

## Discovering Live Systems

### Step 1: Scan using ifconfig.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::1b8:7b77:a494:6799 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 1144 bytes 79769 (77.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3305 bytes 219482 (214.3 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 677 bytes 62146 (60.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 677 bytes 62146 (60.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Step 2: Scan with netdiscover.

```
(kali㉿kali)-[~]
$ sudo netdiscover -r 192.168.1.0/24
```

```
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.1.1  | 08:00:27:b5:9c:82 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.1.101 | 08:00:27:0d:22:3d | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.1.103 | 08:00:27:d7:cc:d8 | 1     | 60  | PCS Systemtechnik GmbH |
```

### Step 3: Scan with Nmap

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 16:32 EST
Nmap scan report for pfSense.home.arpa (192.168.1.1)
Host is up (0.00059s latency).
Nmap scan report for 192.168.1.100
Host is up (0.0017s latency).
Nmap scan report for 192.168.1.101
Host is up (0.0076s latency).
Nmap scan report for 192.168.1.103
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.54 seconds
```

#### Step 4: Scan using nbtscan

```
(kali㉿kali)-[~]  
$ sudo nbtscan -r 192.168.1.0/24  
Doing NBT name scan for addresses from 192.168.1.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.1.100	<unknown>		<unknown>	
192.168.1.103	VAGRANT-2008R2	<server>	<unknown>	08:00:27:d7:cc:d8
192.168.1.101	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.1.255	Sendto failed: Permission denied			

#### Step 5: Run Nmap against the Metasploitable machine.

```
(kali㉿kali)-[~]  
$ nmap 192.168.1.103  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 16:34 EST  
Nmap scan report for 192.168.1.103  
Host is up (0.0034s latency).  
Not shown: 979 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
3389/tcp  open  ms-wbt-server  
4848/tcp  open  appserv-http  
7676/tcp  open  imqbrokerd  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
8181/tcp  open  intermapper  
8383/tcp  open  m2mservices  
9200/tcp  open  wap-wsp  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49158/tcp open  unknown  
49159/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

## Section 2. Profiling a Target System

**Step 1:** Power on all VMs.

**Step 2:** Use Nmap to find operating systems, versions, and SMB script scanning for Metasploitable 3.

```
(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.103

Not shown: 979 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ ftp-syst:
|_ SYST: Windows_NT
22/tcp    open  ssh          OpenSSH 7.1 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 fd:08:98:ca:3c:e8:c1:3c:ea:dd:09:1a:2e:89:a5:1f (RSA)
|_ 521 7e:57:81:8e:f6:3c:1d:cf:eb:7d:ba:d1:12:31:b5:a8 (ECDSA)
80/tcp    open  http         Microsoft IIS httpd 7.5
|_ http-server-header: Microsoft-IIS/7.5
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  sonal-freemail@thawte.com Windows Server 2008 R2 Standard 7601
Service Pack 1 microsoft-ds
3306/tcp   open  mysql        MySQL 5.5.20-log
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.5.20-log
|_ Thread ID: 4
|_ Capabilities flags: 63487
|_ Some Capabilities: ConnectWithDatabase, ODBCClient, Support41Auth,
SupportsTransactions, SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolOld,
LongColumnFlag, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew,
SupportsCompression, FoundRows, IgnoreSgppipes, LongPassword,
DontAllowDatabaseTableName, SupportsMultipleResults, SupportsAuthPlugins,
SupportsMultipleStatements
|_ Status: Autocommit
|_ Salt: {54E<<W%M6f!!}PXG=<<S
|_ Auth Plugin Name: mysql_native_password
3389/tcp   open  ssl/ms-wbt-server?
|_ rdp-ntlm-info:
|_ Target_Name: VAGRANT-2008R2
|_ NetBIOS_Domain_Name: VAGRANT-2008R2
|_ NetBIOS_Computer_Name: VAGRANT-2008R2
|_ DNS_Domain_Name: vagrant-2008R2
|_ DNS_Computer_Name: vagrant-2008R2
|_ Product_Version: 6.1.7601
|_ System_Time: 2024-02-13T21:57:35+00:00
|_ ssl-cert: Subject: commonName=vagrant-2008R2
|_ Not valid before: 2024-01-07T15:49:21
|_ Not valid after: 2024-07-08T15:49:21
|_ ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.
4848/tcp   open  ssl/http     Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_ ssl-cert: Subject: commonName=localhost/organizationName=Oracle
Corporation/stateOrProvinceName=California/countryName=US
|_ Not valid before: 2013-05-15T05:33:38
|_ Not valid after: 2023-05-13T05:33:38
|_ http-server-header: GlassFish Server Open Source Edition 4.0
|_ ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.
|_ http-title: Did not follow redirect to https://192.168.1.103:4848/
7676/tcp   open  java-message-service Java Message Service 301
8009/tcp   open  ajp13        Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp   open  http         Sun GlassFish Open Source Edition 4.0
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: GlassFish Server Open Source Edition 4.0
|_ http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
8181/tcp   open  ssl/intermapper?
|_ ssl-cert: Subject: commonName=localhost/organizationName=Oracle
Corporation/stateOrProvinceName=California/countryName=US
|_ Not valid before: 2013-05-15T05:33:38
|_ Not valid after: 2023-05-13T05:33:38
|_ ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.
8383/tcp   open  http         Apache httpd

