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	

1

Dichiarazione di copyright

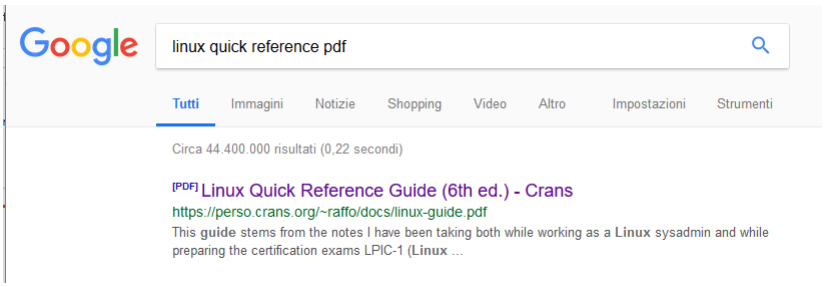
L'utilizzo dei contenuti della lezione sono riservati alla fruizione personale degli studenti iscritti ai corsi dell'Università di Camerino. ***Sono vietate*** *la diffusione intera o parziale di video o immagini della lezione, nonché la modifica dei contenuti senza il consenso, espresso per iscritto, del titolare o dei titolari dei diritti d'autore e di immagine.*

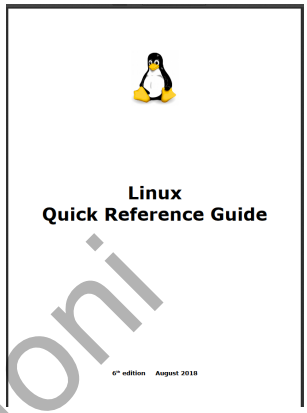
Copyright notice

The contents of this lesson are subject to copyright and intended only for personal use by students enrolled in courses offered by the University of Camerino. For this reason, any partial or total reproduction, adaptation, modification and/or transformation of the contents of this lesson, by any means, without the prior written authorization of the copyright owner, is strictly prohibited.

2

un buon manuale per iniziare



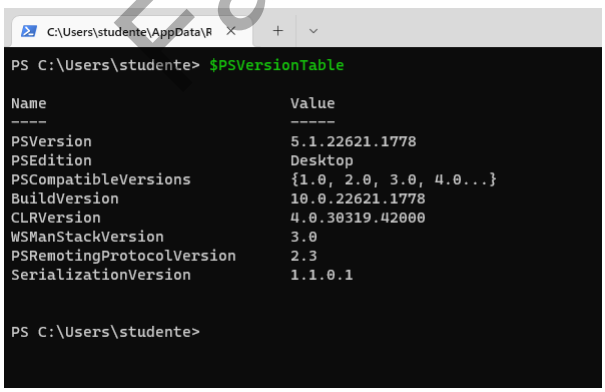


https://dr0.ch/docs/linux-guide-8ed.pdf

3

Che cos'è PowerShell?

