2017 年 5 月 24 日，星期三

File2pcap - Talos 创建 Snort 规则的瑞士军刀

作者：Martin Zeiser。特别感谢 Joel Esler 提供的建议。

对 Talos 而言，监控针对客户网络发起的威胁始终是一项重要的任务，而且为了检测任何攻击，针对最新漏洞创建 Snort 规则也成为防护过程必不可少的组成部分。

为了加深对规则开发过程的了解，您可以研究一下服务器软件 Server2010 中理论上能够远程利用的漏洞。完成概念验证漏洞攻击开发，在虚拟机上设置服务器软件，并捕获攻击者和受害者之间网络中的流量之后，即可启动规则开发。这样理解应该正确吧？

然而，时过境迁，数月甚至数年后，如果需要重新检查规则，那又该如何是好？要解决这个问题，不仅必须找出另一易受攻击版本的 Server2010 并进行重新安装，还必须重新配置易受攻击的参数，如此反复执行测试，才能实现网络流量检查。接下来，在安装服务器后，所用的特定漏洞攻击将不再起作用，因为编写漏洞攻击所用的语言此后已发生变化，代码需要相应地进行修改。所有这一切都需要大量时间，因此规则开发过程不会以这种方式进行。相反，此过程应该是，发现漏洞，编写并运行漏洞攻击之后，使用 Wireshark 捕获攻击。此后，即可使用上文所述的 pcap 文件中的流量开发相应规则。可以使用 tcp 重播实用程序轻松地将 pcap 文件中记录的流量放回线路，还可以直接通过 Snort 读取流量。因此，规则开发人员通常处理的是与攻击对应的 pcap，而不是漏洞攻击。

至于基于文件的漏洞，最初进程用于启动本地 Web 服务器和使用浏览器下载使用漏洞攻击文件，同时使用 Wireshark 记录传输过程。File2pcap 可以轻松模拟流量并创建相应的 pcap，从而彻底改变了这一需求。

支持的协议：

HTTP：

刚开始，File2pcap 作为从输入文件创建 pcap 的工具，可以显示这些文件从 Web 服务器传输到浏览器的过程。通过模拟整个数据交换，它通常可以在几秒钟内为任何输入文件创建 pcap 文件。结果始终显示包括 SYN、FIN 在内的完整 TCP 流，数据包依序排列且校验和正确无误。之后，可将这些 pcap 文件与 tcp 重播工具配合使用（或通过 Snort 读取），针对任何基于文件的攻击创建相应规则。

HTTP/2：

HTTP 在过去数年不断发展，现在 HTTP/2 也获得广泛使用。通常，该协议会在使用时进行加密，但是它还支持纯文本连接，因此我们将 HTTP/2 添加至 File2pcap。

HTTP POST：

虽然 HTTP GET 是来自浏览器的常见请求，但有时也会使用 HTTP POST 上传数据。为确保功能全面性，我们将 HTTP POST 支持也添加至 File2pcap。

SMTP/POP3/IMAP：

基于浏览器的攻击是计算机受到危害的最常见的方式之一，而邮件和附件则是另一个威胁来源。为了让 Snort 规则开发人员以 File2pcap 允许的方式针对基于浏览器的攻击为这些威胁创建 pcap，我们增加了许多新功能。专门支持 SMTP、POP3 和 IMAP 协议。当 File2pcap 得到指令从输入文件构建 SMTP pcap 时，它会模拟从客户端发往邮件服务器的邮件，其中输入文件作为此邮件的附件发送。POP3 和 IMAP 的工作原理类似。命令行交换允许附件的编码从默认 MIME 转换为 Quoted-Printable 编码，甚至是 UU 编码。

FTP：

FTP 协议是 FIe2pcap 支持的另一个典型的文件传输协议，可以在其中创建“主动”和“被动”数据流。

IPV6：

为使 File2pcap 做好准备更有效地全面应对所有未来的攻击，我们最新增加了 Ipv6 支持。现在，只需一个简单的命令行标志即可将数据交换从默认的 IPv4 切换为 IPv6，同时其他所有设置都保持不变。

Talos GitHub

总之，File2pcap 是一个可以从任何输入文件创建 pcap 的工具，能够模拟此类文件的传输过程，并使用各种协议和编码。而且，生成的 pcap 文件可用于创建 Snort 规则或对其进行测试。由于 File2pcap 能够在可靠运行的同时节省大量开发时间，因此 Talos 内部将其广泛用于规则创建。

File2pcap 可从我们的 Github 页面下载
欢迎您通过 Github 问题页面提出反馈以及功能方面的要求

发布者：WILLIAM LARGENT；发布时间：午夜 12:02
标签：FILE2PCAP、SNORT 规则、TALOS、TCP/IP、威胁情报工具、威胁研究