Supernova测试仪可进行DDoS攻击探测和模糊测试、漏洞扫描和攻击报文重放，支持DDoS攻击类型87种 、漏洞库漏洞数量99369个、攻击库攻击报文10248个

其中： **IPv4报文分片攻击：** 13种
ICMPv4单包攻击： 14种
ICMPv6单包攻击： 2种
IGMPv4单包攻击： 10种
ARPv4单包攻击： 3种
TCPv4单包攻击： 15种
TCPv6单包攻击： 10种
UDPv4单包攻击： 9种
UDPv6单包攻击： 3种
未知IP协议报文攻击： 1种
会话攻击类型： 7种

漏洞库漏洞数量共计：99369个
其中：高危漏洞40150个、中等漏洞49359个、低危漏洞9859个。包含主流漏洞库中的漏洞及部分针对工业互联网业务、物联网业务等的漏洞。

攻击库攻击报文数量共计：10248个
其中：涉及HTTP、HTTPS、UDP、SMTP、Microsoft、MySQL、Oracle、DNS等攻击类型。

攻击	类型	攻击描述
IPv4报文分片攻击	TEARDROP_UDP_FLOOD	TearDrop攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为36字节，protocol为UDP；第二个分片Offset = 24，protocol为UDP，第二片包含在第一个分片中，偏移量小于第一片结束的位移）致系统崩溃或重启。
	TEARDROP_TCP_FLOOD	TearDrop攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为36字节，protocol为TCP；第二个分片Offset = 24，protocol为TCP，第二片包含在第一个分片中，偏移量小于第一片结束的位移）致系统崩溃或重启。
	NEWTEAR_FLOOD	NewTear攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为28字节；第二个分片Offset = 24，第二片包含在第一个分片中，偏移量小于第一片结束的位移）致系统崩溃或重启。
	FAWX_FLOOD	Fawx攻击是发送大量错误的IGMP分片报文（即第一个分片IP载荷为9字节；第二个分片Offset = 8，第二片载荷长度为16字节，没有结束分片）致系统崩溃或重启。
	BONK_FLOOD	Bonk攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为36字节；第二个分片Offset = 32，第二片包含在第一个分片中，偏移量小于第一片结束的位移）致系统崩溃或重启。
	NESTA_FLOOD	Nesta攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为18字节，protocol为UDP，检验和为0；第二个分片Offset = 48，IP载荷为116字节；第三片Offset = 0，more frag为1，也就是还有分片，40字节的IP option，都是EOL，IP载荷为224字节）致系统崩溃或重启。
	ROSE_TCP_FLOOD	Rose攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为48字节（包含TCP头部）；第二个分片Offset = 65408，IP载荷为32字节，more frag为0，即最后一片）致系统崩溃或重启。
	ROSE_UDP_FLOOD	Rose攻击是发送大量错误的IP分片报文（即第一个分片IP载荷为40字节（包含UDP头部）；第二个分片Offset = 65408，IP载荷为32字节，more frag为0，即最后一片）致系统崩溃或重启。
	LARGE_OFFSET_FRAG_FLOOD	巨大offset攻击是向目标设备发送一个 Offset 值超大的分片报文（Offset 字段的最大取值为 65528，但是在正常情况下， Offset 值不会超过 8190（如果offset=8189*8， IP 头部长度为 20，最后一片报文最多只有 3 个字节 IP 载荷，所以正常 Offset 的最大值是 8189），所以如果 Offset 值超过 8190，则这种报文即为恶意攻击报文，设备直接丢弃。）从而导致目标设备分配巨大的内存空间来存放所有分片报文，消耗大量资源。
