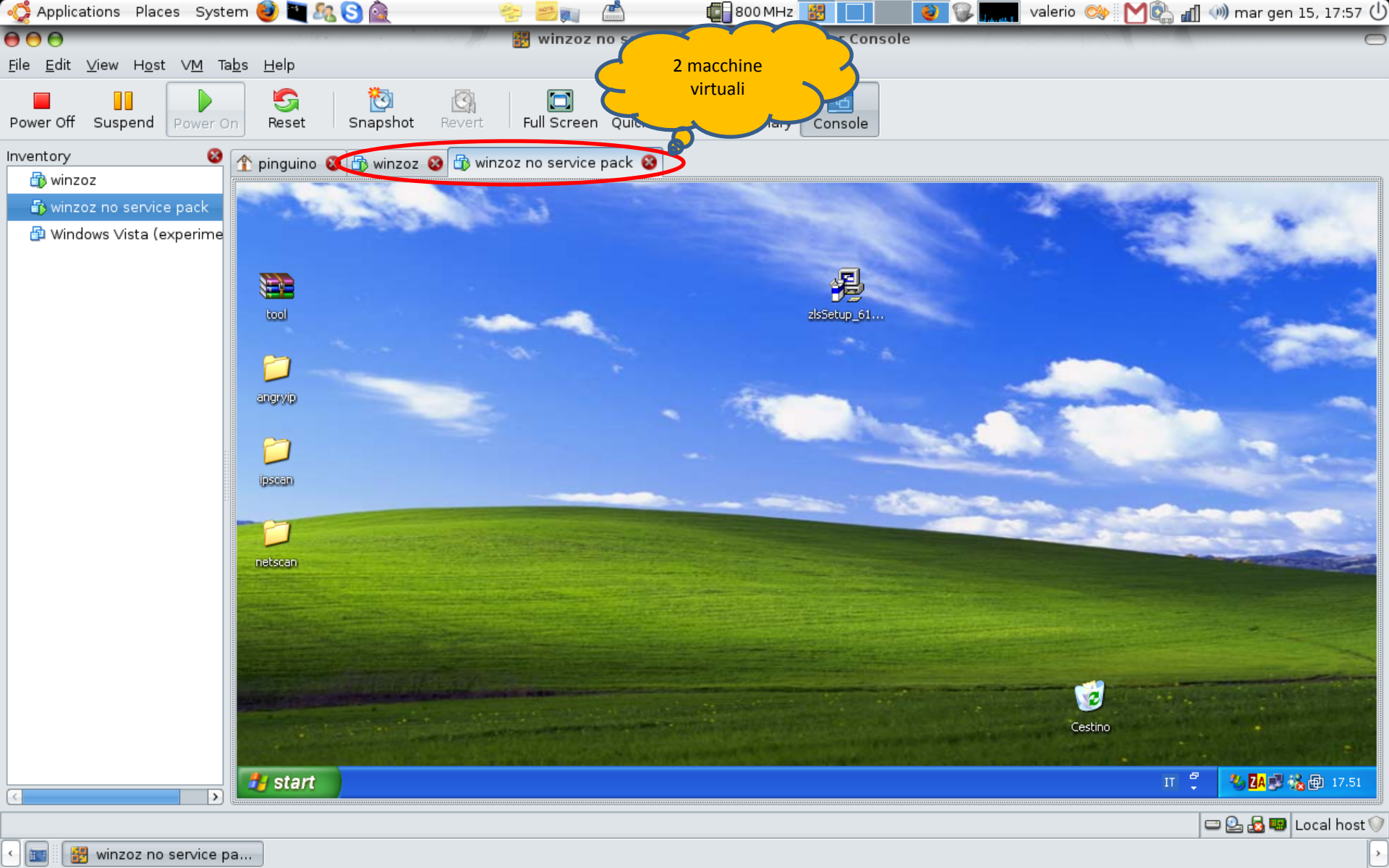
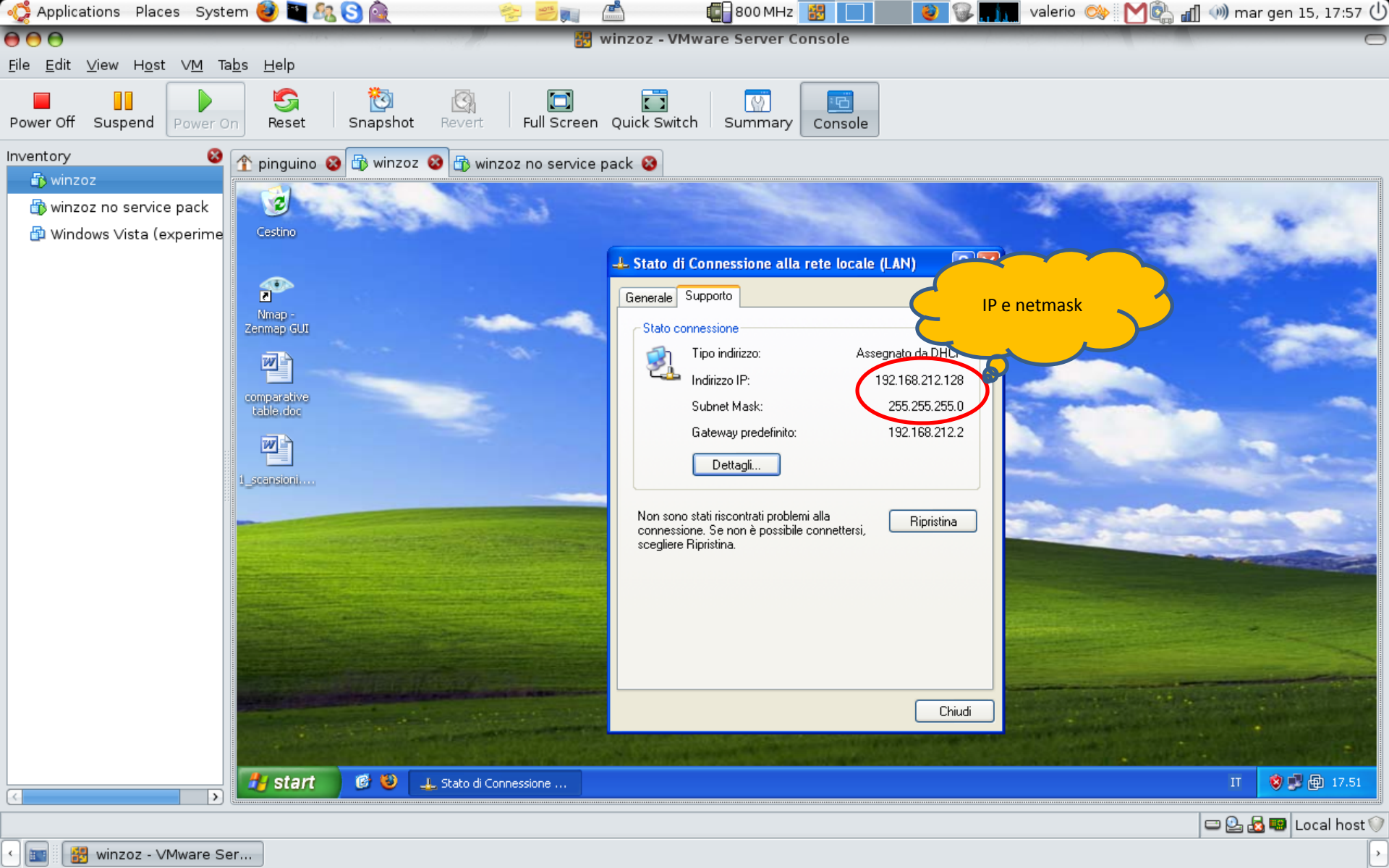
