ITIS LEONARDO DA VINCI
Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail itis@itis.pr.it - cf.80007330345 - PRTF010006

CORSO DI CYBER SECURITY

Incontro #02

Prof. Ugolotti 2023-2024

Obiettivi del corso:

OLIMPIADI ITALIANE DI CYBERSICUREZZA

CYBER CHALLENGE.IT

Selezione scolastica
16/12/2023

Preselezione
? Febbraio 2024

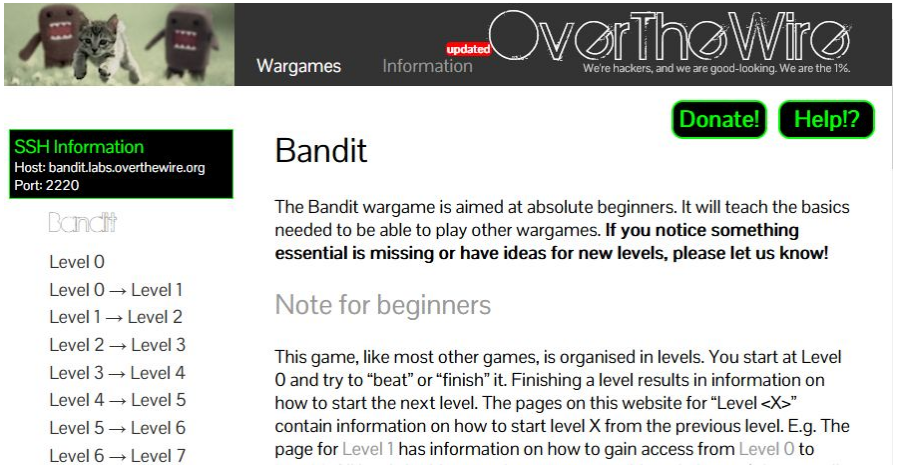
Correggiamo i compiti : Bandit 12

Wargames: Bandit

- **Terminale ssh:**
  - da shell DOS
  - da shell Linux
  - **scaricate Putty portable**
- **Colleghiamoci all' Host:**

`bandit.labs.overthewire.org`

Porta: `2220`



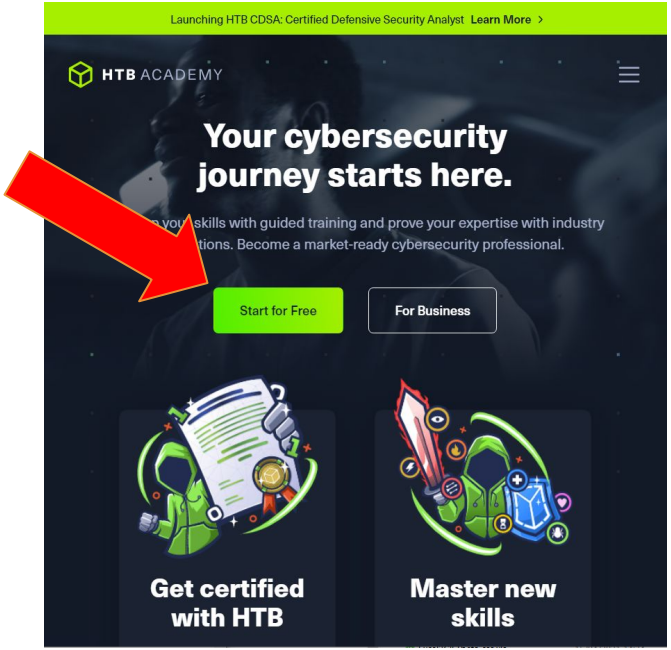
Dalla teoria alla pratica: Testiamo le nostre competenze

1) HackTheBox Academy

- Registratevi su:

  https://academy.hackthebox.com/

- Scegliete i corsi gratuiti



Dalla teoria alla pratica: Testiamo le nostre competenze

2) Training Olicyber.it

- Registratevi su:

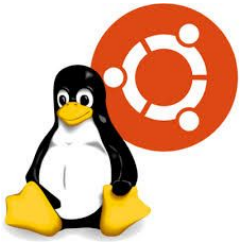
  https://training.olicyber.it

- Capture The Flag challenge (CTF)

Per affrontare OliCyber.it

Compitino:

Nelle prossime puntate faremo uso di tools che troviamo nativamente in Linux, organizzatevi per avere un PC/Laptop con un sistema nativo o una virtual machine del Pinguino.