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



4

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>
```


5

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.

6

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

7

FINE

Conoscere Linux - male non fa, anzi …

8

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

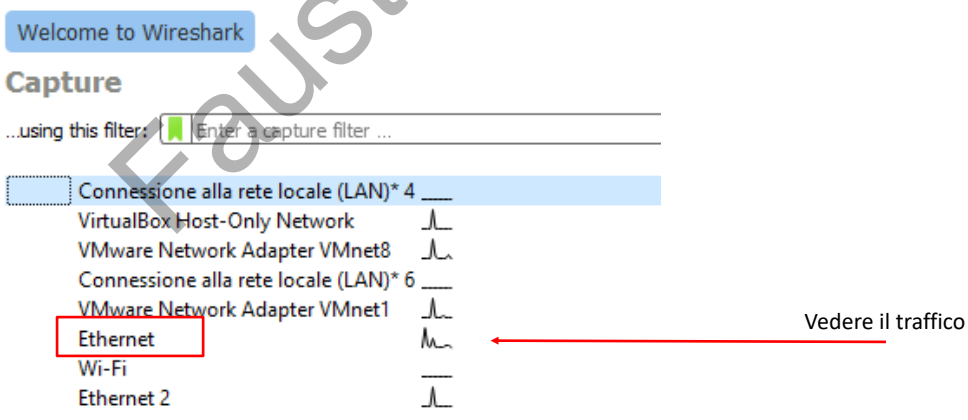
https://www.areanetworking.it/corso-wireshark-prima-lezione.html

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

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

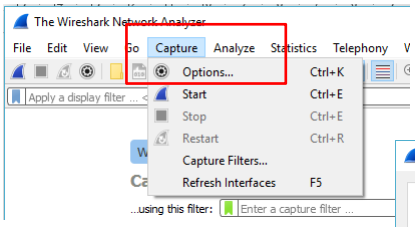
9

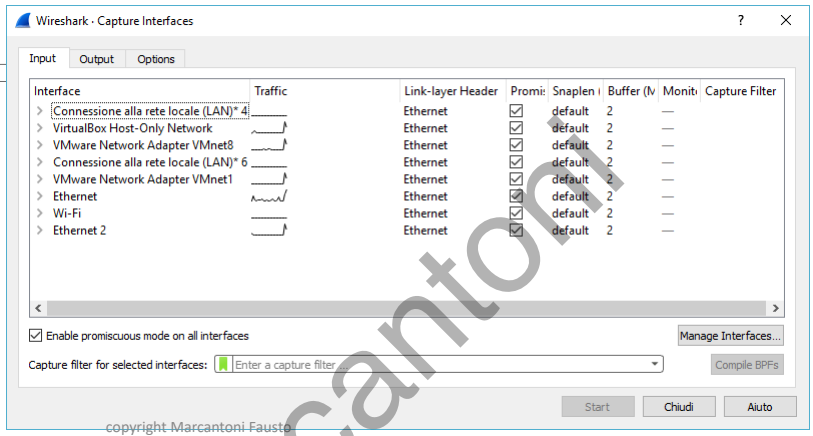
Wireshark – scegliere l'interfaccia



10

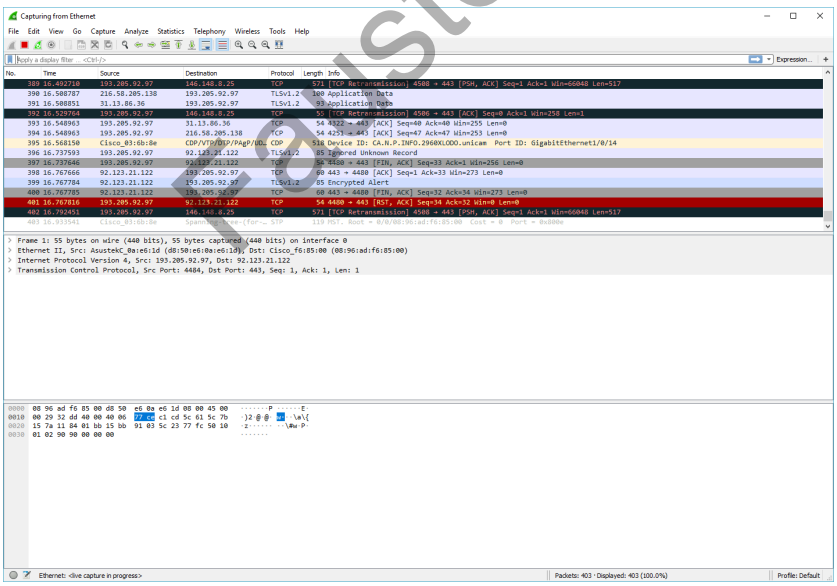
Wireshark – scegliere l'interfaccia





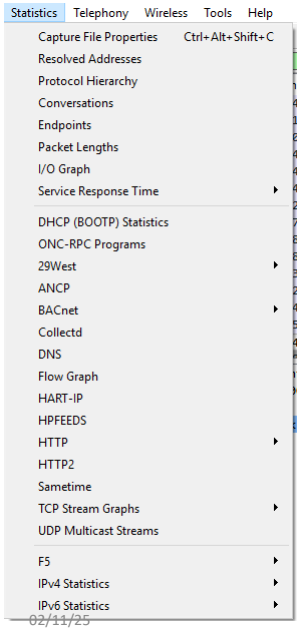
11

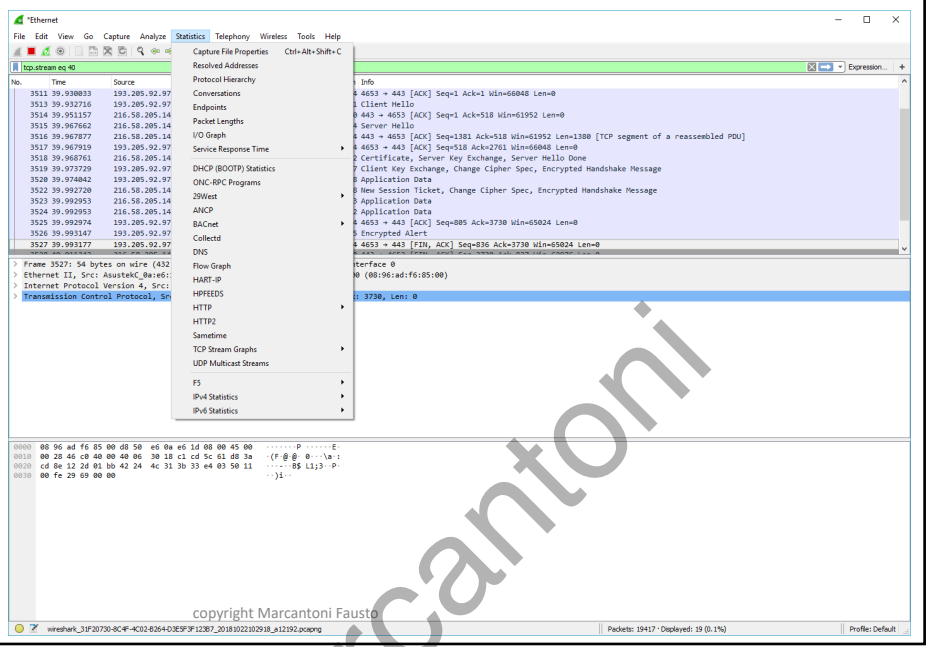
Wireshark – pagina principale



12

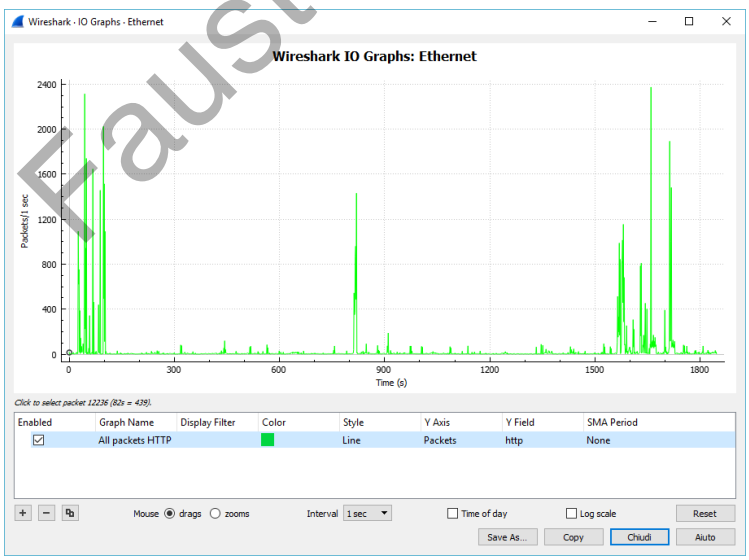
Wireshark – Statistiche





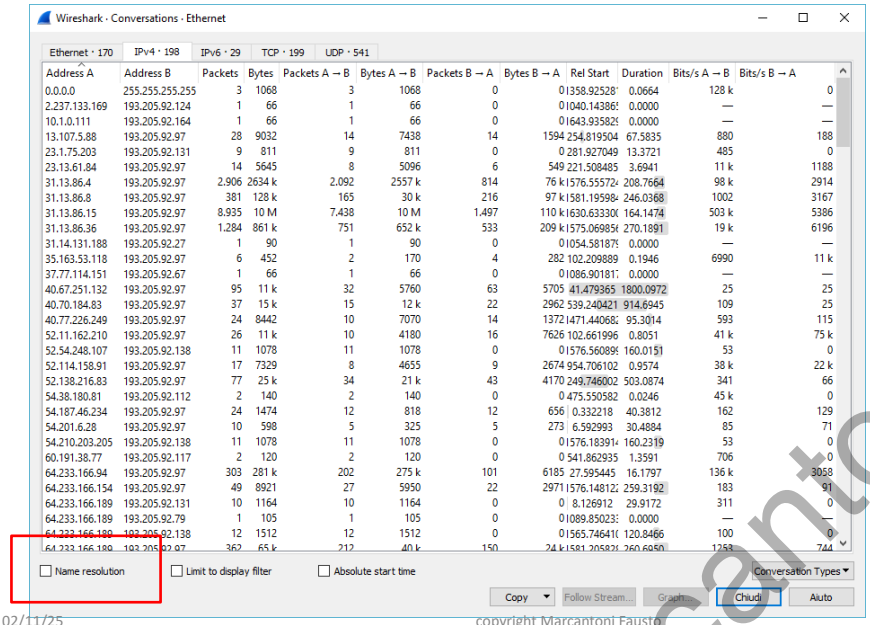
13

Wireshark – Statistiche - I/O Graph



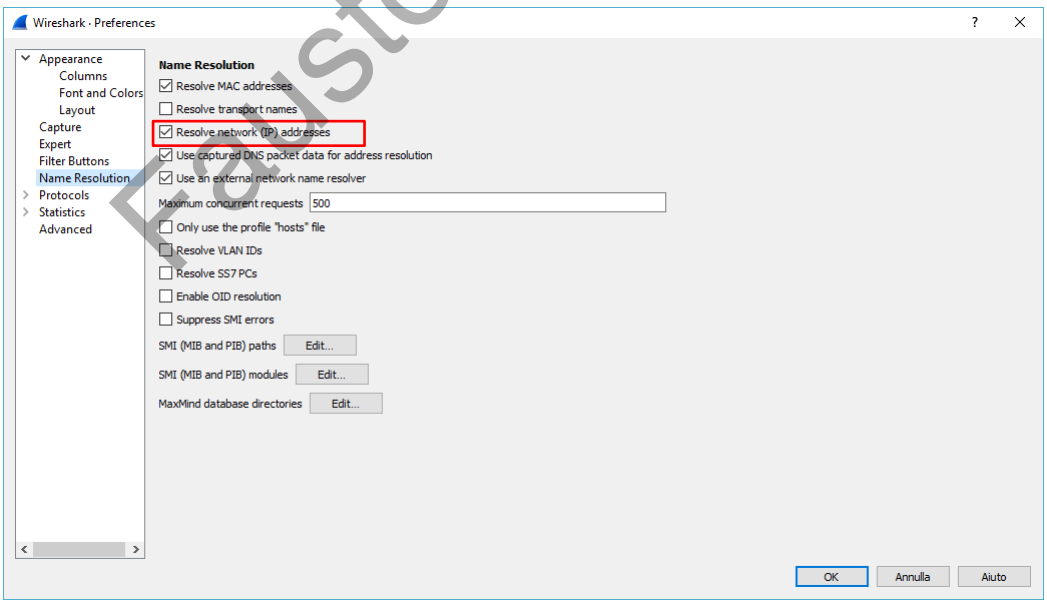
14

Wireshark – Statistiche - Conversation



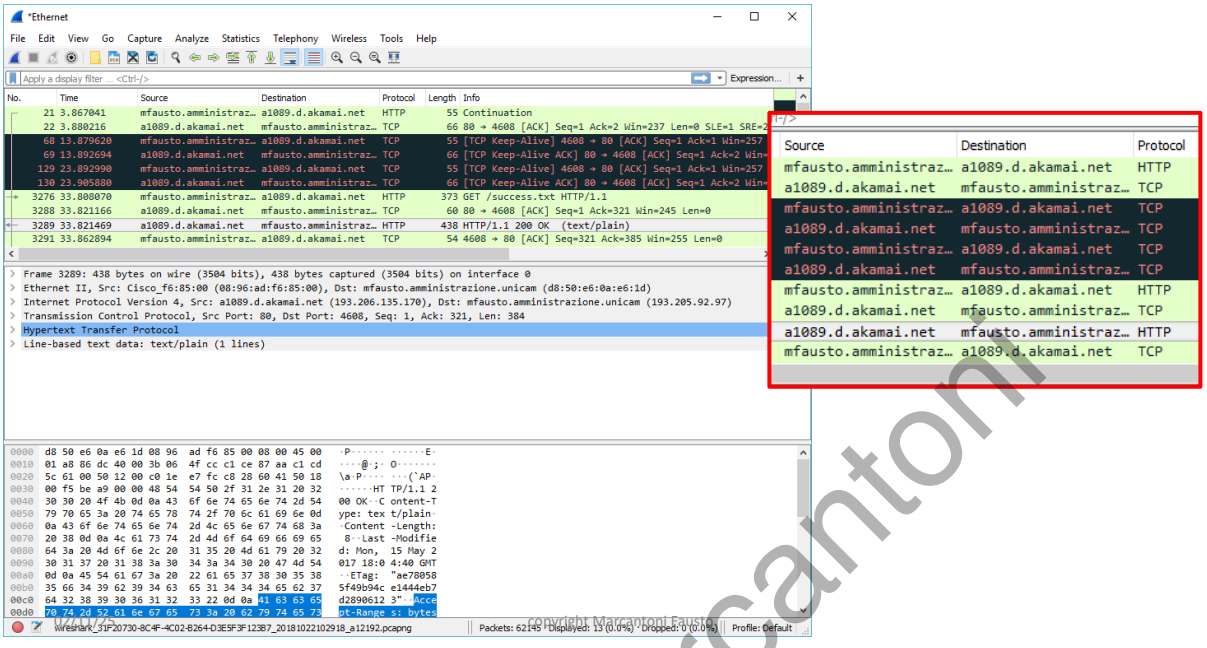
15

Wireshark – Preferences



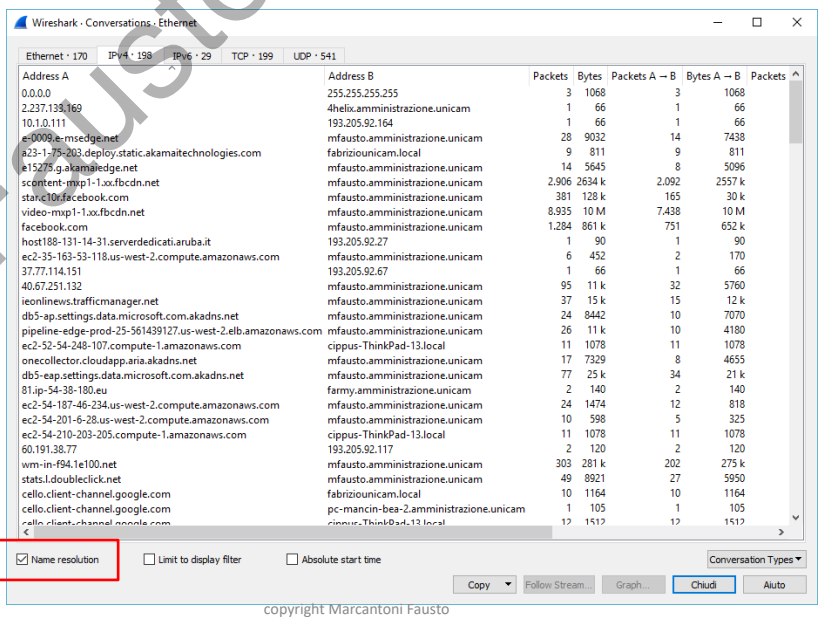
16

Wireshark – Statistiche - Conversation



17

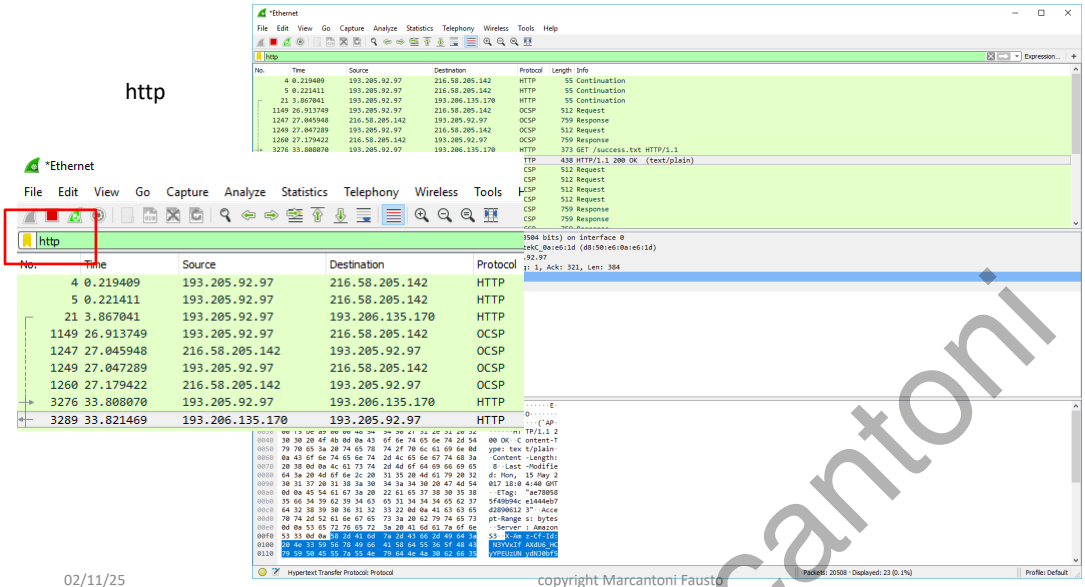
Wireshark – Statistiche - Conversation



18

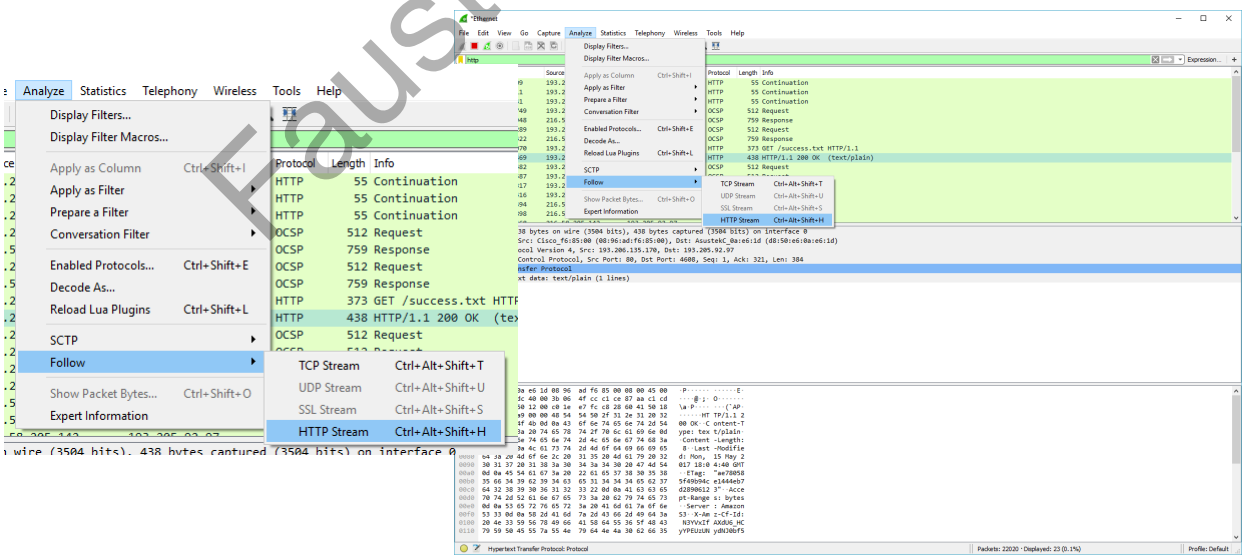
Wireshark – filtro http

http



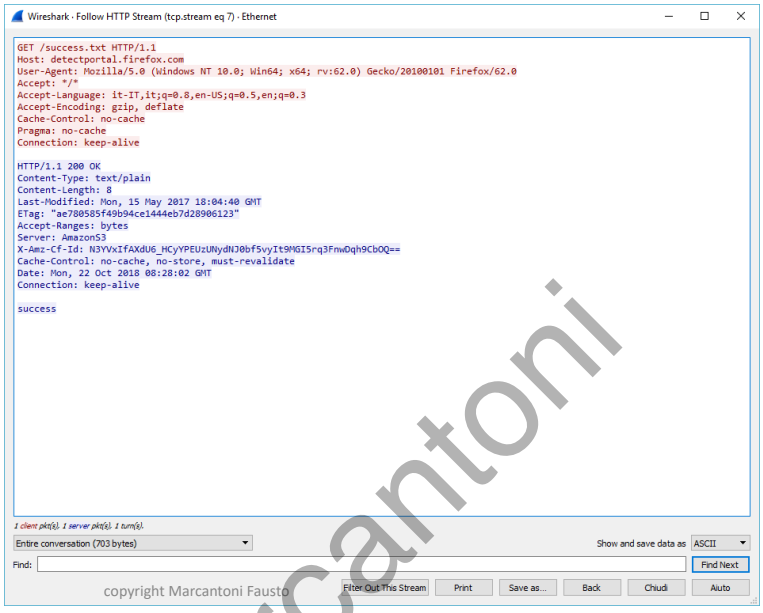
19

Wireshark – Analizza



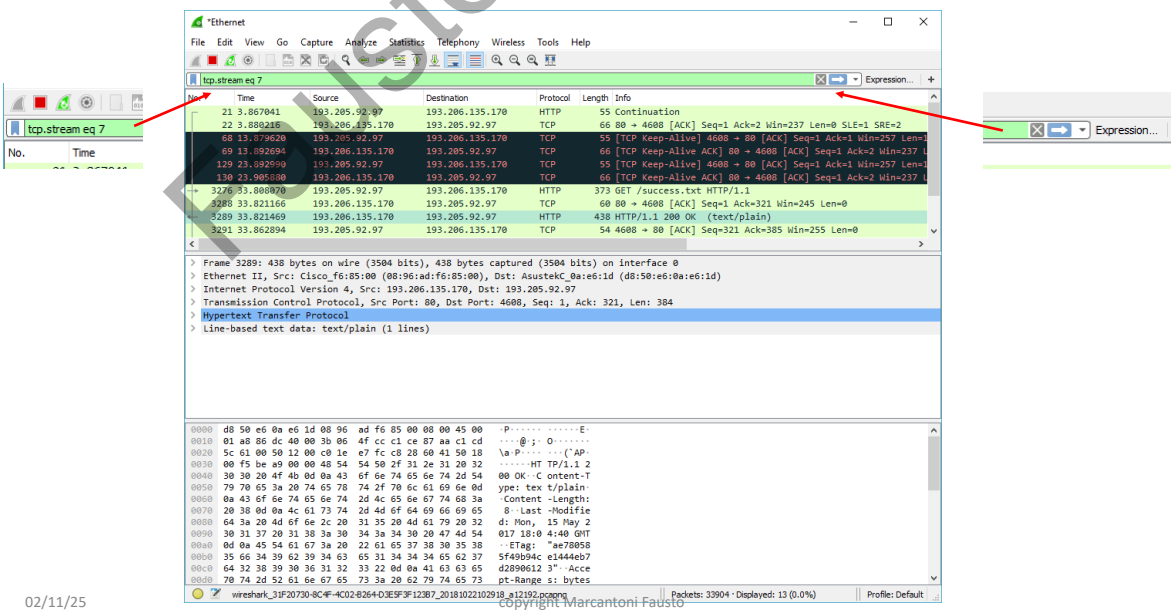
20

Wireshark – Follow HTTP Stream



21

Wireshark – rimuovere filtri

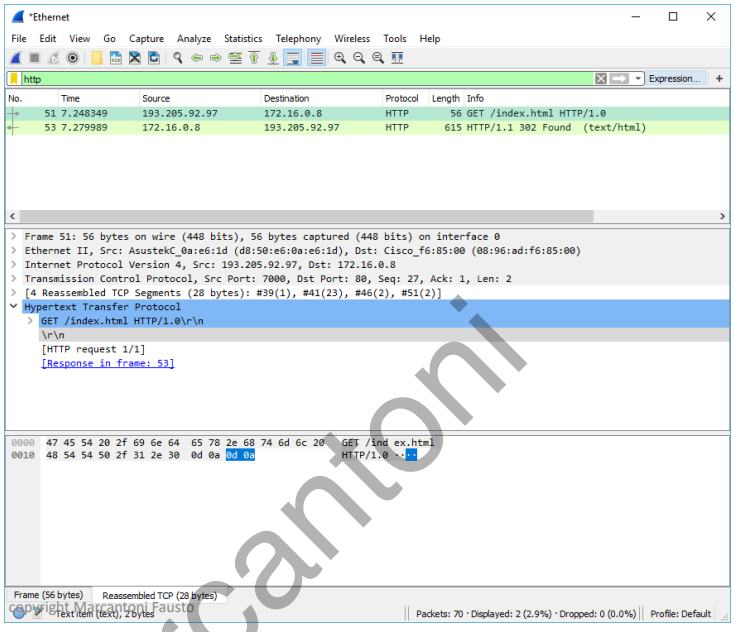


22

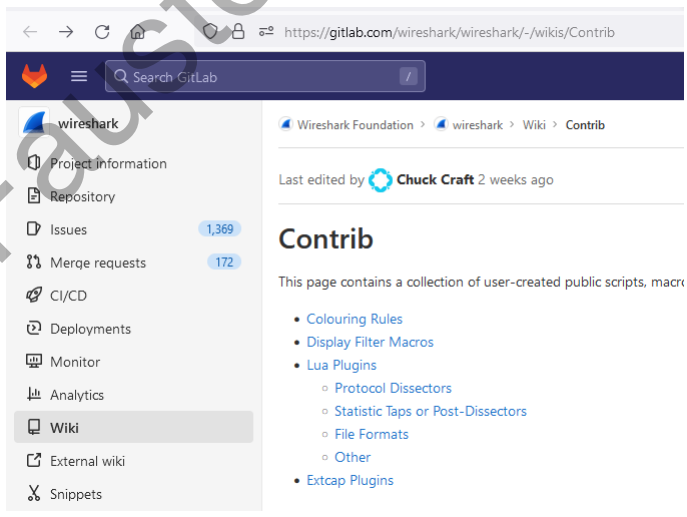
Wireshark – esercitazione individuale

