

# TRACCIA 4

## Report di Analisi – Estrazione di un Eseguibile da un PCAP

OS:

Strumento utilizzato: Wireshark

File analizzato: nimda.download.pcap

Obiettivo: Identificare ed estrarre un file eseguibile da un file di cattura del traffico di rete (PCAP).

## 1. Obiettivo del Laboratorio

L'analisi del traffico di rete è fondamentale per individuare transazioni sospette e attacchi informatici. In questo laboratorio, si è analizzato un file di cattura per identificare ed estrarre un eseguibile scaricato attraverso il protocollo HTTP.

## 2. Procedura

### Parte 1: Analisi del traffico catturato

#### 1. Accesso ai file PCAP

Il file nimda.download.pcap è stato localizzato nella directory:  
/home/analyst/lab.support.files/pcaps

```
[analyst@sec0ps ~]$ cd lab.support.files/pcaps
[analyst@sec0ps pcaps]$ ls 01
ls: cannot access '01': No such file or directory
[analyst@sec0ps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download.pcap
```

#### 2. Apertura del file con Wireshark per l'analisi dei pacchetti

Si analizza il flusso di traffico registrato.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.202.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0 WS=512
2	0.000259	209.165.202.133	209.165.202.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3023496465 TSecr=4051203246 WS=512
3	0.000297	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246 TSecr=3023496465
4	0.000565	209.165.202.235	209.165.202.133	HTTP	230	GET /WS2.Nimda.Amm.exe HTTP/1.1
5	0.000588	209.165.202.133	209.165.202.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=0 TSval=3023496465 TSecr=4051203246
6	0.000708	209.165.202.133	209.165.202.235	TCP	324	6666 → 48598 [PSH, ACK] Seq=1 Ack=165 Win=30208 Len=258 TSval=3023496465 TSecr=4051203246 [TCP segment of a reassembled PDU]
7	0.000827	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Len=0 TSval=4051203246 TSecr=3023496465
8	0.004594	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=259 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of a reassembled PDU]
9	0.004602	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 Len=0 TSval=4051203247 TSecr=3023496466
10	0.004605	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=1707 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of a reassembled PDU]
11	0.004610	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=3155 Win=36352 Len=0 TSval=4051203247 TSecr=3023496466
12	0.004611	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=3155 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of a reassembled PDU]
13	0.004612	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=4603 Win=39424 Len=0 TSval=4051203247 TSecr=3023496466
14	0.004613	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=4603 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of a reassembled PDU]
15	0.004614	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=6051 Win=41984 Len=0 TSval=4051203247 TSecr=3023496466
16	0.004615	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=6051 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203246 [TCP segment of a reassembled PDU]
17	0.004617	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=7499 Win=45056 Len=0 TSval=4051203247 TSecr=3023496466
18	0.004706	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=7499 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203247 [TCP segment of a reassembled PDU]
19	0.004710	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=8947 Win=48128 Len=0 TSval=4051203247 TSecr=3023496466
20	0.004711	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=8947 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203247 [TCP segment of a reassembled PDU]
21	0.004713	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=10395 Win=50688 Len=0 TSval=4051203247 TSecr=3023496466
22	0.004713	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=10395 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203247 [TCP segment of a reassembled PDU]
23	0.004715	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=11843 Win=53760 Len=0 TSval=4051203247 TSecr=3023496466
24	0.004716	209.165.202.133	209.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=11843 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=4051203247 [TCP segment of a reassembled PDU]
25	0.004717	209.165.202.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=13291 Win=56832 Len=0 TSval=4051203247 TSecr=3023496466

### 3. Identificazione del traffico sospetto

I primi **tre pacchetti** del PCAP rappresentano la **stretta di mano TCP** (SYN, SYN-ACK, ACK).

