

BÁO CÁO PHÂN TÍCH SỰ KIỆN AN NINH - PHÁT HIỆN HÀNH VI TẤN CÔNG QUA WIRESHARK

1. Thông tin sự kiện

- Người phân tích: Nguyễn Hoàng Đạt
- Thời gian phát hiện: 11/07/2025
- Nguồn dữ liệu: File ghi lại lưu lượng mạng capture_2025-07-11_21-50-44.pcapng

2. Mục tiêu phân tích

Xác định các hành vi tấn công tiềm ẩn từ lưu lượng mạng đã ghi nhận, phục vụ điều tra sự cố và hỗ trợ đề xuất biện pháp phòng vệ.

3. Công cụ và dữ liệu sử dụng

- Công cụ phân tích: Wireshark GUI
- Nguồn dữ liệu: File PCAP capture_2025-07-11_21-50-44.pcapng
- Môi trường mạng: Mạng nội bộ 192.168.88.0/24 (giả lập attacker và nạn nhân)
- Giả định: Máy 192.168.88.145 là attacker (Kali Linux), 192.168.88.164 là máy mục tiêu

4. Phân tích kỹ thuật

4.1. Hành vi quét cổng (Port Scanning)

- Filter áp dụng:

<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>

- Kết quả :

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 and tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
47068	14159.988970	192.168.88.145	192.168.88.164	TCP	74	33722 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
45297	34434.159791	192.168.88.145	192.168.88.164	TCP	60	34170 → 1 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45978	34435.245804	192.168.88.145	192.168.88.164	TCP	60	34170 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46215	34435.325833	192.168.88.145	192.168.88.164	TCP	60	34170 → 1000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46465	34435.346758	192.168.88.145	192.168.88.164	TCP	60	34170 → 10000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46615	34435.360857	192.168.88.145	192.168.88.164	TCP	60	34170 → 10001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45566	34434.104590	192.168.88.145	192.168.88.164	TCP	60	34170 → 10002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45392	34434.171742	192.168.88.145	192.168.88.164	TCP	60	34170 → 10003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46658	34435.283528	192.168.88.145	192.168.88.164	TCP	60	34170 → 10004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45204	34434.149362	192.168.88.145	192.168.88.164	TCP	60	34170 → 10009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45088	34434.134061	192.168.88.145	192.168.88.164	TCP	60	34170 → 1001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45592	34434.185315	192.168.88.145	192.168.88.164	TCP	60	34170 → 10010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46659	34435.365697	192.168.88.145	192.168.88.164	TCP	60	34170 → 10012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46029	34435.303932	192.168.88.145	192.168.88.164	TCP	60	34170 → 1002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46772	34435.379879	192.168.88.145	192.168.88.164	TCP	60	34170 → 10024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45627	34434.191395	192.168.88.145	192.168.88.164	TCP	60	34170 → 10025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45927	34435.227462	192.168.88.145	192.168.88.164	TCP	60	34170 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46832	34435.388737	192.168.88.145	192.168.88.164	TCP	60	34170 → 10082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45730	34434.292605	192.168.88.145	192.168.88.164	TCP	60	34170 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45169	34434.147757	192.168.88.145	192.168.88.164	TCP	60	34170 → 1010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46432	34435.340765	192.168.88.145	192.168.88.164	TCP	60	34170 → 1011 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46078	34435.319636	192.168.88.145	192.168.88.164	TCP	60	34170 → 10180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45063	34434.130150	192.168.88.145	192.168.88.164	TCP	60	34170 → 1021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45991	34435.249448	192.168.88.145	192.168.88.164	TCP	60	34170 → 10215 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46570	34435.354903	192.168.88.145	192.168.88.164	TCP	60	34170 → 1022 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46231	34435.330100	192.168.88.145	192.168.88.164	TCP	60	34170 → 1023 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45064	34434.130150	192.168.88.145	192.168.88.164	TCP	60	34170 → 1024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45483	34434.178850	192.168.88.145	192.168.88.164	TCP	60	34170 → 10243 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45088	34434.095651	192.168.88.145	192.168.88.164	TCP	60	34170 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 47068: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens33, id 0
 Ethernet II, Src: VMware-da:0a:5f (00:0c:29:da:0a:5f), Dst: VMware-83:1b:1c (00:0c:29:83:1b:1c)
 Internet Protocol Version 4, Src: 192.168.88.145, Dst: 192.168.88.164
 Transmission Control Protocol, Src Port: 33722, Dst Port: 22, Seq: 0, Len: 0

0000 00 0c 29 83 1b 1c 00 0c 29 da 0a 5f 00 00 45 00 ..).....).....E
 0010 00 3c 4 2d 40 00 40 00 44 08 c0 a8 58 91 c0 a8 <.-@.D...X..
 0020 58 a4 83 ba 00 16 99 88 05 45 00 00 00 a0 02 X.....eE.....
 0030 fa f0 a0 2f 00 00 02 94 05 b4 04 02 00 0a 31 61/.....!a
 0040 c6 59 00 00 00 00 01 83 03 07 ..Y.....

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 and tcp.flags.ack == 0

Wireshark - Conversations - capture1.pcapng

Ethernet-25	IPv4-47	IPv6-7	TCP-4404	UDP-371	Bytes	Packets	Bytes A → B	Packets A → B	Bytes B → A	Packets B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
Address A	Port A	Address B	Port B	Packets	Bytes	Bytes A → B	Packets A → B	Bytes B → A	Packets B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
192.168.88.145	46647	192.168.88.164	3389	1	60	1	60	0	0	011282.603215	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	445	1	60	1	60	0	0	011282.603215	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	5900	1	60	1	60	0	0	011282.603242	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	23	3	180	2	120	1	60	011282.603242	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	21	3	180	2	120	1	60	6011282.65129c	0.0120	80 k	48 k	
192.168.88.145	46647	192.168.88.164	80	3	180	2	120	1	60	6011282.65350c	0.0099	97 k	48 k	
192.168.88.145	46647	192.168.88.164	443	1	60	1	60	0	0	011282.65350c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	25	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	110	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	199	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	139	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	113	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	1025	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	993	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	8888	1	60	1	60	0	0	011282.65361c	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	1720	1	60	1	60	0	0	011282.654087	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	143	1	60	1	60	0	0	011282.66598e	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	554	1	60	1	60	0	0	011282.66598e	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	22	3	180	2	120	1	60	6011282.66598e	0.0007	---	---	
192.168.88.145	46647	192.168.88.164	53	1	60	1	60	0	0	011282.666067	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	1723	1	60	1	60	0	0	011282.669322	0.0000	---	---	
192.168.88.145	46647	192.168.88.164	135	1	60	1	60	0	0	011282.669547	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	135	1	60	1	60	0	0	011283.70458e	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	1723	1	60	1	60	0	0	011283.704587	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	53	1	60	1	60	0	0	011283.70482c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	554	1	60	1	60	0	0	011283.706174	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	143	1	60	1	60	0	0	011283.706174	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	1720	1	60	1	60	0	0	011283.706174	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	8888	1	60	1	60	0	0	011283.706174	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	993	1	60	1	60	0	0	011283.70622c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	1025	1	60	1	60	0	0	011283.70710c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	113	1	60	1	60	0	0	011283.70710c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	139	1	60	1	60	0	0	011283.70710c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	199	1	60	1	60	0	0	011283.70710c	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	110	1	60	1	60	0	0	011283.707292	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	25	1	60	1	60	0	0	011283.70761e	0.0000	---	---	
192.168.88.145	46649	192.168.88.164	443	1	60	1	60	0	0	011283.70761e	0.0000	---	---	

Limit to display filter: Absolute start time

Conversation Tunes

- Mô tả:
 - IP 192.168.88.145 gửi liên tiếp các gói SYN tới nhiều cổng đích trên IP 192.168.88.164
 - Giao tiếp không có ACK trả về → đặc điểm của SYN scan
 - Dạng quét phổ biến khi sử dụng công cụ nmap

4.2. Brute-force SSH

- Filter áp dụng:

```
tcp.port == 22 && tcp.len > 0
```

- Kết quả :