```
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



Wireshark contrib



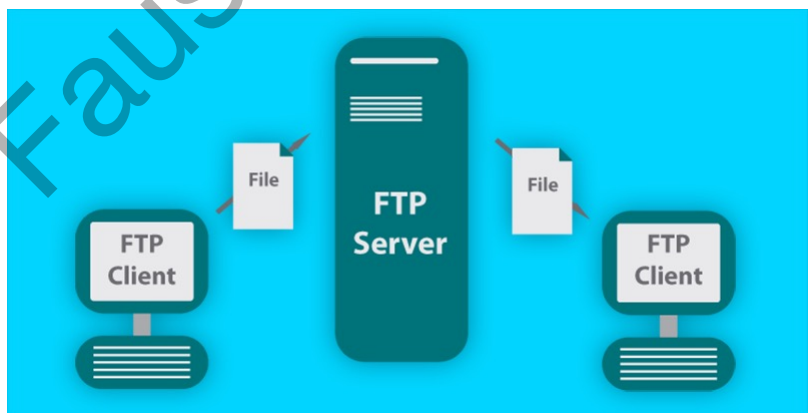
https://gitlab.com/wireshark/wireshark/-/wikis/Contrib

FINE

WIRESHARK

25

FTP

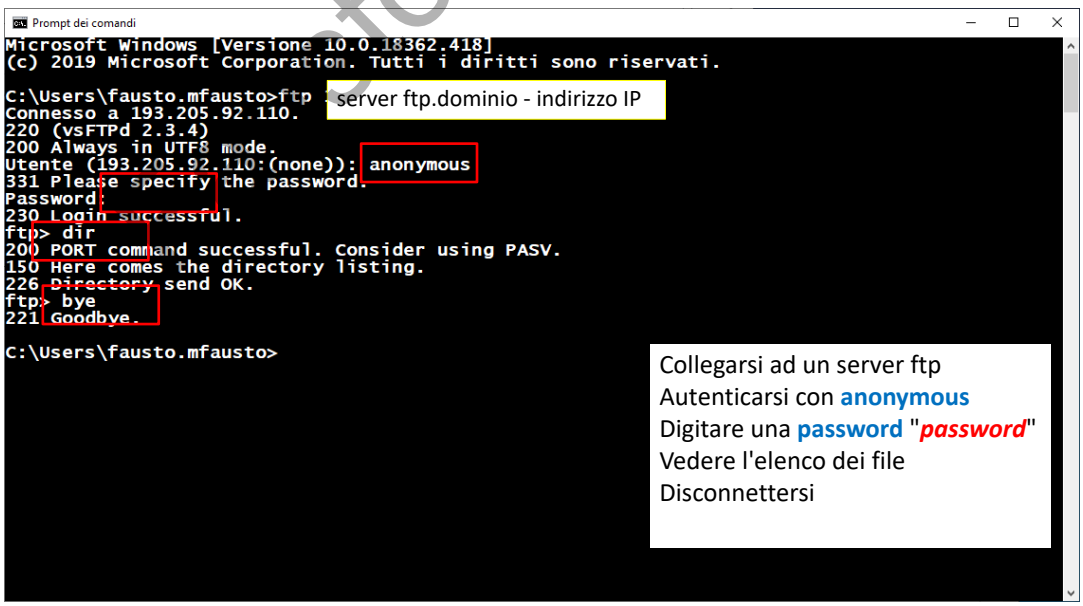


26

Connessione server ftp

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

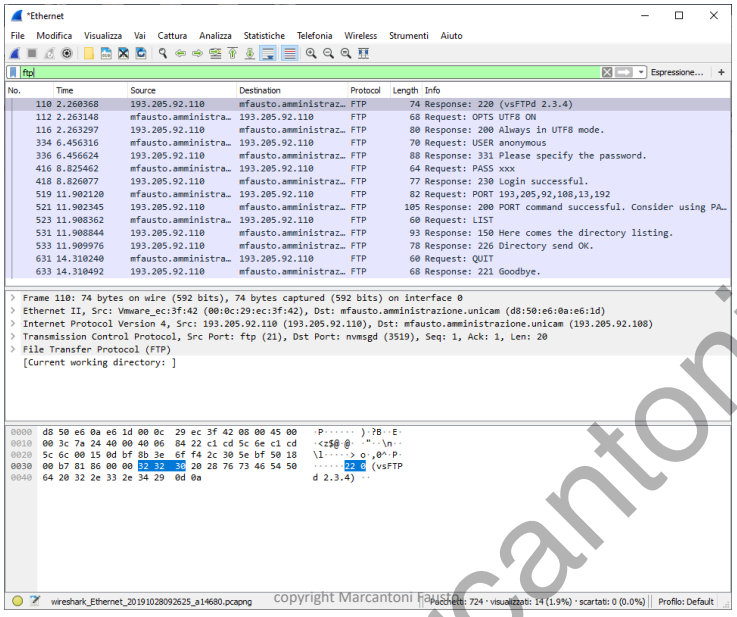
27



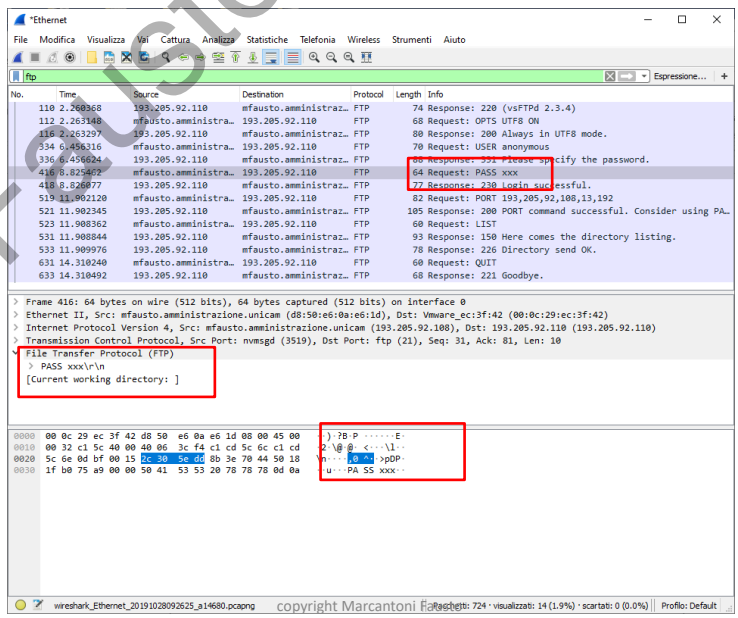
28

ftp con wireshark

Filtro "ftp"



Tutto in ASCII



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

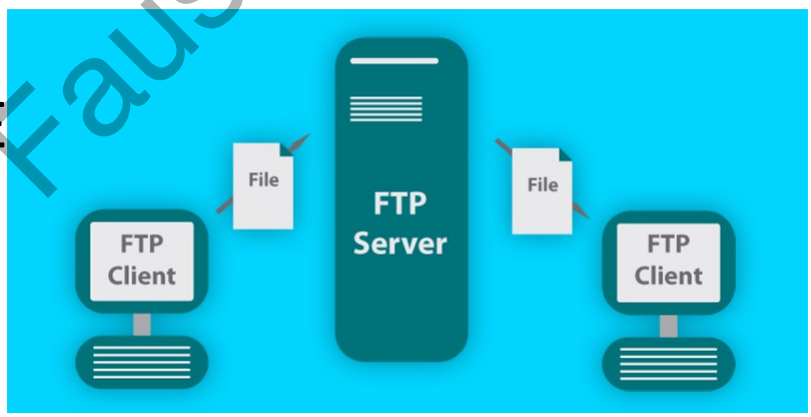
8 Best Free FTP Server Software
https://www.lifewire.com/windows-ftp-servers-free-817577

Best Linux FTP Client: Top 10 Reviewed for Linux Geeks

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

31

FINE



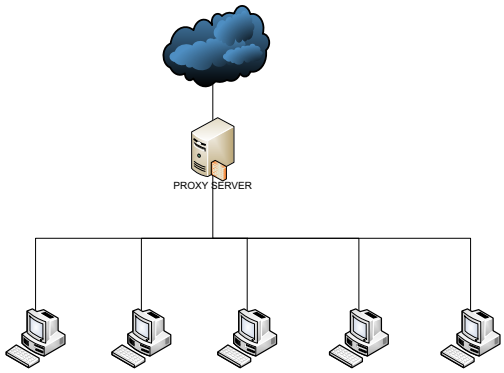
32

proxy

33

server proxy

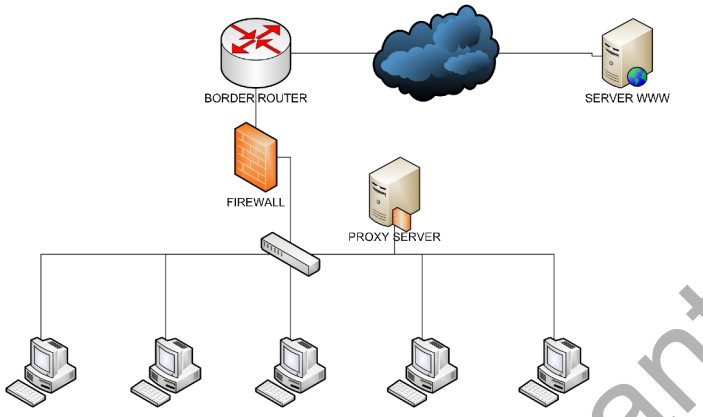
Un server proxy (detto anche «server mandatario») è all'origine un terminale che svolge la funzione di intermediario tra i computer di una rete locale (che usa talvolta dei protocolli diversi dal protocollo TCP/IP) e internet.



34

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,…).



35

Il principio di funzionamento di un proxy

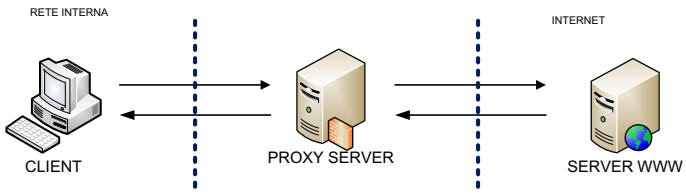
Il principio di funzionamento basico di un server proxy è abbastanza semplice:

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.



