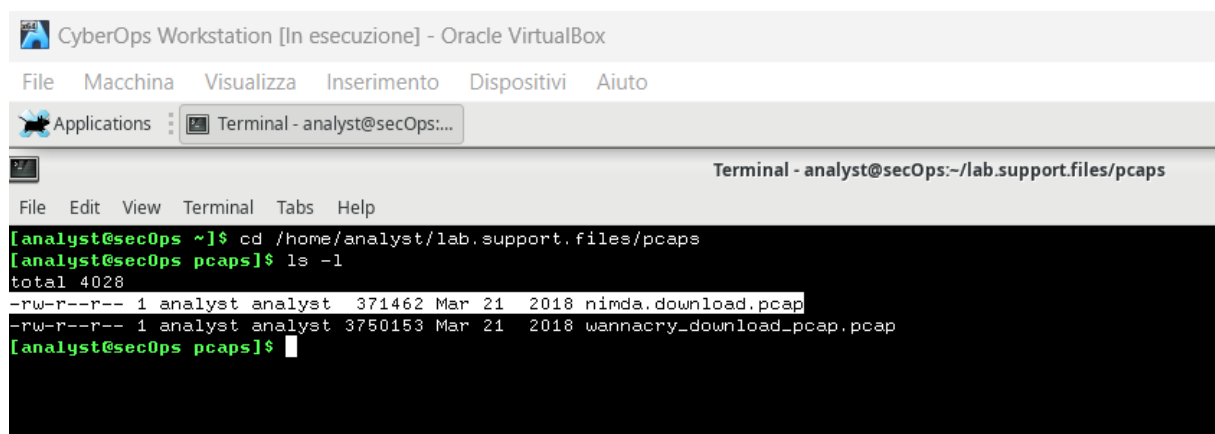


# Lab - Extract an Executable from a PCAP

L'obiettivo di questo esercizio è analizzare il traffico di rete catturato in un file PCAP, in particolare per identificare il download di un file eseguibile malevolo, e successivamente estrarre il file eseguibile da un pacchetto di cattura per un'analisi approfondita.

Per cominciare, apriamo il terminale sulla CyberOps Workstation. Una volta aperto il terminale, dobbiamo spostarci nella directory dove si trova il file di cattura PCAP, che contiene il traffico di rete relativo al download del malware. Utilizziamo il comando `cd` per navigare fino alla cartella `pcaps`.

Una volta che ci troviamo nella cartella, possiamo utilizzare il comando `ls -l` per elencare i file presenti. Notiamo che il file `nimda.download.pcap` è nella lista.



```
CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications : Terminal - analyst@secOps:...
Terminal - analyst@secOps:~/lab.support.files/pcaps
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/pcaps
[analyst@secOps 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.pcap
[analyst@secOps pcaps]$
```

Confermato che il file è presente, possiamo aprirlo con Wireshark. Per aprire il file con Wireshark, basta utilizzare il seguente comando nel terminale:



```
[analyst@secOps ~]$ /usr/bin/wireshark-gtk /home/analyst/lab.support.files/pcaps/nimda.dow
[1] 780
[analyst@secOps ~]$
```

Aperto Wireshark, vediamo una lista di pacchetti catturati nel file PCAP. Per identificare la richiesta HTTP di download del file malevolo, dobbiamo cercare il quarto pacchetto nella lista. Questo pacchetto contiene la richiesta GET per il file malevolo. Possiamo espandere la sezione Hypertext Transfer Protocol (HTTP) per visualizzare i dettagli del pacchetto.

nimda.download.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=2
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1
5	0.000588	209.165.202.133	209.165.200.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=302
6	0.000708	209.165.202.133	209.165.200.235	TCP	324	6666 → 48598 [PSH, ACK] Seq=1 Ack=165 Win

▶ Frame 4: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)

▶ Ethernet II, Src: ea:05:2c:e1:90:3d (ea:05:2c:e1:90:3d), Dst: 16:4c:37:9e:eb:50 (16:4c:37:9e:eb:50)