	PING_OF_DEATH_FLOOD	Ping Of Death 攻击原理是攻击者发送一些尺寸较大（数据部分长度超过 65507 字节）的 ICMP 报文对设备进行攻击。设备在收到这样一个尺寸较大的 ICMP 报文后，如果处理不当，会造成协议栈崩溃。
	JOLT_FLOOD	Jolt 攻击是攻击者发送总长度大于 65535 字节的报文对设备进行攻击。Jolt 攻击报文一共 173 个分片，每个分片报文的 IP 载荷为 380 字节，因此总长度为：173*380+20＝65760，远远超过 65535。设备在收到这样的报文时，如果处理不当，会造成设备崩溃、死机或重启。

	LARGE_NUMBER_OF_FRAG_FLOOD	IP报文中的偏移量是以8字节为单位的。正常情况下，IP报文的头部有20个字节，IP报文的最大载荷为65515。对这些数据进行分片，分片个数最大可以达到8189片，对于超过8189的分片报文，设备在重组这些分片报文时会消耗大量的CPU资源。
	IDENTICAL_REPEAT_OF_FRAG_FLOOD	重复分片攻击就是把同样的分片报文多次向目标主机发送：1、多次发送的分片完全相同，这样会造成目标主机的CPU和内存使用不正常；2、多次发送的分片报文不相同，但Offset相同，目标主机就会处于无法处理的状态：哪一个分片应该保留，哪一个分片应该丢弃，还是都丢弃。这样就会造成目标主机的CPU和内存使用不正常。
ICMPv4单包攻击	**ICMP_FLOOD**	在ICMP FLOOD攻击中，攻击者发送大量的、高欺骗性的ICMP包轰炸目标网络。ICMP FLOOD攻击可以通过ICMP包中目标服务器的端口和IP地址来针对网络中的随机服务器或特定服务器。其攻击的目的是消耗网络中的带宽，直到耗尽。
	ICMP_IP_FRAG_FLOOD	攻击者快速发送高欺骗性的最大分片的ICMP数据包（例如1500字节），这些分片包不能进行重组，会从总体上占用较大的ICMP攻击带宽。被攻击者在试图重新组装这些无用的数据包时，会消耗CPU资源。
	ICMP_TTL_ZERO_FLOOD	TTL=0的ICMP报文泛洪攻击。
	ICMP_TTL_ONE_FLOOD	TTL=1的ICMP报文泛洪攻击。
	ICMP_REPLY_FLOOD	ICMP回应报文攻击。
	ICMP_DESTI_UNREACH_FLOOD	ICMP不可达报文泛洪攻击。
	ICMP_REDIRECT_FLOOD	ICMP重定向报文攻击。
	ICMP_ADDR_MASK_REQUEST_FLOOD	ICMP掩码请求报文攻击。
	ICMP_RECORD_ROUTE_OPTION_FLOOD	带路由记录选项的IP报文攻击。
	ICMP_SECURITY_OPTION_FLOOD	带安全选项的IP报文攻击。
	ICMP_STREAM_OPTION_FLOOD	带流选项的IP报文攻击。
	ICMP_TIME_STAMP_OPTION_FLOOD	带时间戳选项的IP报文攻击。
	ICMP_LOOSE_SOURCE_ROUTE_OPTION_FLOOD	带宽松路由选项的IP报文攻击。
	ICMP_STRICT_SOURCE_ROUTE_OPTION_FLOOD	带严格路由选项的IP报文攻击。
ICMPv6单包攻击	**ICMP_FLOOD**	在ICMP FLOOD攻击中，攻击者发送大量的、高欺骗性的ICMP包轰炸目标网络。ICMP FLOOD攻击可以通过ICMP包中目标服务器的端口和IP地址来针对网络中的随机服务器或特定服务器。其攻击的目的是消耗网络中的带宽，直到耗尽。
	ICMP_IP_FRAG_FLOOD	攻击者快速发送高欺骗性的最大分片的ICMP数据包（例如1500字节），这些分片包不能进行重组，会从总体上占用较大的ICMP攻击带宽。被攻击者在试图重新组装这些无用的数据包时，会消耗CPU资源。