Il **quarto pacchetto** rappresenta una **richiesta GET HTTP** per il download di un file sospetto.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	193.165.202.235	193.165.202.133	TCP	74	48598 → 6666 [VYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=0x1203246 TSecr=0 WS=912
2	0.000239	193.165.202.133	193.165.202.235	TCP	74	6666 → 48598 [VYN,ACK] Seq=0 Ack=1 Win=28660 Len=0 MSS=1460 SACK_PERM=1 TSval=3023496465 TSecr=0x1203246 WS=512
3	0.000297	193.165.202.235	193.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29666 Len=0 TSval=0x1203246 TSecr=3023496465
4	0.000565	193.165.202.235	193.165.202.133	HTTP	230	GET /WS2.Nimda.Ann.exe HTTP/1.1
5	0.000588	193.165.202.133	193.165.202.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=0 TSval=3023496465 TSecr=0x1203246
6	0.000708	193.165.202.133	193.165.202.235	TCP	324	6666 → 48598 [PSH,ACK] Seq=1 Ack=165 Win=30208 Len=258 TSval=3023496465 TSecr=0x1203246 [TCP segment of a reassembled PDU]
7	0.000827	193.165.202.235	193.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Len=0 TSval=0x1203246 TSecr=3023496465
8	0.004954	193.165.202.133	193.165.202.235	TCP	1514	6666 → 48598 [ACK] Seq=259 Ack=165 Win=30208 Len=1448 TSval=3023496466 TSecr=0x1203246 [TCP segment of a reassembled PDU]
9	0.004602	193.165.202.235	193.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 Len=0 TSval=0x1203247 TSecr=3023496466
<b>Frame 23 (23 bytes captured on interface 0)</b> <b>Ethernet II, Src: ead2:50:52:190:3ad:6666 (193.165.202.133), Dst: 194:00:00:00:00:00 (16:00:00:00:00:00)</b> Internet Protocol Version 4, Src: 193.165.202.235, Dst: 193.165.202.133 Transmission Control Protocol, Src Port: 48598, Dst Port: 6666, Seq: 1, Ack: 1, Len: 164 Hypertext Transfer Protocol → GET /WS2.Nimda.Ann.exe HTTP/1.1/1n → [Export Info (ChatSequence): GET /WS2.Nimda.Ann.exe HTTP/1.1/1n] [GET /WS2.Nimda.Ann.exe HTTP/1.1/1n] [Severity level: Chat] [Group: Sequence] Request Method: GET Request URI: /WS2.Nimda.Ann.exe Request Version: HTTP/1.1 User-Agent: Wget/1.19.1 (linux-gnu/x86_64) Accept: */*n Accept-Encoding: identityn Host: 193.165.202.133:6666n Connection: keep-aliven Ver: 1n [Full request URI: http://193.165.202.133:6666/WS2.Nimda.Ann.exe] [HTTP request 1/1] [No options in Frame 20]						
0000	16:4c:3f:7e:50:6a:55:3c:1e:90:3d:08:00:40:05:00:17	IP -> 193.165.202.133				
0001	00:2f:4e:40:00:40:00:00:43:81:61:dc:00:00:00:00:00	IP -> 193.165.202.133				
0002	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00	IP -> 193.165.202.133				
0003	00:3a:37:87:00:00:01:00:0a:01:78:74:0e:34:38:77:00	IP -> 193.165.202.133				
0004	00:17:47:45:20:00:01:00:00:00:00:00:00:00:00:00	IP -> 193.165.202.133				
0005	00:16:6d:6e:43:78:65:30:00:00:00:00:00:00:00:00	IP -> 193.165.202.133				
0006	00:31:05:25:73:65:72:4d:47:67:65:6a:73:5a:20:57:00	IP -> 193.165.202.133				
0007	00:70:75:74:31:20:39:20:39:20:39:20:39:20:39:20:39	IP -> 193.165.202.133				
0008	78:2d:67:75:29:6d:5a:41:63:63:63:63:63:63:63:63:63	IP -> 193.165.202.133				
0009	29:27:2a:00:0a:01:63:63:63:63:63:63:63:63:63:63	IP -> 193.165.202.133				
0010	69:49:67:78:30:20:64:67:67:67:67:67:67:67:67:67	IP -> 193.165.202.133				
0011	8d:49:67:73:74:30:20:30:20:30:20:30:20:30:20:30	IP -> 193.165.202.133				
0012	00:22:01:33:33:33:33:33:33:33:33:33:33:33:33:33	IP -> 193.165.202.133				
0013	74:59:69:6f:3e:3e:3e:3e:3e:3e:3e:3e:3e:3e:3e:3e	IP -> 193.165.202.133				
0014	78:65:02:0a:00:00:00:00:00:00:00:00:00:00:00:00	IP -> 193.165.202.133				

#### 4. Analisi del contenuto della richiesta HTTP

Selezionato il **quarto pacchetto**, è stata espansa la sezione **Hypertext Transfer Protocol (HTTP)** per visualizzare il contenuto della richiesta.

Si è confermato che il download del file avveniva tramite HTTP, utilizzando una richiesta **GET**.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP		Mark Packet (toggle)
2	0.000259	209.165.202.133	209.165.200.235	TCP		Ignore Packet (toggle)
3	0.000297	209.165.200.235	209.165.202.133	TCP		Set Time Reference (toggle)
4	0.000565	209.165.200.235	209.165.202.133	HTTP		Time Shift...
5	0.000588	209.165.202.133	209.165.200.235	TCP		Packet Comment...
6	0.000708	209.165.202.133	209.165.200.235	TCP		Manually Resolve Address
7	0.000827	209.165.200.235	209.165.202.133	TCP		Apply as Filter
8	0.004594	209.165.202.133	209.165.200.235	TCP		Prepare a Filter
9	0.004602	209.165.200.235	209.165.202.133	TCP		Conversion Filter
						Colorize Conversation
						SCTP
						Follow TCP Stream
						Follow UDP Stream

## 5. Ispezione del traffico binario

È stato utilizzato **Follow TCP**

**Stream** su Wireshark per ricostruire il traffico.

Il contenuto visualizzato presentava **caratteri binari e stringhe leggibili**, suggerendo la presenza di un file eseguibile.



## Parte 2: Estrazione dell'eseguibile

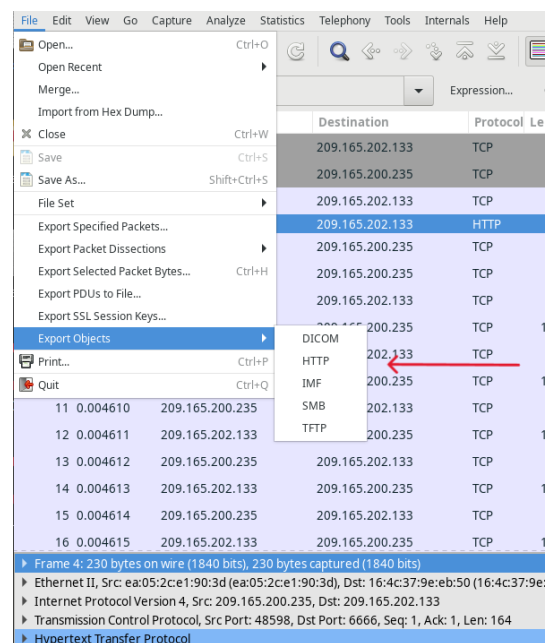
## 1. Individuazione del file scaricato

Si è identificato che la richiesta GET  
proveniva da:

209.165.200.235 → 209.165.202.133

## 2. Esportazione dell'oggetto HTTP

- Selezionato il pacchetto contenente la richiesta GET.
- Navigato su **File > Export Objects > HTTP** in Wireshark.
- L'elenco degli oggetti HTTP conteneva un solo file:  
**W32.Nimda.Amm.exe.**



Wireshark: HTTP object list				
Packet num	Hostname	Content Type	Size	Filename
309	209.165.202.133:6666	application/octet-stream	345 kB	W32.Nimda.Amm.exe

- Il file è stato salvato nella directory /home/analyst.

### 3. Identificazione del tipo di file

Con il tool **file** (da cli) si identifica la tipologia del file estratto; ovvero un file

```
[analyst@sec0ps pcaps]$ ls -l /home/analyst
total 356
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Feb 3 05:13 W32.Nimda.Amm.exe
[analyst@sec0ps pcaps]$ file /home/analyst/W32.Nimda.Amm.exe
/home/analyst/W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@sec0ps pcaps]$
```

**eseguitibile Windows per architetture x86-64.**

## 3. Risultati e Conclusioni

- Il **malware Nimda** è stato identificato all'interno della cattura PCAP.
- Il file è stato estratto con successo utilizzando Wireshark.
- Il file **W32.Nimda.Amm.exe** è stato confermato come un eseguibile Windows.
- L'analisi del flusso TCP ha mostrato **stringhe leggibili**, possibili indicatori delle funzioni del malware.

## 4. Mitigazione e Contromisure

### Isolare il file in un ambiente controllato

- Spostare il file in una sandbox (es. Cuckoo, Any.Run) per ulteriori analisi.

### Eseguire un'analisi statica e dinamica

- Analisi statica con strumenti come **strings**, **PEStudio**, **die (Detect It Easy)**.
- Analisi dinamica con strumenti come **Process Monitor**, **Wireshark**, e **Regshot**.

### Verificare Indicatori di Compromissione (IoC)

- Controllare hash del file con **VirusTotal**.
- Identificare eventuali IP/Domini sospetti collegati al file.

### Aggiornare firewall e antivirus

- Bloccare eventuali comunicazioni malevole.
- Aggiornare il database delle firme malware.