure
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd

┌──(kali㉿kali)-[~/Downloads]
└─$  sudo systenctl status nessud
sudo: systenctl: command not found

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status neddusd
Unit neddusd.service could not be found.

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2023-11-06 12:30:39 EST; 10min ago
   Main PID: 231843 (nessus-service)
      Tasks: 14 (limit: 2255)
     Memory: 188.0M
        CPU: 1min 41.312s
     CGroup: /system.slice/nessusd.service
             ├─231843 /opt/nessus/sbin/nessus-service -q
             └─231845 nessusd -q

Nov 06 12:30:39 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Nov 06 12:30:42 kali nessus-service[231845]: Cached 0 plugin libs in 1msec
Nov 06 12:30:42 kali nessus-service[231845]: Cached 0 plugin libs in 0msec

┌──(kali㉿kali)-[~/Downloads]
└─$
```

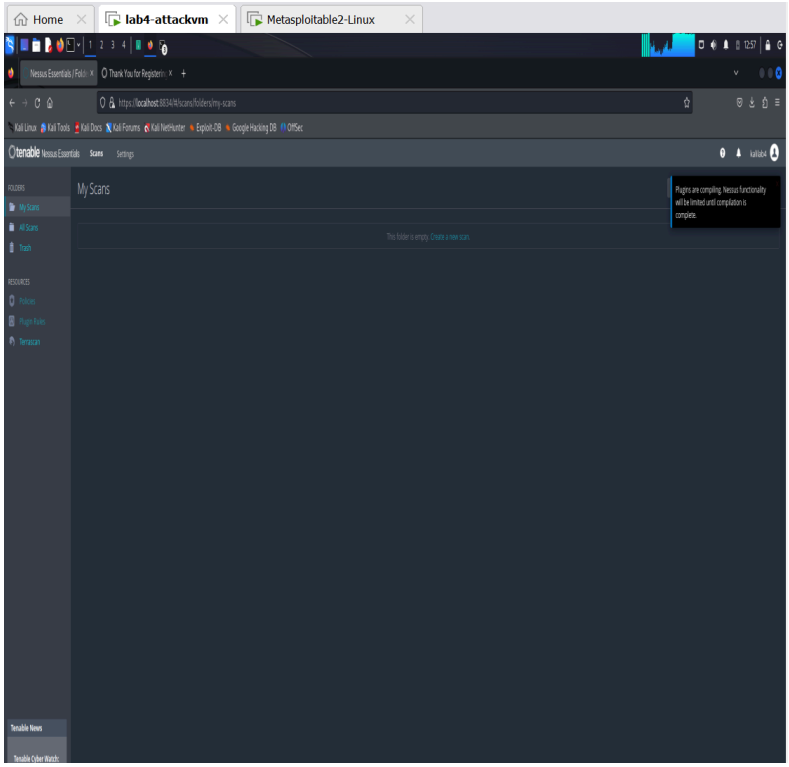
These are the commands that install nessus on the kali vm.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop]
└─$ touch file1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ echo "FW79-PLY3-DN7X-5UQ6-KCXQ"> file1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$
```