...e se non sapete cos'è una macchina virtuale ⇒ **QUI**

Per affrontare OliCyber.it

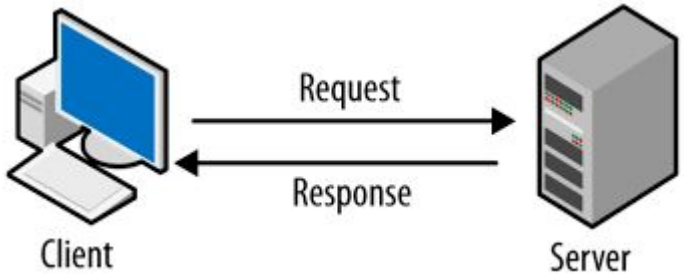
https://olicyber.it/materiale

La Selezione scolastica (16 Dic 2023)

- networking
- Indirizzamento IPv4
- Funzioni ricorsive
- Operatori bitwise

Modello Client-Server

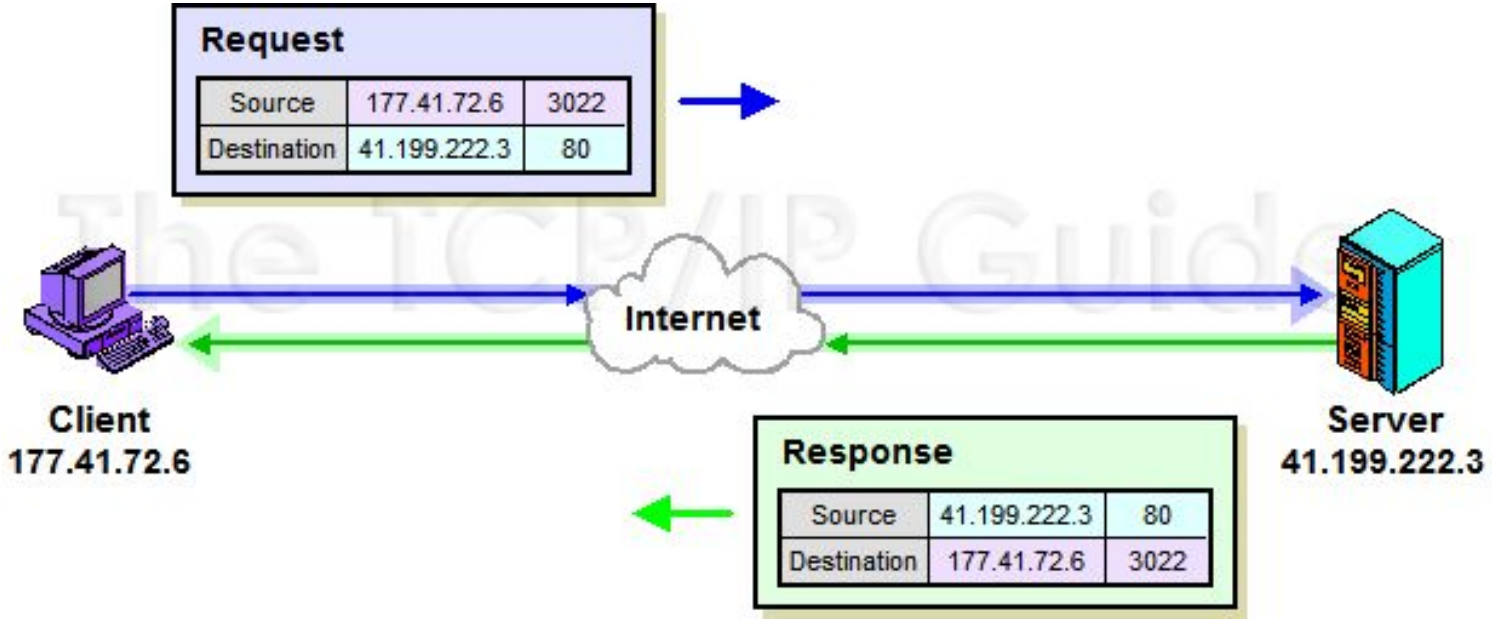
In realtà in questo caso, è più corretto pensare ai software (e non all'hardware):



