Scanning

Chapter 5

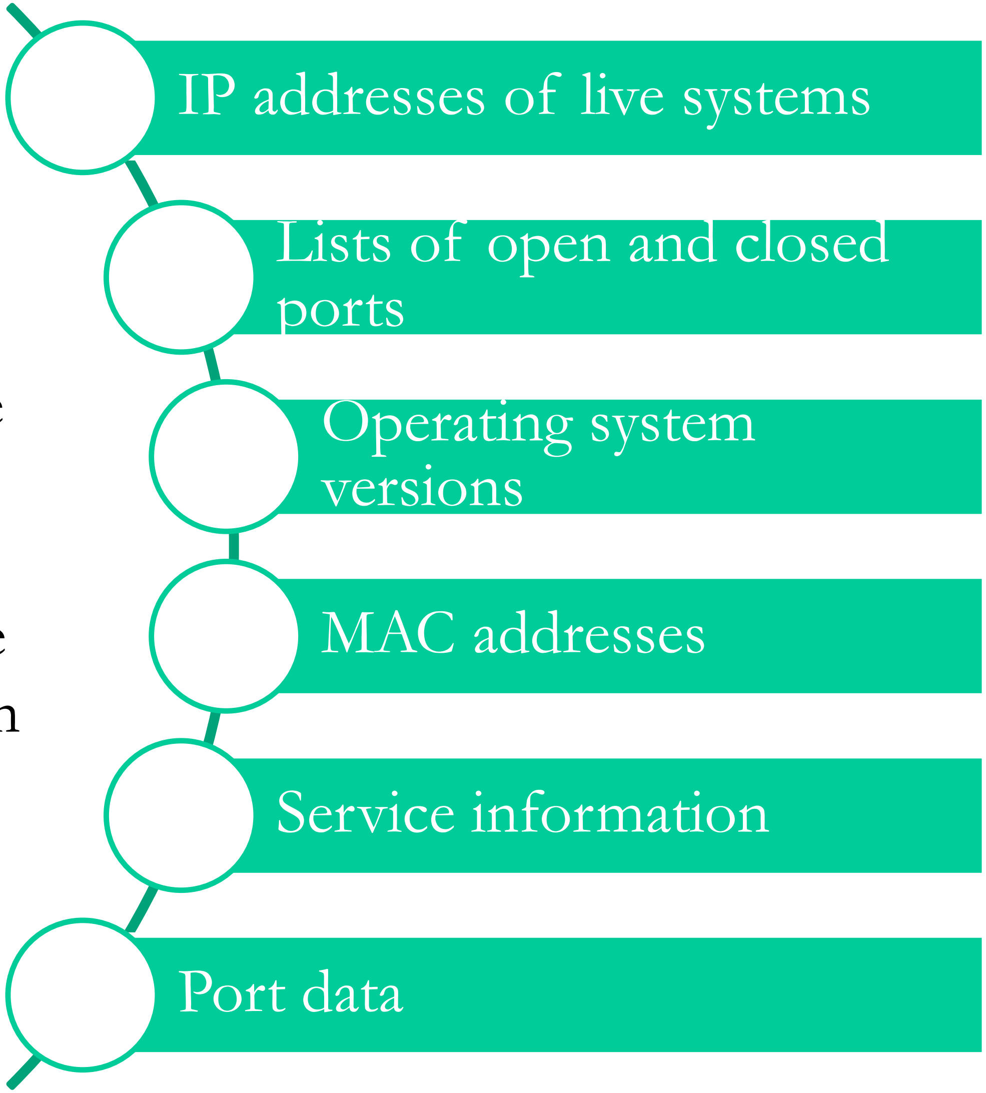
The Role of Scanning

Each scan type is like a piece of a larger puzzle that can be assembled to gain a clearer view of the overall target.

- **Ping sweep**
- **Port scanning**
- **Vulnerability scanning**

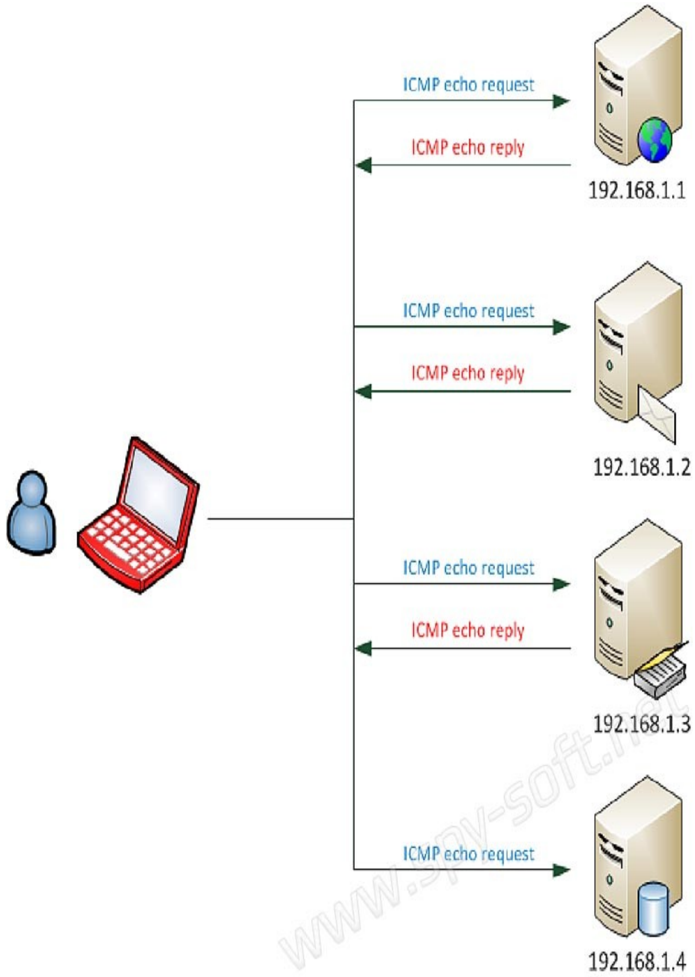
Getting Started with Scanning

Network scanning is an intense and methodical process of uncovering the structure of the network and hosts on it. The information gathered here can refine the enumeration process later.



