REPORT S5/L1

Nell'esercizio di oggi, lo studente effettuerà una simulazione della fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i principali strumenti della fase di information gathering.

Ho scelto come target il dominio www.multiplayer.it, e su questo andrò ad esegure l' ***information gathering*** che è una delle fasi piu importanti e delicate del ***pen-testing***.

Per prima cosa mi servo di google per raccogliere delle info preliminari riguardanti il domnio target. Faremo una ricerca mediante la stringa "***site:multiplayer.it contatti***" in maniera tale da andare a limitare la ricerca alle sole pagine del sito riguardanti i contatti che fanno riferimento al dominio in questione. ***Figura 1***

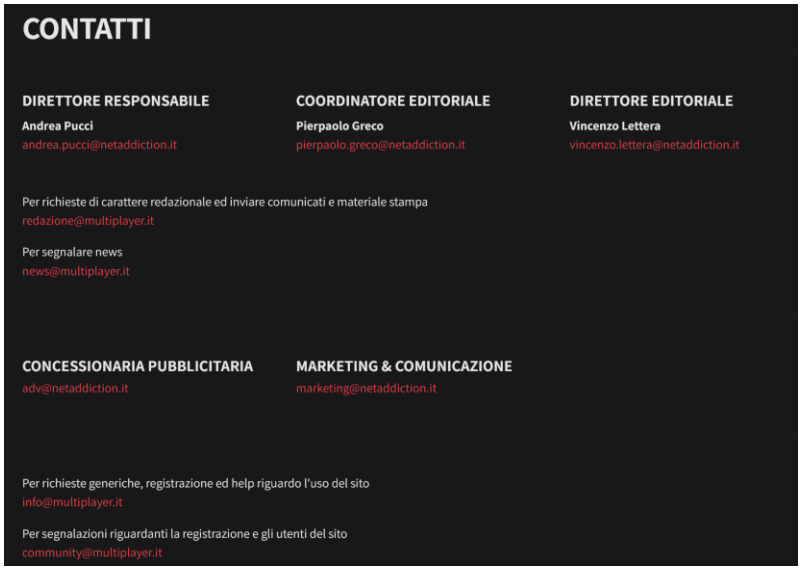

Figura 1

Per ottenere informazioni riguardanti i vari sottodomini del dominio principale andrò mediante google ad eseguire una ricerca con la stringa "site:multiplayer.it – site:www.multiplayer.it" , in questo modo verrà escluso il domino principale e verrano restituiti solo i sottodomini del target. ***Figura 2***

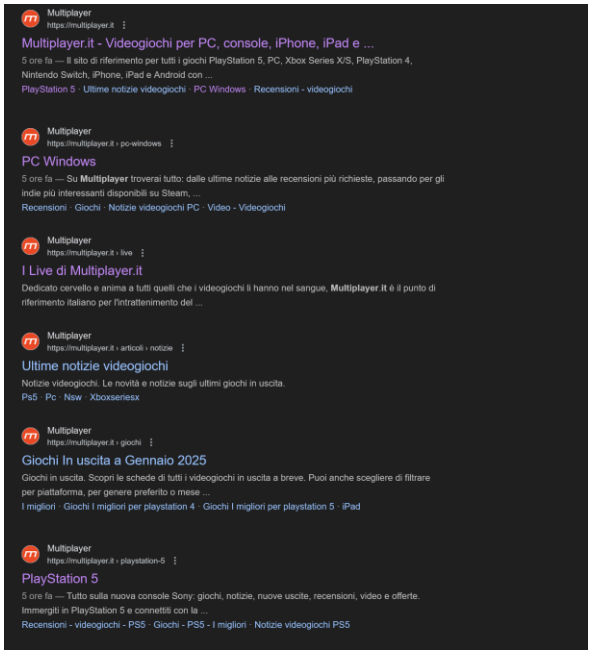

Figura 2

Mi muovo poi andando ad utilizzare ***whois***, uno strumento messo a disposizione da kali che mi permette di raccogliere info su un dominio. Procedo quindi con il comando "whois multiplayer.it". ***Figura 3***

```
└─$ whois multiplayer.it

************************************************************************
* Please note that the following result could be a subgroup of      *
* the data contained in the database.                               *
*                                                                   *
* Additional information can be visualized at:                      *
* http://web-whois.nic.it                                           *
************************************************************************

Domain:             multiplayer.it
Status:             ok
Signed:             no
Created:            1999-02-03 00:00:00
Last Update:        2024-04-27 00:50:56
Expire Date:        2025-04-11

Registrant
  Organization:     Netaddiction SRL
  Address:          Via Piave 51
                    Terni
                    05100
                    TR
                    IT
  Created:          2007-03-01 10:41:44
  Last Update:      2010-11-22 12:12:37

Admin Contact
  Name:             Pucci Andrea
  Organization:     Netaddiction SRL
  Address:          Via Piave 51
                    Terni
                    05100
                    TR
                    IT
  Created:          2008-01-30 17:42:47
  Last Update:      2010-11-22 12:12:37

Technical Contacts
  Name:             Technical Support
  Organization:     Register SpA
  Address:          Viale Giulio Cesare, 29
                    Bergamo
                    24124
                    BG
                    IT
  Created:          2009-09-28 11:01:09
  Last Update:      2024-06-12 12:09:06

Registrar
  Organization:     Register S.p.a.
  Name:             REGISTER-REG
  Web:              https://www.register.it
  DNSSEC:           yes


Nameservers
  phil.ns.cloudflare.com
  ruth.ns.cloudflare.com
```