▶ Internet Protocol Version 4, Src: 209.165.200.235, Dst: 209.165.202.133

▶ Transmission Control Protocol, Src Port: 48598, Dst Port: 6666, Seq: 1, Ack: 1, Len: 164

▼ Hypertext Transfer Protocol

▼ GET /W32.Nimda.Amm.exe HTTP/1.1\r\n

▶ [Expert Info (Chat/Sequence): GET /W32.Nimda.Amm.exe HTTP/1.1\r\n]

Request Method: GET

Request URI: /W32.Nimda.Amm.exe

Request Version: HTTP/1.1

User-Agent: Wget/1.19.1 (linux-gnu)\r\n

Accept: \*/\*\r\n

Accept-Encoding: identity\r\n

Host: 209.165.202.133:6666\r\n

Connection: Keep-Alive\r\n

0040 e5 11 47 45 54 20 2f 57 33 32 2e 4e 69 6d 64 61 ...GET /W 32.Nimda

0050 2e 41 6d 6d 2e 65 78 65 20 48 54 54 50 2f 31 2e ...Amm.exe HTTP/1.

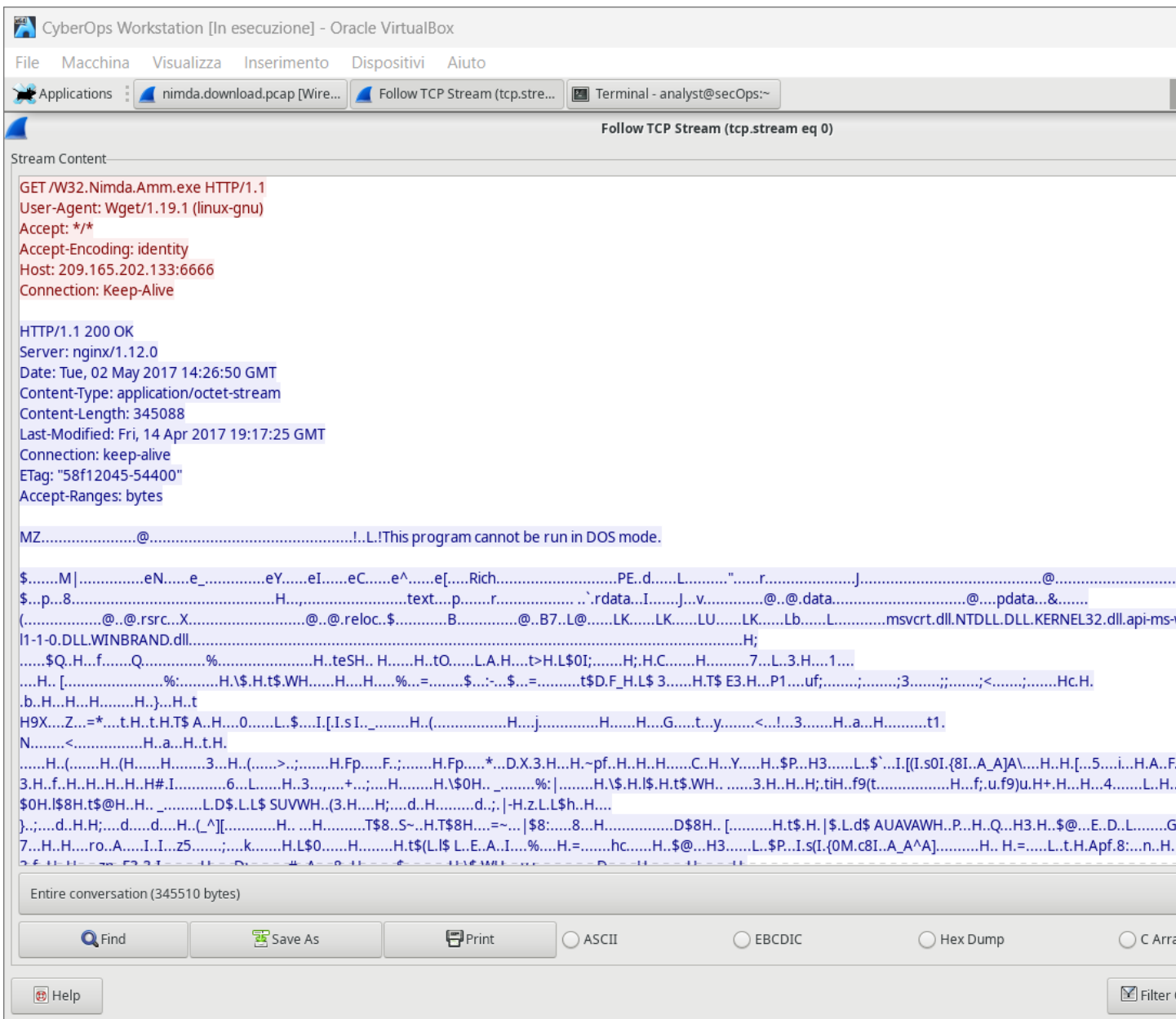
0060 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 57 ...1..User-Agent: W