il **client** è l'applicazione che 'gira' sulla macchina "client" e che inoltra al server le richieste, attraverso la porta che il server stesso ha lasciato aperta (ad esempio nell'http il server risponde sulla porta 80)

Il **server** è l'applicazione che 'gira' sulla macchina "server" (intendendo un hardware con prestazioni sufficienti a consentire la gestione di traffico elevato) e a cui corrisponde una PORTA aperta (in ascolto).

Modello Client-Server: approfondiamo



Modello Client-Server: controllo remoto tramite ssh

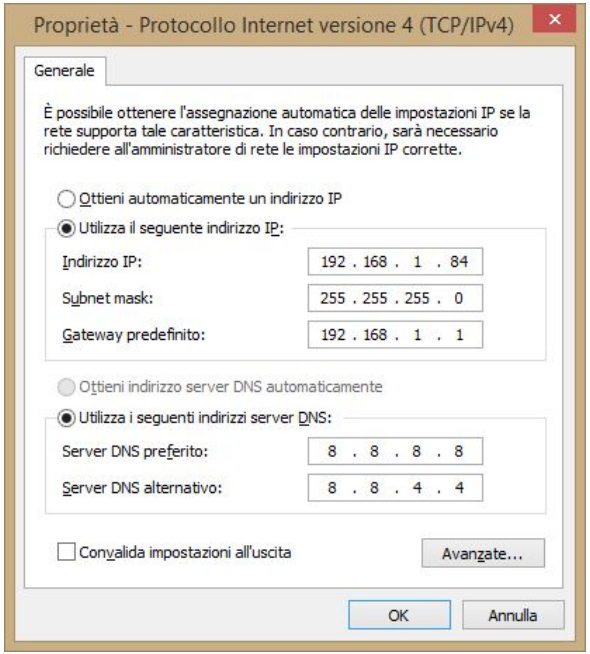
Se volete connettervi da Windows, oltre alla shell DOS:

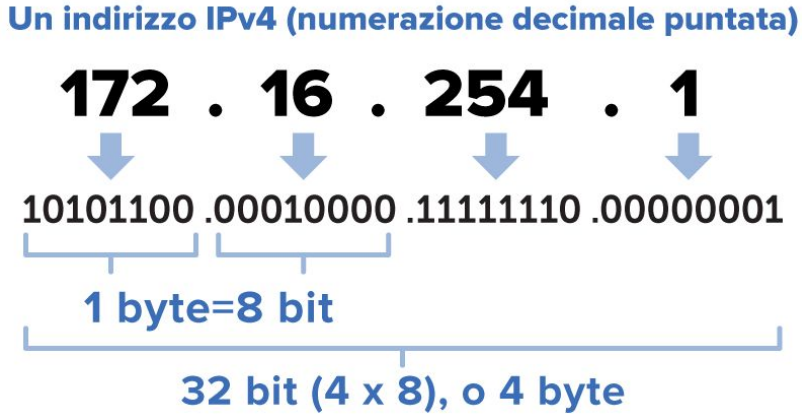
- client Putty (portable): supporta altri protocolli oltre a ssh, permette di amministrare molteplici account remoti

- VMPlayer: usiamo linux su windows

Tutorial per la connessione con PUTTY

Indirizzi IP





- In realtà un indirizzo IP è un numero a 32 bit
- per semplificarne l'uso lo si rappresenta mediante quattro numeri decimali separati da punti