36

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

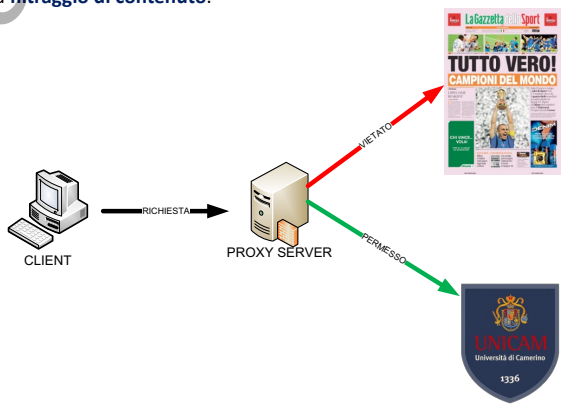
Questa funzionalità implementata in alcuni server proxy permette da una parte di **ridurre l'uso della banda passante** verso internet e dall'altra di **ridurre i tempi di accesso** per gli utenti ai documenti.

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.

37

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**.



38

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**…

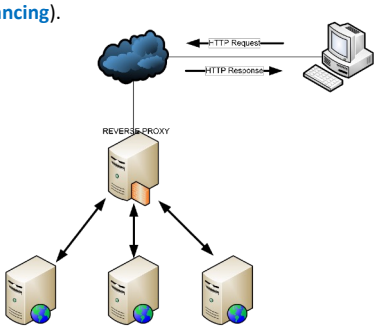
39

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.

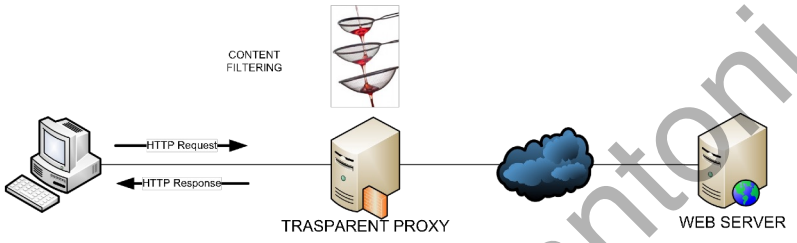
Il reverse-proxy serve anche da collegamento per gli utenti internet che desiderano accedere ad un sito web interno trasmettendogli indirettamente le richieste. Grazie al reverse-proxy, il **server web è protetto** dagli attacchi diretti dall'esterno, cosa che rinforza la sicurezza della rete interna. 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**).



40

trasparent proxy

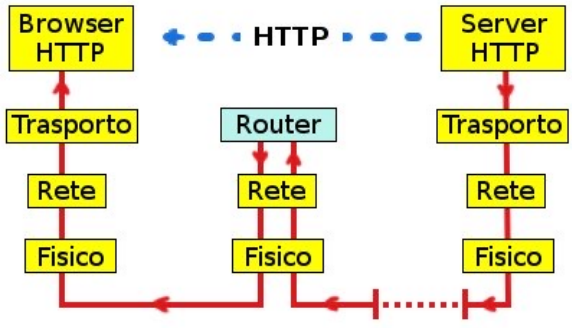
La funzione del **Transparent Proxy** è **quella di intercettare ogni richiesta di un particolare servizio** (in questo caso richiesta *HTTP*) per poi redirigerla a un proxy affinchè svolga tutte le funzioni del caso (semplice **content filtering piuttosto che caching**).



41

Browser – Server HTTP

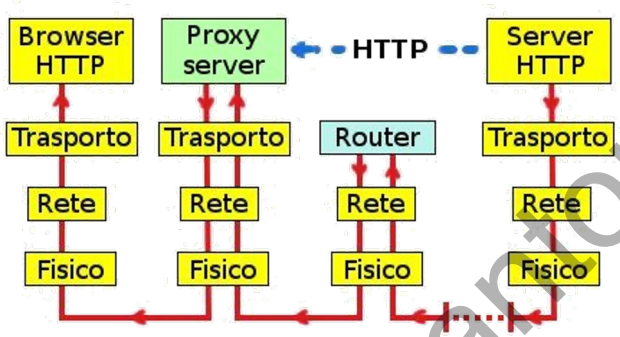
Nell'architettura TCP/IP il browser e il server Web comunicano direttamente a livello di applicazione senza alcuna intermediazione



42

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



43

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

44

squid proxy

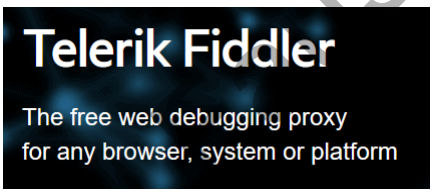
1. installare (http://www.squid-cache.org/)
2. attivare/provare
3. monitorare (SquidAnalyzer, Calamaris, …)
4. filtrare (SquidGuard, DansGuardian, …)

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

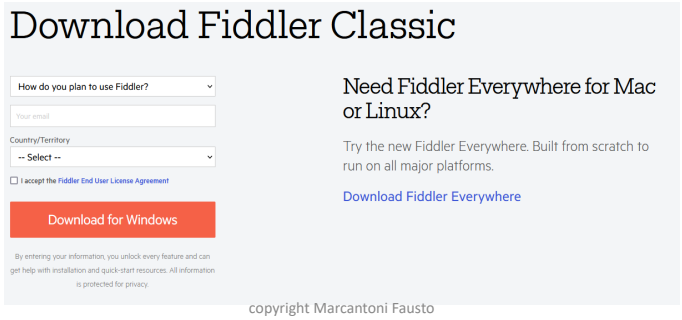
non funziona sempre

45

fiddler proxy



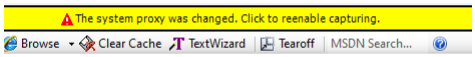
https://www.telerik.com/fiddler

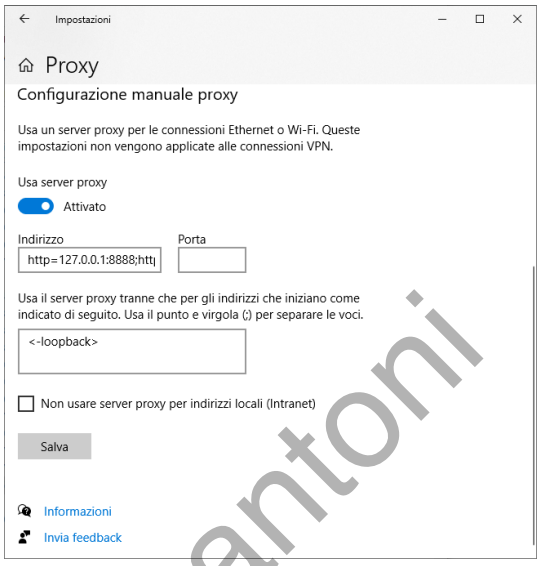


46

fiddler proxy

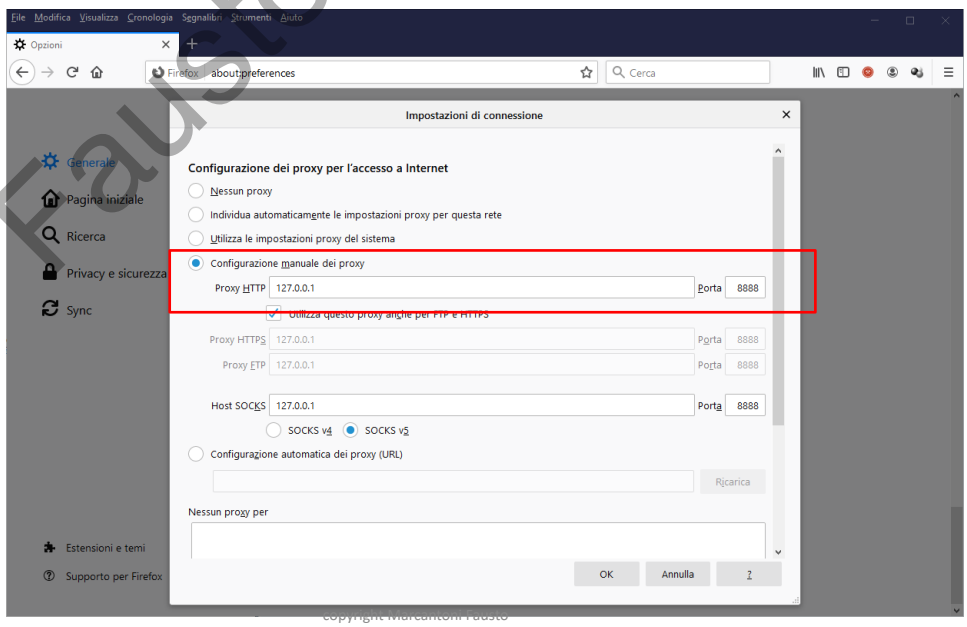
http=127.0.0.1:8888;https=127.0.0.1:8888





47

fiddler proxy



48

owasp zap proxy

owasp zap proxy

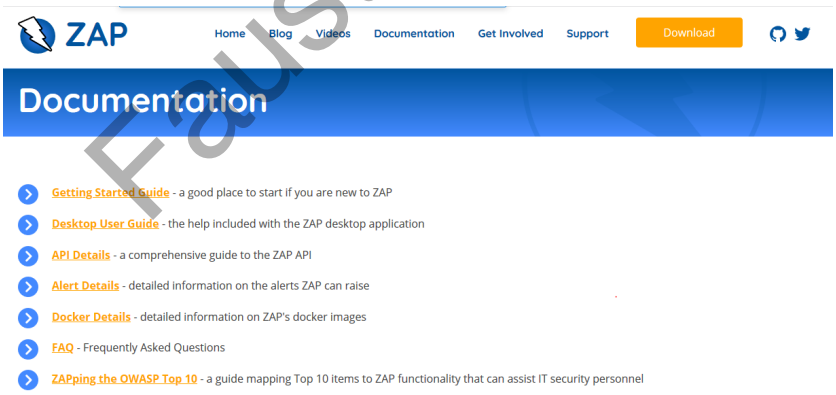
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP Zed Attack Proxy (ZAP)

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

49

owasp zap proxy



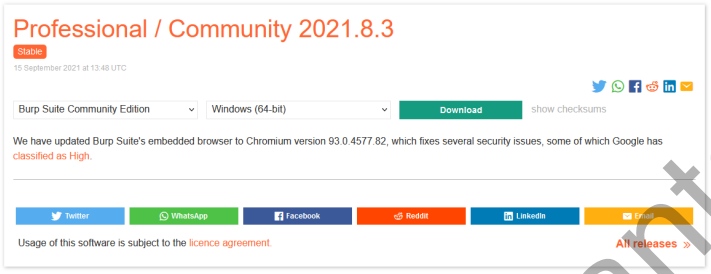
https://www.zaproxy.org/docs/

50

Burp Suite proxy

Burp Suite Community Edition

https://portswigger.net/burp



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

51

Burp Suite proxy

Support Center » Documentation » Desktop editions

Professional Community

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

52

FINE

53

SMTP

54

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

55

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/

56

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

57

smtp

FINE

58

Virtual Machine

59

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/

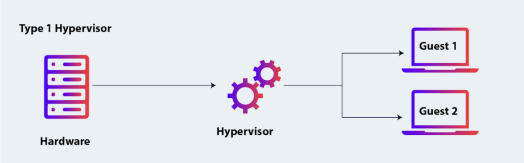
60

Hypervisor di Tipo 1 e 2

Gli hypervisor possono essere classificati in **due categorie** principali:

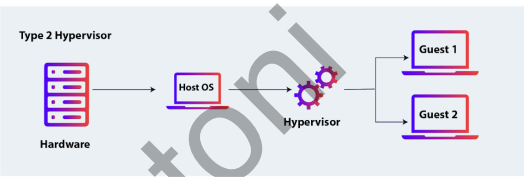
Hypervisor di Tipo 1

è definito anche **Native Hypervisor o Bare Metal**, e viene eseguito direttamente sull'hardware host per gestire i sistemi operativi guest. Questo tipo di hypervisor è indicato principalmente per gli utenti che vogliono utilizzarlo per creare un server per la virtualizzazione, mentre è troppo complesso per progetti più piccoli in ambito personale.



Hypervisor di Tipo 2

è denominato anche **Hosted Hypervisor** e viene eseguito su un sistema operativo esistente con un software o un'applicazione, perciò viene installato come un qualsiasi altro programma. L'hypervisor si occupa, quindi, della virtualizzazione delle risorse. Tuttavia, una gran parte delle risorse viene già persa nel sistema operativo host. Gli hypervisor di tipo 2 si adattano perfettamente anche a progetti di piccole dimensioni.



61

Docker

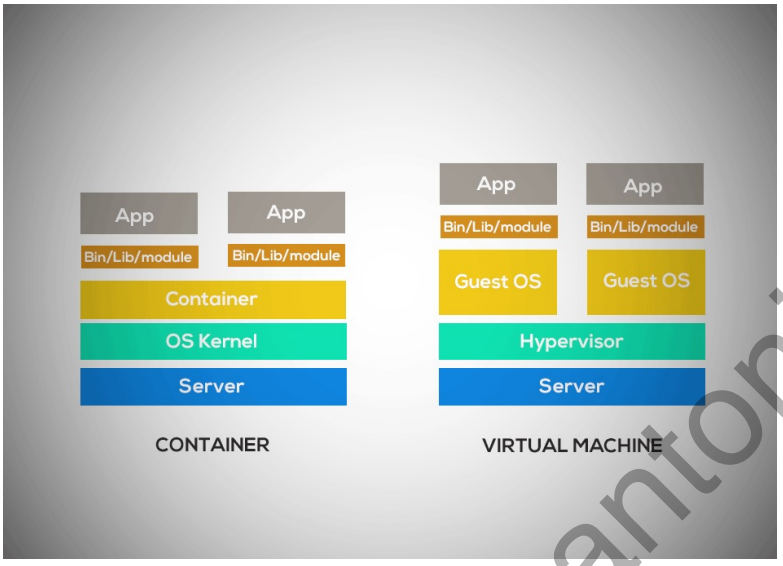
https://www.docker.com/ https://www.docker.com/products/docker-desktop/

Docker è una piattaforma software che permette di **creare, testare e distribuire applicazioni** con la massima rapidità. Docker raccoglie il software in unità standardizzate chiamate **container** che offrono tutto il necessario per la loro corretta esecuzione, incluse librerie, strumenti di sistema, codice e runtime. Con Docker, è possibile distribuire e ricalibrare le risorse per un'applicazione in qualsiasi ambiente, tenendo sempre sotto controllo il codice eseguito.