0070 67 65 74 2f 31 2e 31 39 2e 31 20 28 6c 69 6e 75 ...get/1.19.1 (linu

Text item (text), 33 bytes

Packets: 316 · Displayed: 316 (100.0%) · Load time: 0:00.025

Successivamente, per analizzare in dettaglio il flusso di dati che ha portato al download del malware, selezioniamo il primo pacchetto TCP della cattura. Questo pacchetto è il primo della sequenza e contiene il flag SYN, che indica l'inizio di una connessione TCP. Facciamo clic destro su questo pacchetto e selezioniamo l'opzione Follow > TCP Stream. Questo comando fa sì che Wireshark mostri il contenuto completo della connessione TCP tra i due dispositivi.



La finestra che si apre ci mostra i dati trasmessi, e possiamo notare che i simboli che vediamo sono in gran parte incomprensibili. Questo perché Wireshark sta cercando di interpretare un file binario (l'eseguibile) come testo. I simboli strani non sono altro che i byte del file che sono stati trasmessi durante la connessione. Tuttavia, tra questi simboli ci sono alcune stringhe leggibili. Queste stringhe non sono altro che messaggi o comandi incorporati nel codice eseguibile. Analizzando queste stringhe, si scopre che il file non è il famoso virus Nimda, ma un file cmd.exe di Windows.

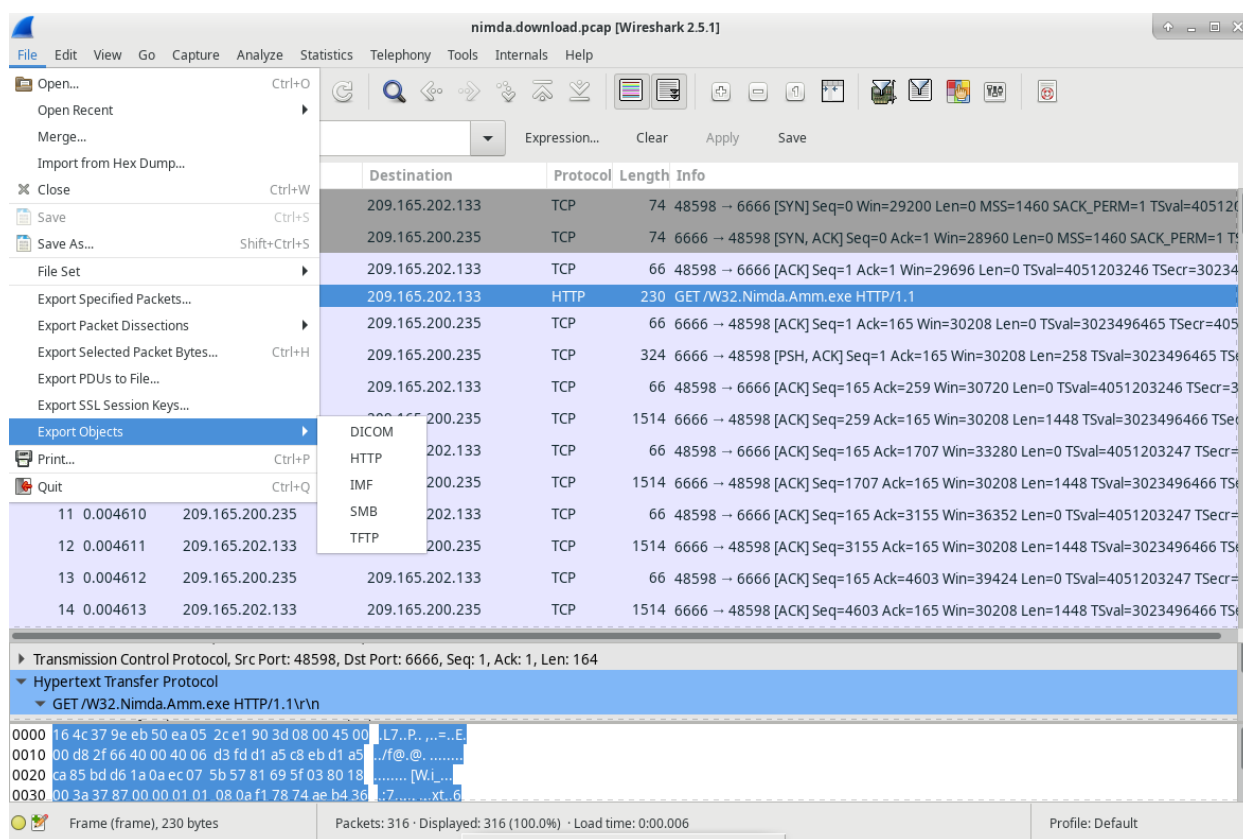
```

.....00.....h.....(.....00.....h.....00.....%.....h.....
.....4..V.S._V.E.R.S.I.O.N._I.N.F.O.....jD.....jD?...String.File.Info.....0.4.0.9.0.4.B.0...L.....Company.Name.....Micro.s.o.f.t..C.o.r.
\.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.....W.i.n.d.o.w.s..C.o.m.m.a.n.d..P.r.o.c.e.s.s.o.r.....F.i.l.e.V.e.r.s.i.o.n.....6...1...7.6.0.1...1.7.5.1.4..(w.in.7.sp.1...r.t.m...1.0.1.1.9.-1.8.5.0.)...
(.....I.n.t.e.r.n.a.l.N.a.m.e.....c.m.d.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.....M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n...A.l.l..r.i.g.h.t.s..r.e.s.e.r.v.e.d.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...C.m.
%...P.r.o.d.u.c.t.N.a.m.e.....M.i.c.r.o.s.o.f.t..W.i.n.d.o.w.s...O.p.e.r.a.t.i.n.g..S.y.s.t.e.m.....B....P.r.o.d.u.c.t.V.e.r.s.i.o.n...6...1...7.6.0.1...1.7.5.1.4....D....V.a.r.F.i.l.e.I.n.f.o....
$.T.r.a.n.s.l.a.t.i.o.n.....J..7.....0...@.../...!
8...d.....M.U.I.....M.U.I.....e.n.-U.S.....
0.8.@.H.P.X.h.x.....p.....(.@.H.`h.....(.@.H.`h.....(.@.H.`h.....(.@.H.`h.....(.@.H.`h.....H.h.....
(.@.H.`h.....

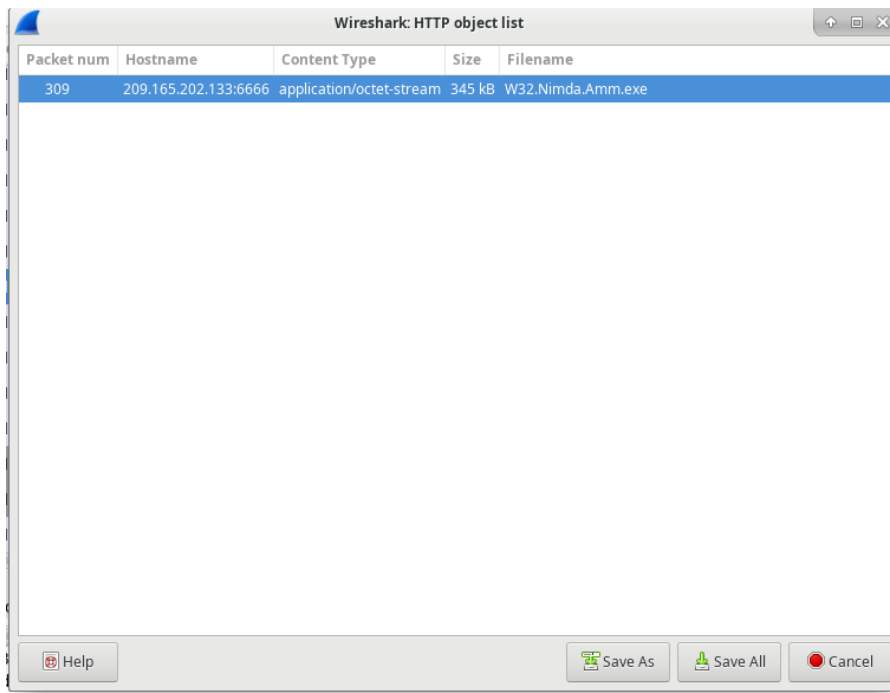
```

Una volta che abbiamo capito qual è il file che stiamo cercando, il prossimo passo consiste nell'estrarlo dal traffico di rete. Torniamo al file in Wireshark e selezioniamo nuovamente il pacchetto che contiene la richiesta GET.

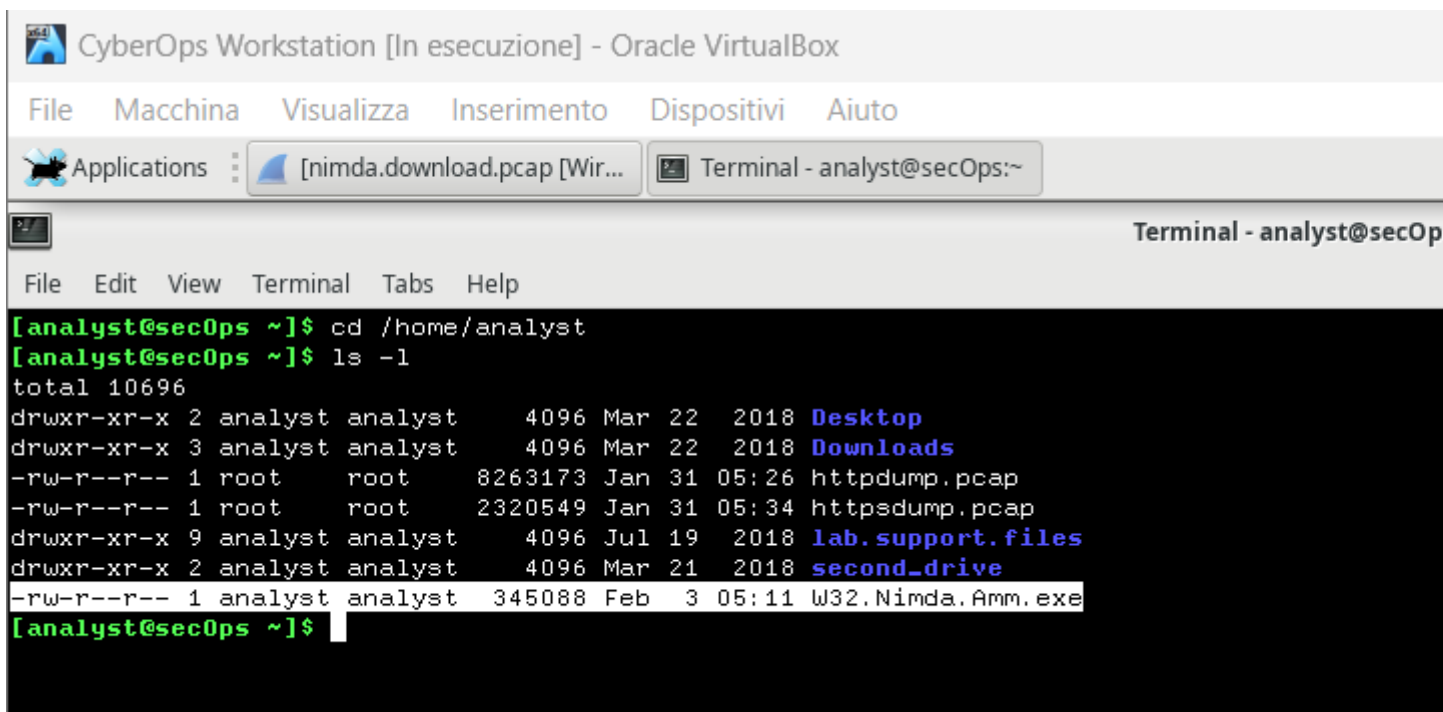
A questo punto, possiamo esportare il file eseguibile dal traffico HTTP catturato. Con il pacchetto GET selezionato, andiamo nel menu di Wireshark e selezioniamo File > Export Objects > HTTP.