- IP addresses of live systems
- Lists of open and closed ports
- Operating system versions
- MAC addresses
- Service information
- Port data

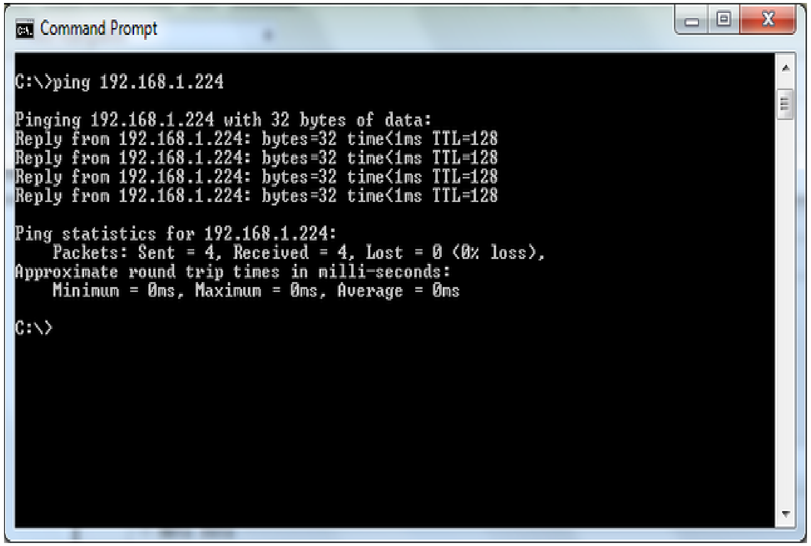
Target Up or Down



- Important to locate which systems are online
- Not every address in a range of IP addresses is "on"
- Need to eliminate systems that are off from those that are on
- Scans to locate "on" or "off" systems are called *ping sweeps* or *ICMP scans*

A quick way to check for live systems is to use the ping function to perform a ping sweep or ICMP scan. Pinging is the process of using the ping command to ascertain the status of a given system, specifically if it is responsive or not.