No.	Time	Source	Destination	Protocol	Length	Info
43066	31396.433874..	192.168.88.164	192.168.88.145	TCP	88	22 -> 57948 [PSH, ACK] Seq=1 Ack=24 Win=65152 Len=22 TSval=332...
43068	31396.433959..	192.168.88.164	192.168.88.145	TCP	88	22 -> 57962 [PSH, ACK] Seq=1 Ack=24 Win=65152 Len=22 TSval=332...
42885	31395.896815..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
42995	31396.094466..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
42998	31396.189342..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43086	31396.167956..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43038	31396.239964..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43075	31396.441054..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43078	31396.480660..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43090	31396.536434..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43121	31396.636514..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43143	31396.772955..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43146	31396.797739..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43166	31396.880717..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43192	31396.988301..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43205	31397.035564..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43218	31397.085599..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43313	31425.118251..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43364	31425.449564..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43365	31425.450103..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43367	31425.450887..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
43369	31425.452269..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
47019	34461.786069..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
47060	34462.582677..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
47085	34463.008143..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
47088	34463.010556..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
47095	34463.034536..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
50170	35251.270394..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
50211	35252.227498..	192.168.88.145	192.168.88.164	SSHv2	114	Client: Diffie-Hellman Key Exchange Init

Frame 42878: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface ens33, id 0
Ethernet II, Src: VMware-da:0a:5f (00:0c:29:da:0a:5f), Dst: VMware_83:1b:1c (00:0c:29:83:1b:1c)
Internet Protocol Version 4, Src: 192.168.88.145, Dst: 192.168.88.164
Transmission Control Protocol, Src Port: 57820, Dst Port: 22, Seq: 1, Ack: 1, Len: 23
SSH Protocol

0000 00 0c 29 83 1b 1c 00 0c 29 da 0a 5f 00 00 45 00 --).....)....E-
0010 00 4b a5 81 40 00 40 06 62 a5 c0 a8 58 91 c0 a8 K' @ @ b...X..
0020 58 a4 e1 dc 00 16 19 9d 2a d1 8e f0 02 3e 80 18 X.....>.....
0030 01 f6 e7 b4 00 00 01 01 08 9a 31 33 01 62 c6 3e13 b>
0040 70 4b 53 40 2d 32 2e 30 2d 6c 09 62 73 73 68 pKSSH-2, 0-libssh
0050 5f 30 2e 31 31 2e 31 0d 0a ..0.11.1..

No.	Time	Source	Destination	Protocol	Length	Info
43159	31396.867324..	192.168.88.164	192.168.88.145	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43180	31396.968715..	192.168.88.164	192.168.88.145	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43207	31397.050869..	192.168.88.164	192.168.88.145	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43223	31397.108801..	192.168.88.164	192.168.88.145	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43236	31397.133304..	192.168.88.164	192.168.88.145	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43315	31425.126100..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43370	31425.463868..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43372	31425.465278..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43374	31425.465922..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43375	31425.465989..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
47021	34461.858081..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
47062	34462.623914..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
47090	34463.822210..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
47092	34463.825972..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
47097	34463.846606..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
50172	35251.389203..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
50217	35252.271111..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
50234	35252.590926..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
50251	35252.702214..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
50265	35252.878684..	192.168.88.145	192.168.88.164	SSHv2	550	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=276)
43243	31398.374773..	192.168.88.164	192.168.88.145	SSHv2	94	Server: Encrypted packet (len=28)
43436	31432.944691..	192.168.88.164	192.168.88.145	SSHv2	94	Server: Encrypted packet (len=28)
47163	34470.497520..	192.168.88.145	192.168.88.164	SSHv2	94	Server: Encrypted packet (len=28)
50293	35259.713147..	192.168.88.145	192.168.88.164	SSHv2	94	Server: Encrypted packet (len=28)
42891	31395.147216..	192.168.88.164	192.168.88.145	SSHv2	110	Server: Encrypted packet (len=44)
43012	31396.174265..	192.168.88.164	192.168.88.145	SSHv2	110	Server: Encrypted packet (len=44)
43019	31396.194879..	192.168.88.164	192.168.88.145	SSHv2	110	Server: Encrypted packet (len=44)
43038	31396.241005..	192.168.88.164	192.168.88.145	SSHv2	110	Server: Encrypted packet (len=44)
43056	31396.326306..	192.168.88.164	192.168.88.145	SSHv2	110	Server: Encrypted packet (len=44)