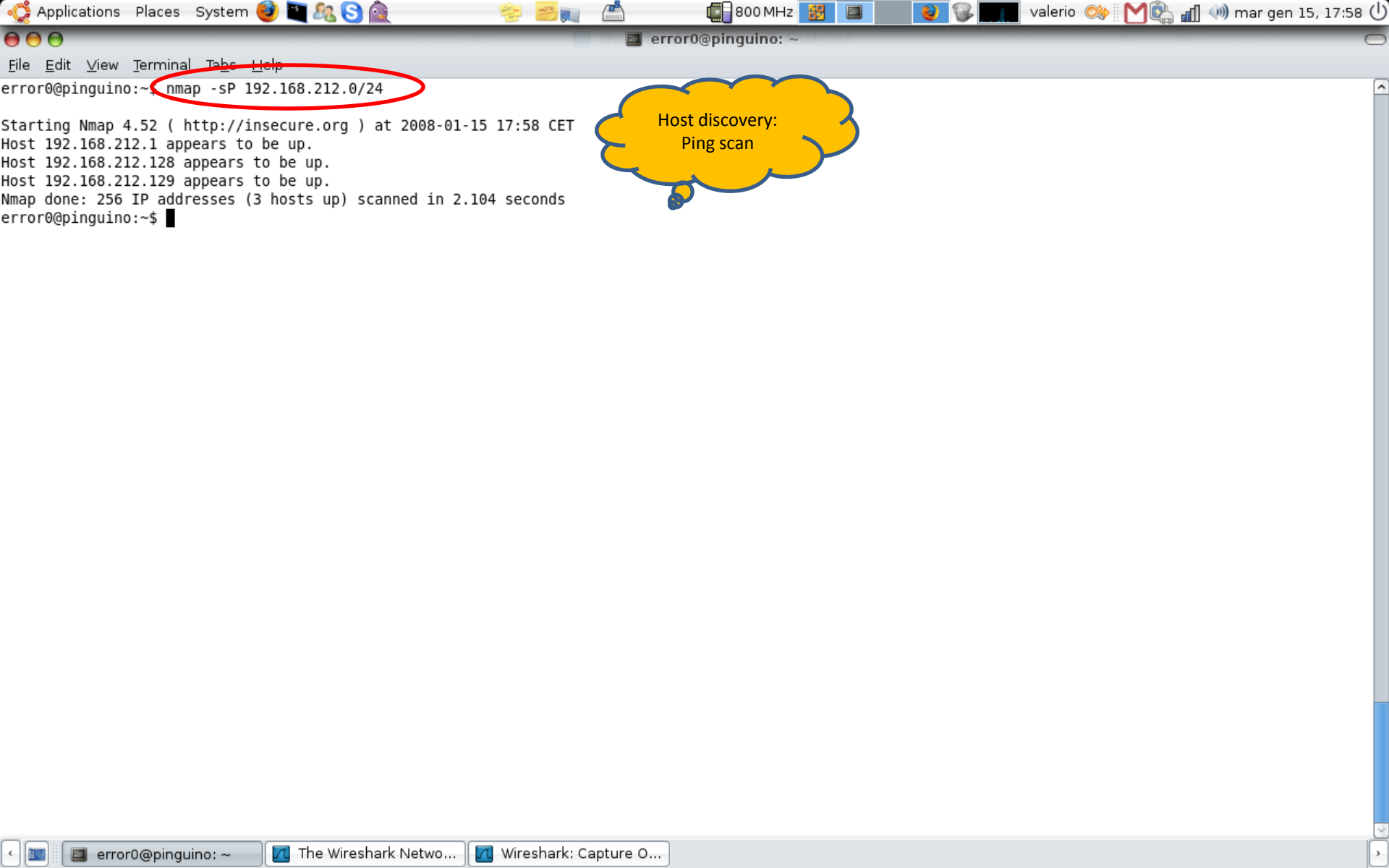
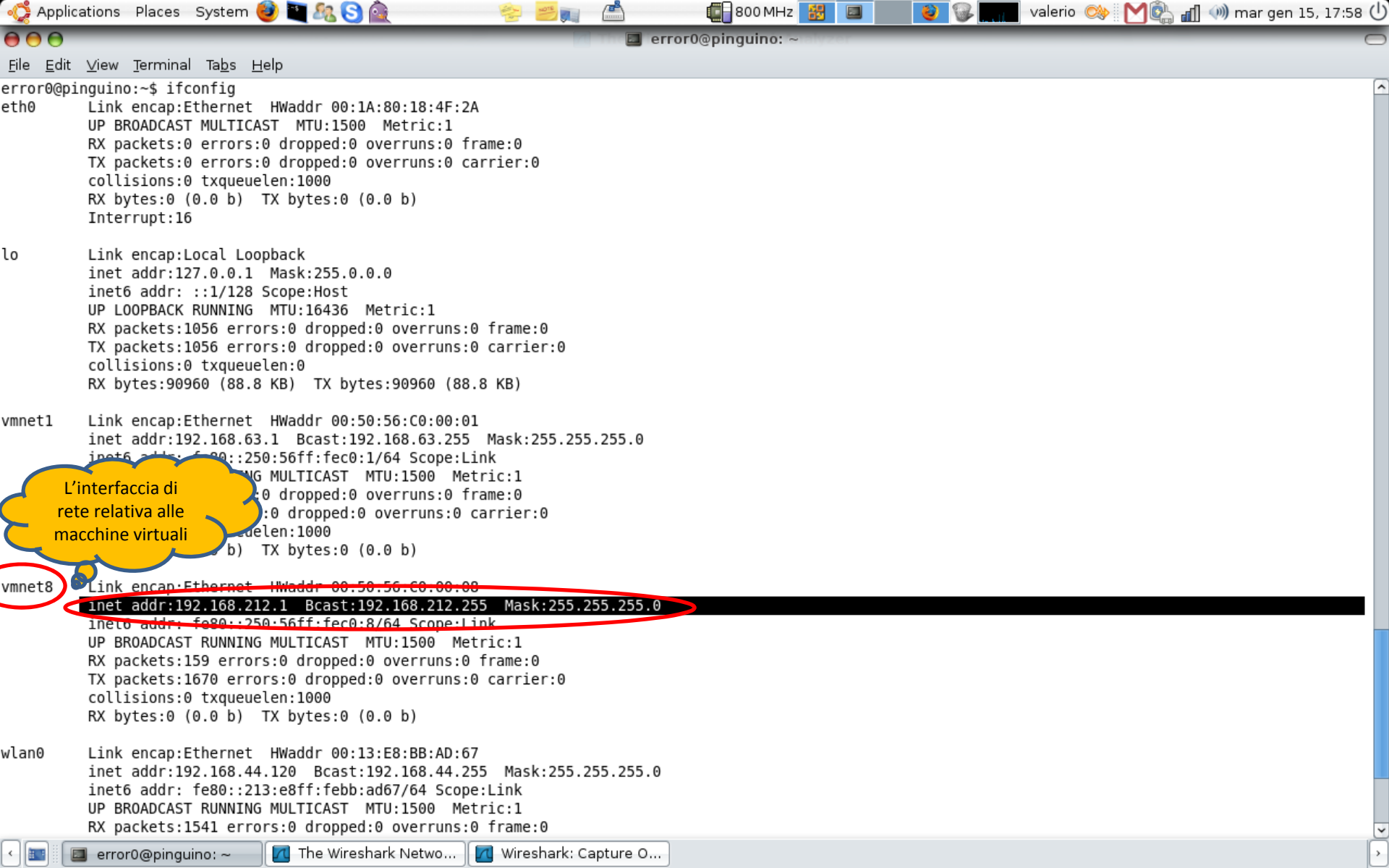