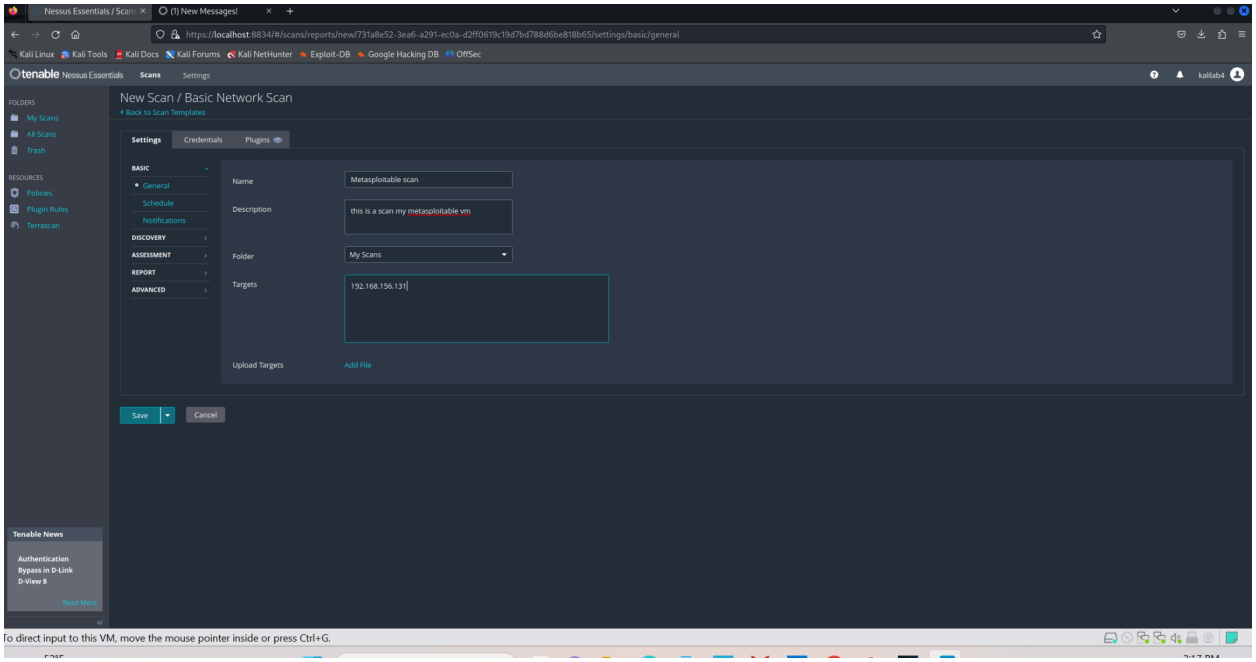
The echo command is the accesses code for nessus, and i made that file1.txt so it can be accessed in the future.

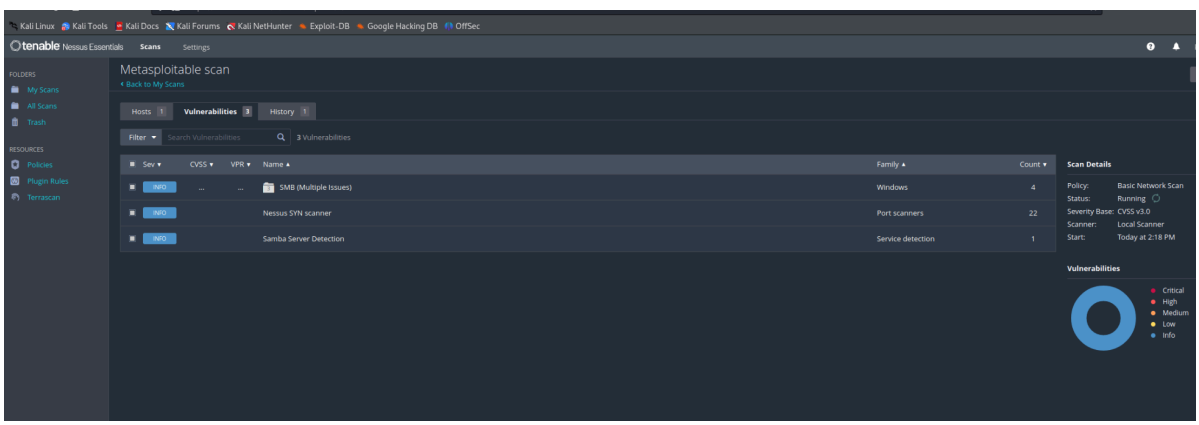


I had to create and account, I used a one time email website for this, so that I didn't connect any of my actual emails to this website for this lab, and so i wouldn't have to create a real email for this.