|_ http-server-header: Apache
|_ http-title: 400 Bad Request
9200/tcp   open  wap-wsp?
|_ fingerprint-strings:
|_ FourOhFourRequest:
|_ HTTP/1.0 400 Bad Request
|_ Content-Type: text/plain; charset=UTF-8
|_ Content-Length: 80
|_ handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
|_ GetRequest:
|_ HTTP/1.0 200 OK
|_ Content-Type: application/json; charset=UTF-8
|_ Content-Length: 307
|_ "status" : 200,
|_ "name" : "Gravity",
|_ "version" : {
|_ "number" : "1.1.1",
|_ "build_hash" : "f1585f096d3f3985e73456ebdc1a0745f512bbc",
|_ "build_timestamp" : "2014-04-16T14:27:12Z",
|_ "build_snapshot" : false,
|_ "lucene_version" : "4.7"
|_ "tagline" : "You Know, for Search"
|_ HTTPOptions:
|_ HTTP/1.0 200 OK
|_ Content-Type: text/plain; charset=UTF-8
|_ Content-Length: 0
|_ RTSPRequest, SIPOptions:
|_ HTTP/1.1 200 OK
|_ Content-Type: text/plain; charset=UTF-8
|_ Content-Length: 0
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49158/tcp  open  java-rmi      Java RMI
49159/tcp  open  tcpwrapped
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS
MAC: 08:00:27:d7:cc:d8 (Oracle VirtualBox virtual NIC)
|_ smb-os-discovery:
|_ OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008
R2 Standard 6.1)
|_ OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|_ Computer name: vagrant-2008R2
|_ NetBIOS computer name: VAGRANT-2008R2\x00
|_ Workgroup: WORKGROUP\x00
|_ System time: 2024-02-13T13:57:32-08:00
|_ smb2-time:
|_ date: 2024-02-13T21:57:32
|_ start_date: 2024-02-13T21:27:20
|_ smb2-security-mode:
|_ 2:1:0:
|_ Message signing enabled but not required
|_ smb-security-mode:
|_ account_used: <blank>
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 1h08m34s, deviation: 3h01m25s, median: 0s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.61 seconds

(kali㉿kali)-[~]
└─$
```

### Step 3: Use Nmap to find operating systems, versions, and SMB script scanning for Metasploitable.

```
(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.101

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 17:01 EST
Nmap scan report for 192.168.1.101
Host is up (0.00095s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|ftp-syst:
|STAT:
|FTP server status:
|Connected to 192.168.1.100
|Logged in as ftp
|TYPE: ASCII
|No session bandwidth limit
|Session timeout in seconds is 300
|Control connection is plain text
|Data connections will be plain text
|vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|ssh-hostkey:
|1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|sslv2:
|SSLv2 supported
|ciphers:
|SSL2_RC2_128_CBC_WITH_MD5
|SSL2_DES_64_CBC_WITH_MD5
|SSL2_RC4_128_WITH_MD5
|SSL2_RC4_128_EXPORT40_WITH_MD5
|SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-02-13T22:02:12+00:00; -1s from scanner time.
|ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=There is no such thing outside US/countryName=XX
|Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain   ISC BIND 9.4.2
|dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
|rpcinfo:
|program version port/proto service
|100000 2 111/tcp rpcbind
|100000 2 111/udp rpcbind
|100003 2,3,4 2049/tcp nfs
|100003 2,3,4 2049/udp nfs
|100005 1,2,3 40316/udp mountd
|100005 1,2,3 57301/tcp mountd
|100021 1,3,4 50276/tcp nlockmgr
|100021 1,3,4 60764/udp nlockmgr
|100024 1 41106/tcp status
|100024 1 41428/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb      Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath gmirregistry
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
|mysql-info:
|Protocol: 10
|Version: 5.0.51a-3ubuntu5
|Thread ID: 10
|Capabilities flags: 43564
```

```
|Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsCompression,
SupportsTransactions, SwitchToSSLAfterHandshake, Support41Auth,
ConnectWithDatabase
|Status: Autocommit
|_Salt: ACKs*!1YMWObIzgs,1^
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|ssl-cert: Subject:
commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=There is no such thing outside US/countryName=XX
|Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2024-02-13T22:02:12+00:00; -1s from scanner time.
5900/tcp  open  vnc      VNC (protocol 3.3)
|vnc-info:
|Protocol version: 3.3
|Security types:
|_VNC Authentication (2)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd
|irc-info:
|users: 1
|servers: 1
|lusers: 1
|lservers: 0
|server: irc.Metasploitable.LAN
|version: Unreal3.2.8.1. irc.Metasploitable.LAN
|uptime: 0 days, 0:35:30
|source ident: nmap
|source host: 37D4021C.78DED367.FFFA6D49.IP
|_error: Closing Link: jesoagrijl[192.168.1.100] (Quit: jesoagrijl)
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|smb-os-discovery:
|OS: Unix (Samba 3.0.20-Debian)
|Computer name: metasploitable
|NetBIOS computer name:
|Domain name: localdomain
|FQDN: metasploitable.localdomain
|_System time: 2024-02-13T17:02:00-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|smb-security-mode:
|account_used: <blank>
|authentication_level: user
|challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_lock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s
```

Service detection performed. Please report any incorrect results at  
<https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 25.34 seconds

```
(kali㉿kali)-[~]
└─$
```