What Does a Ping Look Like?



```
C:\>ping 192.168.1.224

Pinging 192.168.1.224 with 32 bytes of data:
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Ping is used diagnostically to ensure that the host computer the user is trying to reach is actually operating. Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply.

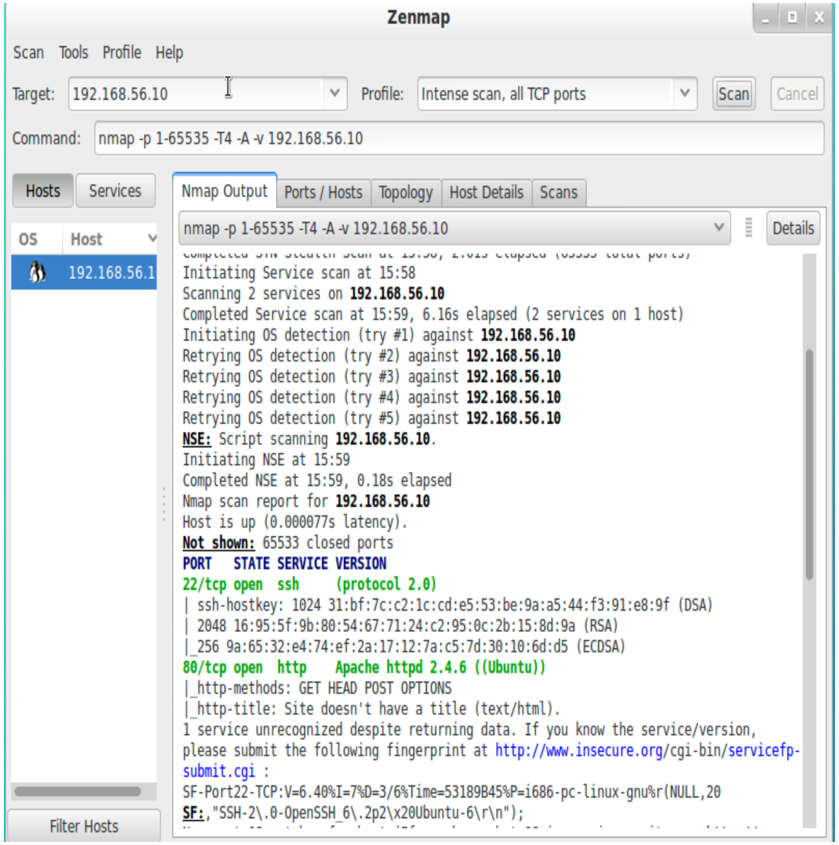
- Ping is a common network diagnostic utility
- Used to diagnose network problems
- Present in every operating system
- Uses the Internet Control Message Protocol (ICMP)
- Sends a packet to a remote system and waits for a response
- If no response within a set time, the target is listed as unreachable

Angry IP Scanner

- Common scanner used to perform ping scans
- Can scan a range of IP addresses and their ports
- Pings each address to determine whether it’s alive
- Can scan a range of IP addresses extremely fast
- Can save results to a file for later use

Introducing NMAP

The utility is used for everything from performing network inventory to security auditing as well as monitoring systems.



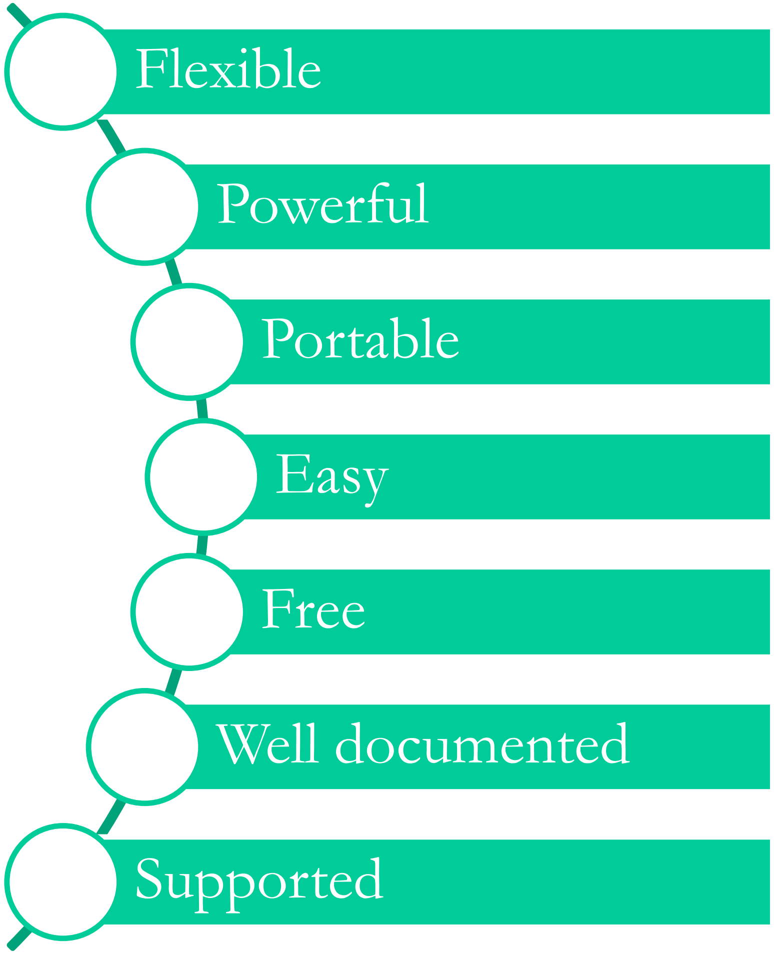
Target: 192.168.56.10

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.56.10

```
nmap -p 1-65535 -T4 -A -v 192.168.56.10
```

```
Initiating Service scan at 15:58
Scanning 2 services on 192.168.56.10
Completed Service scan at 15:59, 6.16s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.10
Retrying OS detection (try #2) against 192.168.56.10
Retrying OS detection (try #3) against 192.168.56.10
Retrying OS detection (try #4) against 192.168.56.10
Retrying OS detection (try #5) against 192.168.56.10
NSE: Script scanning 192.168.56.10.
Initiating NSE at 15:59
Completed NSE at 15:59, 0.18s elapsed
Nmap scan report for 192.168.56.10
Host is up (0.000077s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
| ssh-hostkey: 1024 31:bf:7c:c2:1c:cd:e5:53:be:9a:a5:44:f3:91:e8:9f (DSA)
| 2048 16:95:5f:9b:80:54:67:71:24:c2:95:0c:2b:15:8d:9a (RSA)
|_256 9a:65:32:e4:74:ef:2a:17:12:7a:c5:7d:30:10:6d:d5 (ECDSA)
80/tcp open  http    Apache httpd 2.4.6 ((Ubuntu))
|_http-methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-
submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=3/6%Time=53189B45%P=i686-pc-linux-gnu%r(NULL,20
SF:,"SSH-2\.0-OpenSSH_6\.2p2\x20Ubuntu-6\r\n");
```



Flexible

Powerful

Portable

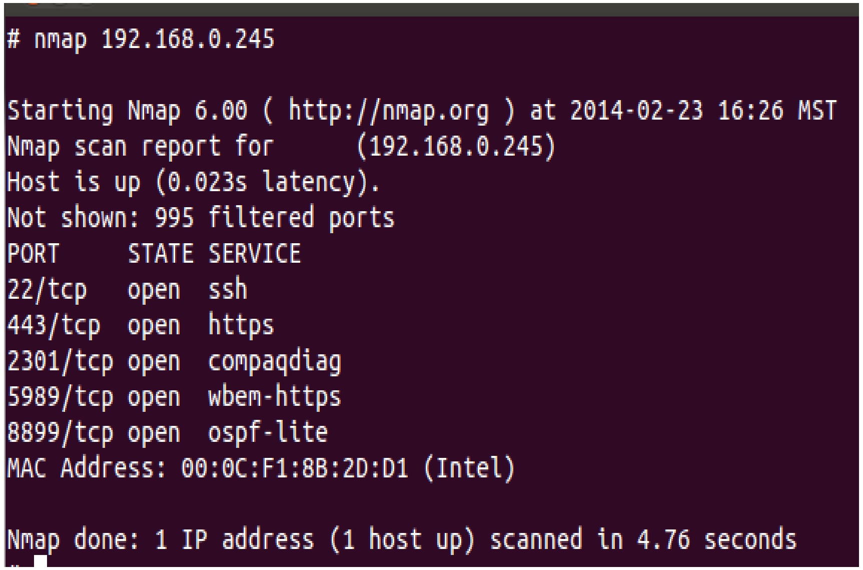
Easy

Free

Well documented

Supported

What Is a Port Scan?