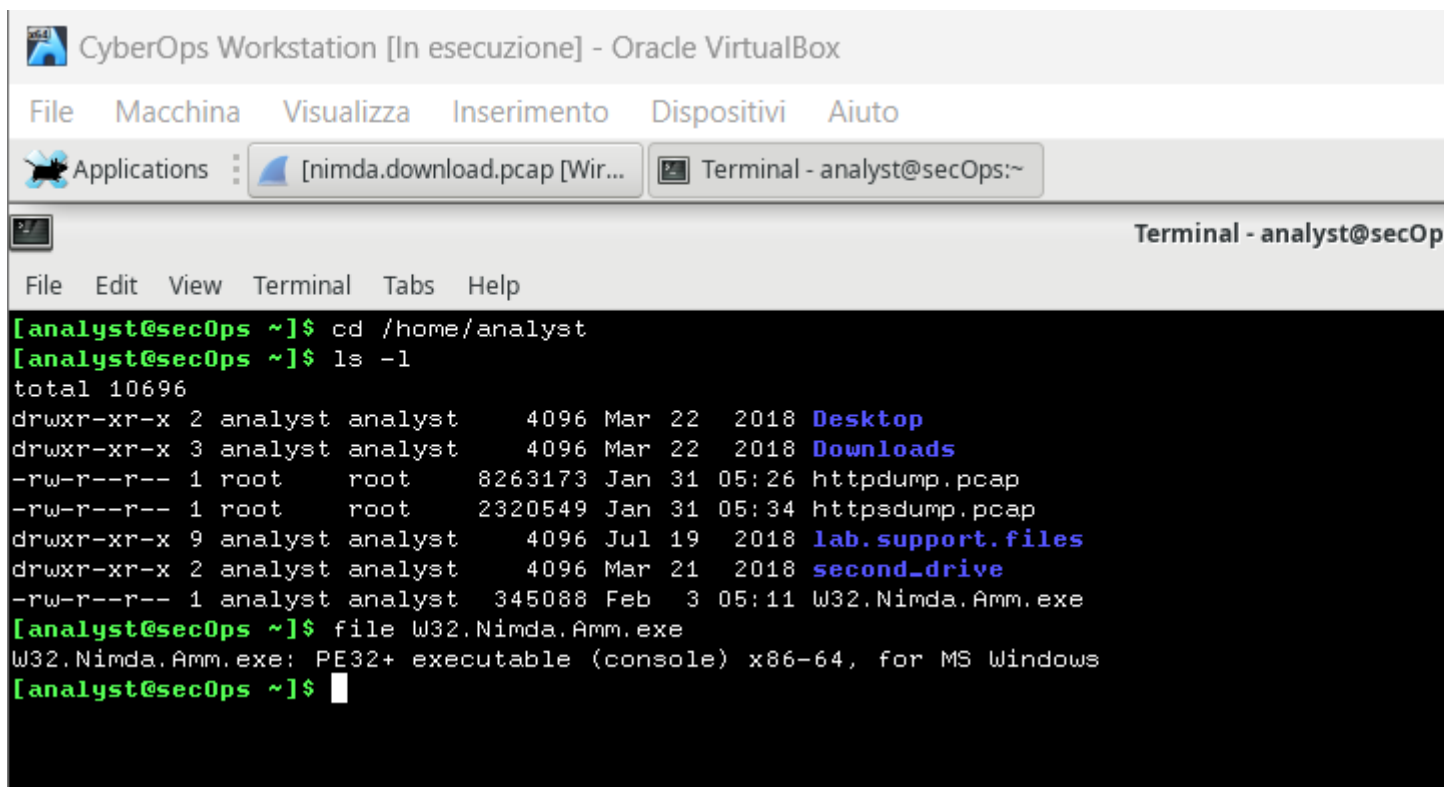
Selezioniamo il file W32.Nimda.Amm.exe e clicchiamo su Save As per salvarlo nella cartella /home/analyst/



