浅析网络入侵监测系统-IDS的应用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022__E6_B5_85_E6_9E_90_E7_BD_91_E7_c101_251039.htm 很多文章介绍了如何通过建立，改善，以及分析服务器日记文件的种种方式，监测出来黑客入侵行为，但这些都是过去式，都是在入侵发生后你才知道存在这种行为而加以防范。最好的方法是能够在当场就能监测出恶意的网络入侵行为，并且马上采取防范反击措施加以纠正。因此即时监测黑客入侵行为并以程序自动产生响应的网络入侵监测系统（又称IDS）产生了。 1、何谓IDS？ 简单的说，设立IDS的唯一目的就是当场监测到网络入侵事件的发生。IDS就是一个网络上的系统，这个系统包含了下面三个组件：（1）网络监测组件，用以捕捉在网络线上传递的封包。（2）接口组件，用以决定监测中的资料传递是否属于恶意行为或恶意的使用。在网络传递时，用来比较的资料样式（pattern），以监测恶意网络活动。（3）响应组件，针对当时的事件予以适当的响应。这个响应可以是简单的，例如寄发一个电子邮件讯息给系统管理者，或者是复杂的，例如暂时将违规者的IP地址过滤掉，不要让他连到这个网络来。 2、IDS如何通过网页监测网络入侵事件 IDS系统不只必须监测各式各样，从大到小，以及各种系列的系统上的网络攻击事件，它还必须能够快速及时地的在第一时间内监测到入侵事件的发生。因此，IDS的数据库以及式样比对（pattern-matching）机制是复杂到令人难以置信的。 要使IDS能够监测通过网页的入侵事件，其中的网络监测组件就必须要能够捕捉所有通过网页通讯端口上，借着HTTP 通讯协议

传递的网络资料往来。（注意，SSL的网络交通是完全绕过IDS的网络监测的，因为这些网络交换资料都是经过加密的。）式样比对组件在这里，主要是用于比较URL解析的结果，看看是否符合数据库中的恶意的HTTP回询（request）。 接下来，我介绍如何制作两个快速而简易的IDS，用来监测可疑的网页回询活动。这些解决方案的目的是在于提供系统管理者，让他们拥有一个特别针对他们网络而设计的监测/响应系统。 3、制作快速而简易的IDS （1）Network Grep 工具 我们先从一个简单的网络监视程序开始，这个程序是用来监测 HTTP 通讯协议的网络资料往来。HTTP回询的特色是，它使用以下的语法：〈HTTP-Request-Method〉〈URL〉 HTTP/〈version〉 这个可在Packetfactory入口网站寻获的程序ngrep针对在网络上传递往来的资料，执行正则表示法（regular expression）式样比对。我们可以用以下的指令来利用ngrep拦截并显示所有纯文字形式的 HTTP 资料往来： #ngrep-iqt “ ^GET|^HEAD|^TRACE|^POST|^PUT and HTTP ”以上指令中，-iqt 选项是指示ngrep不要区分资料中的大小写，并且只有显示封包中有符合式样比对的资料，以及在显示资料时加上日期以及时间的标题。（注：比对的式样，是基于 GET，HEAD，TRACE，POST，PUT，以及 HTTP 等关键词。欲知更多有关如何在ngrep使用正则表示法，你可以到http://www.packetfactory.net/Projects/Ngrep/查看相关资料。） 以上面我们建议的方式使用ngrep再加上运行越来越受欢迎的 Whisker程序，监测地址为 10.1.1.2 的IIS5.0 服务器平台，我们得到了以下的结果： T 03:37:30.041739 10.1.1.21:2425 -> 10.1.1.2:80 [AP]HEAD / HTTP/1.0..User-Agent: Mozilla/5.0 [en]

（Win95. U）..Referer: http://10.1.1.2/..Connection: close.... T
2001/01/16 03:37:30.108630 10.1.1.21:2426 -> 10.1.1.2:80 [AP]GET
/cfdocs/ HTTP/1.0..User-Agent: Mozilla/5.0 [en] （Win95. U
）..Cookie:
ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPB
CFD.path=/..Referer:http://10.1.1.2/..Connection: close.... T
2001/01/16 03:37:31.842452 10.1.1.21:2427 -> 10.1.1.2:80 [AP]GET
/scripts/ HTTP/1.0..User-Agent: Mozilla/5.0 [en] （Win95. U
）..Cookie:
ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPB
CFD.path=/..Referer:http://10.1.1.2/..Connection: close.... T
2001/01/16 03:37:31.854206 10.1.1.21:2428 -> 10.1.1.2:80 [AP]GET
/scripts/cfcache.map HTTP/1.0..User-Agent: Mozilla/5.0 [en]
（Win95. U）..Cookie:
ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPB
CFD.path=/..Referer: http://10.1.1.2/..Connection: close.... T
2001/01/16 03:37:33.644534 10.1.1.21:2429 -> 10.1.1.2:80 [AP]GET
/cfcache.map HTTP/1.0..User-Agent: Mozilla/5.0 [en] （Win95. U
）..Cookie:
ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPB
CFD.path=/..Referer:http://10.1.1.2/..Connection: close.... 现在你就可以采取行动了！ （2）执行式样比对 使用ngrep拦截网络资料往来很简单。然而，分析捕捉到的资料并从中抽取URL则略具难度。因为ngrep将资料输出拆成一行一行的，所以我们必须额外耗费很多精力，去重组输出的资料，并将该资料中的URL与已知的网络攻击行为模式做比对。 此时，我向大

家介绍另一个用来监测网页传送的犀利工具软件了。这个软件就叫做urlsnarf，它是由Dug Song写成的dsniff工具软件套件的一部份。urlsnarf 从所拦截的网络资料传送中，捕捉所有的 HTTP 回询，并且将结果以共享日记文件格式（Common Log Format ,CLF）显示出来，这种格式就跟市面上的网页服务器，诸如Apache或者是IIS所用的格式一样。 跟当初我们用ngrep的方式一样，我们使用urlsnarf并且在 10.1.1.2 的服务器上执行Whisker，所得到的结果如下： # urlsnarfurlsnarf: listening on eth010.1.1.21 - - [16/02/2001:03:58:43 0530] "HEAD http://10.1.1.2/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:43 0530] "GET http://10.1.1.2/cfdocs/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:45 0530] "GET http://10.1.1.2/scripts/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:45 0530] "GET http://10.1.1.2/scripts/cfcache.map HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:48 0530] "GET http://10.1.1.2/cfcache.map HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:50 0530]"GEThttp://10.1.1.2/cfide/Administrator/startstop.html HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 10.1.1.21 - - [16/02/2001:03:58:52 0530] "GET http://10.1.1.2/cfappman/index.cfm HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95. U）" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com