```
# nmap 192.168.0.245

Starting Nmap 6.00 ( http://nmap.org ) at 2014-02-23 16:26 MST
Nmap scan report for       (192.168.0.245)
Host is up (0.023s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
2301/tcp open  compaqdiag
5989/tcp open  wbem-https
8899/tcp open  ospf-lite
MAC Address: 00:0C:F1:8B:2D:D1 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Used to identify the open and closed ports on a system

A port is a virtual endpoint on a system

Examples are port 80 for HTTP and 21 for FTP

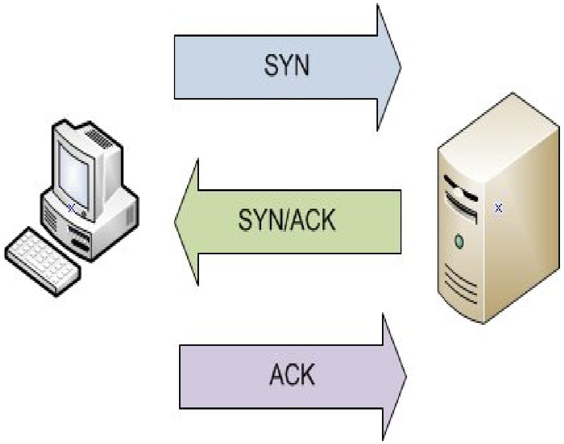
When combined with an IP address, they form a socket

A socket identifies which service to connect to on a system

Port scans allow an attacker to locate potential entry points

TCP and the Three-Way Handshake

TCP establishes connections and then verifies that each and every packet makes it to their destination in the right order. To accomplish this, TCP uses the three-way handshake.



Ports can be TCP or UDP.

TCP is a connection-oriented protocol.

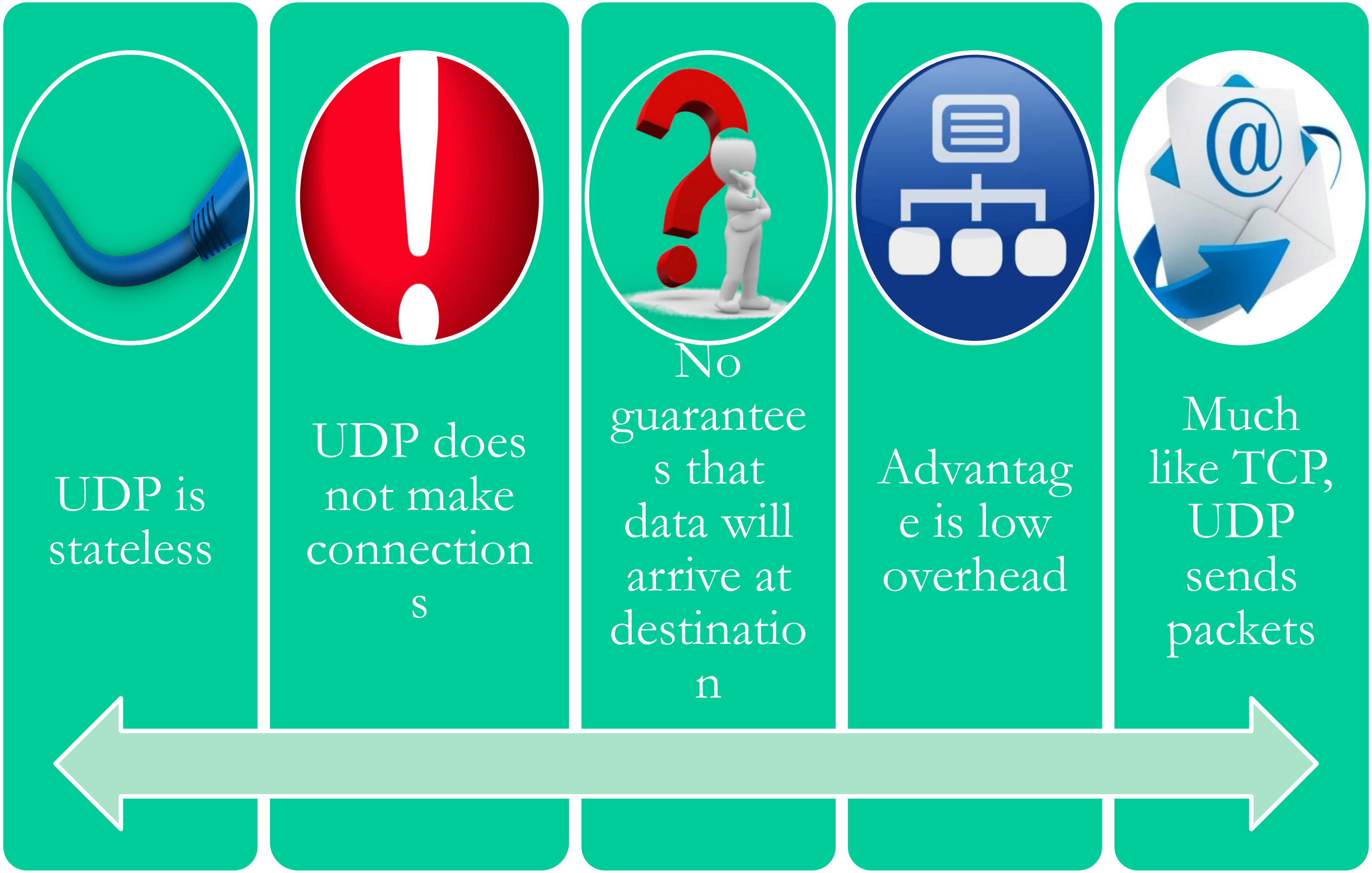
The three-way handshake is used to establish a connection.

