**UDP scan:**

**DESCRIPTION:**

UDP scanning methods involve **sending a UDP datagram to the target port and looking for evidence that the port is closed**. Open UDP ports usually do not respond to UDP datagrams as there is no stateful mechanism within the protocol that requires building or establishing a session.

An adversary engages in UDP scanning to gather information about UDP port status on the target system. UDP scanning methods involve sending a UDP datagram to the target port and looking for evidence that the port is closed. Open UDP ports usually do not respond to UDP datagrams as there is no stateful mechanism within the protocol that requires building or establishing a session. Responses to UDP datagrams are therefore application specific and cannot be relied upon as a method of detecting an open port. UDP scanning relies heavily upon ICMP diagnostic messages in order to determine the status of a remote port.

**Extended Description:**

During a UDP scan, a datagram is sent to a target port. If an 'ICMP Type 3 Port unreachable' error message is returned then the port is considered closed. Different types of ICMP messages can indicate a filtered port. UDP scanning is slower than TCP scanning. The protocol characteristics of UDP make port scanning inherently more difficult than with TCP, as well as dependent upon ICMP for accurate scanning. Due to ambiguities that can arise between open ports and filtered ports, UDP scanning results often require a high degree of interpretation and further testing to refine. In general, UDP scanning results are less reliable or accurate than TCP-based scanning.

**PREREQUISITES:**

The ability to send UDP datagrams to a host and receive ICMP error messages from that host. In cases where particular types of ICMP messaging is disallowed, the reliability of UDP scanning drops off sharply.

**UDP port scan attack**:

A port scan is **a common technique hackers use to discover open doors or weak points in a network**. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

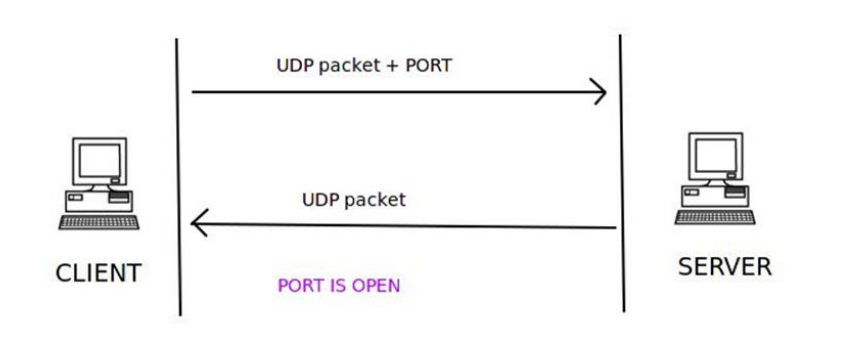
**EXECUTION FLOW**:

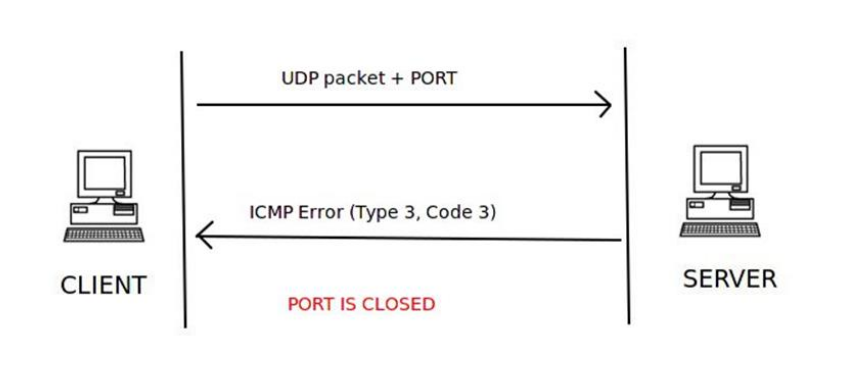
* An adversary sends UDP packets to target ports.
* An adversary uses the response from the target to determine the port's state. Whether a port responds to a UDP packet is dependent on what application is listening on that port. No response does not indicate the port is not open.

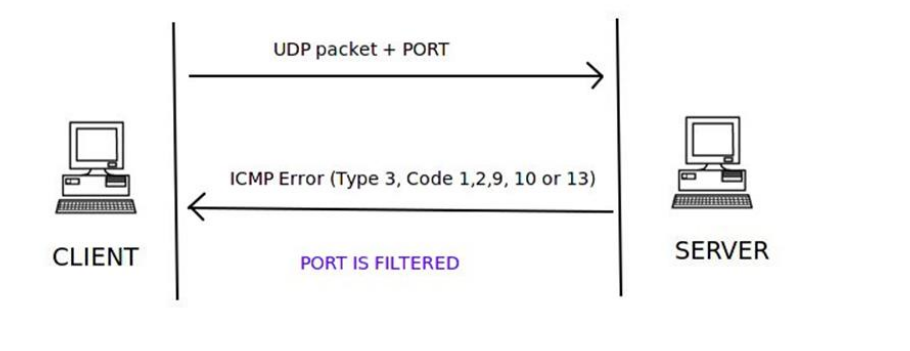
**DRAWBACKS**:

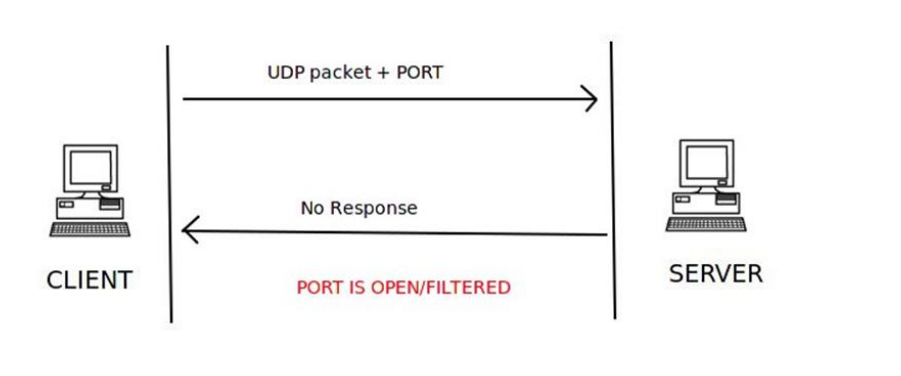
* The major drawback of UDP scan is **the scan is slow**.
* Since there is no response from the open port, the scanner has to resent the packet multiple times leading to the delay.

**STRUCTURE:**





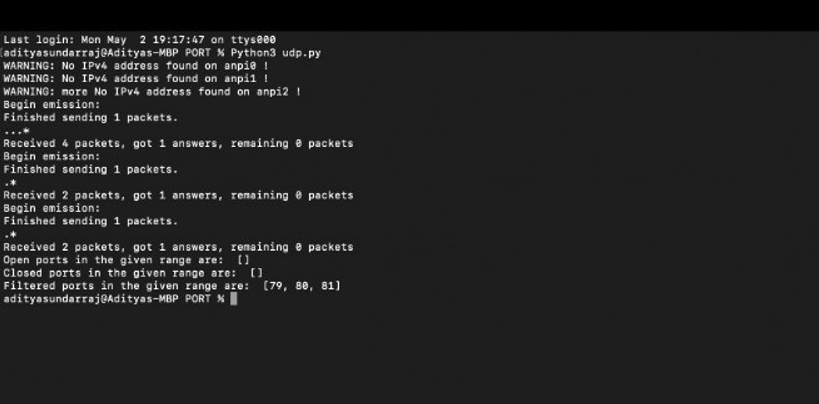




**CODE:**



**OUTPUT**:



**NULL SCAN**:

**DESCRIPTION:**

 An adversary uses a TCP NULL scan **to determine if ports are closed on the target machine**. This scan type is accomplished by sending TCP segments with no flags in the packet header, generating packets that are illegal based on RFC 793.

In a NULL scan, no flag is set inside the TCP packet. The TCP packet is sent along with the port number only to the server. If the server sends no response to the NULL scan packet, then that particular port is open

An adversary uses a TCP NULL scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with no flags in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behaviour is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

**Extended Description:**

In addition to being fast, the major advantage of this scan type is its ability to scan through stateless firewall or ACL filters. Such filters are configured to block access to ports usually by preventing SYN packets, thus stopping any attempt to 'build' a connection. NULL packets, like out-of-state FIN or ACK packets, tend to pass through such devices undetected. Additionally, because open ports are inferred via no responses being generated, one cannot distinguish an open port from a filtered port without further analysis. For instance, NULL scanning a system protected by a stateful firewall may indicate all ports being open. Because of their obvious rule-breaking nature, NULL scans are flagged by almost all intrusion prevention or intrusion detection systems

**DRAWBACKS**:

Exposure of Sensitive Information to an Unauthorized Actor

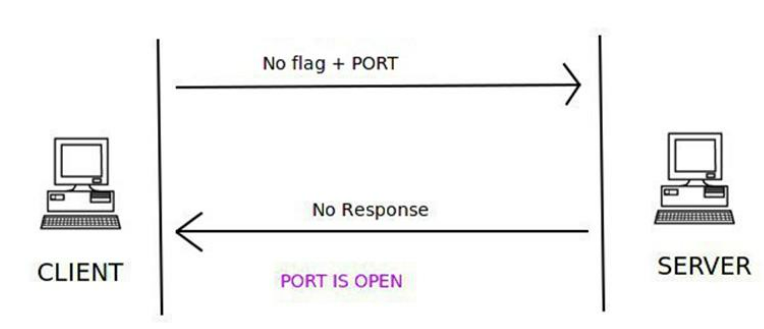
**EXECUTION FLOW**:

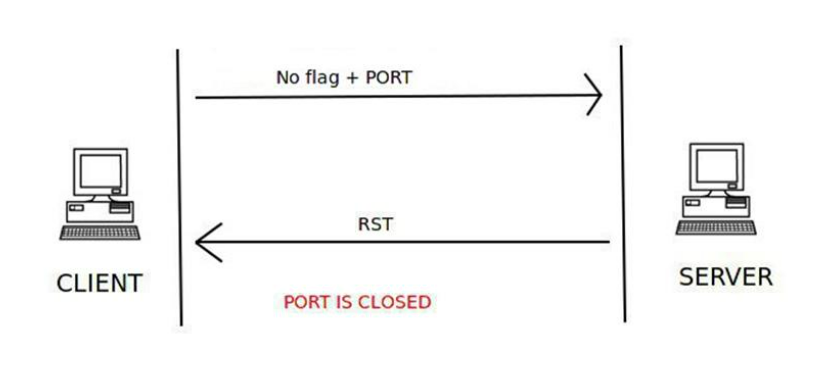
* An adversary sends TCP packets with no flags set and that are not associated with an existing connection to target ports.
* An adversary uses the response from the target to determine the port's state. If no response is received the port is open. If a RST packet is received then the port is closed.

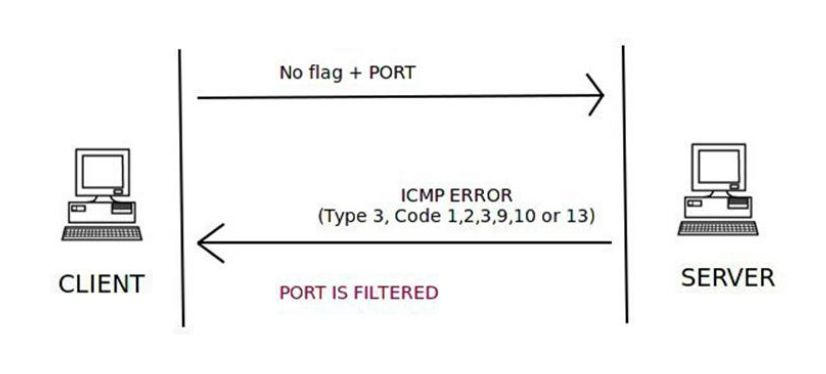
**CONSEQUENCES:**

|  |  |
| --- | --- |
| **Scope** | **Impact** |
| Confidentiality | Other |
| Confidentiality  Access Control  Authorization | Bypass Protection Mechanism  Hide Activities |

**STRUCTURE**:

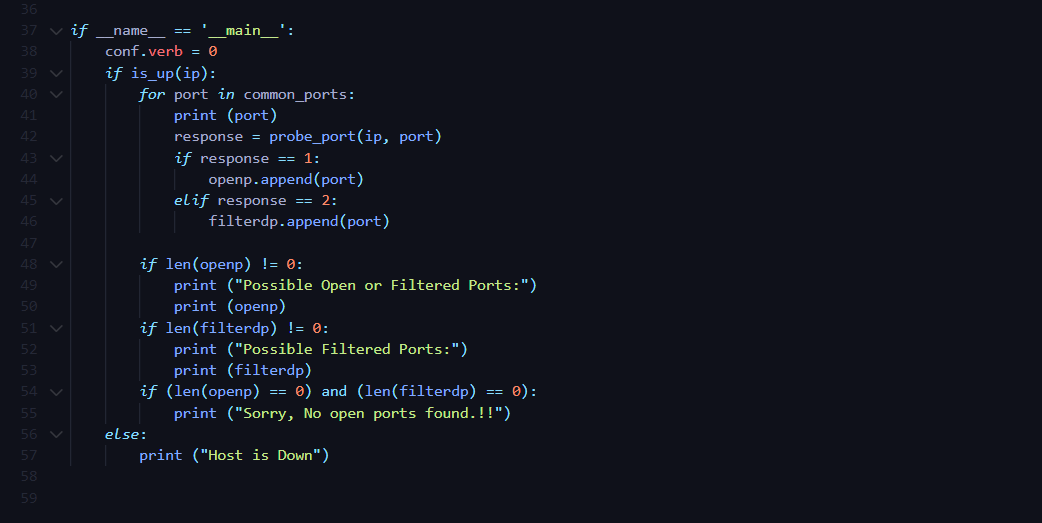






**CODE**:





**OUTPUT**:

