BUUCTF-wireshark



| <u>^</u> | |
|--|-------|
| 名称 修改日期 | |
| ☐ dianli_jbctf_MISC_T10075_20150707 2015/7/7 10:31 PCAP 文件 | 63 KB |

https://blog.csdn.net/li2254477890

这个文件传到linux虚拟机中然后用虚拟机中的wireshark(这个可能是kali中的自带的。好久了忘了)

| | 💪 Wireshark |
|--|--|
| | |
| | dianli_jbctf_MISC_T10075_20150707_wireshark.pcap _ 🗆 🗙 |
| | <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp |
| | |
| | Apply a display filter < <tr>+</tr> |
| | |
| | Source Destination Protocol Length Info 202.101.172.47 192.168.1.102 DNS 297 Standard query response 0x2c57 A bdimg.share.b |
| | 192.168.1.102 115.231.236.116 TCP 54 22494 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0 192.168.1.102 115.231.236.116 HTTP 863 POST /user.php?action=login&do=login HTTP/1.1 115.231.236.116 192.168.1.102 TCP 54 80 - 22494 [ACK] Seq=1 Ack=810 Win=31744 Len=0 115.231.236.116 192.168.1.102 TCP 990 80 - 22494 [PSH. AcK] Seq=1 Ack=810 Win=31744 |
| | <pre>(TCP Segment Len: 809) Sequence Number: 1 (relative sequence number) Sequence Number (raw): 2631588181 (May Economeco Number: 840 (relative sequence number)]</pre> |
| | Acknowledgment Number: 1 (relative sequence namber)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 1334323082 0101 = Header Length: 20 bytes (5) Elass: 0x018 (PSH. ACK) |
| | |
| | 0020 ec 74 57 de 00 50 9c da d9 55 4f 88 27 8a 50 18 ··t₩··P·· 0030 40 b0 dd 44 00 00 50 4f 53 54 20 2f 75 73 65 72 @··D··P0 ST / |
| | 0040 2e 70 68 70 3f 61 63 74 69 6f 6e 3d 6c 6f 67 69 .php?act |
| | 0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 e 77 0070 6f 6f 70 75 6a 2a 6f 72 67 40 40 55 72 65 72 2d 1.1 Host t: |
| | 0080 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent M ozilla/ |
| | 00a0 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 33 38 .1; W0W6 4; rv: |
| | 0000 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) Geck o/ 00c0 30 31 20 46 69 72 65 66 6f 78 2f 33 38 2e 30 0d 01 Firef ox/ |
| | 00d0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 Accept: text/ |
| | Flags (12 bits) (tcp.flags), 2 bytes Packets: 356 · Displayed: 356 (100.0%) Profile: Default |
| | |
| | https://blog.csdp.pet/li2254477890 |





户名和密码(也就是flag)

flag{ffb7567a1d4f4abdffdb54e022f8facd}



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