The completion of three-way handshake is used before sending packets.

The three-way handshake does not handle security.

TCP also provides sequence numbers for the reassembly of data.

User Datagram Protocol (UDP)



UDP is stateless

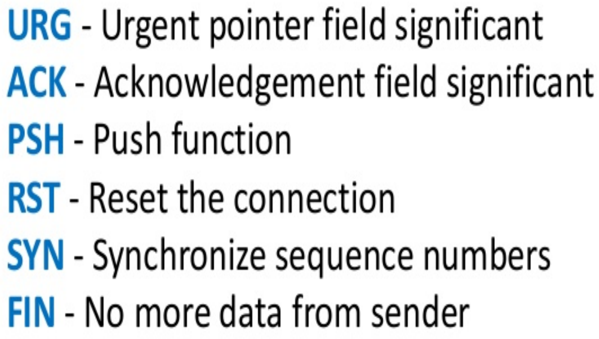
UDP does not make connections

No guarantees that data will arrive at destination

Advantage is low overhead

Much like TCP, UDP sends packets

TCP Flags



URG - Urgent pointer field significant
ACK - Acknowledgement field significant
PSH - Push function
RST - Reset the connection
SYN - Synchronize sequence numbers
FIN - No more data from sender

SYN: Used to initiate a connection between two different hosts in order to facilitate communications

ACK: Used to acknowledge the receipt of a packet of information

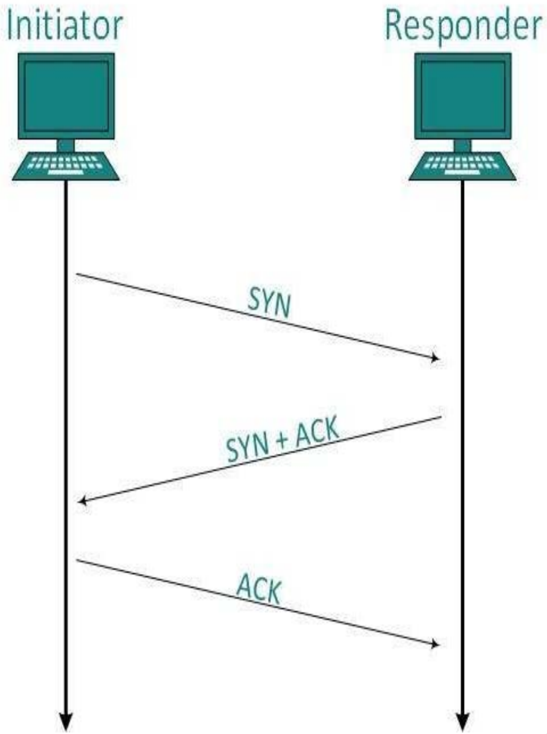
URG: States that the data contained in the packet should be processed immediately

PSH: Instructs the sending system to send all buffered data immediately

FIN: Tells the remote system that no more information will be sent. In essence this is gracefully closing a connection.

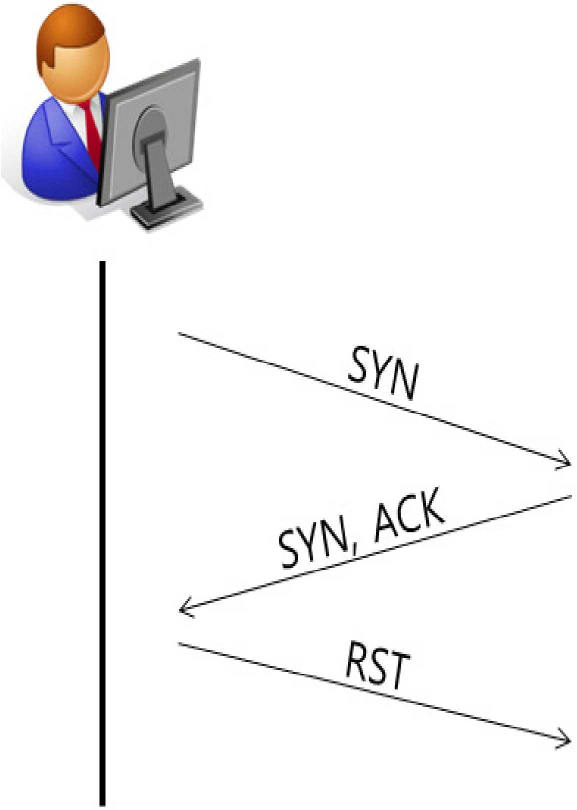
RST: Represents a reset packet that is used to reset a connection.