I container sono unità eseguibili di software che creano pacchetti del codice dell'applicazione insieme alle relative librerie e dipendenze. Consentono l'esecuzione del codice in qualsiasi ambiente informatico, che si tratti di desktop, IT tradizionale o infrastruttura cloud.

62

Qual è la differenza tra Docker e una VM?



63

The Top Open-Source Hypervisor Technologies

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

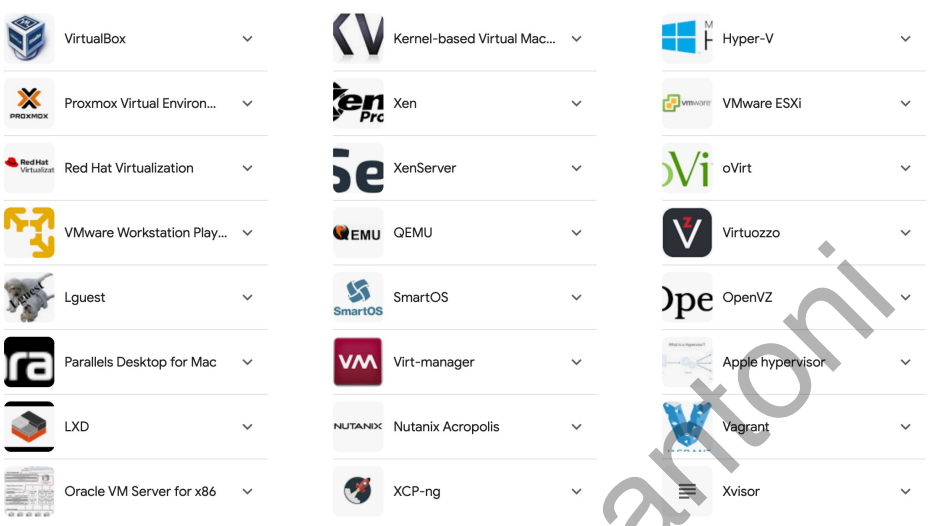
https://wire19.com/comparison-top-server-virtualization-software/

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

64

The Top Open-Source Hypervisor Technologies



65

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.

66

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

67

Cloud computing

Il **cloud computing** consente di sfruttare potenza di calcolo, spazio di archiviazione, servizi e software attraverso internet, sgravando così le risorse interne all'azienda: **flessibilità, scalabilità e minori costi** sono i vantaggi principali, ai quali se ne accodano altri

Infrastructure-as-a-Service (IaaS): offre agli utenti risorse di elaborazione, rete e storage.

Platforms-as-a-Service (PaaS): offre agli utenti una piattaforma per l'esecuzione delle applicazioni, oltre a tutta l'infrastruttura IT necessaria.

Software-as-a-Service (SaaS): fondamentalmente, offre agli utenti un'applicazione cloud, la piattaforma su cui viene eseguita e l'infrastruttura alla base della piattaforma.

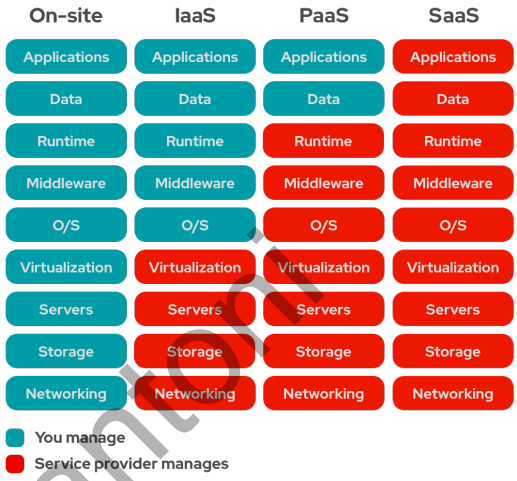
68

Cloud Computing

Esistono tre tipologie principali di cloud computing "as a Service", che si distinguono per il diverso livello di gestione affidato all'utente:

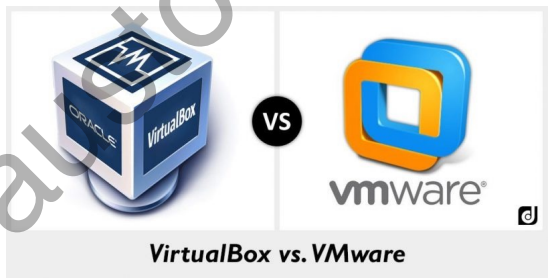
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

https://www.redhat.com/it/topics/cloud-computing/iaas-vs-paas-vs-saas



69

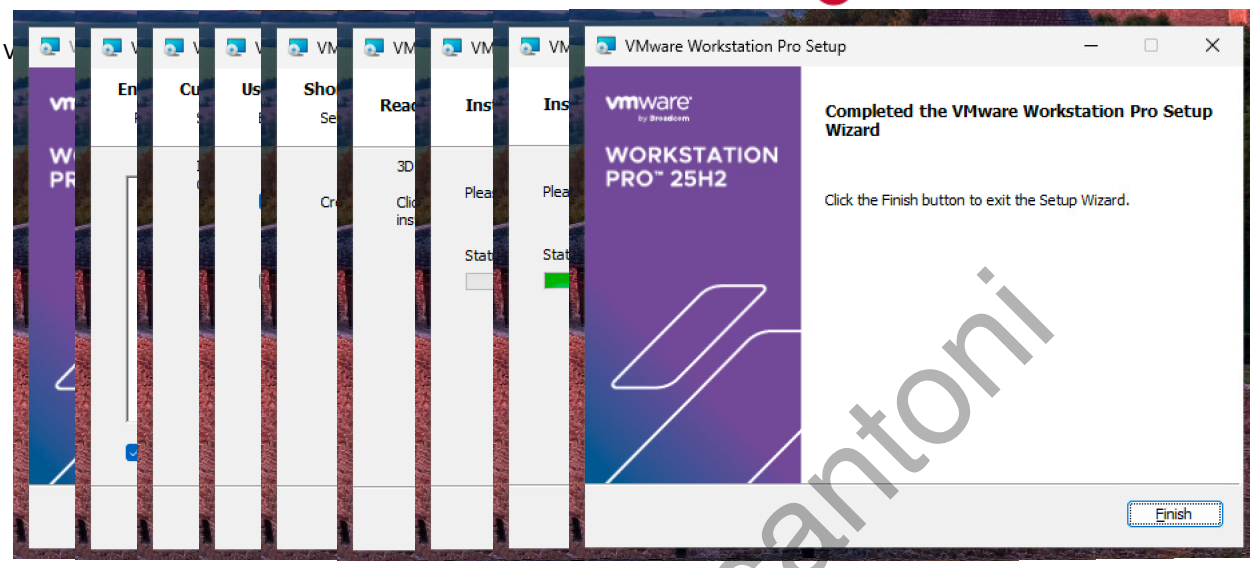
https://www.youlicense.com/virtualbox-vs-vmware-comparison/



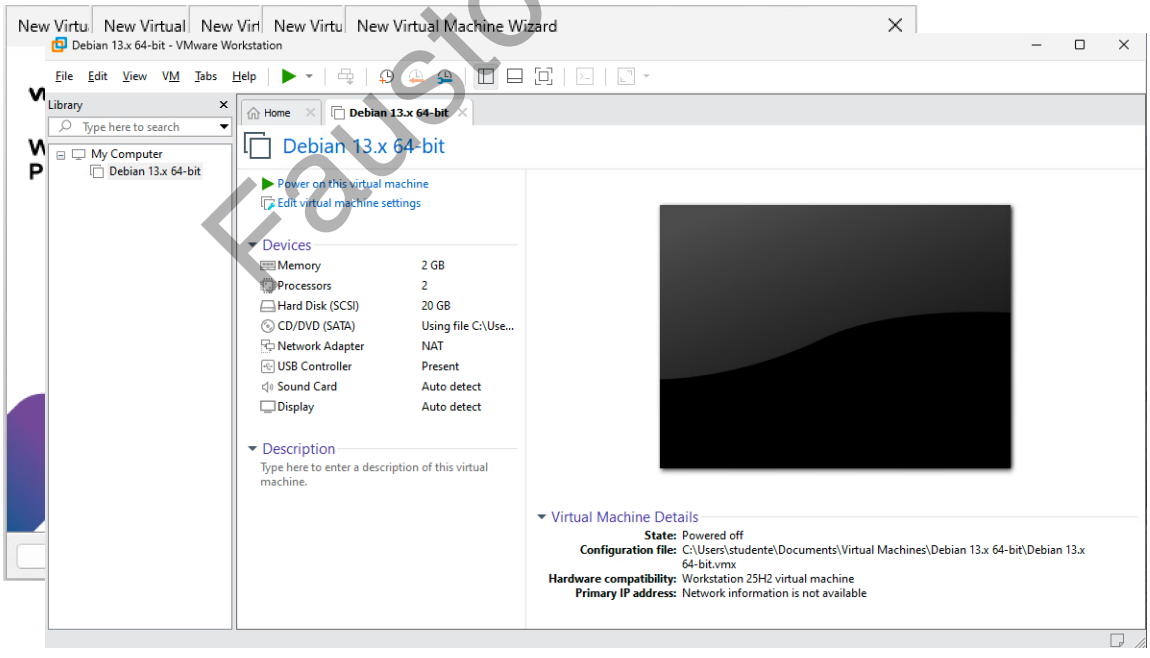
70

installare VMware Workstation

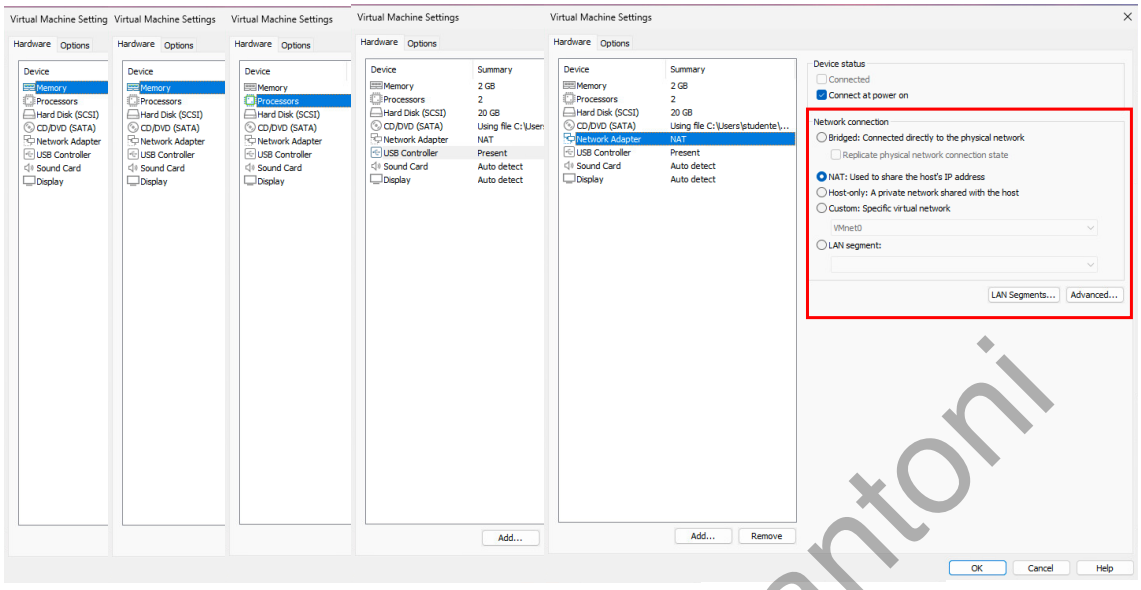
BROADCOM



71



72



73

🟢

1. Bridged (Scheda di rete in bridge)
Significato: la VM è **collegata direttamente alla rete fisica** del computer host, come se fosse un altro PC sulla stessa LAN.
La VM riceve un IP dal router o server DHCP della rete reale.
Può comunicare con host, altre VM e altri dispositivi della rete.

✅ **Vantaggi:**
Accesso completo alla rete locale e a Internet.
Può essere vista da altri dispositivi come un normale computer.

⚠️ **Svantaggi:**
Meno isolamento; la VM è esposta alla rete esterna.

74

🟡

2. NAT (Network Address Translation)
Significato: la VM **usa la connessione Internet del computer host**, ma **resta dietro un NAT**, come un router virtuale.
VMware crea una **rete virtuale privata** (tipicamente VMnet8).
La VM ha un IP virtuale, e l'host "traduce" le richieste verso Internet.

✅ **Vantaggi:**
Accesso a Internet funzionante subito, senza configurazioni speciali.
Buon isolamento: la VM non è visibile nella rete reale.

⚠️ **Svantaggi:**
Le altre macchine della rete fisica **non possono accedere direttamente** alla VM (serve port forwarding).