Subnet Mask

- In realtà un indirizzo IP da solo è piuttosto inutile
- Ogni indirizzo è abbinato ad una Maschera (Subnet Mask)
- Dobbiamo immaginare ogni indirizzo IP suddiviso in due parti:
  - **Net-ID**: la parte che identifica la rete di appartenenza
  - **Host-ID**: la parte che identifica il singolo Host della rete individuata
- La Subnet Mask ci permette di distinguere tra NetID e HostID

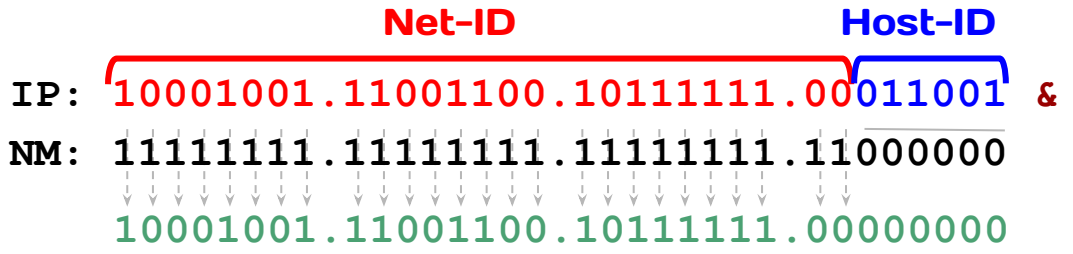
Consideriamo il seguente indirizzo IP

137.204.191.25/26

/26 significa che la NetMask è composta da 26 bit a 1 consecutivi, seguiti da 6 bit a 0 (completa i 32b); in ottetti diventa

255.255.255.192

Convertendo entrambe in binario e mettendoli in AND (&) bit a bit:



Si ottiene così il **nome della rete**: 137.204.192.0/26.
Tale operazione è detta di *MASCHERAMENTO*, perché i bit a *1* della **NetMask** "lasciano passare" solo i bit del NetID mentre quelli a *0* "bloccano" l'HostID

Nome della rete e Indirizzo di Broadcast

In ogni rete ci sono due indirizzi IP riservati che non possono essere utilizzati dagli host

- Indirizzo della rete: Il primo indirizzo della rete (quello in cui tutti i bit relativi all'host sono uguali a 0), esso identifica la rete

- Indirizzo di Broadcast: l'ultimo indirizzo della rete (quello in cui tutti I bit relativi all'host sono uguali a 1). I pacchetti inviati a questo indirizzo si intendono inviati a tutti i nodi di quella rete

11000000 10101000 01100100 11001000 address

192 . 168 . 100 . 200

11111111 11111111 11111111 00000000 netmask (**/24**)

255 . 255 . 255 . 0

11000000 10101000 01100100 **00000000** network addr.

192 . 168 . 100 . 0

11000000 10101000 01100100 **11111111** broadcast addr.

192 . 168 . 100 . 255

NB. tutti gli indirizzi IP compresi tra questi identificano Host della stessa rete

Nome della rete e Indirizzo di Broadcast

In ogni rete ci sono due indirizzi IP riservati che non
posson

- In
  (
  u

- In
  r
  u
  ir

dress

etmask (/24)

ork addr.

adcast addr.

sti

Si consideri la seguente rete: **172.16.100.0/20**

Quale tra i seguenti indirizzi appartengono ad host della stessa rete?