TCP Full Connect Scan



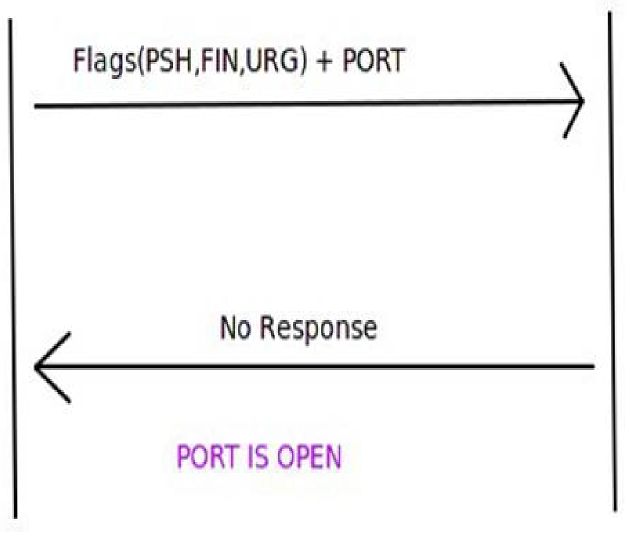
- Utilizes the three-way handshake
- Completed handshake indicates open port
- Incomplete handshake indicates closed
- Scan gives most accurate picture of port status
- Drawback is scan can be easily logged
- nmap –sT–v <target IP address>

Half Open Scans



- Starts like full connect scan
- Scan does not complete the final step of the handshake
- Benefit is scan has lower chance of being logged
- Scan tends to be faster than full connect
- nmap –sS –v <target IP address>

XMAS Scan



A packet is sent with PSH, URG, and FIN all set at once

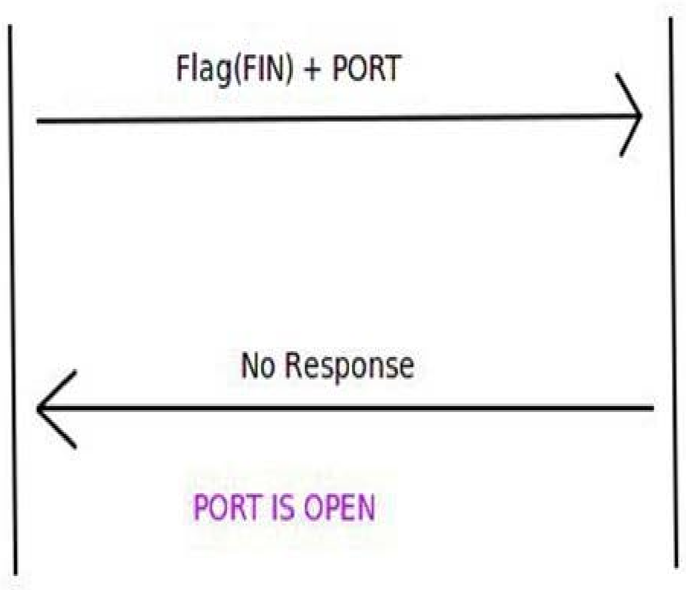
Combination of flags is illogical and illegal

Some software developers do not implement TCP correctly

Does not work on most modern systems

nmap –sX –v <target IP address>

FIN Scan



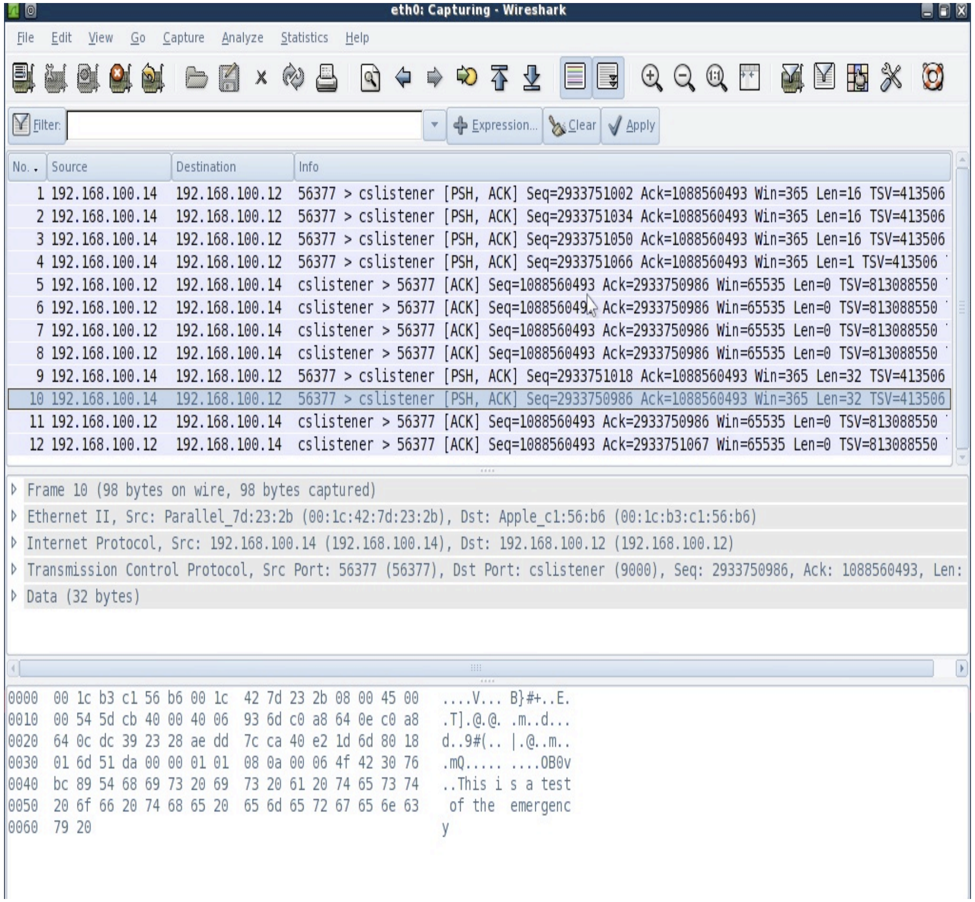
Occurs when a packet is sent with the FIN flag set