75

🔵

3. Host-Only
Significato: la VM comunica **solo con il computer host** e con altre VM nella stessa rete host-only.
Nessun accesso diretto a Internet o alla rete fisica.
VMware crea una rete virtuale isolata (tipicamente VMnet1).

✅ **Vantaggi:**
Massimo isolamento (utile per test o ambienti di laboratorio).

⚠️ **Svantaggi:**
Nessuna connessione Internet o LAN esterna (a meno di configurazioni manuali).

76

⚫

4. Custom / VMnet personalizzata
Significato: puoi scegliere manualmente una rete virtuale creata da VMware (ad es. VMnet2, VMnet3…).
Serve per creare topologie di rete complesse (es. più VM con reti simulate diverse).

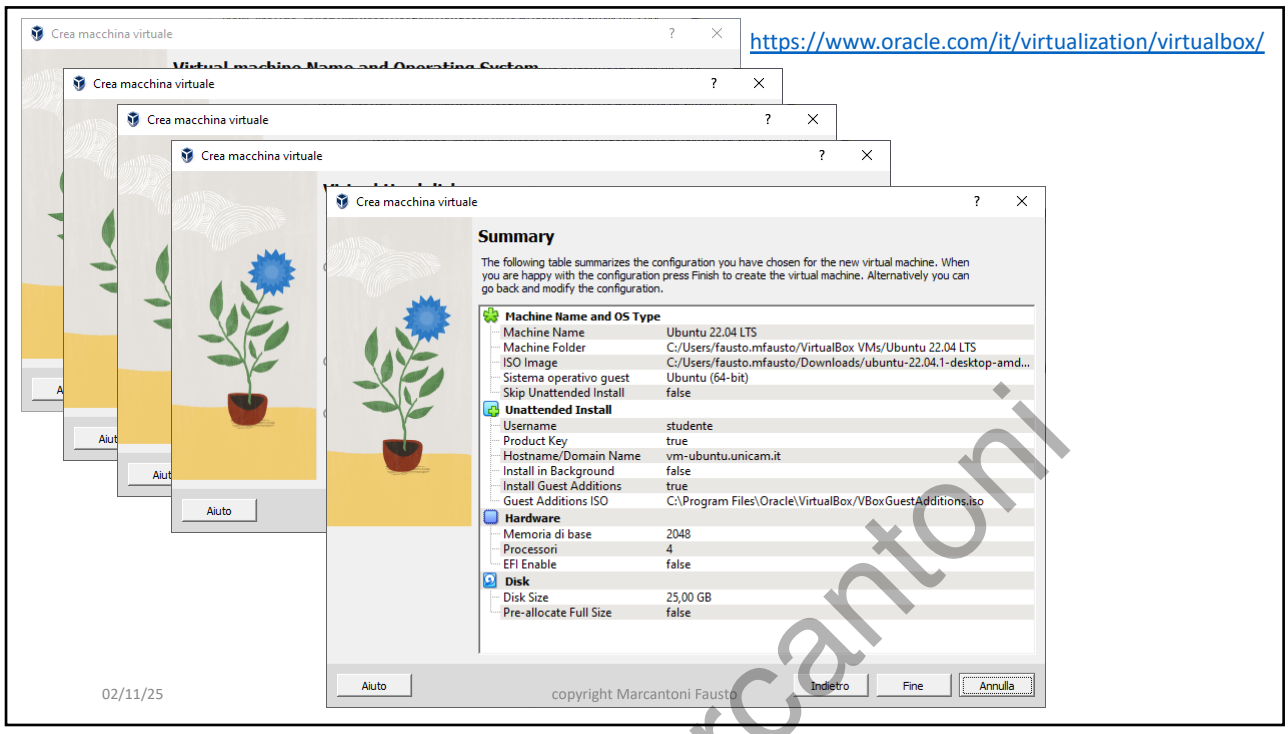
✅ **Vantaggi:**
Flessibilità totale per test e simulazioni di rete.

⚠️ **Svantaggi:**
Richiede più configurazione.

77

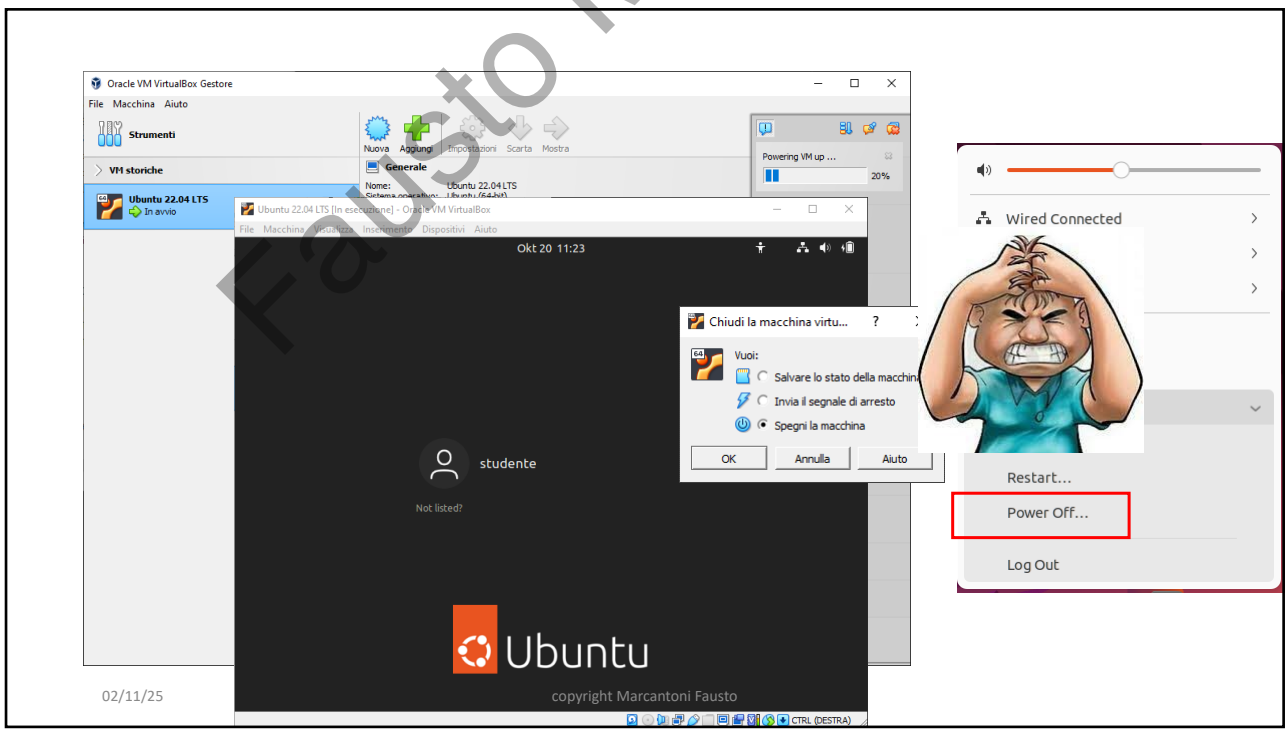
Tipo connessione	Accesso Internet	Visibile in LAN	Isolamento	Tipico utilizzo
Bridged	✅	✅	❌	VM come PC reale sulla rete
NAT	✅	❌	🟡	Uso Internet sicuro e semplice
Host-Only	❌	❌	✅	Test in locale isolato
Custom (VMnet)	Dipende	Dipende	Variabile	Laboratori complessi
LAN Segment	❌	❌	✅✅	Simulazioni completamente isolate

