PortMap:

The port mapper (rpc.portmap or just portmap, or rpcbind) is an Open Network Computing Remote Procedure Call (ONC RPC) service that runs on network nodes that provide other ONC RPC services.

Version 2 of the port mapper protocol maps ONC RPC program number/version number pairs to the network port number for that version of that program. When an ONC RPC server is started, it will tell the port mapper, for each particular program number/version number pair it implements for a particular transport protocol (TCP or UDP), what port number it is using for that particular program number/version number pair on that transport protocol. Clients wishing to make an ONC RPC call to a particular version of a particular ONC RPC service must first contact the port mapper on the server machine to determine the actual TCP or UDP port to use.

Versions 3 and 4 of the protocol, called the rpcbind protocol, map a program number/version number pair, and an indicator that specifies a transport protocol, to a transport-layer endpoint address for that program number/version number pair on that transport protocol.

The port mapper service always uses TCP or UDP port 111; a fixed port is required for it, as a client would not be able to get the port number for the port mapper service from the port mapper itself.

The port mapper must be started before any other RPC servers are started.

LDAP:

Attackers are abusing yet another widely used protocol in order to amplify distributed denial-of-service attacks: the Lightweight Directory Access Protocol (LDAP), which is used for directory services on corporate networks.

DDoS mitigation provider Corero Network Security recently observed an attack against its customers that was reflected and amplified through Connectionless LDAP (CLDAP), a variant of LDAP that uses the User Datagram Protocol (UDP) for transport.

DDoS reflection is the practice of sending requests using a spoofed source IP address to various servers on the Internet, which will then direct their responses to that address instead of the real sender. The spoofed IP address is that of the intended victim.

MSSQL:

The attack manifests in the form of Microsoft SQL Server responses to a client query or request via abuse of the Microsoft SQL Server Resolution Protocol (MC-SQLR), which listens on UDP port 1434.

MC-SQLR lets clients identify the database instance with which they are attempting to communicate when connecting to a database server or cluster with multiple database instances. Each time a client needs to obtain information on configured MS SQL servers on the network, the SQL Resolution Protocol can be used. The server responds to the client with a list of instances.

Attackers abuse SQL servers by executing scripted requests and spoofing the source of the query with the IP address of the intended target. Depending on the number of instances present in the abused SQL server, the amplification factor varies.

The attack presents a specific payload signature, producing an amplification factor of nearly 25x. In this case, the attacker's request totaled 29 bytes, including IP and UDP headers, and triggered a response of 719 bytes including headers. Some servers may produce a larger or smaller response depending on their configuration.

Other tools publicly available on the Internet could reproduce this attack as well. Replicating this attack does not require a high level of technical skill. A scripted attack would only require a list of SQL servers exposed on the Internet that respond to the query. Attackers could use a unicast client request 0x03 or a broadcast request 0x02. Both are requests with a data length of 1 byte that will produce the same type of response from SQL servers.

Netbios:

The NetBIOS reflection DDoS attack – specifically NetBIOS Name Service (NBNS) reflection – was observed by Akamai as occurring sporadically from March to July 2015. The primary purpose of NetBIOS is to allow applications on separate computers to communicate and establish sessions to access shared resources and to find each other over a local area network.  
  
This attack generates 2.56 to 3.85 times more response traffic sent to the target than the initial queries sent by the attacker. Akamai observed four NetBIOS names server reflection attacks, with the largest recorded at 15.7 Gbps. Although legitimate and malicious NetBIOS name server queries are a common occurrence, a response flood was first detected in March 2015 during a DDoS attack mitigated for an Akamai customer.

Synflood:

A SYN flood (half-open attack) is a type of [denial-of-service (DDoS) attack](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/) which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

UDPFlood:

A UDP flood is a type of [denial-of-service](https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/) attack in which a large number of [User Datagram Protocol (UDP)](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/) packets are sent to a targeted server with the aim of overwhelming that device’s ability to process and respond. The [firewall](https://www.cloudflare.com/learning/security/what-is-a-firewall/) protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.