

知 安全设备IPS抓包信息下载查看方法

IPS防攻击 曾招维 2022-05-12 发表

问题描述

安全设备开启IPS抓包后，抓包信息如何？



解决方法

命令行:

```
<F1030-NEW>dir flash:/dpi/ips/pcap/
Directory of flash:/dpi/ips/pcap/
 0 -rw-      861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547618883_23525.pcap
 1 -rw-      861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547623598_23525.pcap

<F1030-NEW>dir flash:/dpi/ips/pcap/
<F1030-NEW>dir flash:/dpi/ips/pcap/
Directory of flash:/dpi/ips/pcap
 0 -rw-      861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547618883_23525.pcap
 1 -rw-      861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547623598_23525.pcap
 2 -rw-      861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547626253_23525.pcap
```

FTP/TFTP下载:

```
<F1030-NEW>ftp 192.168.10.200
Press CTRL+C to abort.
Connected to 192.168.10.200 (192.168.10.200).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.10.200:(none)): zzw
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/dpi/ips/pcap/ips_192.168.10.200_20220512_140547618883_23525.pcap
227 Entering passive mode (192,168,10,200,165,246)
125 Using existing data connection
.
226 Closing data connection; File transfer successful.
861 bytes sent in 0.001 seconds (1.21 Mbytes/s)
```

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows a single packet: a GET request for the file 'ips_192.168.10.200_20220512_140547618883_23525.pcap' from the source IP 192.168.10.200 to the destination IP 192.168.13.174. The packet details pane shows the following information:

- Frame 1: 821 bytes on wire (6568 bits), 821 bytes captured (6568 bits)
- Ethernet II, Src: Hangzhou_03:31:8e (60:0b:03:df:31:8e), Dst: Hangzhou_a5:7b:f2 (74:1f:4a:a5:7b:f2)
- Internet Protocol Version 4, Src: 192.168.10.200, Dst: 192.168.13.174
- Transmission Control Protocol, Src Port: 25273, Dst Port: 80, Seq: 1, Ack: 1, Len: 767
- Hypertext Transfer Protocol
 - GET //wja?page=../../ HTTP/1.1
 - Host: 192.168.13.174
 - User-Agent: Mozilla/5.0 (Windows NT 6.3; win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Connection: keep-alive
 - [truncated]Cookie: supportLang=cn%2Cen; lang=cn; login=false; sessionId=2000010b4890e3612331e2ef0375e161dd57; loginid=87f358908bc29052e625e8
 - Upgrade-Insecure-Requests: 1

The 'Full request URI' is highlighted in red: `http://192.168.13.174/wja?page=../../`