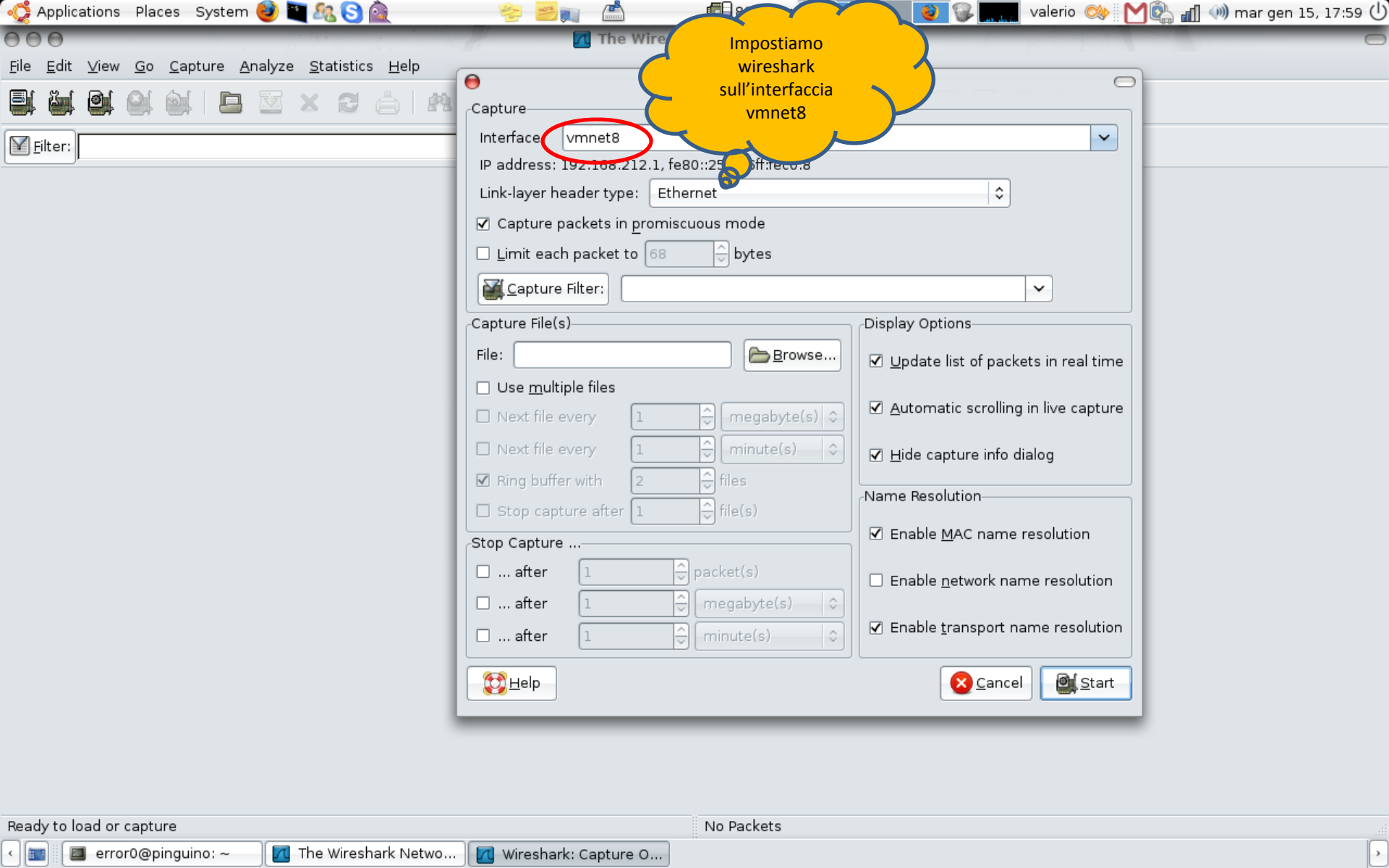
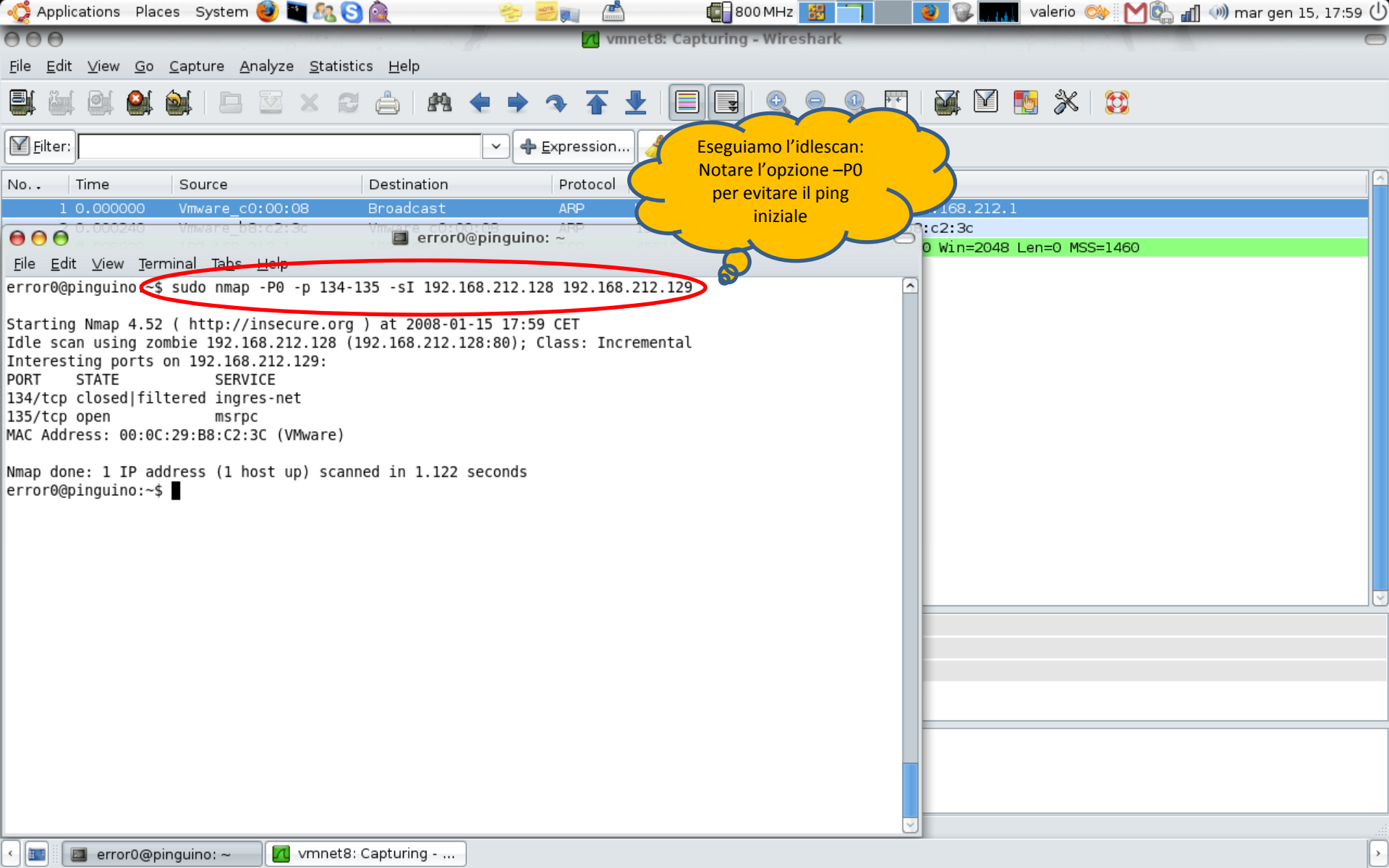