IGMPv4单包攻击	**IP_MULTICAST_FLOOD**	向用户指定的多播IP内加入的主机不断发送攻击报文，造成网络变慢，阻塞等问题。
	IGMPV3_GRAMMAR_FLOOD	将IGMPv3应答报文中的reserved的范围设为300-999(正确的范围是:0-255)，测试IGMPv3协议的健壮性。
	IGMPV3_QUERY_FLOOD	将IGMPv3查询报文中的reserved的范围设为20-99(正确的范围是:0-15)，测试IGMPv3协议的健壮性。
	IGMPV1_GRAMMAR_FLOOD	将IGMPv1应答报文中的type的范围设为16-99(正确的范围是:0-15)，测试IGMPv1协议的健壮性。
	IGMPV2_REQUEST_FLOOD	攻击者不断的发送IGMPv2查询报文，造成指定多播IP内的主机网络阻塞等问题。
	IGMPV2_RESPONSE_FLOOD	攻击者不断的发送IGMPv2应答报文，造成指定多播IP内的主机网络阻塞等问题
	IGMPV2_GRAMMAR_FLOOD	将IGMPv2查询报文中的response time的范围设为300-999(正确的范围是:0-255)，测试IGMPv2协议的健壮性。
	IGMPV1_TTL_ZERO_FLOOD	TTL=0的IGMPV1报文泛洪攻击

	IGMPV2_TTL_ZERO_FLOOD	TTL=0的IGMPV2报文泛洪攻击
	IGMPV3_TTL_ZERO_FLOOD	TTL=0的IGMPV3报文泛洪攻击
ARPv4单包攻击	**ARP_REQUEST_FLOOD**	攻击者向目标主机发送大量的，不同的源ip，源MAC的请求报文，使网络资源被大量占用，造成网络中断，掉线等问题。
	ARP_RESPONSE_FLOOD	攻击者向目标主机发送大量的，不同的源ip，源MAC的应答报文，不断更新本地ARP缓存，使网络资源被大量占用，造成网络中断，掉线等问题。
	ARP_GRAMMAR_FLOOD	将ARP请求报文中OPCODE和PRTOCOL SIZE关键字段分别设为0xFF，测试ARP协议的健壮性。
TCPv4单包攻击	**SYN_FLOOD**	攻击者向目标主机发送大量的、伪造源IP地址的SYN连接请求。这种攻击一直持续到耗尽服务器的连接表（用于存储并处理这些传入的SYN包）内存。
	SYN_ACK_FLOOD	攻击者利用大型僵尸网络或冒充被攻击的IP地址范围发送SYN-ACK数据包轰炸网络。
	ACK_FLOOD	在ACK_FLOOD攻击中，攻击者以非常高的速率发送欺骗性ACK包，这些包不属于当前防火墙状态表或服务器连接表中的任何会话。防火墙或服务器将消耗系统资源查询、比较这些传入数据包与现有会话。
	PUSH_ACK_FLOOD	在TCP-SYN会话期间，PUSH ACK包携带信息往返于主机和客户机，直到会话结束。PUSH ACK Flood攻击，会向目标服务器发送大量欺骗性的PUSH ACK包，消耗服务器资源。
	RESET_FLOOD	攻击者以极高的速率发送欺骗性RST包，这些包不属于当前防火墙状态表或服务器连接表中的任何会话。防火墙或服务器将消耗系统资源查询、比较这些传入数据包与现有会话。
	FIN_FLOOD	在TCP-SYN会话建立成功之后，服务器交换FIN包，以关闭主机和客户机之间的TCP-SYN会话。在FIN Flood攻击中，目标服务器将接收到大量欺骗性的、不属于目标服务器任何会话的FIN包。
	TCP_FRAG_ACK_FLOOD	攻击者快速发送高欺骗性的最大分片的TCPv4数据包（例如1500字节），这些分片包不能进行重组，会从总体上占用较大的TCP攻击带宽。被攻击者在试图重新组装这些无用的数据包时，会消耗CPU资源。
	TCP_IP_FRAG_FLOOD	基于TCP的分片攻击通常针对目标系统或安全组件的分片整理机制。在极端情况下，发送的重叠包可能导致目标系统宕机。
	LAND_ATTACK	LAND攻击是拒绝服务攻击（DoS攻击）的一种，通过发送精心构造的、具有相同源地址和目标地址的欺骗数据包，致使缺乏相应防护机制的目标设备瘫痪。