Salvato il file, possiamo tornare al terminale e verificare che il file sia stato correttamente salvato nella directory giusta. Usiamo il comando `cd` per navigare nella cartella `/home/analyst/` e poi con il comando `ls -l` controlliamo che il file `W32.Nimda.Amm.exe` sia presente.



Usiamo il comando `file` per ottenere informazioni sul tipo di file e assicurarci che si tratti di un eseguibile Windows.



The screenshot shows a terminal window titled "CyberOps Workstation [In esecuzione] - Oracle VirtualBox". The terminal interface includes a menu bar with "File", "Macchina", "Visualizza", "Inserimento", "Dispositivi", and "Aiuto". Below the menu bar, there are tabs for "Applications", "[nimda.download.pcap [Wir...", and "Terminal - analyst@secOps:~". The terminal window itself has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows the following commands and output:

```
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 10696
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22 2018 Downloads
-rw-r--r-- 1 root root 8263173 Jan 31 05:26 httpdump.pcap
-rw-r--r-- 1 root root 2320549 Jan 31 05:34 httpsdump.pcap
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 05:11 W32.Nimda.Amm.exe
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

A questo punto, abbiamo estratto con successo il file eseguibile dal traffico di rete. Il prossimo passo per un analista di sicurezza sarebbe eseguire il malware in un ambiente isolato, come una sandbox, per monitorarne il comportamento. In un ambiente sandbox, possiamo osservare come il malware interagisce con il sistema, quali file modifica, quale tipo di traffico di rete genera e così via, senza rischiare di compromettere il sistema principale.

Un altro passaggio utile sarebbe caricare il file su VirusTotal, un servizio online che analizza automaticamente i file con diversi motori antivirus. Questo aiuterà a determinare se il file è già noto come malware e fornirà informazioni aggiuntive sulle sue capacità.

VirusTotal - File - db06c3

1234

https://www.virustotal.com/gui/file/db06c3534964e3fc79d2763144ba53742d7fa250ca336f4a0fe724b75aaff386

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

URL, IP address, domain or file hash

0

/ 71

Community Score

413

File distributed by Computernewb.com

Reanalyze

db06c3534964e3fc79d2763144ba53742d7fa250ca336f4a0fe724b75aaff386

Size

337.00 KB

Last Analysis

10 days ago

Cmd.Exe

peexeassemblydirect-cpu-clock-accessattachmentlegitidleruntime-moduleslong-sleeps64bitsdetect-debug-environmentknown-distributed

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to see more?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
Bkav Pro	Undetected	ClamAV	Undetected