

The image shows two windows from Sysinternals. The left window is Process Explorer, displaying a list of running processes with columns for Process, PID, CPU, and Privilege. The right window is TCPView, displaying a list of network connections with columns for Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State.

Process	PID	CPU	Priv...
System Idle Process	0	70.64	0 K
System	4	0.89	48 K
csrss.exe	268	5.23	0 K
wininit.exe	412	1.184...	872 K
services.exe	512	0.04	3.736...
svchost.exe	636	< 0.01	2.512...
svchost.exe	716	0.04	2.144...
svchost.exe	844	13.76...	
svchost.exe	894	2.34	30.10...
dmv.exe	1168	2.45	60.16...
svchost.exe	912	12.61...	
svchost.exe	1064	4.296...	
svchost.exe	1224	0.04	10.92...
spoolsv.exe	1312	5.372...	
svchost.exe	1348	6.336...	
svchost.exe	1408	3.216...	
vmtoolsd.exe	1532	0.18	5.592...
svchost.exe	1752	1.108...	
dllhost.exe	1924	0.01	2.948...
msdtc.exe	2016	1.952...	
taskhost.exe	1816	2.432...	
SearchIndexer.exe	2476	0.01	23.26...

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	528	TCP	0.0.0.0	1028	0.0.0.0	0	LISTENING
lsass.exe	528	TCPV6	[0:0:0:0:0:0:0:0]	1028	[0:0:0:0:0:0:0:0]	0	LISTENING
nc.exe	2156	TCP	0.0.0.0	50500	0.0.0.0	0	LISTENING
services.exe	512	TCP	0.0.0.0	1029	0.0.0.0	0	LISTENING
services.exe	512	TCPV6	[0:0:0:0:0:0:0:0]	1029	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	716	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING
svchost.exe	844	TCP	0.0.0.0	1026	0.0.0.0	0	LISTENING
svchost.exe	912	TCP	0.0.0.0	1027	0.0.0.0	0	LISTENING
svchost.exe	912	UDP	0.0.0.0	500	*	*	
svchost.exe	912	UDP	0.0.0.0	4500	*	*	
svchost.exe	1224	UDP	0.0.0.0	5355	*	*	
svchost.exe	716	TCPV6	[0:0:0:0:0:0:0:0]	135	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	844	TCPV6	[0:0:0:0:0:0:0:0]	1026	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	912	TCPV6	[0:0:0:0:0:0:0:0]	1027	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	912	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*	
svchost.exe	912	UDPV6	[0:0:0:0:0:0:0:0]	4500	*	*	
svchost.exe	1224	UDPV6	[0:0:0:0:0:0:0:0]	5355	*	*	
svchost.exe	844	UDPV6	[fe80::0:0:31d...	546	*	*	
System	4	TCP	192.168.1.10	139	0.0.0.0	0	LISTENING
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING
System	4	UDP	192.168.1.10	137	*	*	
System	4	UDP	192.168.1.10	138	*	*	
System	4	TCPV6	[0:0:0:0:0:0:0:0]	445	[0:0:0:0:0:0:0:0]	0	LISTENING
wininit.exe	412	TCP	0.0.0.0	1025	0.0.0.0	0	LISTENING
wininit.exe	412	TCPV6	[0:0:0:0:0:0:0:0]	1025	[0:0:0:0:0:0:0:0]	0	LISTENING

The image shows the Wireshark interface with a packet capture from the eth0 interface. The filter is set to 'Expression...'. The packet list shows a single packet of type DHCPv6, length 156, with source fe80::31d7:ceb9:e8f6:b3d and destination ff02::1:2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::31d7:ceb9:e8f6:b3d	ff02::1:2	DHCPv6	156	Solicit

The image shows the Process Explorer window with a list of running processes. The processes are sorted by PID. The CPU and Privilege columns are highlighted in green and orange respectively.