Applications
Places
System
800 MHz
valerio
mar gen 15, 17:57
File
Edit
View
Host
VM
Tabs
Help
Power Off
Suspend
Power On
Reset
Snapshot
Revert
Full Screen
Console
2 macchine virtuali
Inventory
winzoz
winzoz no service pack
Windows Vista (experime
pinguino
winzoz
winzoz no service pack
tool
zlsSetup_61...
angryip
ipscan
netscan
Cestino
start
IT
17.51
Local host
winzoz no service pa...

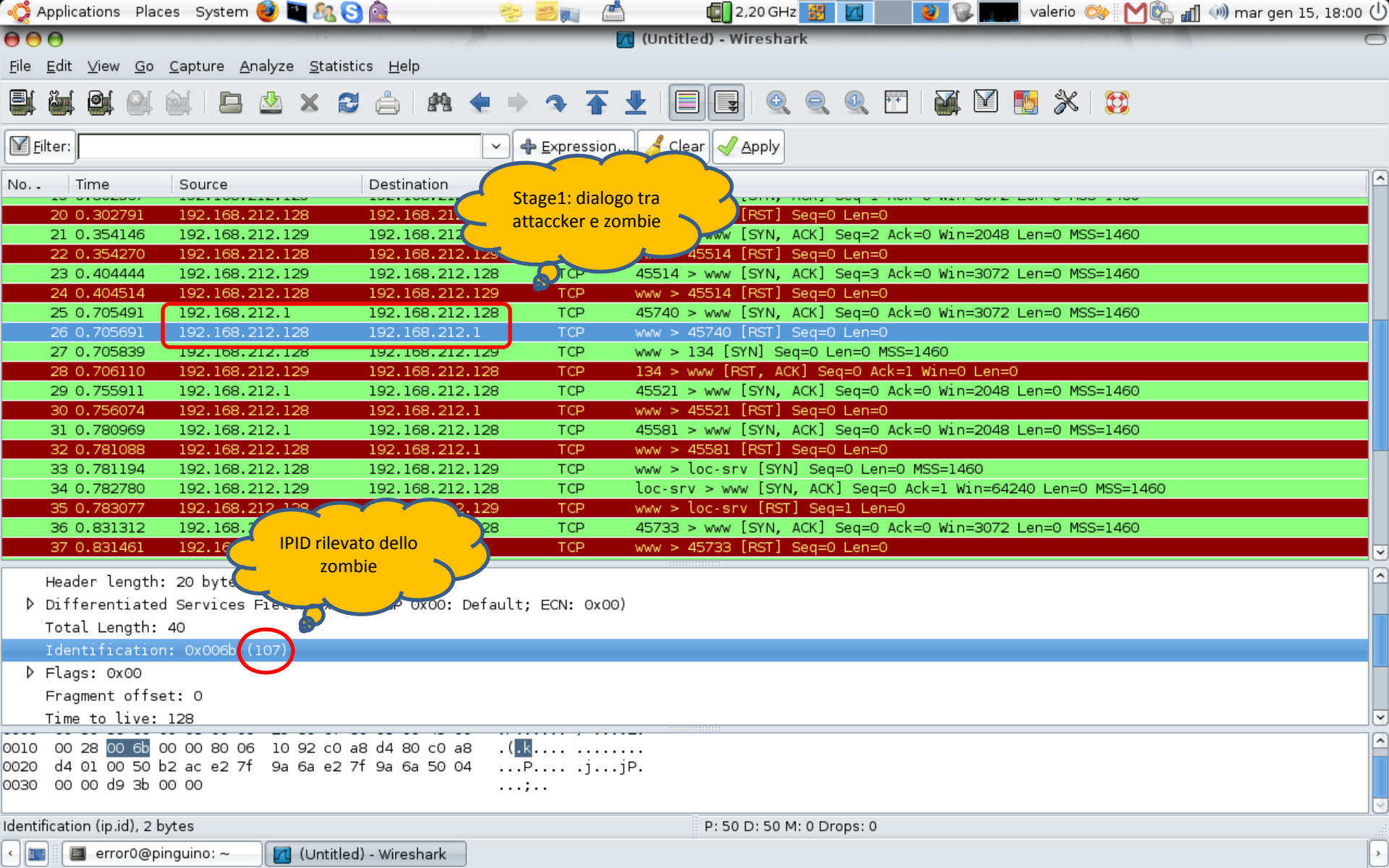

Applications Places System
800 MHz
valerio
mar gen 15, 17:57
winzoz - VMware Server Console
File Edit View Host VM Tabs Help
Power Off
Suspend
Power On
Reset
Snapshot
Revert
Full Screen
Quick Switch
Summary
Console
Inventory
winzoz
winzoz no service pack
Windows Vista (experime
pinguino
winzoz
winzoz no service pack
Cestino
Nmap - Zenmap GUI
comparative table.doc
1_scansioni....
Stato di Connessione alla rete locale (LAN)
Generale
Supporto
Stato connessione
Tipo indirizzo:
Assegnato da DHCP
Indirizzo IP:
192.168.212.128
Subnet Mask:
255.255.255.0
Gateway predefinito:
192.168.212.2
Dettagli...
Non sono stati riscontrati problemi alla connessione. Se non è possibile connettersi, scegliere Ripristina.
Ripristina
Chiudi
IP e netmask
start
Stato di Connessione ...
IT
17.51
Local host
winzoz - VMware Ser...

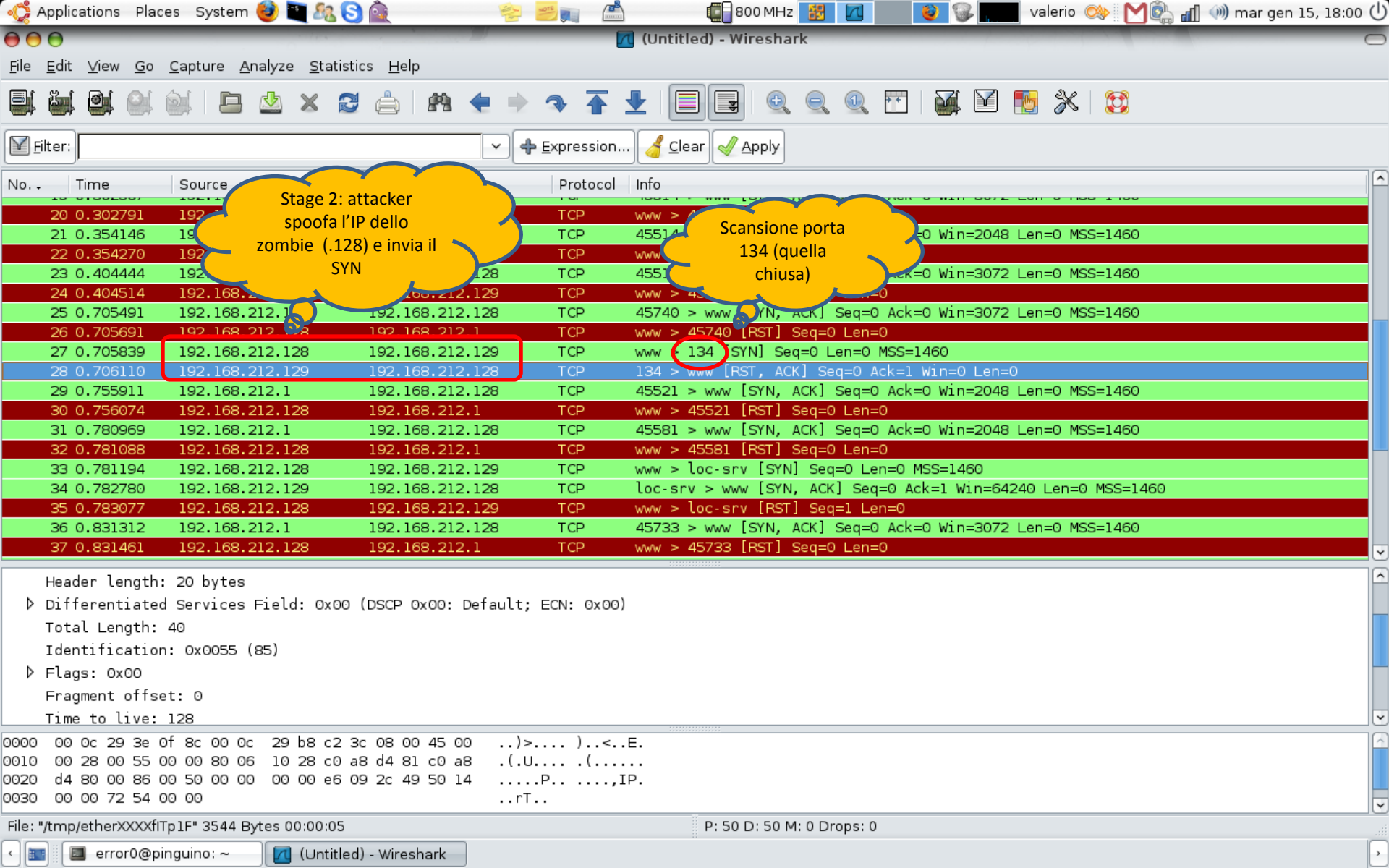

Applications Places System
800 MHz
valerio
mar gen 15, 17:58
error0@pinguino: ~
File Edit View Terminal Tabs Help
error0@pinguino:~$ nmap -sP 192.168.212.0/24
Starting Nmap 4.52 (http://insecure.org) at 2008-01-15 17:58 CET
Host 192.168.212.1 appears to be up.
Host 192.168.212.128 appears to be up.
Host 192.168.212.129 appears to be up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.104 seconds
error0@pinguino:~$
Host discovery:
Ping scan
error0@pinguino: ~
The Wireshark Netwo...
Wireshark: Capture O...

