Port Scanning Techniques

Interesting notes:

- Most of the scan types are only available to privileged users. This is because they send and receive **raw packets** (that is simple bit strings).
- Only one method may be used at a time, except that UDP scan (`-sU`) may be combined with any one of the TCP scan types.
- Port scan type options are of the form `-sC`, where *C* is a prominent character in the scan name, usually the first. The one exception to this is the deprecated FTP bounce scan (`-b`).
- By default, Nmap performs a **SYN Scan**, though it substitutes a connect scan (using the **connect() syscall**) if the user does not have proper privileges to send raw packets (requires root access on Unix) or if IPv6 targets were specified. Unprivileged users can only execute connect and FTP bounce scans.

Scan types:

1. **`-sS` (TCP SYN scan)**
   - You send a **SYN packet**, as if you are going to open a real connection and then wait for a response.
   - A **SYN/ACK** indicates the port is listening (**open**), while a **RST** (reset) is indicative of a **non-listener**. If no response is received after several retransmissions, the port is marked as **filtered**. The port is also marked filtered if an **ICMP unreachable error** (type 3, code 1,2, 3, 9, 10, or 13) is received.
2. **`-sT` (TCP connect() scan)**
   - Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to **establish a connection with the target machine and port** by issuing the `connect()` **system call**.
   - The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does.
3. **`-sU` (UDP scans)**
   - UDP scan works by sending an empty (no data) UDP header to every targeted port.
   - If an **ICMP port unreachable error** (type 3, **code 3**) is returned, the port is `closed`. Other ICMP unreachable errors (type 3, **codes 1, 2, 9, 10, or 13**) mark the port as `filtered`. Occasionally, a service will respond with a UDP packet, proving that it is `open`.
   - If no response is received after retransmissions, the port is classified as `open|filtered`. This means that the port could be open, or perhaps packet filters are blocking the communication. **Versions scan (`-sV`)** can be used to help differentiate the truly open ports from the filtered ones.
4. **`-sN; -sF; -sX` (TCP Null, FIN, and Xmas scans)**
   - These three scan types exploit a subtle loophole in the TCP RFC to differentiate between `open` and `closed` ports.
   - When scanning systems compliant with this RFC text, **any packet not containing SYN, RST, or ACK bits** will result in a returned **RST** if the port is **closed** and **no response** at all if the port is **open**. As long as none of those three bits are included, any combination of the other three (**FIN, PSH, and URG**) are useful.

➢ **Null scan (`-sN`)**
  - Does not set any bits (**TCP flag header is 0**).

➢ **FIN scan (`-sF`)**
  - Sets just the **TCP FIN bit**.

➢ **Xmas scan (`-sX`)**
  - Sets the **FIN, PSH, and URG flags**, lighting the packet up like a Christmas tree.

- If a **RST packet** is received, the port is considered `closed`, while **no response** means it is `open|filtered`. The port is marked `filtered` if an **ICMP unreachable error** (type 3, code 1, 2, 3, 9, 10, or 13) is received.

5. **`-sA` (TCP ACK scan)**
   - This scan never determines `open` (or even `open|filtered`) ports. It is used to map out **firewall rulesets**, determining whether they are stateful or not and which ports are filtered.
   - The ACK scan probe packet has only the ACK flag set.
   - When scanning unfiltered systems, `open` and `closed` ports will both return a RST packet. Nmap then labels them as `unfiltered`, meaning that they are reachable by the ACK packet, but whether they are `open` or `closed` is undetermined.
   - **Ports that don't respond, or send certain ICMP error messages back (type 3, code 1, 2, 3, 9, 10, or 13), are labelled `filtered`.**
6. **`-sW` (TCP Window scan)**
   - Window scan is exactly the same as ACK scan except that **it exploits an implementation detail of certain systems to differentiate open ports from closed ones, rather than always printing `unfiltered` when a RST is returned.**
   - It does this by **examining the TCP Window field** of the **RST packets returned**.
   - On some systems, **open ports** use a **positive window size** (even for RST packets) while **closed ones** have a **zero window**.
   - So instead of always listing a port as `unfiltered` when it receives a RST back, Window scan lists the port as `open` or `closed` if the TCP Window value in that reset is positive or zero, respectively.
7. **`-sM` (TCP Maimon scan)**
   - his technique is exactly the same as Null, FIN, and Xmas scans, except that the probe is **FIN/ACK.**
   - According to RFC 793 (TCP), a **RST packet** should be generated in response to such a probe whether the port is open or closed.
8. **`--scanflags` (Custom TCP scan)**
   - The `--scanflags` option allows you to design your own scan by specifying arbitrary TCP flags.
   - The order these are specified in is irrelevant.
   - You can use symbolic names (`URG`, `ACK`, `PSH`, `RST`, `SYN` and `FIN`)
     For example, `--scanflags URGACKPSHRSTSYNFIN` sets everything
9. **`-sI` (Idlescan)**
   - This advanced scan method allows for a **truly blind TCP port scan** of the target (meaning **no packets are sent to the target from your real IP address**).
   - This scan technique exploits **predictable IP fragmentation ID sequence** generation on the **zombie host** to glean information about the open ports on the target.
   - **The zombie host should not have much traffic (hence the name Idle Scan)** and should offer

predictable IPID values.

- Every IP packet on the Internet has a "fragment identification" number. Many operating systems simply increment this number for every packet they send. So probing for this number can tell an attacker **how many packets have been sent since the last probe.**
- **IDS systems** will display the **scan** as **coming from the zombie machine** you specify (which must be up and meet certain criteria).

10. `-sO` **(IP protocol scan)**
    - IP protocol scan allows you to **determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported** by target machines.
    - This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.
    - Instead of iterating through the port number field of a UDP packet, it sends IP packet headers and iterates through the **8-bit IP protocol field**.
    - Instead of watching for ICMP port unreachable messages , protocol scan is on the lookout for **ICMP *protocol* unreachable messages**. If Nmap receives any response in any protocol from the target host, Nmap **marks that protocol as** `open`. An ICMP protocol unreachable error (type 3, code 2) causes the protocol to be **marked as** `closed.` Other **ICMP unreachable errors** (type 3, **code 1, 3, 9, 10, or 13**) cause the protocol to be **marked** `filtered` (**though they prove that ICMP is** `open` **at the same time**). If no response is received after retransmissions, the protocol is marked `open|filtered.`
11. `-b` **(FTP bounce scan)**
    - This scan exploits an interesting feature of the FTP protocol: its support for **proxy FTP connections .**
    - Through this technique is possible to cause the FTP server to port scan other hosts. Simply ask the FTP server to send a file to each interesting port of a target host in turn. The error message will describe whether the port is open or not.
    - Nmap supports FTP bounce scan with the `-b` option. It takes an argument of the form `username:password@server:port`. `Server` is the name or IP address of **a vulnerable FTP server.**
    - As with a normal URL, you may omit `username:password`, in which case anonymous login credentials (user: `anonymous` password:`-wwwuser@`) are used. The port number (and preceding colon) may be omitted as well, in which case the default FTP port (21) on `server` is used.

Barbagallo Valerio
Da Lozzo Giordano
Mellini Giampiero