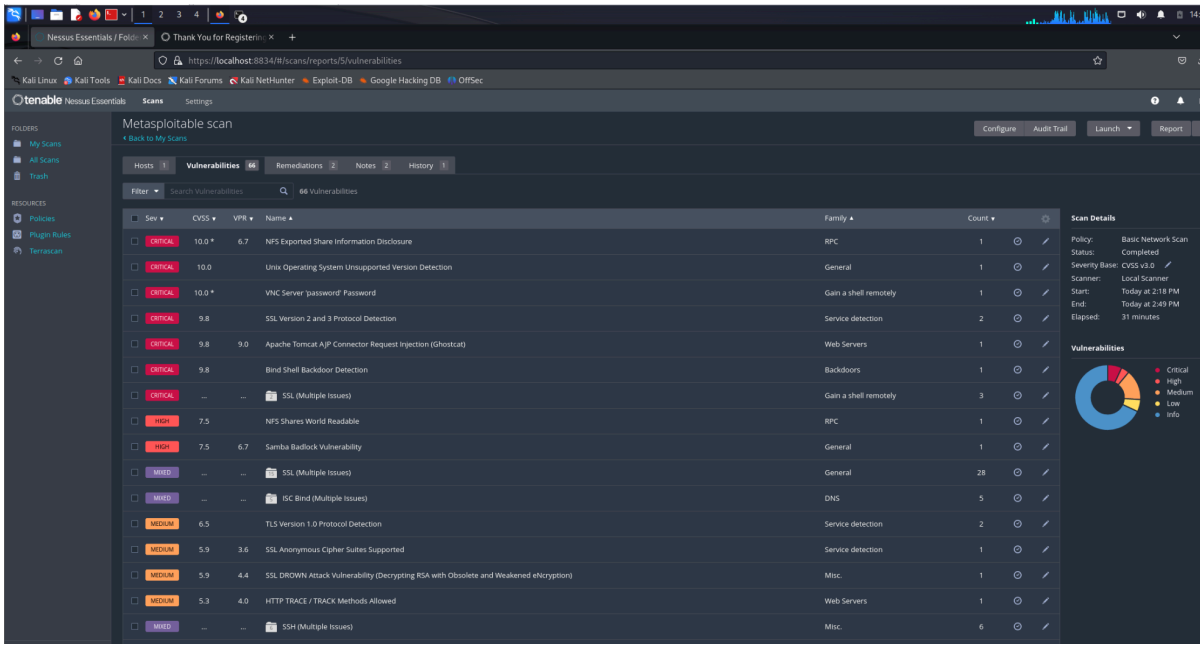


Running scan on the metasploitable VM

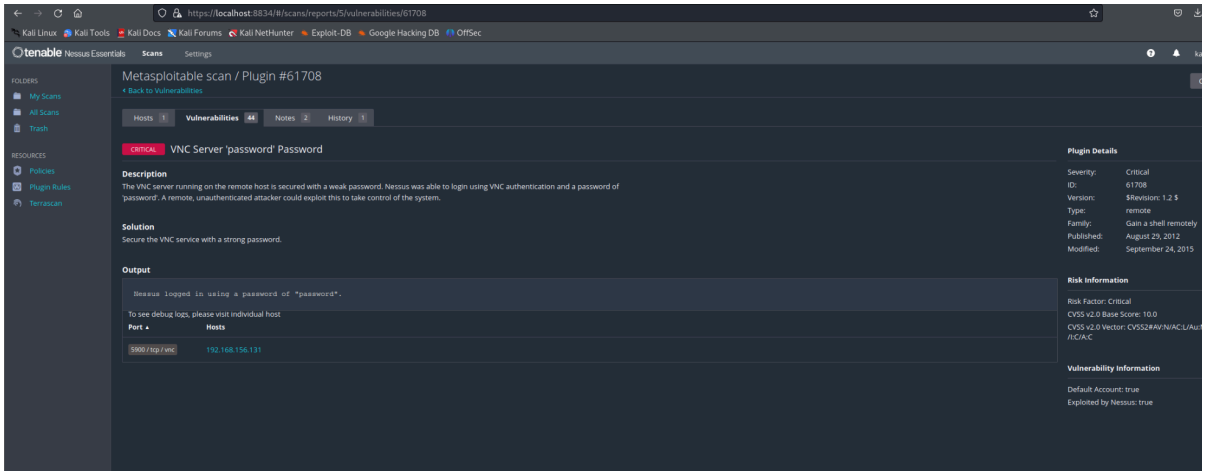


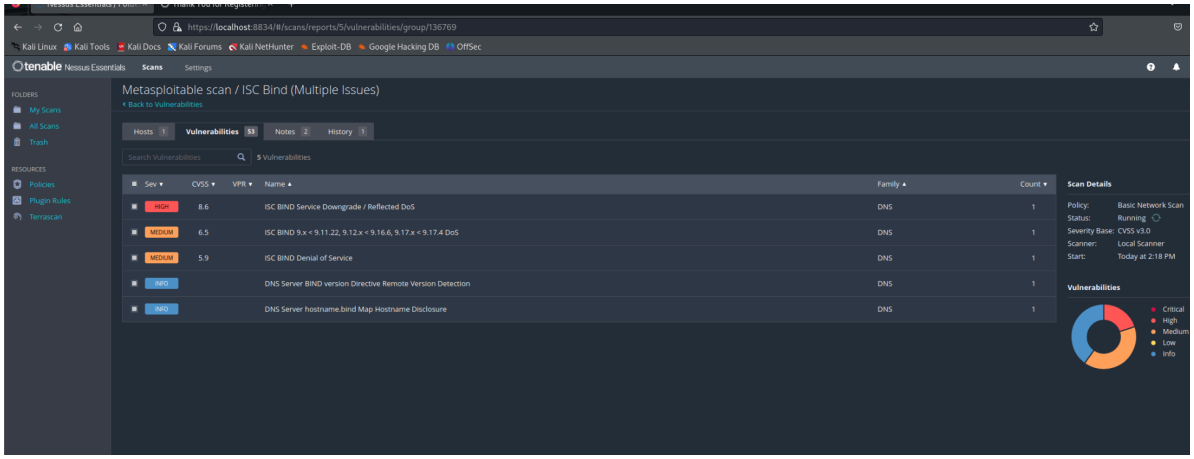


I do believe that some of my targeted services contain exploitable vulnerabilities. The vulnerabilities found by nessus were weak passwords, backdoor detection, weak encryption, and a lot of no authentication in place. I cannot find if it says what services I used caused some of these vulnerabilities, but I read in the scan report commands and outputs that were generated by my services.



These are the results of the scan, Nessus gives the results of this scan in a easy to understand format, I especially like how the critical vulnerabilities are in bright red, and at the top. This list is ordered by most critical vulnerabilities at the top, in descending order.





I loved this tool, it was so much fun to use and I was able to gather a lot of important information about vulnerabilities. I loved how this tool made it easy to gather this information and how it gave a detailed report of its findings.

Netcat

```
┌──(kali㉿kali)-[~]
└─$ netcat -z -n -v 192.168.156.131 1-1000
(UNKNOWN) [192.168.156.131] 514 (shell) open
(UNKNOWN) [192.168.156.131] 513 (login) open
(UNKNOWN) [192.168.156.131] 512 (exec) open
(UNKNOWN) [192.168.156.131] 445 (microsoft-ds) open
(UNKNOWN) [192.168.156.131] 139 (netbios-ssn) open
(UNKNOWN) [192.168.156.131] 111 (sunrpc) open