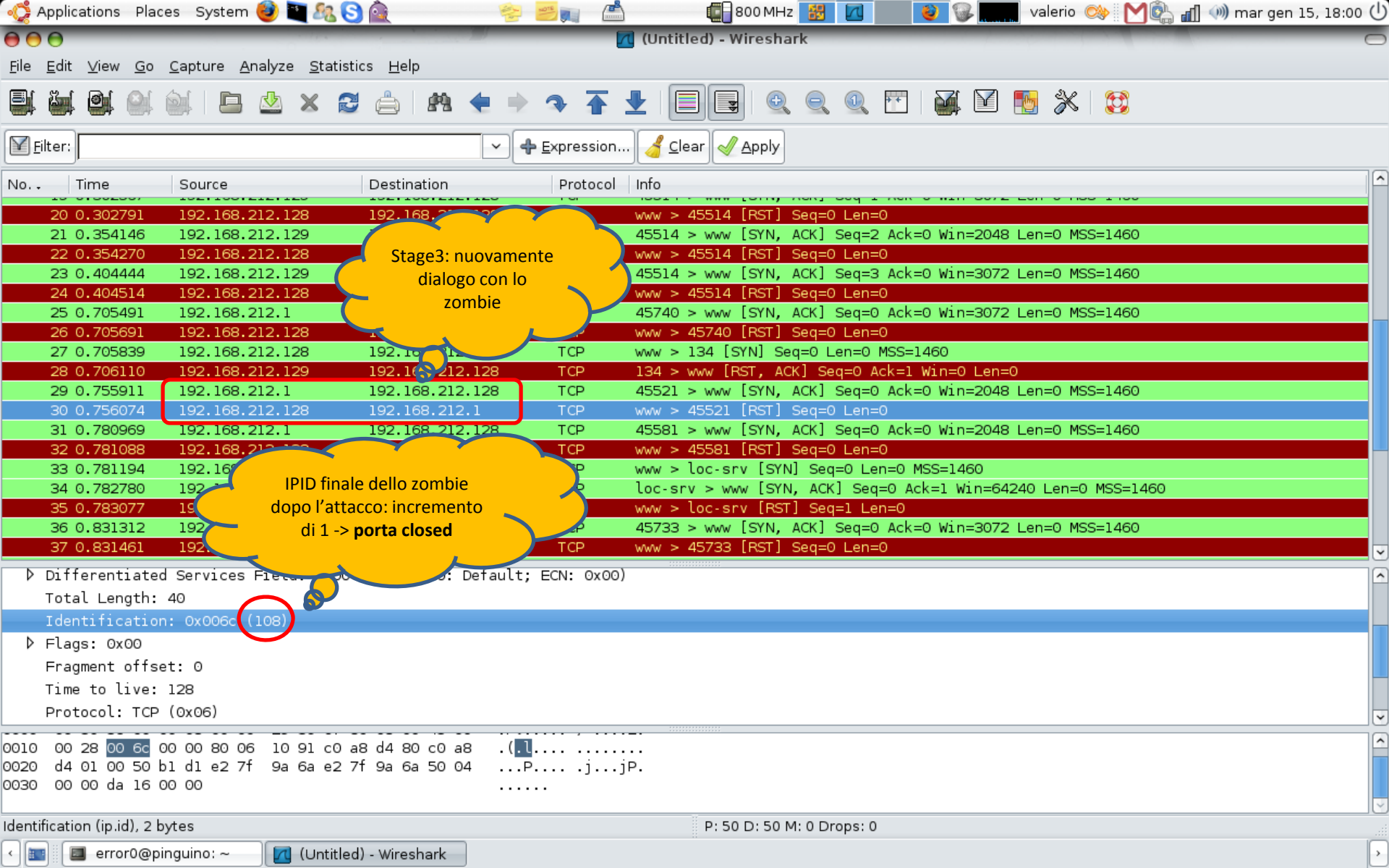

Applications Places System
800 MHz
valerio
mar gen 15, 17:58
error0@pinguino: ~
File Edit View Terminal Tabs Help
error0@pinguino:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:1A:80:18:4F:2A
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:16
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1056 errors:0 dropped:0 overruns:0 frame:0
TX packets:1056 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:90960 (88.8 KB) TX bytes:90960 (88.8 KB)
vmnet1 Link encap:Ethernet HWaddr 00:50:56:C0:00:01
inet addr:192.168.63.1 Bcast:192.168.63.255 Mask:255.255.255.0
L'interfaccia di rete relativa alle macchine virtuali
vmnet8 Link encap:Ethernet HWaddr 00:50:56:C0:00:08
inet addr:192.168.212.1 Bcast:192.168.212.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:159 errors:0 dropped:0 overruns:0 frame:0
TX packets:1670 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
wlan0 Link encap:Ethernet HWaddr 00:13:E8:BB:AD:67
inet addr:192.168.44.120 Bcast:192.168.44.255 Mask:255.255.255.0
inet6 addr: fe80::213:e8ff:febb:ad67/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1541 errors:0 dropped:0 overruns:0 frame:0
error0@pinguino: ~
The Wireshark Netwo...
Wireshark: Capture O...

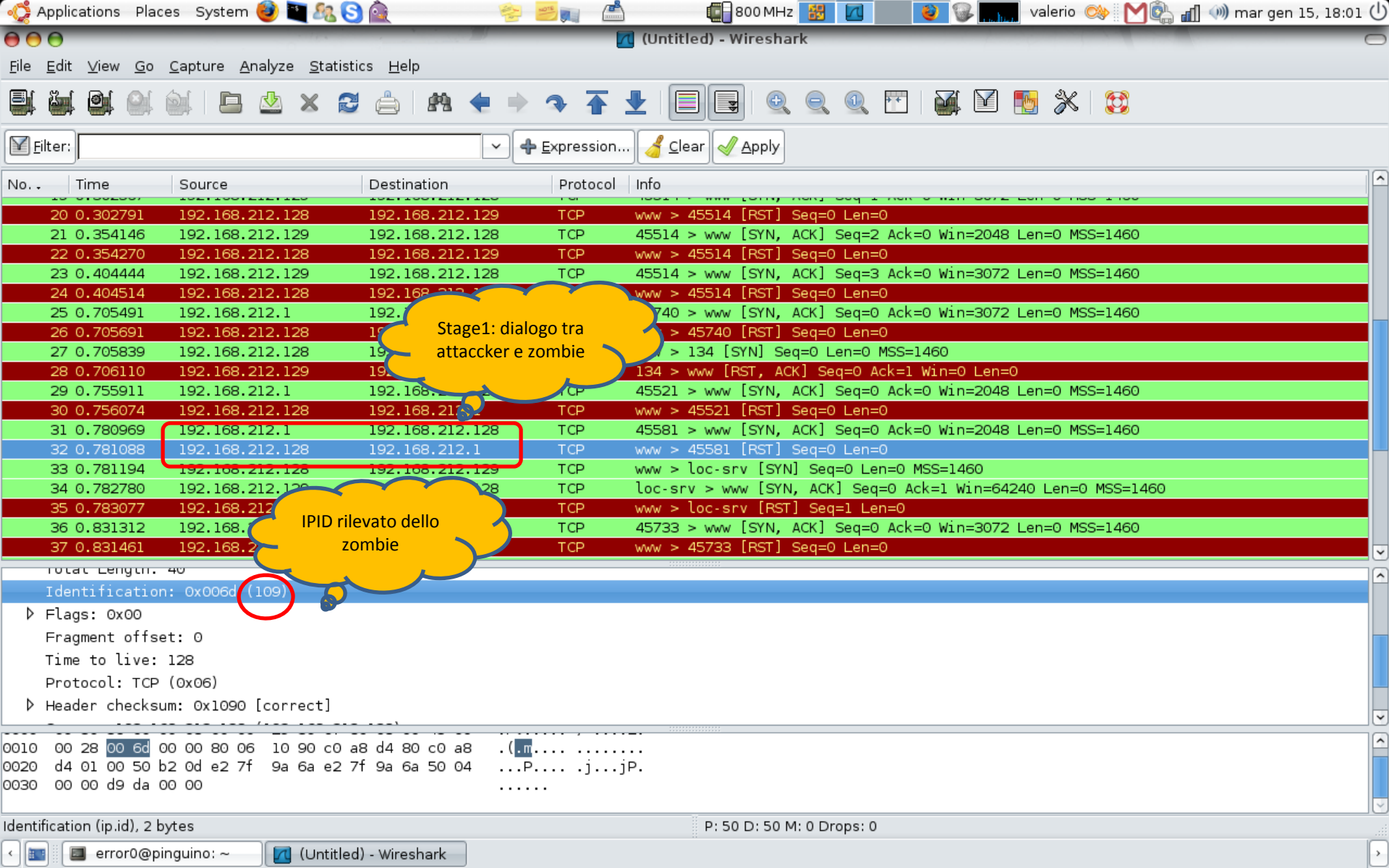

Applications Places System
valerio
mar gen 15, 17:59
File Edit View Go Capture Analyze Statistics Help
Filter:
Impostiamo wireshark sull'interfaccia vmnet8
Capture
Interface: vmnet8
IP address: 192.168.212.1, fe80::25
Link-layer header type: Ethernet
Capture packets in promiscuous mode
Limit each packet to 68 bytes
Capture Filter:
Capture File(s)
File:
Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Help
Cancel
Start
Ready to load or capture
No Packets
error0@pinguino: ~
The Wireshark Netwo...
Wireshark: Capture O...

