新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/9/15-2008/9/28 第76期

多功能UTM / MS系列报导

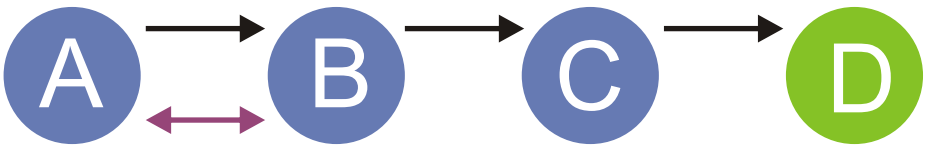
技术浅谈与应用 - 入侵侦测防御特征名称的意义说明(二)

『ip record route』

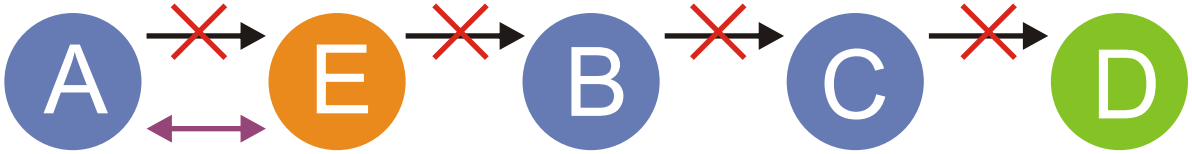
攻击者可以利用此漏洞制作特殊的来源路由封包，造成系统无条件接收这些恶意封包。

『ip strict src record route』

严格的封包路由。简单来说，严格受控来源端路由，意指：发送端给予封包指定路径，强迫该封包应经过指定的路径点到达目的端。而使用者可以指定较顺畅或是较快速、安全的路径，将封包送达目的端，而若是指定的路径发生问题。例如：(图一)封包要经过A点→B点→C点的路径，将封包丢到D的目的端，则若是在B路径发生路由停止服务，或是路由繁忙时，封包会在A到B的线路上徘徊，则时间过久TTL(Time to Live)将会把讯息传达给ICMP，而停止该封包的运作。再者若是给予错误路径，例如：(图二)A点→B点→C点，而正常路径为：A点→E点→B点→C点，则因没有给予正确讯息，则封包是不会经过未指定的E点，也将会导致无法将封包送达目的端D点。对于路径上的Segment，会传达已传送地址后下一个目的地地址非紧邻不可的讯息。



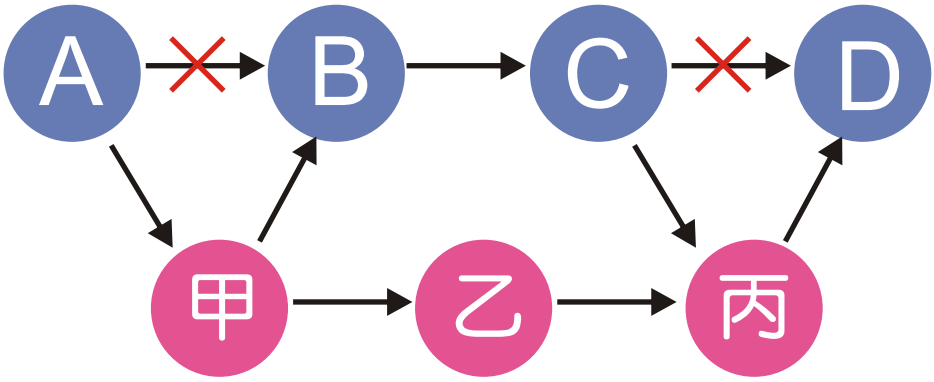
图一



图二

『ip loose src record route』

宽松的封包路由。意指：发送端给予了封包必须经过的路径，但如果它需要，也可以经过一些其它的路径。换句话说，不用考虑封包经过的确切地址，只要它经过这些路径即可。例如：(图三)当来源端给予路径A、B、C，将封包丢给D目的端，而不一定要沿着指定A→B→C→D可以选择经过其它路径，只需经过指定的路径即可并非强迫式，若A到B的点繁忙或是有其它状况可将其判断，将封包可以从A点到甲点，再由甲点B点一直到送到D目的端如此。