(UNKNOWN) [192.168.156.131] 80 (http) open
(UNKNOWN) [192.168.156.131] 53 (domain) open
(UNKNOWN) [192.168.156.131] 25 (smtp) open
(UNKNOWN) [192.168.156.131] 23 (telnet) open
(UNKNOWN) [192.168.156.131] 22 (ssh) open
(UNKNOWN) [192.168.156.131] 21 (ftp) open

┌──(kali㉿kali)-[~]
└─$
```

These are the results of running the command Netcat -z -n 0v 192.168.156.131 1-1000, these are the ports from 1-1000, what their services are, if they are open, and the host.

Arping

```
┌──(kali㉿kali)-[~]
└─$ sudo arping -c 10 192.168.156.131
ARPING 192.168.156.131
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=0 time=1.145 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=1 time=1.082 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=2 time=1.031 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=3 time=818.718 usec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=4 time=2.108 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=5 time=1.426 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=6 time=15.229 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=7 time=2.882 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=8 time=1.401 msec
60 bytes from 00:0c:29:c3:e2:2e (192.168.156.131): index=9 time=6.244 msec

— 192.168.156.131 statistics —
10 packets transmitted, 10 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.819/3.337/15.229/4.249 ms

┌──(kali㉿kali)-[~]
└─$
```