Frame 42878: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface ens33, id 0
Ethernet II, Src: VMware-da:0a:5f (00:0c:29:da:0a:5f), Dst: VMware_83:1b:1c (00:0c:29:83:1b:1c)
Internet Protocol Version 4, Src: 192.168.88.145, Dst: 192.168.88.164
Transmission Control Protocol, Src Port: 57820, Dst Port: 22, Seq: 1, Ack: 1, Len: 23
SSH Protocol

0000 00 0c 29 83 1b 1c 00 0c 29 da 0a 5f 00 00 45 00 --).....)....E-
0010 00 4b a5 81 40 00 40 06 62 a5 c0 a8 58 91 c0 a8 K' @ @ b...X..
0020 58 a4 e1 dc 00 16 19 9d 2a d1 8e f0 02 3e 80 18 X.....>.....
0030 01 f6 e7 b4 00 00 01 01 08 9a 31 33 01 62 c6 3e13 b>
0040 70 4b 53 40 2d 32 2e 30 2d 6c 09 62 73 73 68 pKSSH-2, 0-libssh
0050 5f 30 2e 31 31 2e 31 0d 0a ..0.11.1..

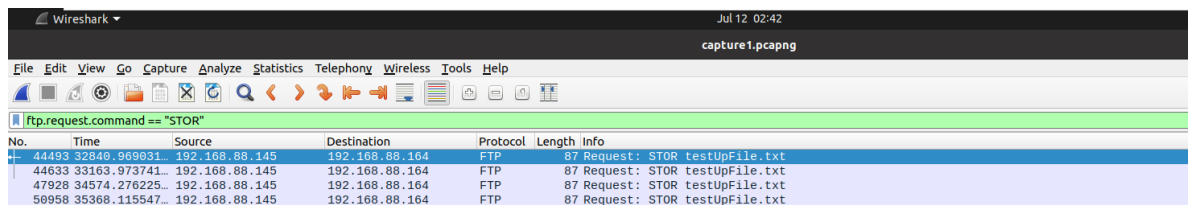
- Dấu hiệu:
 - IP 192.168.88.145 gửi liên tục các gói tin tới SSH server 192.168.88.164
 - Xuất hiện hàng chục gói tin với protocol SSHv2, chứa nội dung Client: Diffie-Hellman Key Exchange Init, Client: Protocol (SSH-2.0-libssh_0.11.1) và New Keys
 - Các gói có độ dài dao động từ 82 đến 970 bytes, được gửi lặp lại liên tục trong thời gian ngắn → không hoàn tất quá trình xác thực
 - Các phản hồi từ phía máy chủ (192.168.88.164) bao gồm: Server: Diffie-Hellman Key Exchange Reply, New Keys, và Encrypted packet (len=276) hoặc (len=28/44), cho thấy server đang từ chối hoặc cắt kết nối liên tục với các yêu cầu không hợp lệ
 - Đây là biểu hiện rõ ràng của brute-force SSH sử dụng công cụ hydra, nơi attacker cố gắng đăng nhập bằng nhiều username/password nhưng đều bị từ chối
 - Việc thiết lập lại quá trình handshake cho thấy server liên tục reset kết nối với attacker

4.3. FTP Upload file nghi ngờ

- Filter áp dụng:

```
ftp.request.command == "STOR"
```

- Kết quả :



Wireshark capture showing FTP traffic. The packet list shows three frames (44493, 44633, 47928) from 192.168.88.145 to 192.168.88.164, all with protocol FTP and length 87. The packet details for frame 44493 show the command 'STOR testUpFile.txt'.