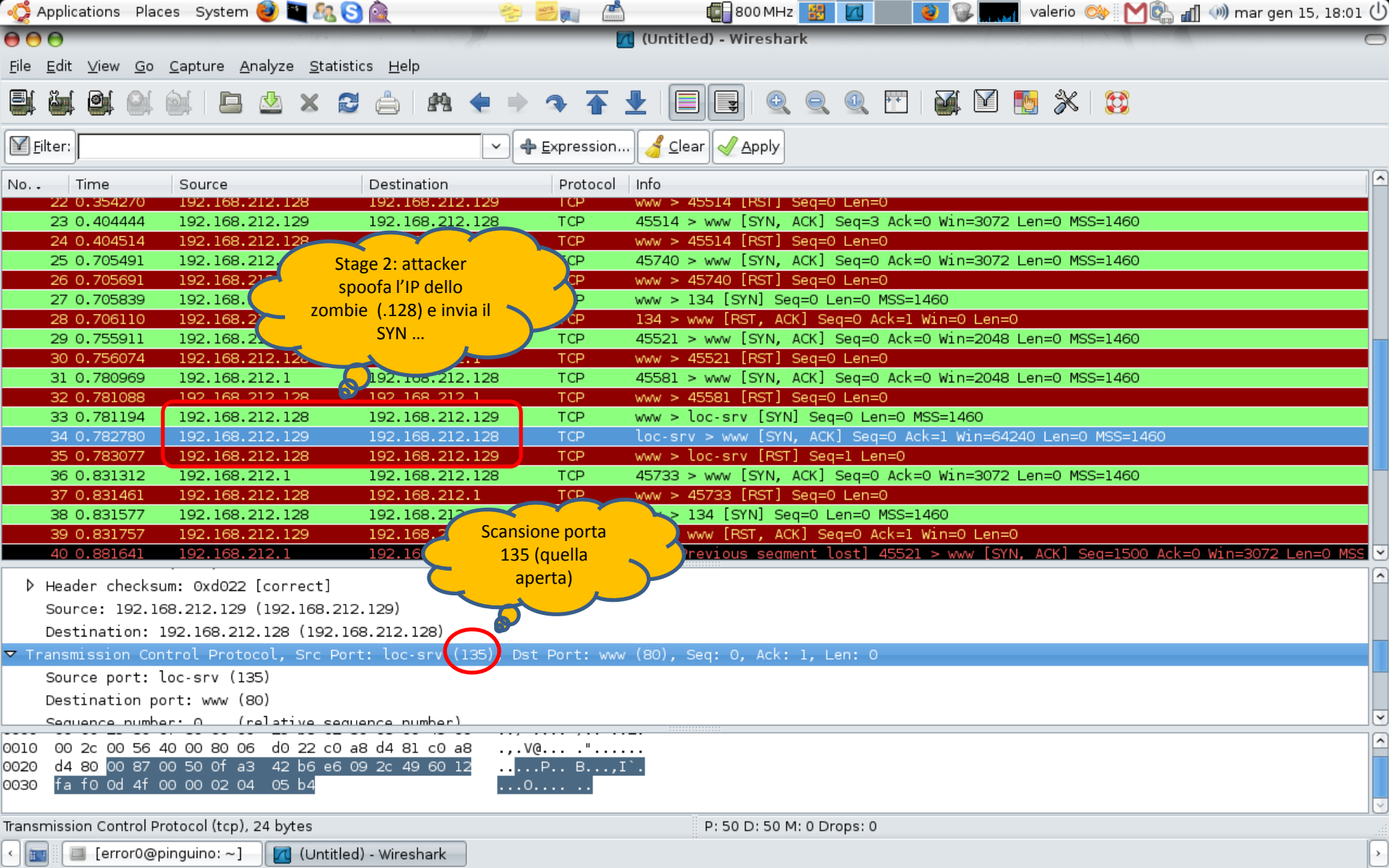

Applications Places System
800 MHz
valerio
mar gen 15, 17:59
vmnet8: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
No. Time Source Destination Protocol
1 0.000000 Vmware_c0:00:08 Broadcast ARP
Eseguiamo l'idlescan: Notare l'opzione –P0 per evitare il ping iniziale
error0@pinguino: ~
File Edit View Terminal Tabs Help
error0@pinguino:~$ sudo nmap -P0 -p 134-135 -sI 192.168.212.128 192.168.212.129
Starting Nmap 4.52 (http://insecure.org) at 2008-01-15 17:59 CET
Idle scan using zombie 192.168.212.128 (192.168.212.128:80); Class: Incremental
Interesting ports on 192.168.212.129:
PORT STATE SERVICE
134/tcp closed|filtered ingres-net
135/tcp open msrpc
MAC Address: 00:0C:29:B8:C2:3C (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.122 seconds
error0@pinguino:~$
error0@pinguino: ~
vmnet8: Capturing - ...

