新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/9/1-2008/9/14 第75期

多功能UTM / MS系列报导

技术浅谈与应用 - 入侵侦测防御特征名称的意义说明(一)

在多功能UTM中，位于“入侵侦测防御 > 特征设定 > 异常侦测”，下所存在的内建特征名称有许多种，但这些名称是代表着什么意思？用来做什么用的？相信也有不少管理人员抱有着相同的疑问。其实这些让人会产生疑问的名词指的是黑客常用来攻击的方式，而这些名词大多是都没有正式的中文名称。

位于系统中的特征名称所代表的意思，以下将一一的来作介绍说明：

『syn flood』

此种攻击主要是利用TCP连结时的三向交握讯息（three way handshake）来造成的。当攻击者恶意地送出许多TCP SYN封包给被攻击端，在被攻击端回复接受讯息(SYN + ACK)后，而攻击端后续没有再返回一个确认报讯息给被攻击端时，这种情况下被攻击端服务器会将攻击端的位置暂时做储存，过段时间后再重试（再次发送接受讯息给攻击者）。此种攻击就是利用这方式，以数以万计的半连接来消耗被攻击端非常多的CPU时间和内存，让被攻击端不断对暂存于内存列表中的IP进行回复讯息(SYN + ACK)的重试，因而导致暂停服务。

『udp flood』

又称为Fragile攻击，它是透过UDP protocol送出假造来源的UDP broadcast封包至目标网络，以产生放大的数据流，当目的网域中的众多主机响应之后，便可以造成网络的壅塞。即使某些IP地址没有响应，但产生的ICMP封包（type 3，Destination Unreachable）仍然可以达到DoS攻击的效果。

『icmp flood』

此种攻击方式是发送ICMP者假造来源IP之后，再将ICMP封包大量的送至被害者主机，则服务器主机会响应等量的ICMP封包到所假造的来源IP网络上，直接造成被害者与被假造来源的IP两个网络之间的网络流量大量增加。造成没有多余的带宽可以让一般正常使用者使用，以达到Denial-of-Service的攻击。

『syn fin』

过滤不合规范的IP封包，利用tcp连接的建立到终止都跟踪检测的方式，来做详细过滤。在同一个tcp连接中，封包的关系是相互关联的，先是syn封包→数据封包→fin封包。但如果分割这些关系，单独的只过滤数据封包的话，很容易被精心所构造的攻击数

据封包欺骗，有心的黑客可利用 syn 封包、fin 封包，来探测防火墙后面的网络，也就是所谓的后门，事后来进行入侵。

『tcp no flag』

丢弃不含或含不合规范标志位的 TCP 封包。蠕虫通常会尝试透过内建的名单或是随机产生感染的目标，就但并不是每一次都能顺利的连结成功。由于 NetFlow 会将每个 session 中所有传输时的 TCP 控制旗标全部储存在封包控制旗标（TCP Flag）这个字段中，因此透过这个字段中的信息来协助我们推测特定主机联机的特性。在一个 Flow 正常的建立 TCP 连结后，就其封包控制旗标（TCP Flag）字段会记录的包含 ACK、SYN、FIN 等控制旗标，就但是如果蠕虫进行感染的动作时，就由于随机选取的主机并不一定存在，就或是即使存在但目标主机没有开放蠕虫所要感染的 TCP port，在这种情况下，就 NetFlow 信息中由受感染主机对外联机所产生的 Flow 封包控制旗标(TCP Flag)字段会只存在 SYN 这个 TCP 控制旗标，就所以可根据这种特性来过泸不合规范的封包。

『fin no ack』

通常，在设置了 FIN 标志的 TCP 封包，同时也会配置了 ACK 标志(以确认接收到的前一个封包)。所以设置了 FIN 标志但未设置 ACK 标志的 TCP 封包是异常的 TCP 行为。一般操作系统可能会通过发送设置了 RST 标志的 TCP 封包来做出响应，而受害者的响应则会给攻击者提供有关其操作系统的线索，让攻击者有入侵的管道。

『tcp land』

此种手法是利用特殊的 TCP 封包传送至目标主机，使被攻击端因为无法判别而当机或被迫重新启动，攻击者所利用的就是 TCP 通讯协议中，定义规则与操作系统之间漏洞所造成的攻击手法。攻击者利用 IP 伪装的技术修改即将送出的封包，将其来源与目的 IP 地址均改成是目标机器的 IP 地址，以及将来源与目标连接端口也改为一样，来使得某些操作系统或网络设备当机无法正常运作。