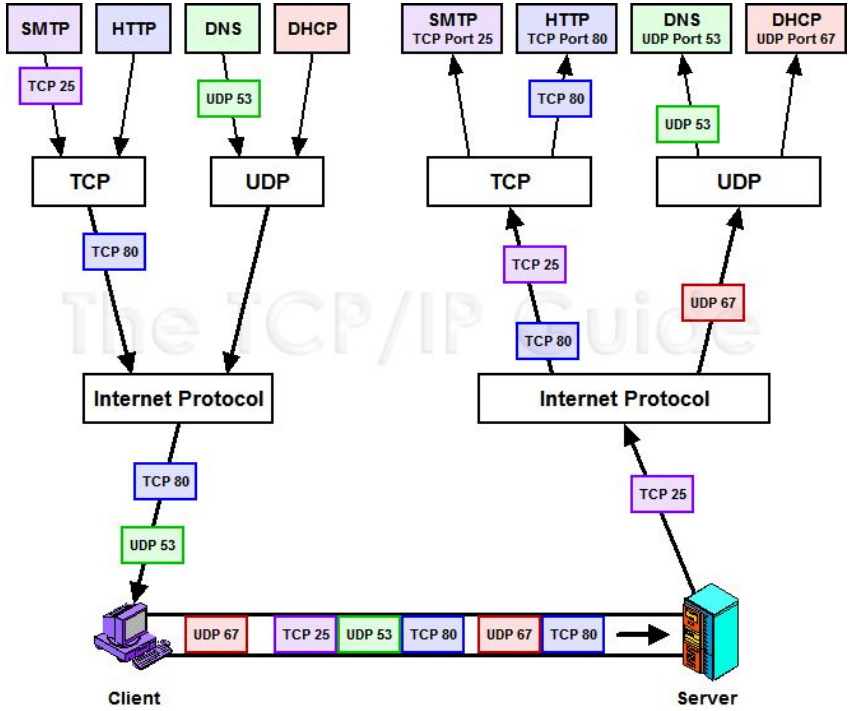
1. **172.17.100.1**
2. **172.16.96.0**
3. **172.16.101.55**
4. **172.16.100.255**
5. **172.16.111.255**
6. **172.16.96.1**

Le Porte

Se l'IP server a identificare un Host sulla rete,

le Porte servono ad **identificare un processo** tra i molti in esecuzione nello stesso Host.

Port Number	Protocol
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet Protocol
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	HyperText Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
137	NetBIOS Name Service
143	Internet Message Access Protocol (IMAP4)
443	Secure HTTP (HTTPS)
445	Microsoft-DS (Active Directory)



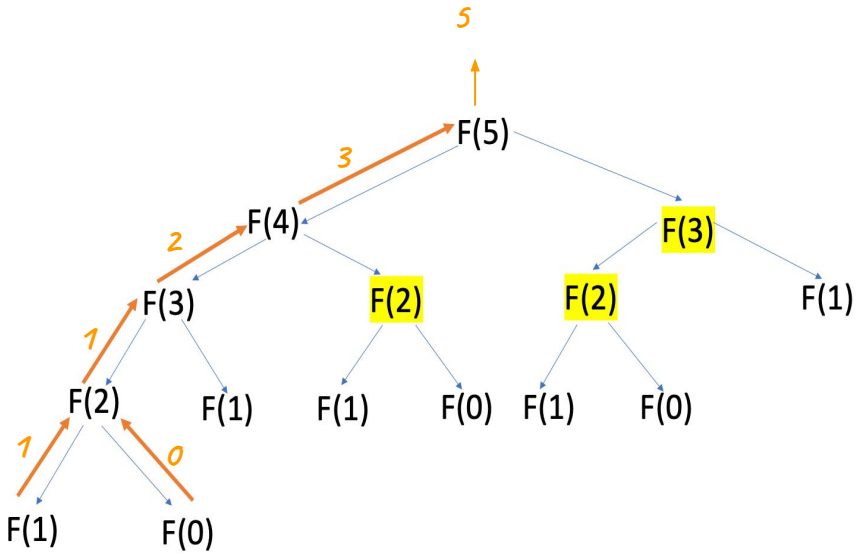
Ricorsione (per capire)

Si consideri la sequenza di Fibonacci così definita:

$$f(n) = \begin{cases} 0 & if \quad n = 0 \\ 1 & if \quad n = 1 \\ F(n-1) + F(n-2) & if \quad n > 1 \end{cases}$$

si vede che per ***n*** che va da 1 a 15, tale definizione ricorsiva produce la seguente sequenza

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,144, 233, 377, 610…



Riproducendo l'albero delle chiamate e risalendo ogni volta che si raggiungono le foglie terminali è possibile calcolare la soluzione