Used to determine whether ports are open or closed

May not function on newer targets

Can be blocked by some firewalls

Fragmenting


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

No.	Source	Destination	Info
1	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933751002 Ack=1088560493 Win=365 Len=16 TSV=413506
2	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933751034 Ack=1088560493 Win=365 Len=16 TSV=413506
3	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933751050 Ack=1088560493 Win=365 Len=16 TSV=413506
4	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933751066 Ack=1088560493 Win=365 Len=1 TSV=413506
5	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=1088560493 Ack=2933750986 Win=65535 Len=0 TSV=813088550
6	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=108856049 Ack=2933750986 Win=65535 Len=0 TSV=813088550
7	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=1088560493 Ack=2933750986 Win=65535 Len=0 TSV=813088550
8	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=1088560493 Ack=2933750986 Win=65535 Len=0 TSV=813088550
9	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933751018 Ack=1088560493 Win=365 Len=32 TSV=413506
10	192.168.100.14	192.168.100.12	56377 > cslistener [PSH, ACK] Seq=2933750986 Ack=1088560493 Win=365 Len=32 TSV=413506
11	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=1088560493 Ack=2933750986 Win=65535 Len=0 TSV=813088550
12	192.168.100.12	192.168.100.14	cslistener > 56377 [ACK] Seq=1088560493 Ack=2933751067 Win=65535 Len=0 TSV=813088550

```
▷ Frame 10 (98 bytes on wire, 98 bytes captured)
▷ Ethernet II, Src: Parallel_7d:23:2b (00:1c:42:7d:23:2b), Dst: Apple_c1:56:b6 (00:1c:b3:c1:56:b6)
▷ Internet Protocol, Src: 192.168.100.14 (192.168.100.14), Dst: 192.168.100.12 (192.168.100.12)
▷ Transmission Control Protocol, Src Port: 56377 (56377), Dst Port: cslistener (9000), Seq: 2933750986, Ack: 1088560493, Len:
▷ Data (32 bytes)
```

```
0000  00 1c b3 c1 56 b6 00 1c  42 7d 23 2b 08 00 45 00   ....V... B}#+..E.
0010  00 54 5d cb 40 00 40 06  93 6d c0 a8 64 0e c0 a8   .T].@.@. .m..d...
0020  64 0c dc 39 23 28 ae dd  7c ca 40 e2 1d 6d 80 18   d..9#(.. |.@..m..
0030  01 6d 51 da 00 00 01 01  08 0a 00 06 4f 42 30 76   .mQ..... ....OB0v
0040  bc 89 54 68 69 73 20 69  73 20 61 20 74 65 73 74   ..This i s a test
0050  20 6f 66 20 74 68 65 20  65 6d 65 72 67 65 6e 63    of the  emergenc
0060  79 20                                              y
```