78

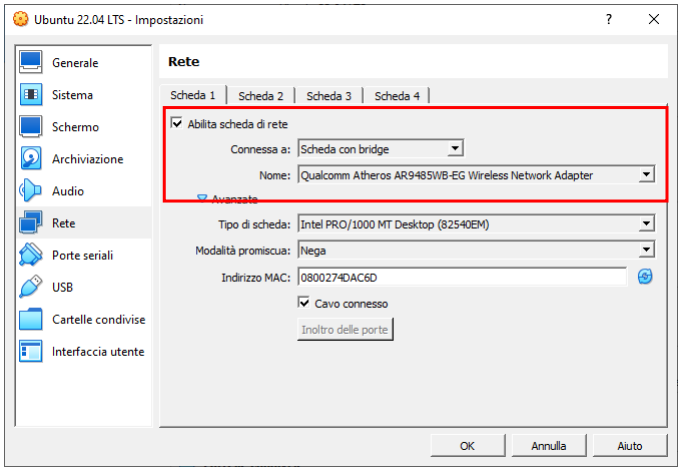


https://www.oracle.com/it/virtualization/virtualbox/

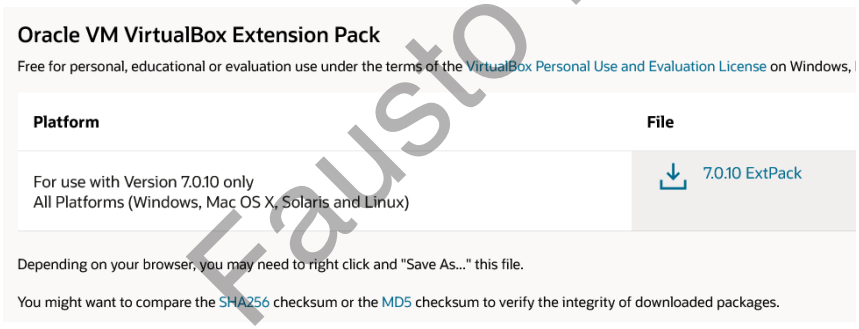
79

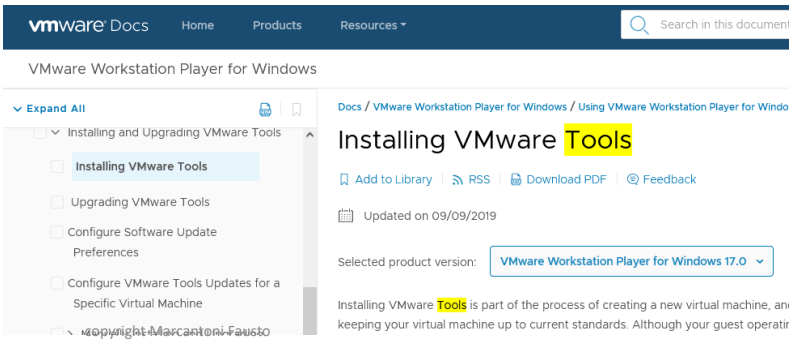


80



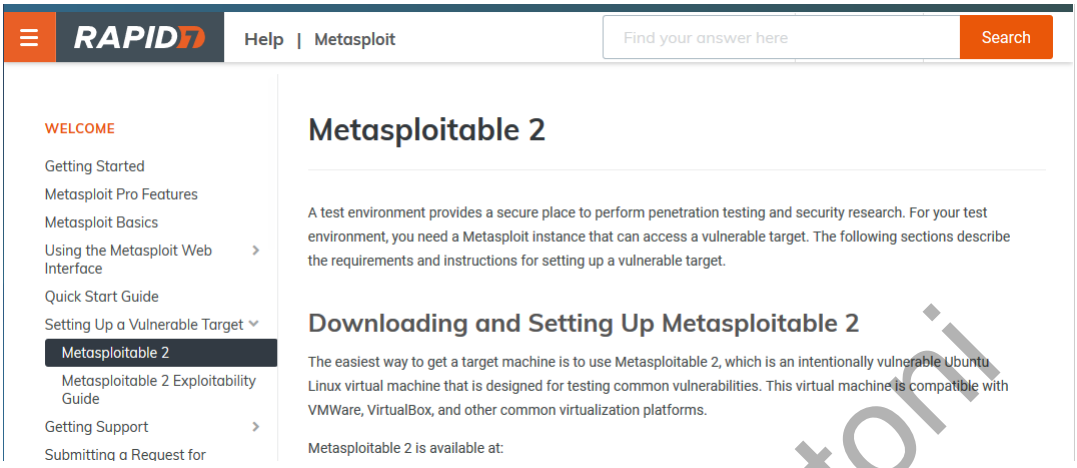
81





82

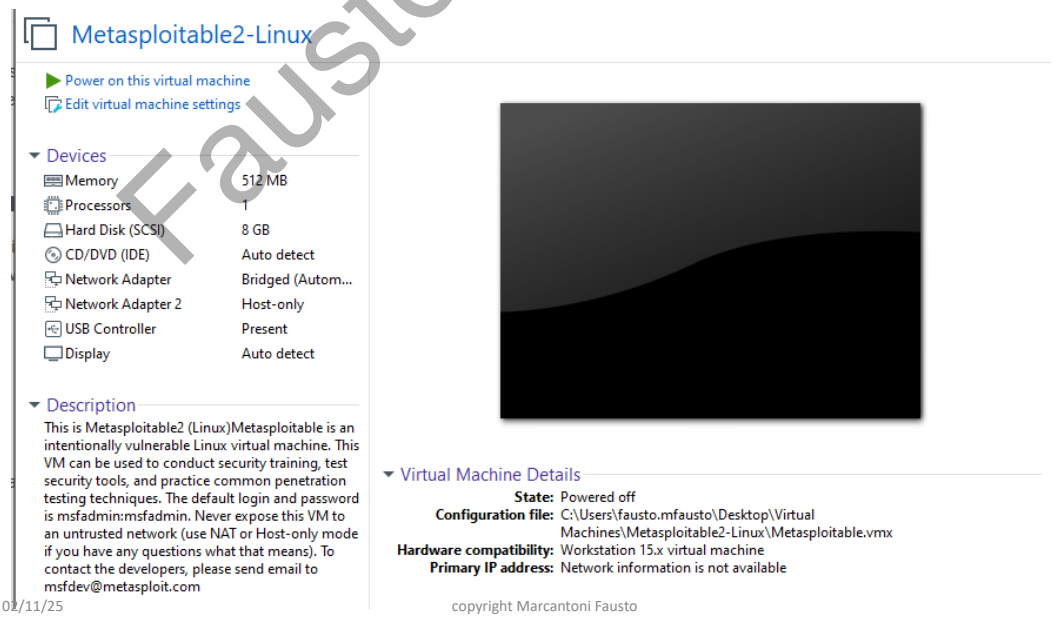
Metasploitable 2



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

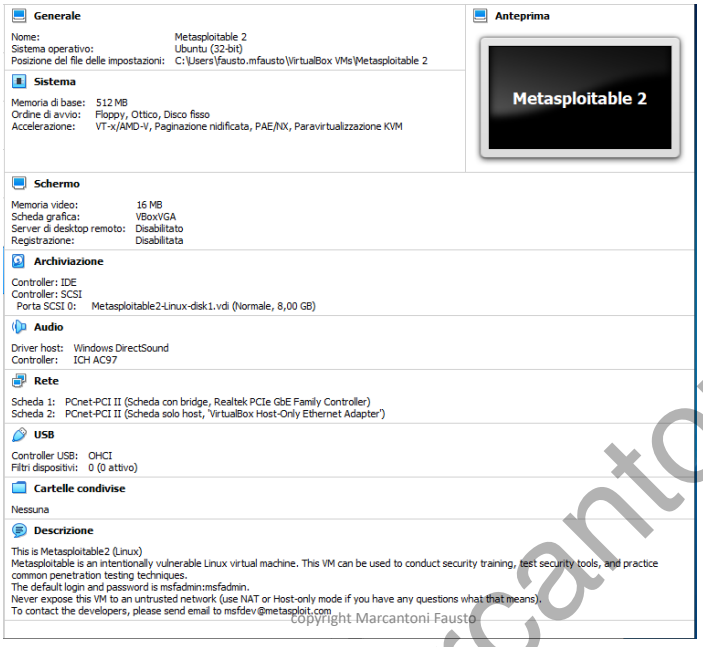
83

Metasploitable 2 - VMWARE



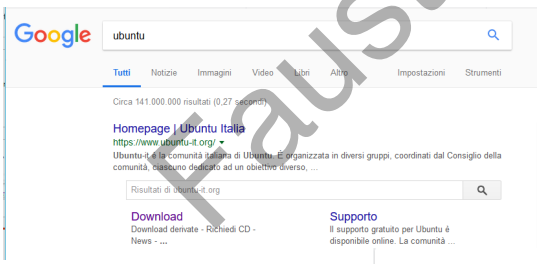
84

Metasploitable 2 – VirtualBox

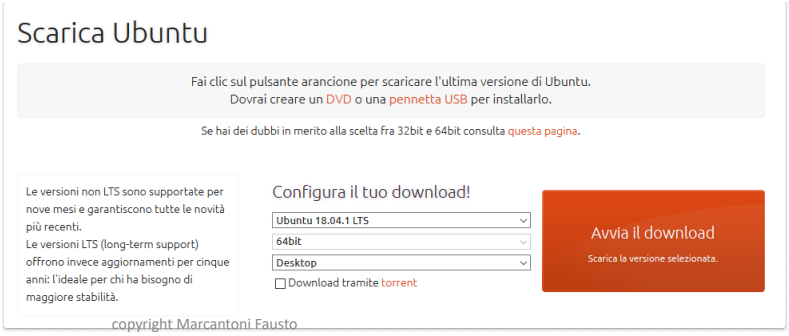


85

Scaricare l'ultima versione della iso di Ubuntu/Debian

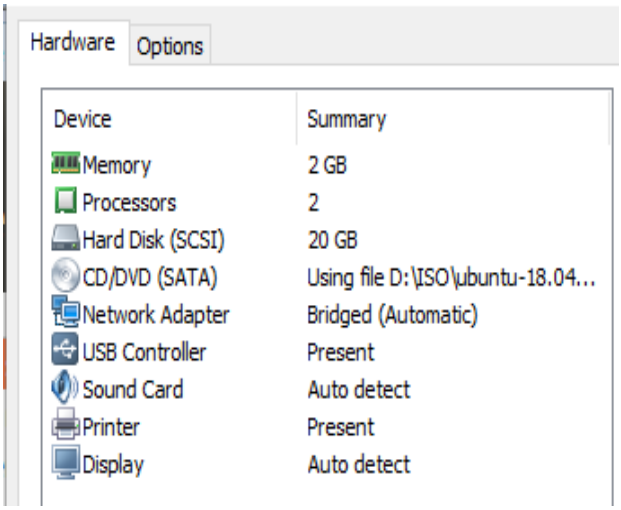


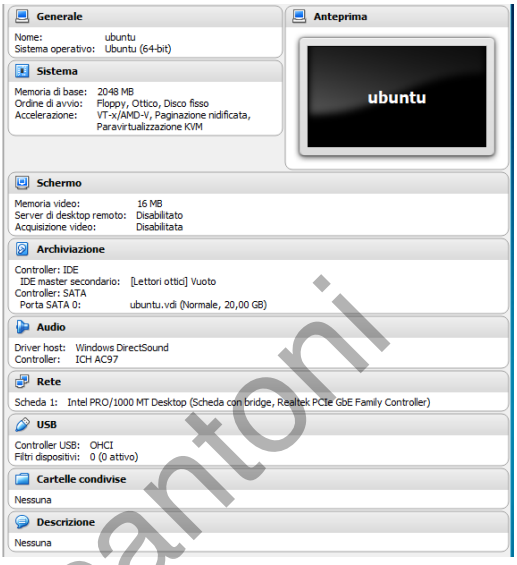
Debian è "la roccia sulla quale è costruita Ubuntu".



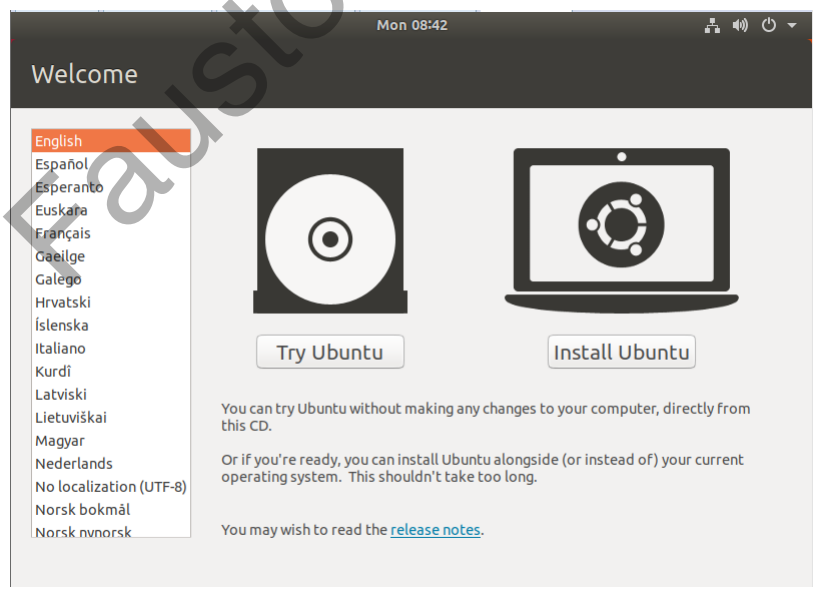
86

Caratteristiche VM





87



88

Virtual Machine

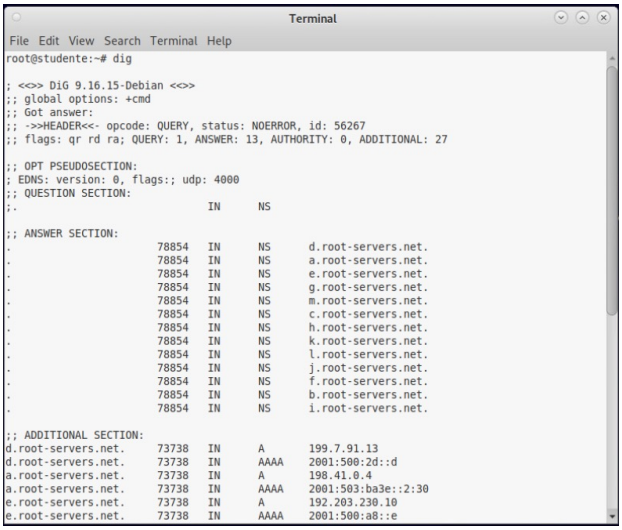
FINE

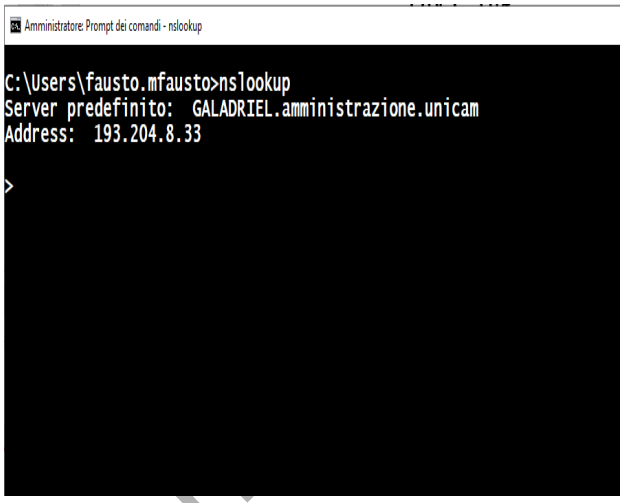
89

dns

90

DNS - dig - nslookup





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)

93

Laboratorio Linux

Linux

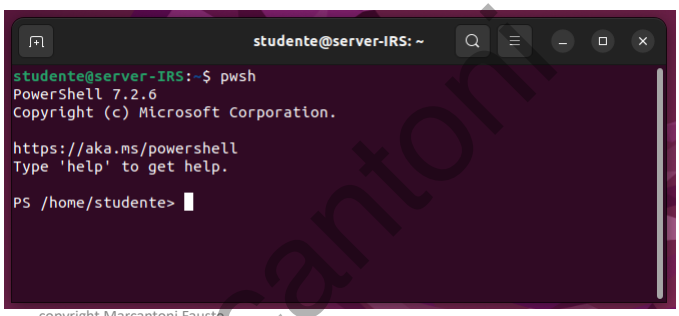
```
dig unicam.it
dig google.it +short
dig unicam.it -t mx +short
dig unicam.it -t ns +short
dig axfr unicam.it
```

```
studente@server-IRS: ~
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:~$
```


94

Installazione di PowerShell in Ubuntu

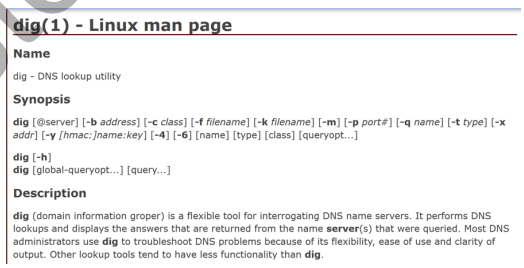
```
# Update the list of packages
sudo apt-get update
# Install pre-requisite packages.
sudo apt-get install -y wget apt-transport-https software-properties-common
# Download the Microsoft repository GPG keys
wget -q "https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/packages-microsoft-prod.deb"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



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

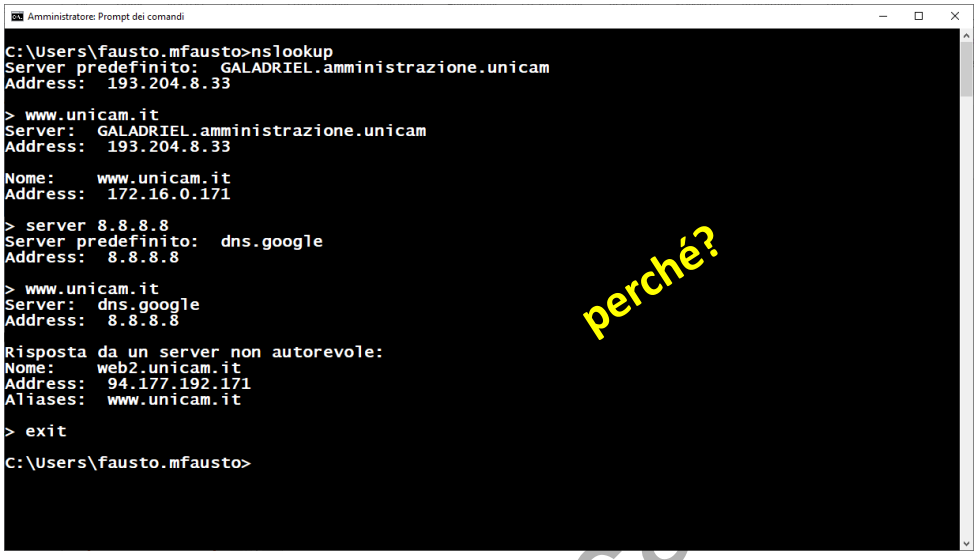
dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name **server**(s) that were queried. Most DNS administrators use **dig** to troubleshoot DNS problems because of its flexibility, ease of 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
dig -x 193.205.92.119
dig google.com +trace
dig google.com +short
dig -f query.txt +short
dig google.com ANY
```

Search For Record Type
Reverse DNS Lookup
Trace DNS Path

Query All DNS Record Types

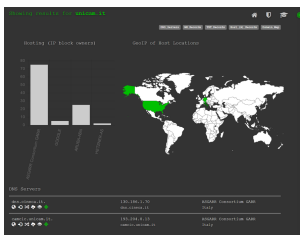
https://www.rootusers.com/12-dig-command-examples-to-query-dns-in-linux/