	TCP_TTL_ZERO_FLOOD	TTL=0的TCP报文泛洪攻击。
	TCP_ERROR_OPTION_FLOOD	错误IP选项的TCP攻击。
	TCP_SYN_FIN_FLAG_FLOOD	SYN和FIN标志同时设置的TCP报文攻击，正常情况下，SYN标志（连接请求标志）和FIN标志（连接拆除标志）不能同时出现在一个TCP报文中，而且RFC也没有规定IP协议栈如何处理这样的畸形报文。因此各个操作系统的协议栈在收到这样的报文后的处理方式也不相同，攻击者就可以利用这个特征，通过发送SYN和FIN同时设置的报文，来判断操作系统的类型，然后针对该操作系统，进行进一步的攻击。
	TCP_NO_FLAG_FLOOD	没有设置任何标志的TCP报文攻击，正常情况下，任何TCP报文都会设置SYN，FIN，ACK，RST，PSH五个标志中的至少一个标志，第一个TCP报文（TCP连接请求报文）设置SYN标志，后续报文都设置ACK标志。有的协议栈基于这样的假设，没有针对不设置任何标志的TCP报文的处理过程，因此这样的协议栈如果收到了这样的报文可能会崩溃。
	TCP_FIN_FLAG_FLOOD	设置了FIN标志却没有设置ACK标志的TCP报文攻击，正常情况下，除了第一报文（SYN报文）外，所有的报文都设置ACK标志，包括TCP连接拆除报文（FIN 标志设置的报文）。但有的攻击者却可能向目标主机发送设置了FIN标志却没有设置ACK标志的TCP报文，这样可能导致目标主机崩溃。
	TCP_WINNUKE	WinNuke攻击通过TCP/IP协议传递一个Urgent紧急数据包到目标计算机的139、138、137、113或53端口，使目标计算机处理异常而崩溃，该数据包URG位设置为1。
	SYN_FLOOD	攻击者向目标主机发送大量的、伪造源IP地址的SYN连接请求。这种攻击一直持续到耗尽服务器的连接表（用于存储并处理这些传入的SYN包）内存。
	SYN_ACK_FLOOD	攻击者利用大型僵尸网络或冒充被攻击的IP地址范围发送SYN-ACK数据包轰炸网络。

TCPv6单包攻击	ACK_FLOOD	在ACK_FLOOD攻击中，攻击者以非常高的速率发送欺骗性ACK包，这些包不属于当前防火墙状态表或服务器连接表中的任何会话。防火墙或服务器将消耗系统资源查询、比较这些传入数据包与现有会话。
	PUSH_ACK_FLOOD	在TCP-SYN会话期间，PUSH ACK包携带信息往返于主机和客户机，直到会话结束。PUSH ACK Flood攻击，会向目标服务器发送大量欺骗性的PUSH ACK包，消耗服务器资源。
	RESET_FLOOD	攻击者以极高的速率发送欺骗性RST包，这些包不属于当前防火墙状态表或服务器连接表中的任何会话。防火墙或服务器将消耗系统资源查询、比较这些传入数据包与现有会话。
	FIN_FLOOD	在TCP-SYN会话建立成功之后，服务器交换FIN包，以关闭主机和客户机之间的TCP-SYN会话。在FIN Flood攻击中，目标服务器将接收到大量欺骗性的、不属于目标服务器任何会话的FIN包。
	TCP_FRAG_ACK_FLOOD	攻击者快速发送高欺骗性的最大分片的TCPv6数据包（例如1500字节），这些分片包不能进行重组，会从总体上占用较大的TCP攻击带宽。被攻击者在试图重新组装这些无用的数据包时，会消耗CPU资源。
	TCP_IP_FRAG_FLOOD	基于TCP的分片攻击通常针对目标系统或安全组件的分片整理机制。在极端情况下，发送的重叠包可能导致目标系统宕机。
	LAND_ATTACK	LAND攻击是拒绝服务攻击（DoS攻击）的一种，通过发送精心构造的、具有相同源地址和目标地址的欺骗数据包，致使缺乏相应防护机制的目标设备瘫痪。
	TCP_WINNUKE	WinNuke攻击通过TCP/IP协议传递一个Urgent紧急数据包到目标计算机的139、138、137、113或53端口，使目标计算机处理异常而崩溃，该数据包URG位设置为1。
UDPv4单包攻击	UDP_MULTICAST_FLOOD	UDP多播风暴是攻击者不断的向监听该组播地址的主机发送报文，造成该组播内的主机网络阻塞等问题。