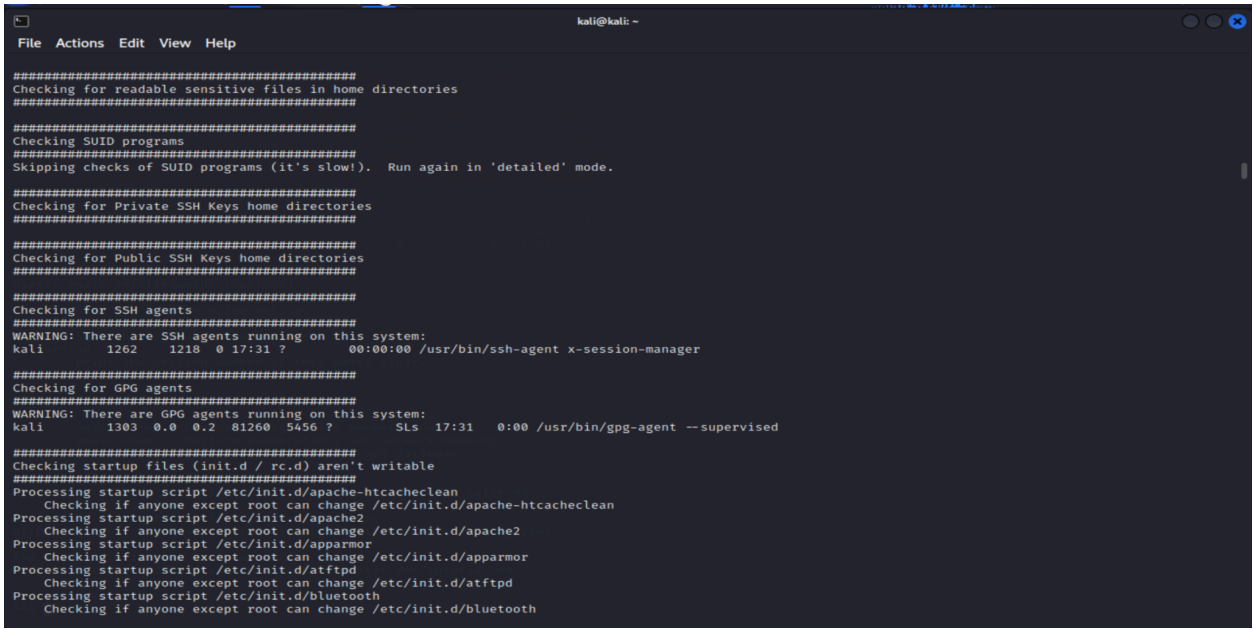
This command gets 10 ARP requests that were sent to the target vm ip address, this checks if the target host is active on a local network

I chose this tool because I was having trouble installing other active discovery tools, and this tool is useful for monitoring packets and gathering the ARP information. I don't really like this service because it can produce a lot of results that is time consuming to produce and to look through. I did like how easy this tool was to use.

Unix-privesc-check:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ unix-privesc-check standard
Assuming the OS is: linux
Starting unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-check )

This script checks file permissions and other settings that could allow
local users to escalate privileges.

Use of this script is only permitted on systems which you have been granted
legal permission to perform a security assessment of.  Apart from this
condition the GPL v2 applies.

Search the output below for the word 'WARNING'.  If you don't see it then
this script didn't find any problems.


###############################################
Recording hostname
###############################################
kali

###############################################
Recording uname
###############################################
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux

###############################################
Recording Interface IP addresses
###############################################
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.156.128  netmask 255.255.255.0  broadcast 192.168.156.255
        inet6 fe80::85a6:88b4:bf57:54b8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:85:19:f1  txqueuelen 1000  (Ethernet)
        RX packets 1288  bytes 82791 (80.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1299  bytes 95318 (93.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.156.130  netmask 255.255.255.0  broadcast 192.168.156.255
        inet6 fe80::a99a:bb7c:dde8:8316  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:85:19:fb  txqueuelen 1000  (Ethernet)
        RX packets 142  bytes 11960 (11.6 KiB)
```

```
        inet 192.168.156.128  netmask 255.255.255.0  broadcast 192.168.156.255
        inet6 fe80::85a6:88b4:bf57:54b8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:85:19:f1  txqueuelen 1000  (Ethernet)
        RX packets 1288  bytes 82791 (80.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1299  bytes 95318 (93.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.156.130  netmask 255.255.255.0  broadcast 192.168.156.255
        inet6 fe80::a99a:bb7c:dde8:8316  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:85:19:fb  txqueuelen 1000  (Ethernet)
        RX packets 142  bytes 11960 (11.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3220 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