Figura 3

Con questo strumento si nota come siano state raccolte già una serie di importanti informazioni, il nome della persona che ha registrato il dominio ***Andrea Pucci***, il nome dell' azienda ***Netaddiction SRL***, l' indirizzo della sede legale della stessa ***Via Piave 51Terni*** e la data di creazione dello stesso ***03/02/1999***. Vado ora ad utilizzare lo strumento ***maltego*** direttamente dalla vm kali, inserendo il dominio www.multiplayer.it e avviando la trasformata "***Mirror: Email addresses found***" per visualizzare i contatti/indirizzi email associati ad esso, in rosso è evidenziato quello del responsabile Andrea Pucci, persona emersa precedentemente da whois**. Figura 4**

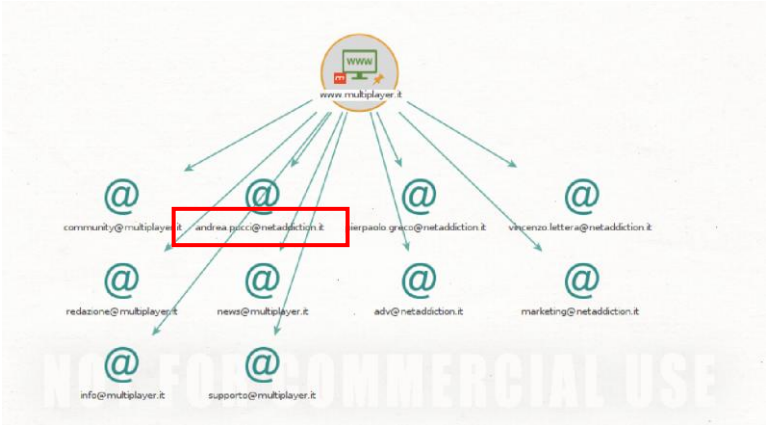

Figura 4

Vado poi ad avviare la trasformata "***Transform To IP Address [DNS]***", da qui avremo l' ip del dominio **152.228.202.195**. **Figura 5**

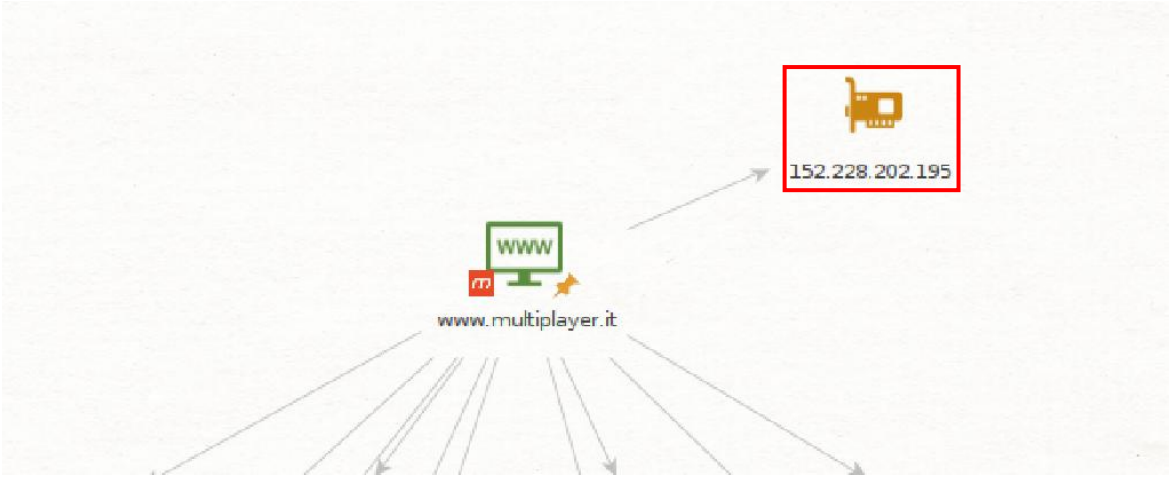

Figura 5

In base alle info raccolte quindi sappiamo che il dominio www.multiplayer.it fa riferimento all' azienda NETADDICTION SRL, azienda che produce contenuti di intrattenimento per il web da piu di 20 anni, con sede legale in Via Piave 51, Terni. Il responsabile del dominio è Andrea Pucci con indirizzo email: andreapucci@netaddiction.it, il dominio è stato registrato del 1999 e contiene al suo interno una serie di sottodomini tutti inerenti il mondo videoludico in ambito recensionistico.