	UDP_BROADCAST_FLOOD	UDP广播风暴就是攻击者向本网络内所有主机发送广播数据包，并占用大量网络带宽，导致正常业务不能运行，甚至彻底瘫痪。
	UDP_FLOOD	在UDP Flood攻击中，DDoS攻击者使用较大的源IP范围，快速发送高欺骗性的UDP数据包。被攻击的网络(路由器、防火墙、IPS/IDS、SLB、WAF或服务器)被大量传入的UDP数据包轰炸。这种攻击通常会消耗网络资源和可用带宽直到其宕机。
	UDP_IP_FRAG_FLOOD	在UDP分片攻击中，攻击者将发送相对少量的、最大分片的UDP 数据包(例如1500字节)消耗更多带宽。这些分片数据包通常是伪造的，无法重新组装，被攻击者将收到这些可能会消耗大量CPU资源的数据包。
	UDP_TTL_ZERO_FLOOD	TTL=0的UDP报文泛洪攻击。
	UDP_ERROR_OPTION_FLOOD	错误IP选项的UDP攻击。
	FRAGGLE_ECHO_ATTACK	UDP端口7（ECHO）在收到UDP报文后，会产生回应。在UDP的7号端口收到报文后，会回应收到的内容。它们都同ICMP一样，会产生大量无用的应答报文，占满网路带宽。
	FRAGGLE_CHARGEN_ATTACK	端口19（Chargen）在收到UDP报文后，会产生回应。UDP的19号端口在收到报文后，会产生一串字符流。它们都同ICMP一样，会产生大量无用的应答报文，占满网路带宽。
	DHCP_FLOOD	攻击者发送大量的Discover报文轰炸目标网络，在没有得到客户端确认的情况下，服务器将会为客户端保留要分配的IP，当在大量泛洪攻击的场景下服务器的地址池很快就会满掉，从而影响正常客户端的使用。
UDPv6单包攻击	UDP_FLOOD	在UDP Flood攻击中，DDoS攻击者使用较大的源IP范围，快速发送高欺骗性的UDP数据包。被攻击的网络(路由器、防火墙、IPS/IDS、SLB、WAF或服务器)被大量传入的UDP数据包轰炸。这种攻击通常会消耗网络资源和可用带宽直到其宕机。
	UDP_IP_FRAG_FLOOD	在UDP分片攻击中，攻击者将发送相对少量的、最大分片的UDP 数据包(例如1500字节)消耗更多带宽。这些分片数据包通常是伪造的，无法重新组装，被攻击者将收到这些可能会消耗大量CPU资源的数据包。
	DHCP_FLOOD	攻击者发送大量的Discover报文轰炸目标网络，在没有得到客户端确认的情况下，服务器将会为客户端保留要分配的IP，当在大量泛洪攻击的场景下服务器的地址池很快就会满掉，从而影响正常客户端的使用。
未知IP协议报文攻击	UNKNOWN_PROTOCOL_ATTACK	未知协议类型的IP报文攻击

会话攻击	**TCP伪装会话攻击**	攻击者发送伪造的SYN数据包，ACK数据包，最后是FIN/RST数据包。所有这些数据包类似于从一个主机发送到另一个主机的真实TCP会话流量。
	TCP新建会话攻击	攻击者首先建立大量的有效会话，然后缓慢地响应一个ACK包和不完整的请求，使会话长时间保持打开状态。
	HTTP快速请求攻击	在GET Flood中，攻击者会向目标服务器发送大量有效的GET请求。此类攻击是非欺骗性的，源IP地址是攻击者计算机（或NAT防火墙）的实际IP。此攻击最终将导致被攻击的服务器无响应。
	HTTP变体请求攻击	攻击机器创建多个HTTP请求，不是在一个HTTP会话攻击期间一个接一个地创建请求，而是创建一个包含多个请求的数据包。它是Excessive Verb攻击的一种变体，攻击者可以用低速率的攻击使被攻击服务器CPU负载过高。
	HTTP递归请求攻击	攻击者会识别多个页面或图像生成HTTP GET请求，试图通过递归这些页面或图像模拟正常用户。
	HTTP并发慢确认攻击	检测受测设备抵御长HTTP会话攻击的能力，每个虚拟用户会创建大量有效会话，在开始下载大型文档、对象后，减慢确认速度，从而过度消耗服务器资源。
	HTTP并发慢请求攻击	检测受测设备抵御长HTTP会话攻击的能力，每个虚拟用户在一个HTTP会话中多次请求并降低请求速率，消耗很少的带宽，致使被攻击的服务器无响应。