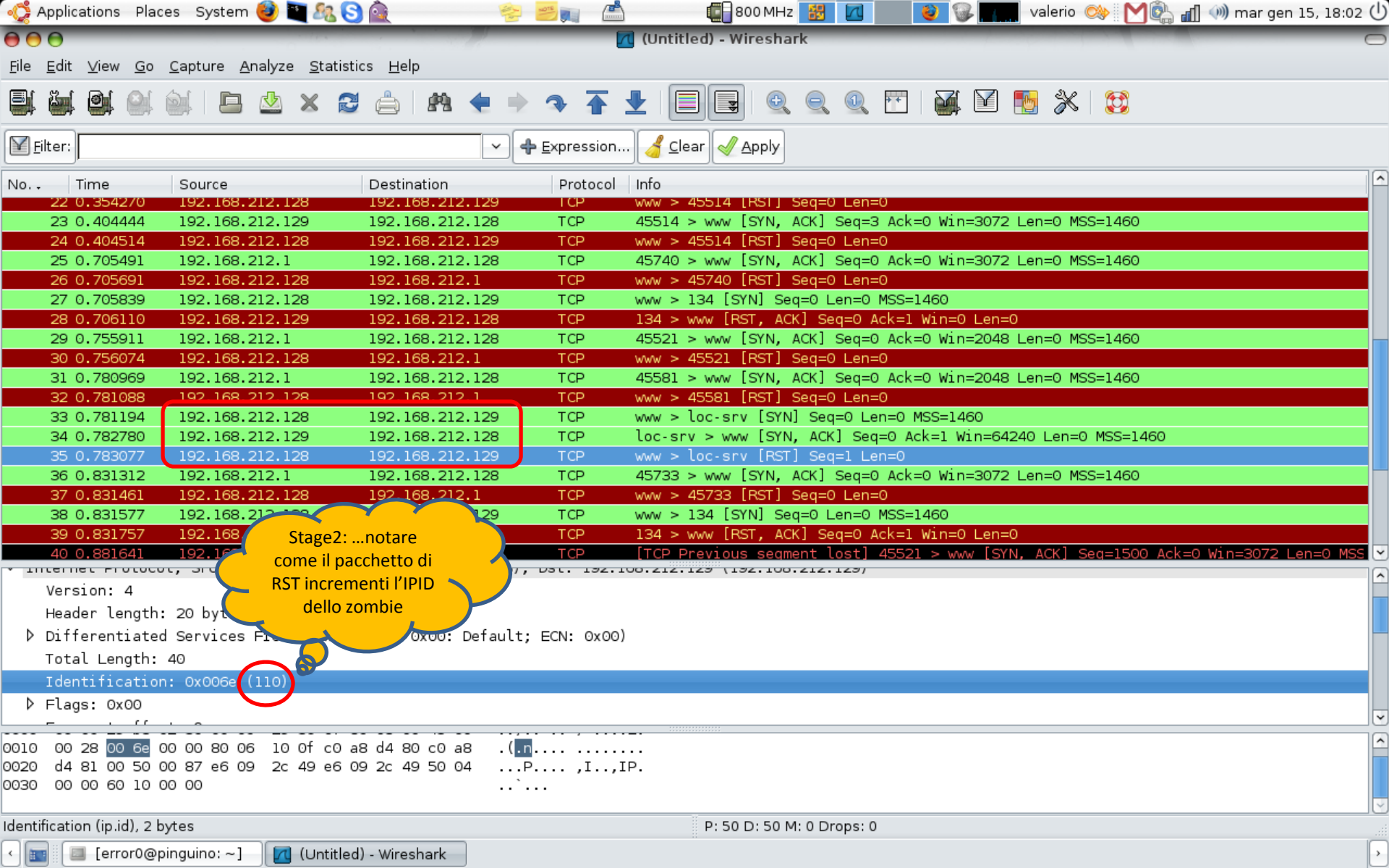

Applications Places System
2,20 GHz
valerio
mar gen 15, 18:00
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination
20 0.302791 192.168.212.128 192.168.21 [RST] Seq=0 Len=0
21 0.354146 192.168.212.129 192.168.212 www [SYN, ACK] Seq=2 Ack=0 Win=2048 Len=0 MSS=1460
22 0.354270 192.168.212.128 192.168.212.129 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212.1 192.168.212.128 TCP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.212.128 192.168.212.1 TCP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 192.168.212.128 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 192.168.212.128 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 192.168.212.1 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 192.168.212.128 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192.168.212.1 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168.212.129 TCP www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212.128 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212 .129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168. 28 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.16 TCP www > 45733 [RST] Seq=0 Len=0
Stage1: dialogo tra attaccker e zombie
IPID rilevato dello zombie
Header length: 20 byte
Differentiated Services Fiel 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x006b (107)
Flags: 0x00
Fragment offset: 0
Time to live: 128
0010 00 28 00 6b 00 00 80 06 10 92 c0 a8 d4 80 c0 a8 .(.k.... ....
0020 d4 01 00 50 b2 ac e2 7f 9a 6a e2 7f 9a 6a 50 04 ...P.... .j...jP.
0030 00 00 d9 3b 00 00 ...;..
Identification (ip.id), 2 bytes
P: 50 D: 50 M: 0 Drops: 0
error0@pinguino: ~
(Untitled) - Wireshark

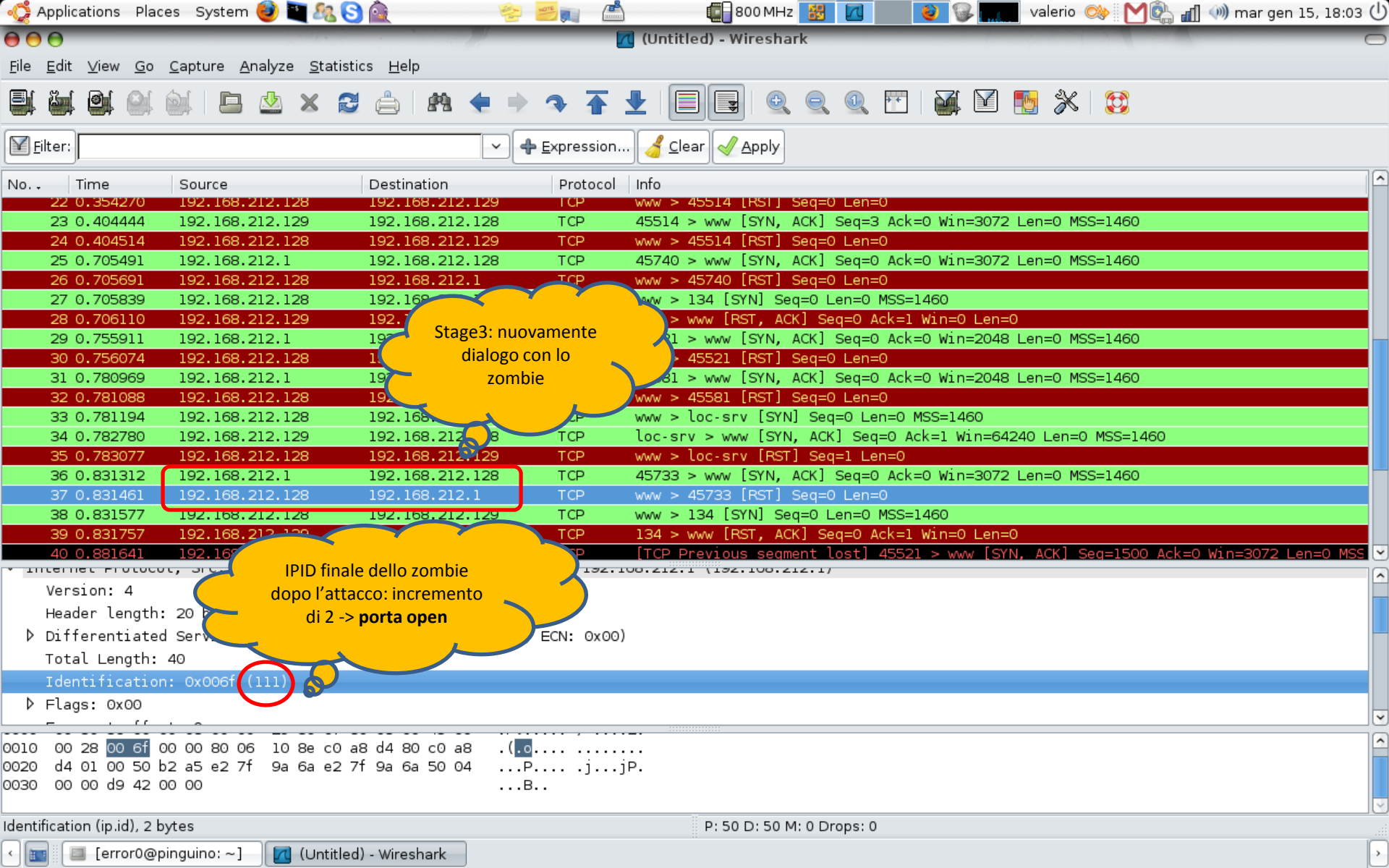

Applications Places System
800 MHz
valerio
mar gen 15, 18:00
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
20 0.302791 TCP www >
21 0.354146 TCP 45514 =0 Win=2048 Len=0 MSS=1460
22 0.354270 TCP www
23 0.404444 TCP 4551 =0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168. .212.129 TCP www > 45 =0
25 0.705491 192.168.212.1 192.168.212.128 TCP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 TCP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 192.168.212.128 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 192.168.212.128 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 192.168.212.1 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 192.168.212.128 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192.168.212.1 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168.212.129 TCP www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212.128 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212.128 192.168.212.129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168.212.1 192.168.212.128 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.168.212.128 192.168.212.1 TCP www > 45733 [RST] Seq=0 Len=0
Stage 2: attacker spoofa l'IP dello zombie (.128) e invia il SYN
Scansione porta 134 (quella chiusa)
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x0055 (85)
Flags: 0x00
Fragment offset: 0
Time to live: 128
0000 00 0c 29 3e 0f 8c 00 0c 29 b8 c2 3c 08 00 45 00 ..)>....)..<..E.
0010 00 28 00 55 00 00 80 06 10 28 c0 a8 d4 81 c0 a8 .(.U.... .(......
0020 d4 80 00 86 00 50 00 00 00 00 e6 09 2c 49 50 14 .....P.. ....,IP.
0030 00 00 72 54 00 00 ..rT..
File: "/tmp/etherXXXXflTp1F" 3544 Bytes 00:00:05
P: 50 D: 50 M: 0 Drops: 0
error0@pinguino: ~
(Untitled) - Wireshark