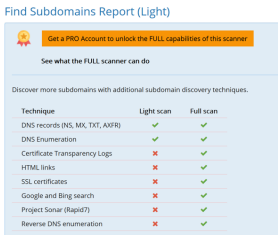
97

DNS Enumeration

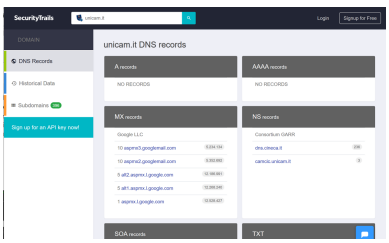
DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems. The list of DNS record provides an overview of types of resource records (database records) 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.



https://dnsdumpster.com/



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



https://securitytrails.com/

98

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/

99

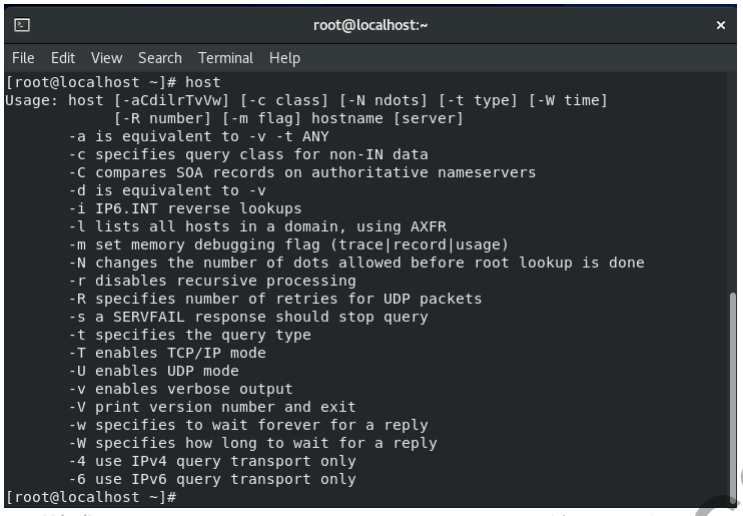
DNS Enumeration

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

100

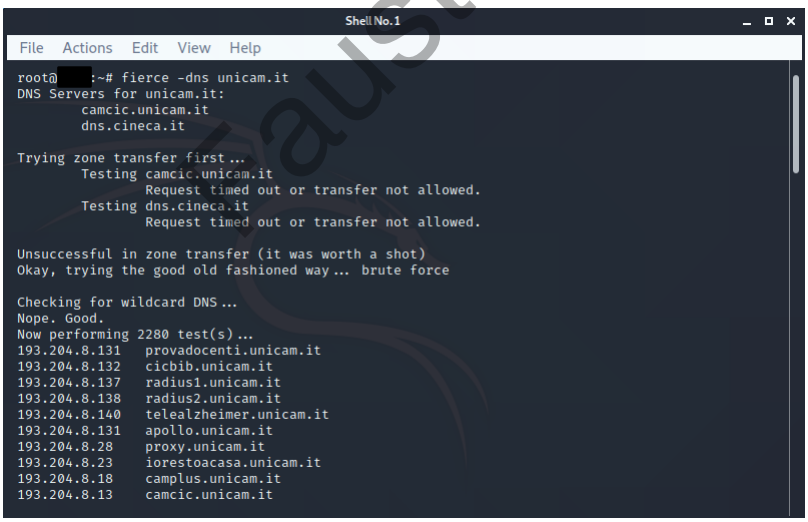
host




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


101

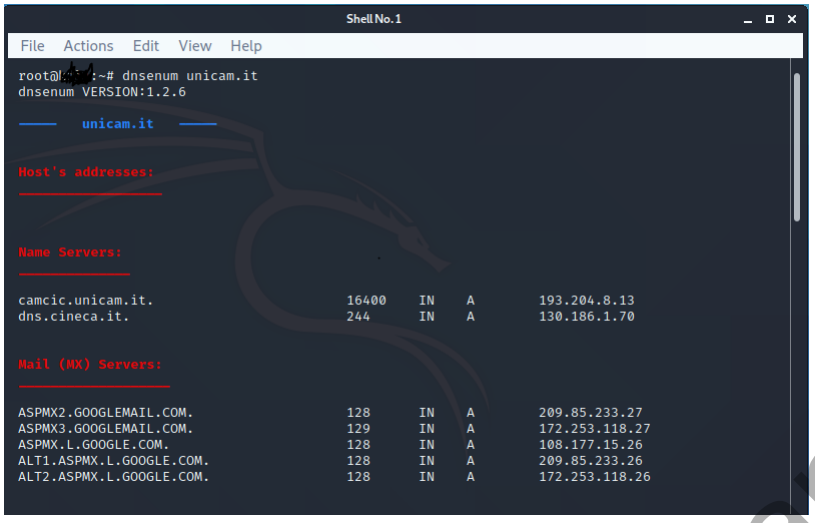
fierce -dns unicam.it



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

102

dnsenum unicam.it

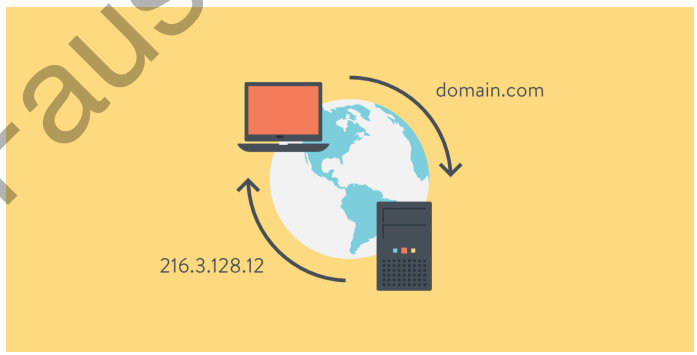


https://github.com/fwaeytens/dnsenum

103

DNS

FINE



104

Metasploitable2

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

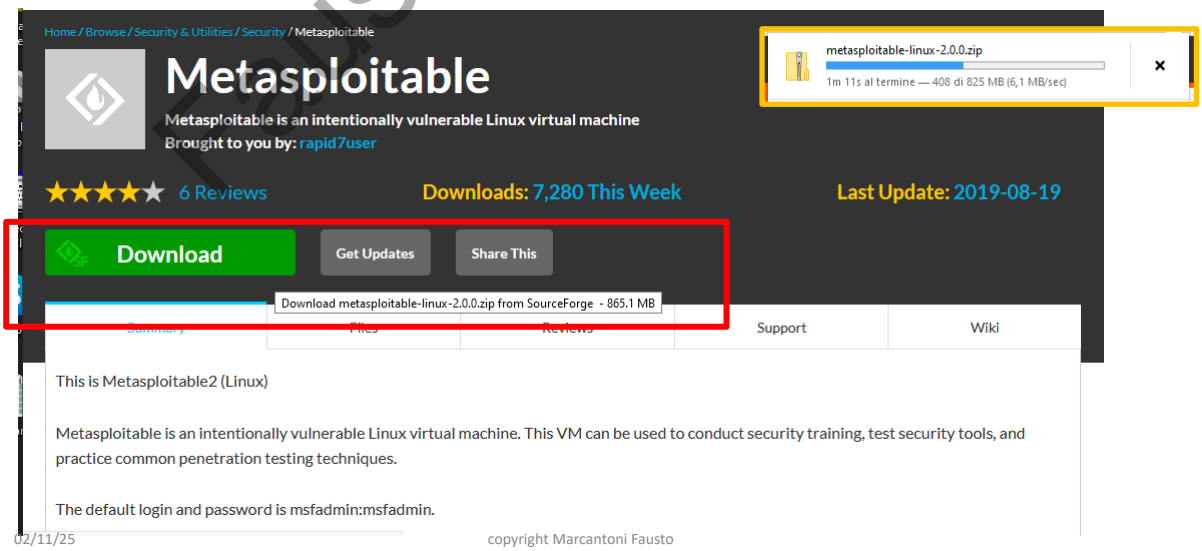
The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.

Metasploitable 2 is available at:
- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

105

Metasploitable2

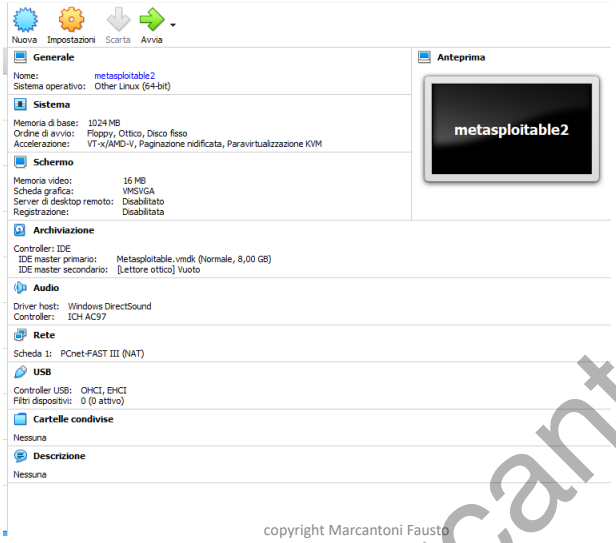
https://sourceforge.net/projects/metasploitable/



106

Metasploitable2

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



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

TENABLE Network Security

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

OpenVAS Open Vulnerability Assessment System

http://www.openvas.org/

VULNERABILITY ASSESSMENT vs PENETRATION TEST

Greenbone Community Documentation

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

111

vulnerability assessment

Versione completa

112

Greenbone Community Documentation

113

Sirius

```
git clone https://github.com/SiriusScan/Sirius.git
cd Sirius
docker-compose up
```

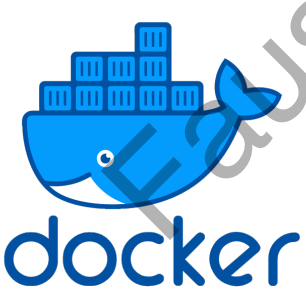

114

Wazuh

https://wazuh.com/

115

Docker



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

116

Gestione docker

https://www.portainer.io/install

https://docs.portainer.io/

117

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/

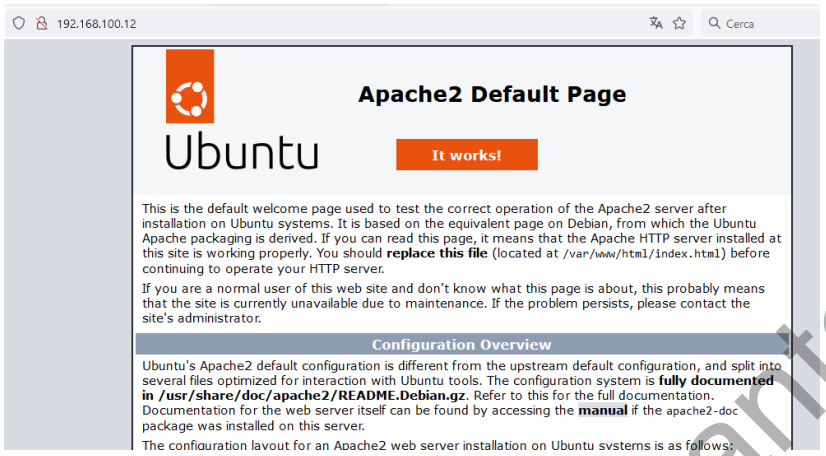
```
$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

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

118

Install Apache - Squid - Webmin

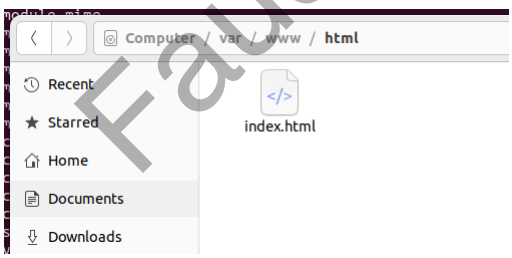
```
$ sudo apt install apache2
```



119

Install Apache - Squid - Webmin

```
$ sudo apt install apache2
```

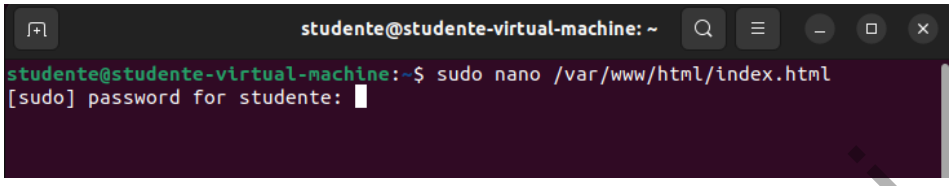



```
$ nano /var/www/html/index.html
```

120

Install Apache - Squid - Webmin

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




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

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


121

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>
```


122

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
```

123

Install squid webmin ubuntu

https://webmin.com/

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

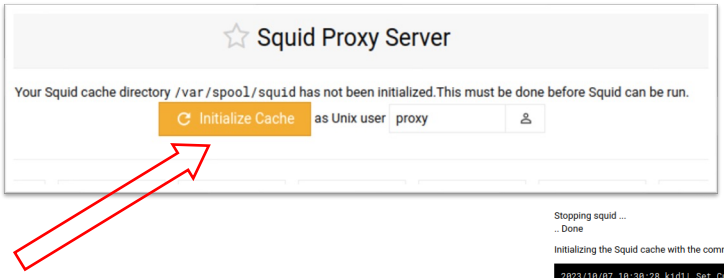
webmin

```
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/

124

Initialize cache proxy



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)
```

Return to squid index

125

Install squid webmin ubuntu

126