**What we already Have:**

We are able to do

1. syn scan.
2. port service discovery.

**SYN Scan:**

So there comes a better way to scan, that called SYN scan. Also known as half-open scan.

It doesn’t need to establish a full TCP connect() and can get information about the port that been scanned. It’s very similar to the TCP scan, but it will tear down the connection immediately when receive a SYN/ACK instead of sending ACK responses back.

So the Scan will look like the diagram below if the port is open:

Host A(status): Host B(status)

Send SYN(seq =x )

Receive SYN(seq = x)

Send SYN/ACK(seq=y,ack=x+1)

Receive SYN/ACK(seq=y,ack=x+1)

Receive RST, connection shut down.

Send RST

And if the port is closed, we will receive a RST/ACK:

Host A (status): Host B (status)

Send SYN(seq =x )

Receive SYN(seq = x)

Send RST/ACK

Receive RST/ACK, then shut down the connection

And if we do the scan in this way, we will always be unlogged by the connection with basic IDS. We can also get the fairly positive information about the port.

And we do save a lot of time by tearing down the connection immediately instead of sending ACK responses. And it has reliable capability to recognize the port that if it’s open or not.

Though the standard Intrusion detection systems, but it was used to avoid the IDS.

**Advantage:**

Due to this type of scan doesn’t need to do the full of TCP connect().

* It’s much more quicker than full TCP connect().
* It’s reliable for recognize a port.
* It can avoid the basic IDS log.
* It needn’t to do the three handshakes.

**Disadvantage:**

* It would cause problem for some network stacks, particular for the simple device, such as printer.
* Only if you have root privilege, you can create yourself SYN pocket.
* Nowadays, rulesets block so many SYN scan attempt.

**Port Service discovery:**

We have a enum type of structure to store the popular service port, such as 25 for smtp and 80 for http.

Once we have detected the number of the port,then we could use the port num to compare with that structure then we will know the service supplied by that port.

**Enhancement for our TCP Scanner:**

Nowadays, many firewall can log syn, so we need an advanced method to avoid logged.

(1)FIN Scan

(2)ACK Scan

These three scans can enhance our TCP Scanner.

**Nmap do have that kinds of Scan:**

* FIN scan(No use for windows): Exploit the theory that once a port is closed it will tend to return a RST. If the port is opened it will ignored the package that have something wrong(reference the RFC 793 page 43).

(reference <http://nmap.org/book/man-port-scanning-basics.html> )

If the port is CLOSE:

Host A (status): Host B (status)

Receive FIN

Send FIN

Send a RST

Receive RST

If the port is open:

Host A (status): Host B (status)

Receive FIN

Send FIN

No reaction.

The Host B tend to throws the Package away.

If we once get the ICMP package, then we could not judge the status about that port

Host A (status): Host B (status)

Receive FIN

Send FIN

Send a ICMP error message

Receive ICMP error message

* ACK scan: It’s an advanced scan type, it does not actually give the information about whether the port is open or closed. But it can use to find the port that unfiltered. It’s used to map firewall rulesets,classifies ports into this state.

Whether it is open or not it will return RST package. Then analyze the package received.

(reference <http://nmap.org/book/man-port-scanning-basics.html> )

Host A (status): Host B (status)

Receive ACK

Send ACK

Send RST

Receive RST