###########################################
Checking if external authentication is allowed in /etc/passwd
###########################################
No +:... line found in /etc/passwd

###########################################
Checking nsswitch.conf for addition authentication methods
###########################################
Neither LDAP nor NIS are used for authentication

###########################################
Checking for writable config files
###########################################
    Checking if anyone except root can change /etc/passwd
    Checking if anyone except root can change /etc/group
    Checking if anyone except root can change /etc/fstab
```



```
kali@kali: ~
File  Actions  Edit  View  Help

##################################################
Checking for readable sensitive files in home directories
##################################################

##################################################
Checking SUID programs
##################################################
Skipping checks of SUID programs (it's slow!).  Run again in 'detailed' mode.

##################################################
Checking for Private SSH Keys home directories
##################################################

##################################################
Checking for Public SSH Keys home directories
##################################################

##################################################
Checking for SSH agents
##################################################
WARNING: There are SSH agents running on this system:
kali        1262    1218  0 17:31 ?        00:00:00 /usr/bin/ssh-agent x-session-manager

##################################################
Checking for GPG agents
##################################################
WARNING: There are GPG agents running on this system:
kali        1303  0.0  0.2  81260  5456 ?        SLs  17:31   0:00 /usr/bin/gpg-agent --supervised

##################################################
Checking startup files (init.d / rc.d) aren't writable
##################################################
Processing startup script /etc/init.d/apache-htcacheclean
    Checking if anyone except root can change /etc/init.d/apache-htcacheclean
Processing startup script /etc/init.d/apache2
    Checking if anyone except root can change /etc/init.d/apache2
Processing startup script /etc/init.d/apparmor
    Checking if anyone except root can change /etc/init.d/apparmor
Processing startup script /etc/init.d/atftpd
    Checking if anyone except root can change /etc/init.d/atftpd
Processing startup script /etc/init.d/bluetooth
    Checking if anyone except root can change /etc/init.d/bluetooth
```

This command checks the file permissions and other settings that would allow local users to escalate their privileges. This is is a good tool to use to monitor the safety of the network youre using.

The best feature of this tool is the in depth results of this scan, the vulnerabilities found through thiis scan make it easy for admin and other controllers to monitor the local networks to ensure no one without permissions are escalating their privileges. I chose this tool because I was struggling with other active discovery tools and this one wasn't giving me as much trouble, but when i researched it more I found how useful this tool is for cybersecurity, pen testing and I found myself really enjoying this tool.

