

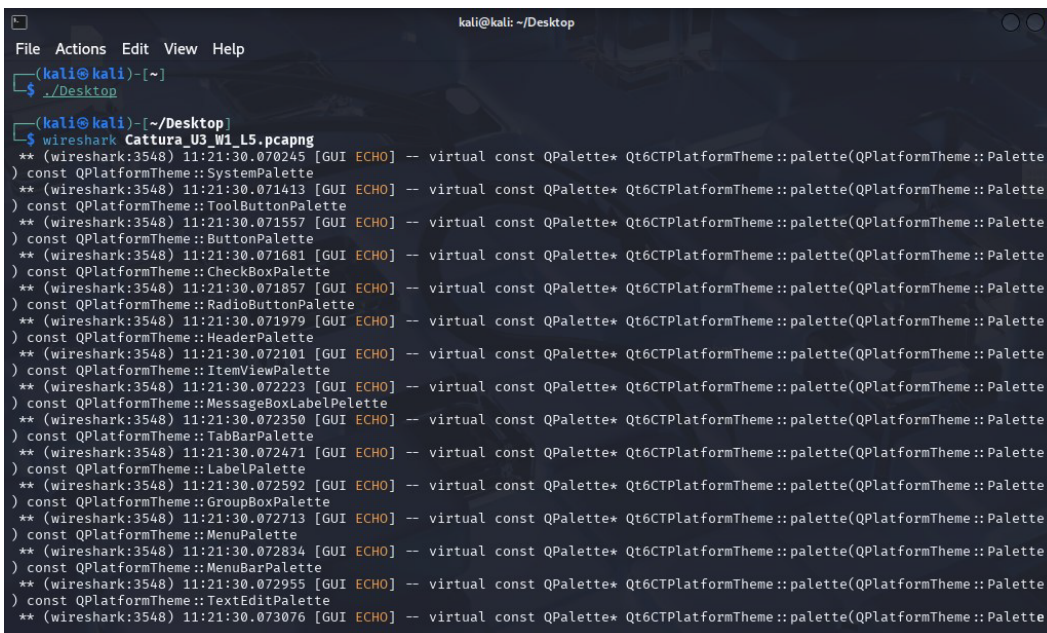
# Analisi Threat Intelligence

## Ambiente di analisi

- Sistema operativo: Kali Linux (in VM)
- Tool utilizzato: Wireshark
- Connessione: ambiente isolato (no Internet)
- File analizzato: Cattura\_U3\_W1\_L5.pcapng

## Obiettivo

Analizzare il file di cattura Cattura\_U3\_W1\_L5.pcapng tramite Wireshark, con lo scopo di identificare eventuali Indicatori di Compromissione (IOC), ipotizzare possibili vettori di attacco e suggerire contromisure adeguate.



```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ ./Desktop
(kali@kali)-[~/Desktop]
$ wireshark Cattura_U3_W1_L5.pcapng
** (wireshark:3548) 11:21:30.070245 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::SystemPalette
** (wireshark:3548) 11:21:30.071413 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::ToolButtonPalette
** (wireshark:3548) 11:21:30.071557 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::ButtonPalette
** (wireshark:3548) 11:21:30.071681 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::CheckBoxPalette
** (wireshark:3548) 11:21:30.071857 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::RadioButtonPalette
** (wireshark:3548) 11:21:30.071979 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::HeaderPalette
** (wireshark:3548) 11:21:30.072101 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::ItemViewPalette
** (wireshark:3548) 11:21:30.072223 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::MessageBoxLabelPalette
** (wireshark:3548) 11:21:30.072350 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::TabBarPalette
** (wireshark:3548) 11:21:30.072471 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::LabelPalette
** (wireshark:3548) 11:21:30.072592 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::GroupBoxPalette
** (wireshark:3548) 11:21:30.072713 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::MenuPalette
** (wireshark:3548) 11:21:30.072834 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::MenuBarPalette
** (wireshark:3548) 11:21:30.072955 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
) const QPlatformTheme::TextEditPalette
** (wireshark:3548) 11:21:30.073076 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette)
```

