**REMOTE/DIRECT PORT SCANNING**

1. An attacker uses a combination of techniques to determine the state of the ports on a remote target. Any service or application available for TCP or UDP networking will have a port open for communications over the network. Collecting this type of information tells the attacker which ports can be attacked directly, which must be attacked with filter evasion techniques like fragmentation, source port scans, and which ports are unprotected (i.e. not firewalled) but aren't hosting a network service. An attacker often combines various techniques in order to gain a more complete picture of the firewall filtering mechanisms in place for a host [1].

*Note:* After an attacker finds out information about the open ports, he/she may use variety of attack techniques to launch attacks and gain information (often by running malicious programs).

1. The information gathered by a port scan has many legitimate uses including network inventory and the verification of the security of a network. Port scanning can, however, also be used to compromise security. Many exploits rely upon port scans to find open ports and send specific data patterns in an attempt to trigger a condition known as a buffer overflow. Such behavior can compromise the security of a network and the computers therein, resulting in the loss or exposure of sensitive information and the ability to do work [2][3].
2. Open ports are used by applications and services and, as any piece of code, they may have vulnerabilities or bugs. The more applications and services run using open ports for Internet communication, the higher the risk of one of them having a vulnerability that can be exploited. A bug in one service reachable from the outside may cause it to crash. Such a crash may lead to execution of arbitrary code on the affected machine, exactly what the attacker needs in order to be successful. Additionally, exploiting application vulnerabilities may give the attacker access to data belonging to the application or the affected computer, as well as the opportunity to install malware, cause downtime or take control of the server [4].

**REFERENCES**

1. <https://capec.mitre.org/data/definitions/300.html>
2. <https://en.wikipedia.org/wiki/Port_scanner#Ethics>
3. Erikson, Jon (1977). HACKING the art of exploitation (2nd ed.). San Francisco: NoStarch Press. p. 264. ISBN 1-59327-144-1.
4. <https://www.acunetix.com/blog/articles/danger-open-ports-trojan-trojan/>