Process	PID	CPU	Priv...
System Idle Process	0	20.96	0 K
System	4	2.39	48 K
csrss.exe	360	1.184...	
wininit.exe	412	872 K	
csrss.exe	420	0.36	4.492...
conhost.exe	2648	6.76	912 K
winlogon.exe	468	< 0.01	1.580...
explorer.exe	1540	24.60	29.37...
vmtoolsd.exe	2136	0.43	9.672...
brbbot.exe	2144	0.01	2.028...
nc.exe	2156	700 K	
Process Explorer 16.04.exe	2124	2.86	8.868...
TCPView 3.05.exe	3528	1.64	5.196...
Desafjo23.exe	3044	20.93	824 K
Desafjo23.exe	3040	8.34	2.920...

Capturing from eth0 [Wireshark 1.8.2] (como superusuario)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Guardar

	Source	Destination	Protocol	Length	Info
2591000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xae39 A malwr.unam.jb
2654000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
27710000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xbd56 A malwr.unam.jb
27766000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
28453000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xed59 A malwr.unam.jb
28663000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
297731000	fe80::705b:4eaf:ff02::1:3	ff02::1:3	LLMNR	84	Standard query 0xf245 A wpaad

Capturing from eth0 [Wireshark 1.8.2] (como superusuario)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply Guardar

	Source	Destination	Protocol	Length	Info
52591000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xae39 A malwr.unam.jb
52654000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
57710000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xbd56 A malwr.unam.jb
57766000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
65453000	192.168.1.10	192.168.1.30	DNS	73	Standard query 0xed59 A malwr.unam.jb
65663000	192.168.1.30	192.168.1.10	ICMP	101	Destination unreachable (Port unreachable)
297731000	fe80::705b:4eaf:ff02::1:3	ff02::1:3	LLMNR	84	Standard query 0xf245 A wpaad

hosts: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
192.168.1.30           malwr.unam.jb
```

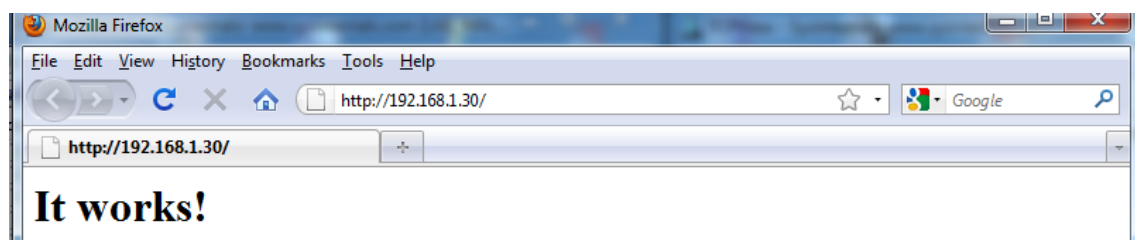
Capturing from eth0 [Wireshark 1.8.2] (como superusuario)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
216	665.434247000	192.168.1.30	192.168.1.10	TCP	54	80 > 1034 [RST, ACK] Seq=1 Ack=1 W
220	695.441091000	192.168.1.10	192.168.1.30	TCP	66	1035 > 80 [SYN] Seq=0 Win=8192 Len
221	695.441140000	192.168.1.30	192.168.1.10	TCP	54	80 > 1035 [RST, ACK] Seq=1 Ack=1 W
222	695.951153000	192.168.1.10	192.168.1.30	TCP	66	1035 > 80 [SYN] Seq=0 Win=8192 Len
223	695.951198000	192.168.1.30	192.168.1.10	TCP	54	80 > 1035 [RST, ACK] Seq=1 Ack=1 W
224	696.464867000	192.168.1.10	192.168.1.30	TCP	62	1035 > 80 [SYN] Seq=0 Win=8192 Len
225	696.464918000	192.168.1.30	192.168.1.10	TCP	54	80 > 1035 [RST, ACK] Seq=1 Ack=1 W
243	726.522036000	192.168.1.10	192.168.1.30	TCP	66	1036 > 80 [SYN] Seq=0 Win=8192 Len
244	726.522085000	192.168.1.30	192.168.1.10	TCP	54	80 > 1036 [RST, ACK] Seq=1 Ack=1 W
245	727.041085000	192.168.1.10	192.168.1.30	TCP	66	1036 > 80 [SYN] Seq=0 Win=8192 Len
246	727.041181000	192.168.1.30	192.168.1.10	TCP	54	80 > 1036 [RST, ACK] Seq=1 Ack=1 W
247	727.555442000	192.168.1.10	192.168.1.30	TCP	62	1036 > 80 [SYN] Seq=0 Win=8192 Len
248	727.555485000	192.168.1.30	192.168.1.10	TCP	54	80 > 1036 [RST, ACK] Seq=1 Ack=1 W