## Attività svolte

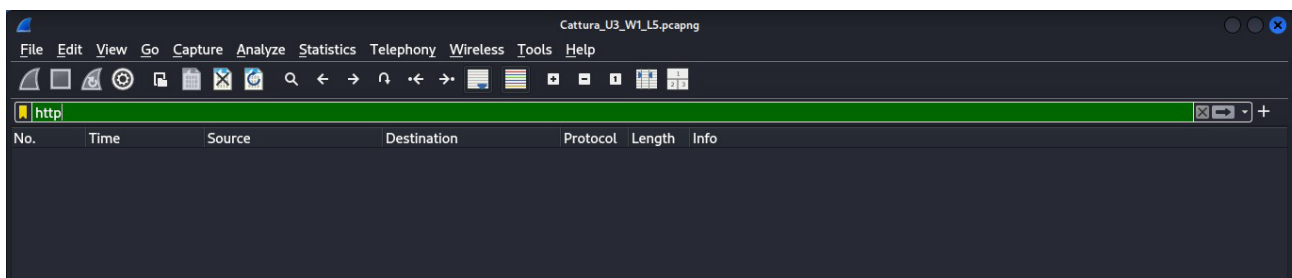
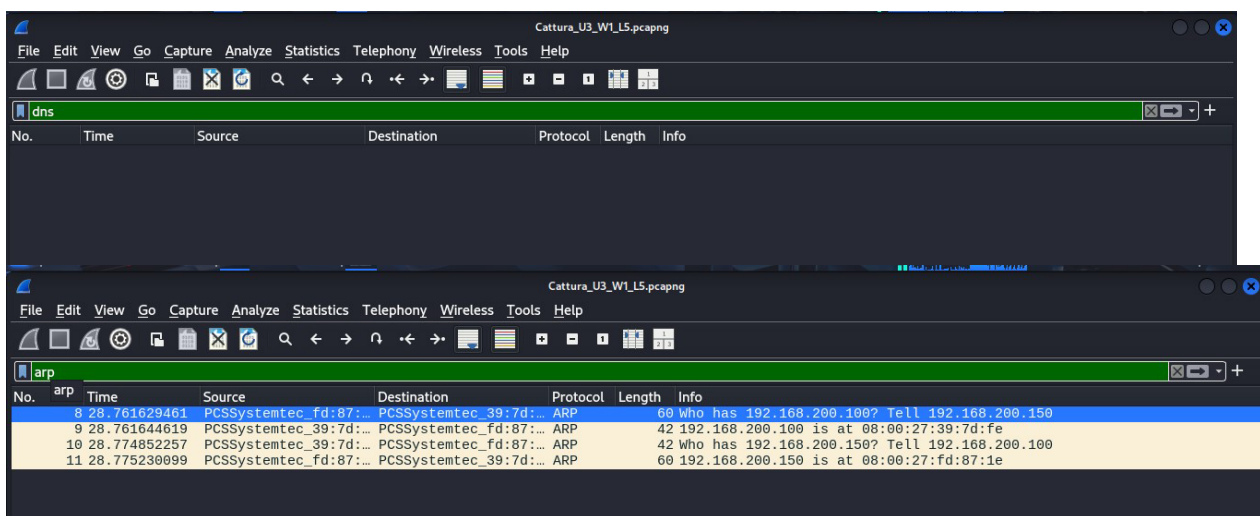
Sono stati applicati filtri manuali su vari protocolli, per individuare comunicazioni sospette o indicatori di compromissione. I filtri applicati sono stati:

- Dns = nessun risultato
- Arp = pochi pacchetti, senza evidenze di spoofing o scansioni
- http = nessun traffico attivo al momento della cattura
- tcp = presenti tentativi su porte comuni e porte non standard

Anche se non è stato osservato traffico HTTP attivo nella cattura, è stato rilevato che la **porta 80** risulta accessibile. Questo rappresenta un potenziale rischio, poiché si tratta di una porta comunemente utilizzata dagli attaccanti per:

- Trasferire file dannosi tramite servizi web
- Stabilire comunicazioni non cifrate con server remoti
- Utilizzare richieste HTTP per esfiltrare dati o inviare comandi

Poiché il protocollo HTTP è in chiaro, un attaccante potrebbe sfruttare la porta 80 per attività malevole.



**Cattura\_U3\_W1\_L5.pcapng**

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=...
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK...
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TS...
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8105224...
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=...
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK...
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK...
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TS...
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 T...
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK...
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TS...
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva...

**Cattura\_U3\_W1\_L5.pcapng**

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105...
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM ...
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4...
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TS...
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105...
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM ...
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4...
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TS...

## Contromisure consigliate

Come abbiamo visto dai risultati delle analisi, si raccomanda un'attività di monitoraggio attivo sugli host coinvolti, in particolare 192.168.200.100 e 192.168.200.150, con una verifica dettagliata dei log di sistema, dei processi attivi e delle connessioni di rete. È importante affiancare a questo una corretta configurazione del firewall interno, bloccando le porte non utilizzate.

Si consiglia un'analisi approfondita degli host sospetti, attraverso strumenti antimalware, controllo dei file di sistema e dei meccanismi di avvio automatico. Particolare attenzione dovrebbe essere posta alla gestione delle porte web: anche in assenza di traffico HTTP osservato, la presenza della porta 80 aperta rappresenta un potenziale vettore d'attacco. Un eventuale servizio HTTP esposto potrebbe essere sfruttato per distribuire file malevoli o stabilire connessioni con server esterni, per questo si consiglia di bloccare la porta 80 se non utilizzata o proteggerla con l'uso di HTTPS.