图三

『invalid url』

传送一个格式有问题的 URL 到正在运行的验证服务 TCP 端口，以达到系统关闭并且重新启动，进一步要求重新启动的 WatchGuard 为它工作。

『winnuke』

利用 Windows 的系统漏洞，通过 TCP/IP 协议向远程机器发送一段可导致 OOB 错误的信息，使计算机屏幕上出现一个蓝屏及提示：「系统出现异常错误」，或者当机，而目前的 WinNuke 系列工具已经从最初的简单选择 IP 攻击某个埠发展到可以攻击一个 IP 区间范围的计算机，并且可以进行连续攻击，还能够验证攻击的效果，还可以对检测和选择埠，所以使用它可以造成某一个 IP 地址区间的计算机全部蓝屏及当机。

『bad ip protocol』

侦测非标准的 IP 通讯协议

『Portscan』

扫 port，一次完整的网络安全扫描分为 3 个阶段：
（1）第 1 阶段：发现目标主机或网络。
（2）第 2 阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。
（3）第 3 阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。原本用来检测自己的计算机，但是常被人拿来做为刺探它人所用。

『http inspect』

检测 http 的封包内容是否包含恶意程序代码。缺少或不正确的通讯协议宣告、缺少欲连结的主机名称、不合法的网站连结路径、不合法的字符存在于欲连结的主机名称中。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 利用多功能 UTM 的垃圾邮件防护机制，能为企业带来什麼样的好处？

电子邮件系统是最常也是最容易遭受攻击的一项管道，同时也是目前最为严重的问题，如垃圾邮件、病毒、间谍软件、钓鱼诈骗攻击等等，这些不请自来的种种问题，进而可能对企业机密数据和业务管理造成相当的危害，相信也都是大家了解的一件事。因此，在企业中部署一个邮件安全网关，以保护所有进出的电子邮件，已经成为企业网络安全策略中不可或缺的环节。

新软系统多功能 UTM 众多功能中，其中就包含了针对垃圾邮件这领域的防护功能，而新软系统多功能 UTM 里，垃圾邮件防护机制所能够为公司带来什么样的好处？

多功能 UTM 中所附属的垃圾邮件防护机制拥有多项功能，垃圾邮件过滤、邮件病毒侦测、邮件通知、邮件稽核备份。这些强大的功能不但能够避免公司内部遭受外部网络层出不穷泛滥的病毒攻击而造成电子邮件服务中断之外，还可准确有效的防范如洪水般的垃圾邮件以及钓鱼信件、病毒邮件的攻击，并且还拥有 Web Mail 的管制功能，让防护更全面、更加的完善，为公司在邮件方面创造干净稳定的环境。

而如此的环境下，连带所产生的另一项更大的价值就是能够有效的提高员工工作效力，让公司在内对外、外对内沟通的管道顺利、稳定情况下，进而可提升公司的生产力及竞争力，并且可降低邮件系统管理负担、节省邮件服务器之数量与储存空间。

多功能 UTM 另一项优点则是多种设备的功能整合后，网管人员不再需要管理众多的 UI 接口，透过新软系统多功能 UTM，只需使用同一个 UI 界面即可管理及控制所有的功能，简单易懂，而且容易操作，即使是初学者也可轻松上手，如此人性化的设计，成功的简化了公司内部安全部署与管理，同时也大大的减轻管理人员的负担，让管理人员有更多的心力去处理其它公司内部相关的事务。

新软系统多功能 UTM - MS 系列产品，针对公司规模大小的不同，而特别设计不同的机型，适用人数从 30 人到超过 300 人，公司可依照本身的规模来选购最合适的设备机型。新软系统多功能 UTM - MS 系列产品拥有最完善的功能设计，加上其它强大功能，所能为公司带来的好处绝对不仅于此，相信新软系统多功能 UTM - MS 系列产品一定是公司、企业最佳的选择。

- 如欲了解更详细、完整的机型内容说明，欢迎至 http://www.nusoft.com.tw

文 陈殿鸿 kim@nusoft.com.tw