Applications Places System
800 MHz
valerio
mar gen 15, 18:00
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
20 0.302791 192.168.212.128 www > 45514 [RST] Seq=0 Len=0
21 0.354146 192.168.212.129 45514 > www [SYN, ACK] Seq=2 Ack=0 Win=2048 Len=0 MSS=1460
22 0.354270 192.168.212.128 www > 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212.1 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.212.128 www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 192.168.212.128 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 192.168.212.1 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 www > loc-srv [RST] Seq=1 Len=0
36 0.831312 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 TCP www > 45733 [RST] Seq=0 Len=0
Stage3: nuovamente dialogo con lo zombie
IPID finale dello zombie dopo l'attacco: incremento di 1 -> porta closed
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x006c (108)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
0010 00 28 00 6c 00 00 80 06 10 91 c0 a8 d4 80 c0 a8 .(.l.... ....
0020 d4 01 00 50 b1 d1 e2 7f 9a 6a e2 7f 9a 6a 50 04 ...P.... .j...jP.
0030 00 00 da 16 00 00 ......
Identification (ip.id), 2 bytes
P: 50 D: 50 M: 0 Drops: 0
error0@pinguino: ~
(Untitled) - Wireshark


Applications Places System
800 MHz
valerio
mar gen 15, 18:01
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
20 0.302791 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
21 0.354146 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=2 Ack=0 Win=2048 Len=0 MSS=1460
22 0.354270 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212.1 192.168.212.128 TCP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.212.128 192.168.212.129 TCP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 192.168.212.128 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 192.168.212.128 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 192.168.212.129 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 192.168.212.128 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192.168.212.1 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168.212.129 TCP www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212.128 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212.128 192.168.212.129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168.212.1 192.168.212.128 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.168.212.128 192.168.212.129 TCP www > 45733 [RST] Seq=0 Len=0
Stage1: dialogo tra attaccker e zombie
IPID rilevato dello zombie
Identification: 0x006d (109)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x1090 [correct]
0010 00 28 00 6d 00 00 80 06 10 90 c0 a8 d4 80 c0 a8 .(.m.... ....
0020 d4 01 00 50 b2 0d e2 7f 9a 6a e2 7f 9a 6a 50 04 ...P.... .j...jP.
0030 00 00 d9 da 00 00 ......
Identification (ip.id), 2 bytes
P: 50 D: 50 M: 0 Drops: 0
error0@pinguino: ~
(Untitled) - Wireshark


Applications Places System
800 MHz
valerio
mar gen 15, 18:01
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
22 0.354270 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 TCP www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212. CP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.21 CP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168. P www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.2 CP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.2 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.12 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 192.168.212.128 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192.168.212.1 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168.212.129 TCP www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212.128 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212.128 192.168.212.129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168.212.1 192.168.212.128 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.168.212.128 192.168.212.1 TCP www > 45733 [RST] Seq=0 Len=0
38 0.831577 192.168.212.128 192.168.212. > 134 [SYN] Seq=0 Len=0 MSS=1460
39 0.831757 192.168.212.129 192.168.2 www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
40 0.881641 192.168.212.1 192.16 revious segment lost] 45521 > www [SYN, ACK] Seq=1500 Ack=0 Win=3072 Len=0 MSS
Stage 2: attacker spoofa l'IP dello zombie (.128) e invia il SYN ...
Scansione porta 135 (quella aperta)
Header checksum: 0xd022 [correct]
Source: 192.168.212.129 (192.168.212.129)
Destination: 192.168.212.128 (192.168.212.128)
Transmission Control Protocol, Src Port: loc-srv (135), Dst Port: www (80), Seq: 0, Ack: 1, Len: 0
Source port: loc-srv (135)
Destination port: www (80)
Sequence number: 0 (relative sequence number)
0010 00 2c 00 56 40 00 80 06 d0 22 c0 a8 d4 81 c0 a8 .,.V@... ."......
0020 d4 80 00 87 00 50 0f a3 42 b6 e6 09 2c 49 60 12 .....P.. B...,I`.
0030 fa f0 0d 4f 00 00 02 04 05 b4 ...O.... ..
Transmission Control Protocol (tcp), 24 bytes
P: 50 D: 50 M: 0 Drops: 0
[error0@pinguino: ~]
(Untitled) - Wireshark


Applications Places System
800 MHz
valerio
mar gen 15, 18:02
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
22 0.354270 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212.1 192.168.212.128 TCP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.212.128 192.168.212.1 TCP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 192.168.212.128 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 192.168.212.128 TCP 45521 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 192.168.212.1 TCP www > 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 192.168.212.128 TCP 45581 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192.168.212.1 TCP www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168.212.129 TCP www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212.128 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212.128 192.168.212.129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168.212.1 192.168.212.128 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.168.212.128 192.168.212.1 TCP www > 45733 [RST] Seq=0 Len=0
38 0.831577 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
39 0.831757 192.168.212.129 192.168.212.128 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
40 0.881641 192.168.212.128 192.168.212.129 TCP [TCP Previous segment lost] 45521 > www [SYN, ACK] Seq=1500 Ack=0 Win=3072 Len=0 MSS
Version: 4
Header length: 20 byt
Differentiated Services Fi 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x006e (110)
Flags: 0x00
0010 00 28 00 6e 00 00 80 06 10 0f c0 a8 d4 80 c0 a8 .(.n.... ....
0020 d4 81 00 50 00 87 e6 09 2c 49 e6 09 2c 49 50 04 ...P.... ,I..,IP.
0030 00 00 60 10 00 00 ..`...
Stage2: ...notare come il pacchetto di RST incrementi l'IPID dello zombie
Identification (ip.id), 2 bytes
P: 50 D: 50 M: 0 Drops: 0
[error0@pinguino: ~]
(Untitled) - Wireshark


Applications Places System
800 MHz
valerio
mar gen 15, 18:03
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
22 0.354270 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
23 0.404444 192.168.212.129 192.168.212.128 TCP 45514 > www [SYN, ACK] Seq=3 Ack=0 Win=3072 Len=0 MSS=1460
24 0.404514 192.168.212.128 192.168.212.129 TCP www > 45514 [RST] Seq=0 Len=0
25 0.705491 192.168.212.1 192.168.212.128 TCP 45740 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
26 0.705691 192.168.212.128 192.168.212.1 TCP www > 45740 [RST] Seq=0 Len=0
27 0.705839 192.168.212.128 192.168 ww > 134 [SYN] Seq=0 Len=0 MSS=1460
28 0.706110 192.168.212.129 192. > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
29 0.755911 192.168.212.1 19 1 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
30 0.756074 192.168.212.128 1 45521 [RST] Seq=0 Len=0
31 0.780969 192.168.212.1 19 81 > www [SYN, ACK] Seq=0 Ack=0 Win=2048 Len=0 MSS=1460
32 0.781088 192.168.212.128 192 www > 45581 [RST] Seq=0 Len=0
33 0.781194 192.168.212.128 192.168 www > loc-srv [SYN] Seq=0 Len=0 MSS=1460
34 0.782780 192.168.212.129 192.168.212 TCP loc-srv > www [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
35 0.783077 192.168.212.128 192.168.212.129 TCP www > loc-srv [RST] Seq=1 Len=0
36 0.831312 192.168.212.1 192.168.212.128 TCP 45733 > www [SYN, ACK] Seq=0 Ack=0 Win=3072 Len=0 MSS=1460
37 0.831461 192.168.212.128 192.168.212.1 TCP www > 45733 [RST] Seq=0 Len=0
38 0.831577 192.168.212.128 192.168.212.129 TCP www > 134 [SYN] Seq=0 Len=0 MSS=1460
39 0.831757 192.168.212 TCP 134 > www [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
40 0.881641 192.16 [TCP Previous segment lost] 45521 > www [SYN, ACK] Seq=1500 Ack=0 Win=3072 Len=0 MSS
Stage3: nuovamente dialogo con lo zombie
Version: 4
Header length: 20
Differentiated Serv ECN: 0x00)
Total Length: 40
Identification: 0x006f (111)
Flags: 0x00
IPID finale dello zombie dopo l'attacco: incremento di 2 -> porta open
0010 00 28 00 6f 00 00 80 06 10 8e c0 a8 d4 80 c0 a8 .(.o.... ....
0020 d4 01 00 50 b2 a5 e2 7f 9a 6a e2 7f 9a 6a 50 04 ...P.... .j...jP.
0030 00 00 d9 42 00 00 ...B..
Identification (ip.id), 2 bytes
P: 50 D: 50 M: 0 Drops: 0
[error0@pinguino: ~]
(Untitled) - Wireshark