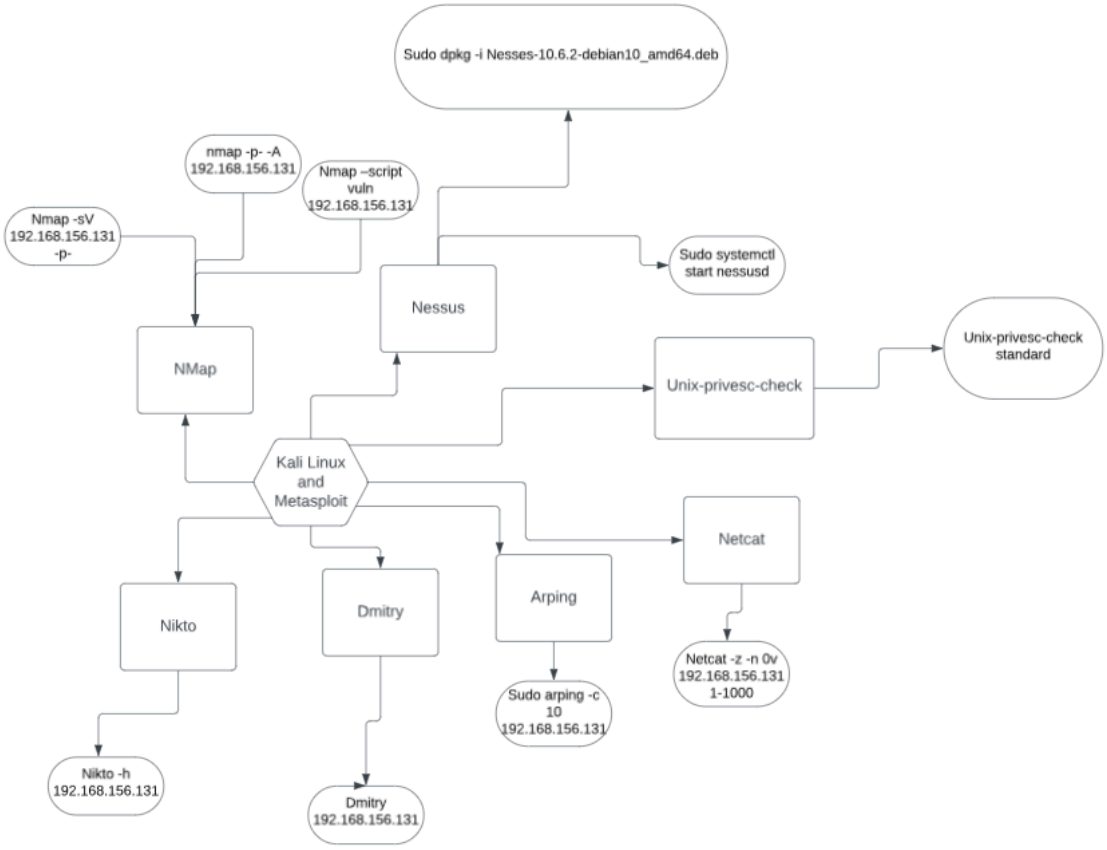
Topology:

Key Syntax:

Nmap -sV 192.168.156.131 -p-	Scans the port numbers, their state, service and the versions installed	nmap
nmap -p- -A 192.168.156.131	Retrieves information about the ports, the -a- in this command makes nmap attempt to identify the targets operating system.	nmap
Nmap –script vuln 192.168.156.131	This runs a scan retrieving possible vulnerabilities that can be exploited.	nmap

Nikto -h 192.168.156.131	This command tells Nikto to perform a series of tests and checks against the web sever to identify issues	Nikto
Netdiscover -i eth0 -r 192.168.156.131/24	This command tells netdiscover to send arp requests to discover and identify hosts on the local network segment specified in the io range	Netdiscover
Dmitry 192.168.156.131	This command gathers the port information for the specific ip address, specifically the port numbers that are open.	Dmity
Sudo dpkg -i Nesses-10.6.2-debian 10_amd64.deb	This is the command that installs nessus on my kali vm	nessus
Sudo systemctl start nessusd	This starts nessus	nessus
Netcat -z -n 0v 192.168.156.131 1-1000	This does a port scan on the target host, for the ports in the range of 1 to 1000, this is a detailed result	netcat
Sudo arping -c 10 192.168.156.131	This command is used to send ARP requests to a specific IP address in arder to determine if the target host is active on a local network.	Arping
Unix-privesc-check standard	This checks the file permissions and other settings that could allow ocal users too escalate their privileges.	unix-privesc-check

Topology:



Conclusion:
This lab utilizes active discovery tools that can be used with Kali Linux, to explore the ways these tools can scan for and exploit vulnerabilities in a system, specifically the target VM metasploitable. I had trouble with getting 3 active discovery tools, specifically because each time I would try to install it on my Kali, i would get an error with my git clone, I had tried to install redHawk, Zenmap, and Sparta but none were successful.

Resources:

(2021). Retrieved from https://www.geeksforgeeks.org/kali-linux-information-gathering-tools/

(2023). Retrieved from https://www.geeksforgeeks.org/using-metasploit-and-nmap-to-scan-for-vulnerabilities-in-kali-linux/

Aleksic, M. (2023). Retrieved from https://phoenixnap.com/kb/kali-linux-tools

Andrew DeVito
, DeVito, A., Andrew is a Content Writer at StationX. He comes from a multi-discipline professional background with over 20 years of combined experience in healthcare compliance, & posts, V. all. (2023). Retrieved from https://www.stationx.net/how-to-scan-vulnerabilities-with-nmap/#:~:text=We%20can%20perform%20such%20a%20scan%20with%20a,risks%20and%20vulnerabilities%20present%20on%20the%20target%20host.

Kumar, V. (2023a). Retrieved from https://www.cyberpratibha.com/blog/netdiscover/

Kumar, V. (2023b). Retrieved from https://www.cyberpratibha.com/blog/netdiscover/

Shivanandhan, M. (2021). Retrieved from https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/