No.	Time	Source	Destination	Protocol	Length	Info
44493	32840.969031	192.168.88.145	192.168.88.164	FTP	87	Request: STOR testUpFile.txt
44633	33163.973741	192.168.88.145	192.168.88.164	FTP	87	Request: STOR testUpFile.txt
47928	34574.276225	192.168.88.145	192.168.88.164	FTP	87	Request: STOR testUpFile.txt
50958	35368.115547	192.168.88.145	192.168.88.164	FTP	87	Request: STOR testUpFile.txt

Frame 44493: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface ens33, id 0
 Ethernet II, Src: VMware_da:0a:5f (00:0c:29:da:0a:5f), Dst: VMware_83:1b:1c (00:0c:29:83:1b:1c)
 Internet Protocol Version 4, Src: 192.168.88.145, Dst: 192.168.88.164
 Transmission Control Protocol, Src Port: 43728, Dst Port: 21, Seq: 50, Ack: 263, Len: 21
 File Transfer Protocol (FTP)
 [Current working directory:]
 [Command response frames: 1]
 [Command response bytes: 51]
 [Command response first frame: 44495]
 [Command response last frame: 44495]

```

0000  00 0c 29 83 1b 1c 00 0c 29 da 0a 5f 08 00 45 10  .....)...E
0010  00 49 73 60 40 00 40 06 94 b8 c8 a8 58 91 c0 a8  .Is'@_...X...
0020  58 a4 aa d0 00 15 b0 dd 8a be 38 6f 08 2c 80 18  X.....80,..
0030  7e a7 3d ae 00 00 01 01 08 0a 31 49 12 00 c6 54  ~=====1I...T
0040  80 ee 53 54 4f 52 20 74 65 73 74 55 70 46 69 6c  ..STOR testUpFil
0050  65 2e 74 78 74 0d 0a                                e.txt..
  
```

- Dấu hiệu:
 - Attacker thực hiện đăng nhập FTP thành công
 - Gửi lệnh STOR để tải lên tệp “testUpFile.txt” (trong thực tế có thể là file shell.php hoặc mã độc)

4.4. Truy cập file qua HTTP (Giả sử file upload là shell.php hoặc mã độc)

- Filter áp dụng:

http.request.uri contains ".php"

- Kết quả : chưa thực hiện được do file up là .txt không phải shell hay mã độc
- Dấu hiệu:
 - Sau khi upload, attacker truy cập file .php từ trình duyệt
 - Có khả năng thực thi lệnh từ xa (RCE) nếu máy chủ bị khai thác

5. Đánh giá tổng hợp

Hành vi	Mức độ nghiêm trọng	Tác động tiềm ẩn
Port scan	Trung bình	Phát hiện dịch vụ mở, chuẩn bị tấn công
Brute-force SSH	Cao	Truy cập trái phép nếu thành công
Upload FTP	Cao	Đưa mã độc/shell độc hại vào hệ thống
Truy cập shell	Rất cao	Có thể chiếm quyền điều khiển server

6. Kiến nghị xử lý

Hành động	Mục tiêu
Chặn IP 192.168.88.145	Ngăn chặn tiếp tục tấn công từ IP này
Kiểm tra log FTP/SSH	Đánh giá thiệt hại hệ thống
Tăng cường giám sát qua SIEM	Cảnh báo sớm các hành vi tương tự
Triển khai IDS/IPS	Phát hiện sớm brute-force & scan
Vô hiệu hóa dịch vụ không cần thiết	Giảm tấn công bề mặt

7. Kết luận

Dựa trên phân tích file PCAP ghi lại lưu lượng mạng nội bộ, có thể kết luận rằng hệ thống đã bị một attacker nội bộ (IP 192.168.88.145) thực hiện chuỗi hành vi tấn công có chủ đích.

Các hành vi bao gồm:

- Quét cổng để phát hiện các dịch vụ đang mở (port scan)
- Thử đăng nhập SSH hàng loạt nhằm chiếm quyền truy cập hệ thống (brute-force)
- Tải tệp đáng ngờ qua giao thức FTP (có khả năng là web shell hoặc mã độc)
- Truy cập file .php qua HTTP để thực thi từ xa (có khả năng là backdoor hoặc remote shell)