```
malware@MalwareAnalysisLab: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@MalwareAnalysisLab:/home/malware# /etc/init.d/apache2 start  
[....] Starting web server: apache2  
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName  
. ok  
root@MalwareAnalysisLab:/home/malware# netstat -nat  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN  
tcp6       0      0 :::80                  :::*                    LISTEN  
tcp6       0      0 :::8834                 :::*                    LISTEN  
root@MalwareAnalysisLab:/home/malware#
```



```
malware@MalwareAnalysisLab: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@MalwareAnalysisLab:/home/malware# touch /var/www/Key.txt  
root@MalwareAnalysisLab:/home/malware# ls -l /var/www/Key.txt  
-rw-r--r-- 1 root root 0 abr 18 14:20 /var/www/Key.txt  
root@MalwareAnalysisLab:/home/malware#
```

```
C:\Users\malware>wget http://192.168.1.30/Key.txt
--14:21:42-- http://192.168.1.30/Key.txt
=> 'Key.txt'
Connecting to 192.168.1.30:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]

[ <=> 1 0 --.--K/s

14:21:42 (0.00 B/s) - 'Key.txt' saved [0/0]
```

Capturing from eth0 [Wireshark 1.8.2] (como superusuario)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Guardar

Source	Destination	Protocol	Length	Info
192.168.1.10	192.168.1.30	TCP	60	1049 > 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.1.10	192.168.1.30	HTTP	160	GET /Key.txt HTTP/1.0
192.168.1.30	192.168.1.10	TCP	54	80 > 1049 [ACK] Seq=1 Ack=107 Win=14600 Len=0
192.168.1.30	192.168.1.10	HTTP	365	HTTP/1.1 200 OK

Key.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

&#84;&#88;&#86;&#106;&#97;&#71;&#57;&#122;&#73;&#71;&#72;&#120;&#98;&#51;&#77;&#98;&#71;&#86;&#50;&#56;&#121;&#66;&#104;&#73;&#71;&#78;&#118;&#98;&#109;&#57;&72;&#78;&#108;&#73;&#72;&#66;&#121;&#90;&#87;&#78;&#112;&#99;&#71;&#108;&#48;&#87;&#70;&#117;&#73;&#71;&#82;&#108;&#73;&#71;&#53;&#118;&#98;&#87;&#74;&#121;&#98;&#121;&#66;&#67;&#100;&#87;&#86;&#117;&#90;&#79;&#49;&#104;&#73;&#71;&#104;&#121;&#66;&#53;&#73;&#71;&#78;&#104;&#56;&#87;&#70;&#105;&#99;&#109;&#70;&#50;&88;&#90;&#118;&#99;&#121;&#66;&#119;&#99;&#109;&#86;&#111;&#97;&#88;&#78;&#48;&

file:///C:/Users/malware/Desktop/ESET

file:///C:/Users/malware/Desktop/safÃ-o23/Key.html

TXVjaG9zIGhxb3MgZGVzcHXpcywgZnJlbnRlIGFsIHBlbG90824gZGUgZnVzaWxhbWllbnRvL