Fragmenting breaks up packets

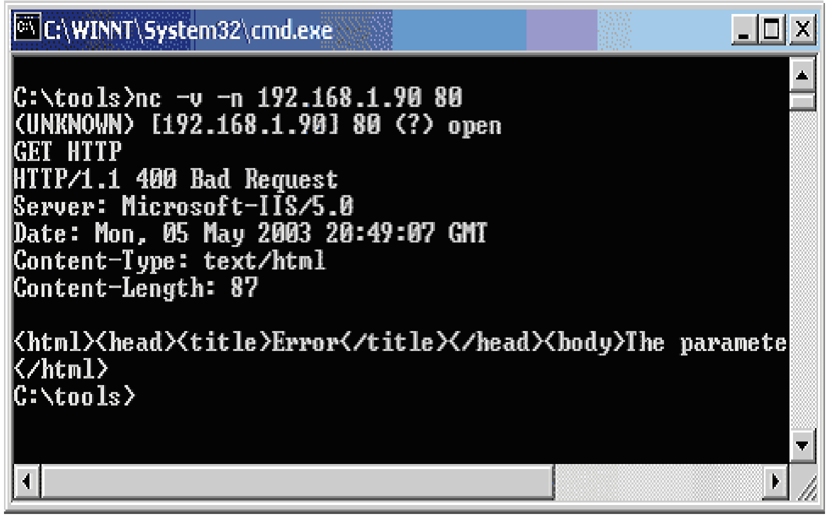
Is reassembled by target

Packets are fragmented when they exceed a network's MTU

Fragmenting can be used to evade detection

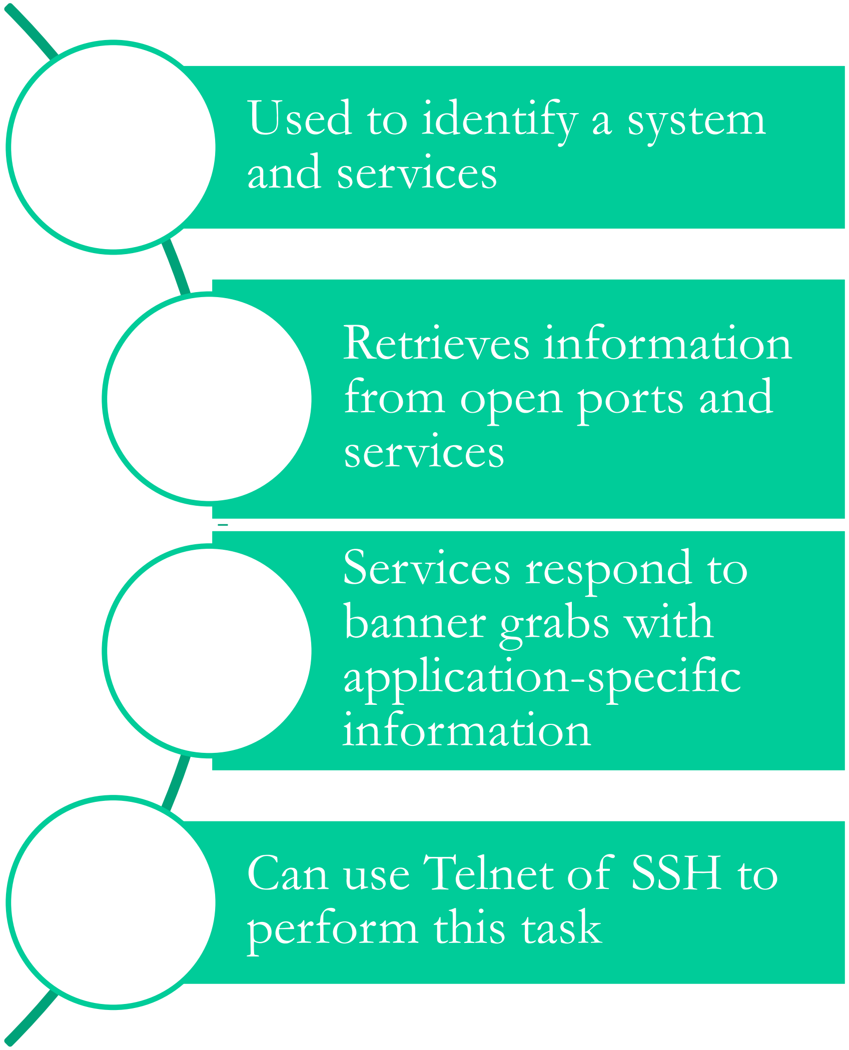
Banner Grabbing

Banner grabbing is an activity that is used to determine information about services that are being run on a remote computer.



```
C:\tools>nc -v -n 192.168.1.90 80
(UNKNOWN) [192.168.1.90] 80 (?) open
GET HTTP
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2003 20:49:07 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The paramete
</html>
C:\tools>
```



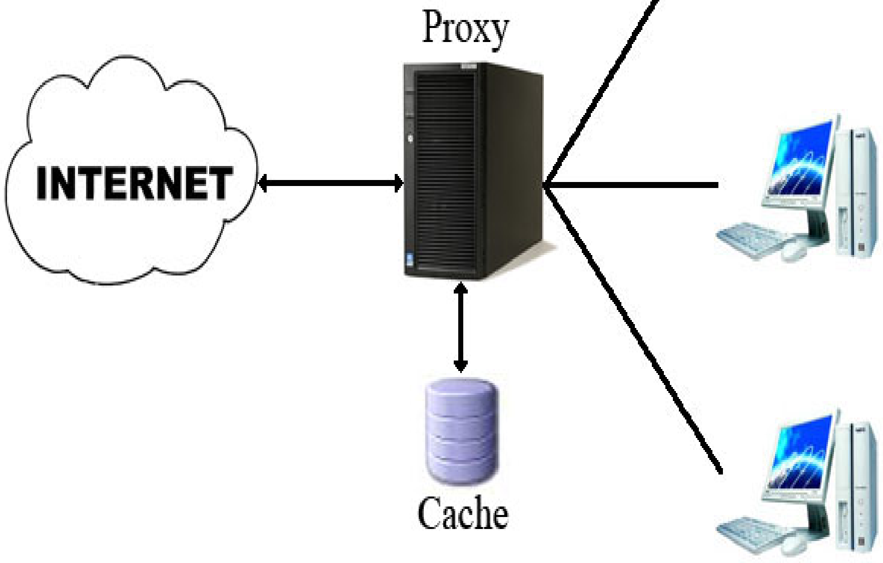
- Used to identify a system and services
- Retrieves information from open ports and services
- Services respond to banner grabs with application-specific information
- Can use Telnet of SSH to perform this task

Vulnerability Scanners

These tools function by checking coding, ports, variables, banners, and many other potential problems areas looking for issues.

- Used to identify known vulnerabilities
- Not typically stealthy
- Generally performed by automated means
- May only catch problems that are already known
- Not a good choice if trying to simulate an attack

Providing Cover with Proxies



- A proxy can lower chances of detection
- Routes traffic through a machine acting as proxy
- Can perform content filtering
- Can provide anonymizing services

Summary

- Scanning requires a good understanding of networking technologies.
- Enumeration follows scanning.
- Enumeration seeks to reveal information from a system.
- Enumeration is an active measure.
- Information can include usernames, group information, printer data, and other data.