『large icmp』

可称为 ICMP 大封包，这种情况多属于异常流量的行为。通常 ICMP 封包都不会太大，但如果封包过大，则表式正处于被攻击，或者有人在测试使用大封包 ping 被攻击端的主机。由于在早期的路由器方面对封包的最大尺寸都有限制，许多操作系统对 ICMP 封包上都是有大小上的规定，而攻击方则利用声称自己的尺寸大小超过 ICMP 上限的封包，也就是所加载的尺寸大小超过所规定的上限时，就会使被攻击方出现内存上分配的错误，因而导致 TCP/IP 堆栈崩溃，致使被攻击方(接受方)当机。

新软系统多功能 UTM 所提供的入侵侦测防御特征码，当然不会仅只有上述的 8 种而已，其余的特征码我们将会于下一期-第 76 期-的新软周报中继续为您来做完整的说明。

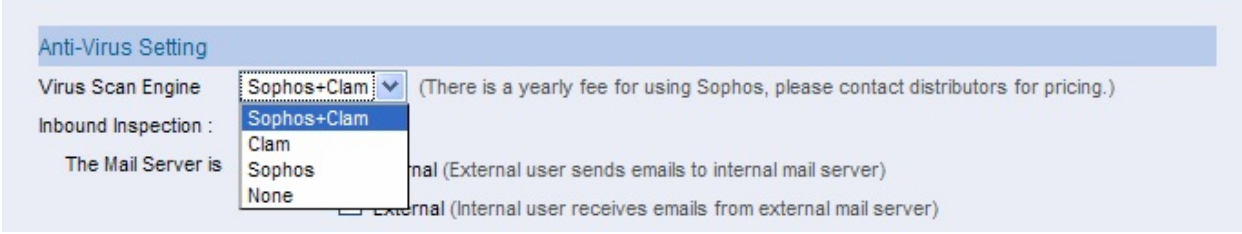
文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 拒绝公司被殭尸病毒入侵

相信前阵子所发生于七夕情人节的新闻报导，有关于电子告白信内含有病毒的事件，大家都还记忆犹新，只要开启信件连结的收件者，就会立即的被所谓的『殭尸病毒』所感染。散播者利用特殊节日的影响下，加上让人心动的标题来降低收件者防备的心态，让收件者开启含有『殭尸病毒』的信件，以达到入侵的目的，一旦收件者因为好奇，按下邮件中所附的连结，那可能会是一场梦魇。根据趋势科技最新发现指出，含有「Stand by my side」、「I want to be with you」以及「Lucky to have you」等告白讯息的电子邮件，都有可能是殭尸网络所散播含有恶意连结的垃圾邮件，当然中文标题也不例外，利用「我爱你」之类耸动人心的标题也是让收件者踏入圈套的一个陷阱。

台湾目前僵尸病毒十分泛滥，每个人于每天所收的邮件当中，经常会发现 10 封信中可能 10 封都是莫名奇妙的垃圾信，面对那些正规的信件，总是被垃圾信所掩盖，而这些令人厌烦的垃圾信则大多是经由已被僵尸病毒侵的僵尸计算机所发送，由于使用者依旧可以正常使用计算机，因此很难察觉自己的计算机其实已经被入侵，甚至已被当作跳板在对外发送垃圾信。若公司成为病毒邮件或垃圾邮件的转送点，不仅会将网络资源消耗殆尽，还会严重的影响公司形象。

针对此问题，新软系统『多功能-UTM』对各式各样的网络服务建置了数种病毒扫描机制，其中就有包含了邮件病毒的过滤。而『多功能-UTM』所采用的扫毒引擎为 Clam、Sophos。



防毒设定画面截图

当邮件传递时，『多功能-UTM』会先行将其信件存放于暂存区内，并针对信件的内容、所夹带的文件扫毒（压缩檔解压扫毒）。若邮件判断为异常（病毒邮件、钓鱼邮件…），『多功能-UTM』会将该邮件依照管理人员所设定的处置方式处理（隔离储存、删除…）剩下的邮件再交由垃圾邮件过滤机制处理。

垃圾邮件过滤画面截图

除此之外『多功能-UTM』同时也包含了 HTTP / Web Mail、FTP 病毒过滤及 IDP 病毒过滤，并且内建的自动在线更新系统，可自动更新病毒码，完全不需管理人员手动更新，即可轻松的享受到在『多功能-UTM』保护下干净的网络环境。

文 陈殿鸿 kim@nusoft.com.tw