W10D1 - Pratica (2)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:

Nell’esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un **target a scelta**.

Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:

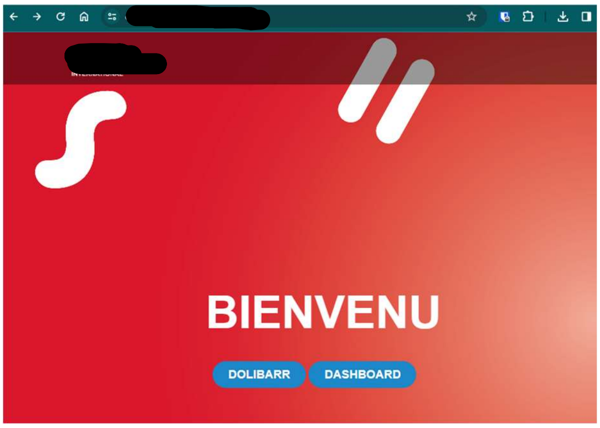
Google, per la raccolta passiva delle info
dmirty
Recon-ng
Maltego

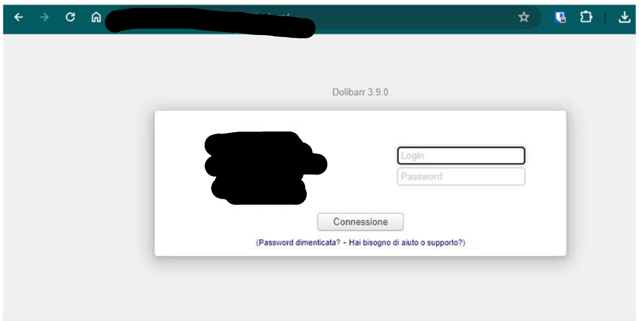
Ricerca con Google:

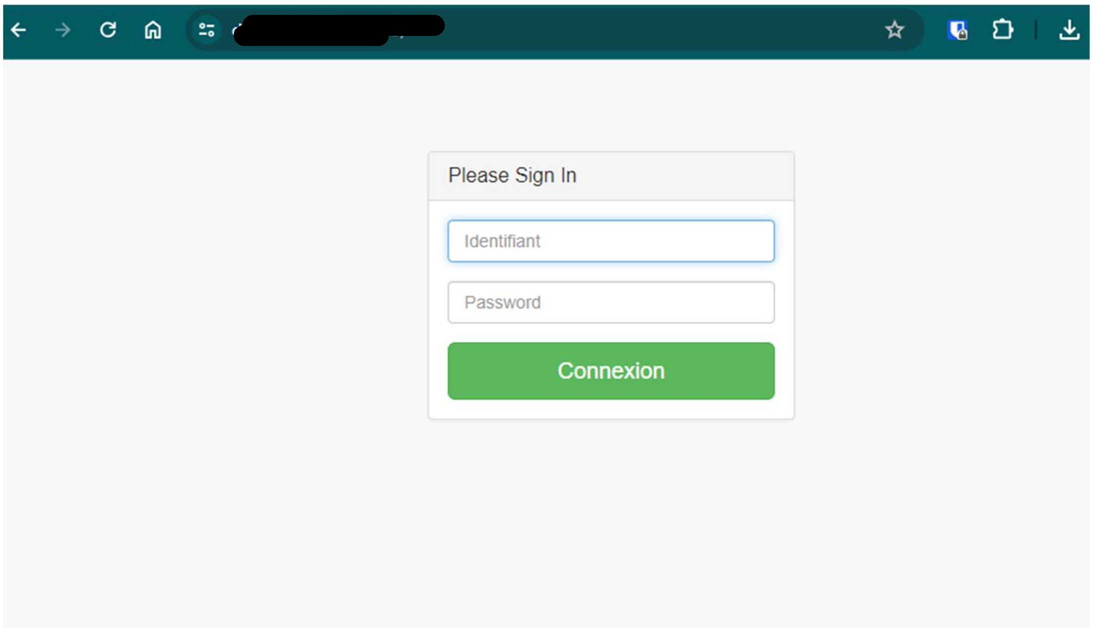
site[redacted]intitle:"Index"

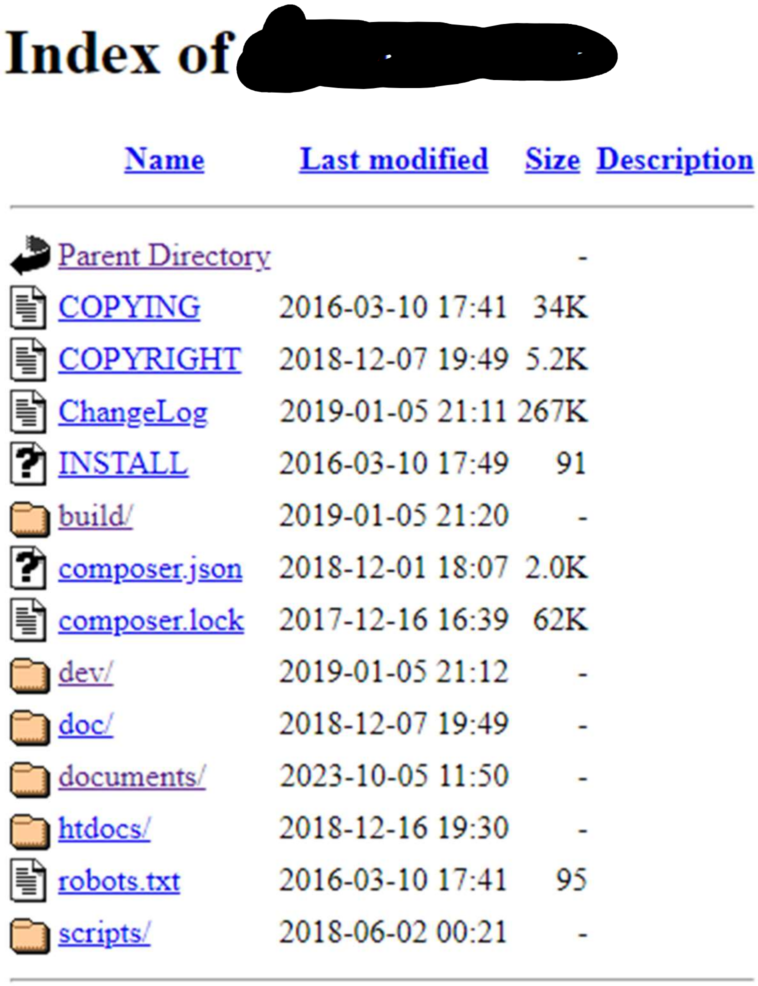
https://[redacted]n/

Esecuzione:





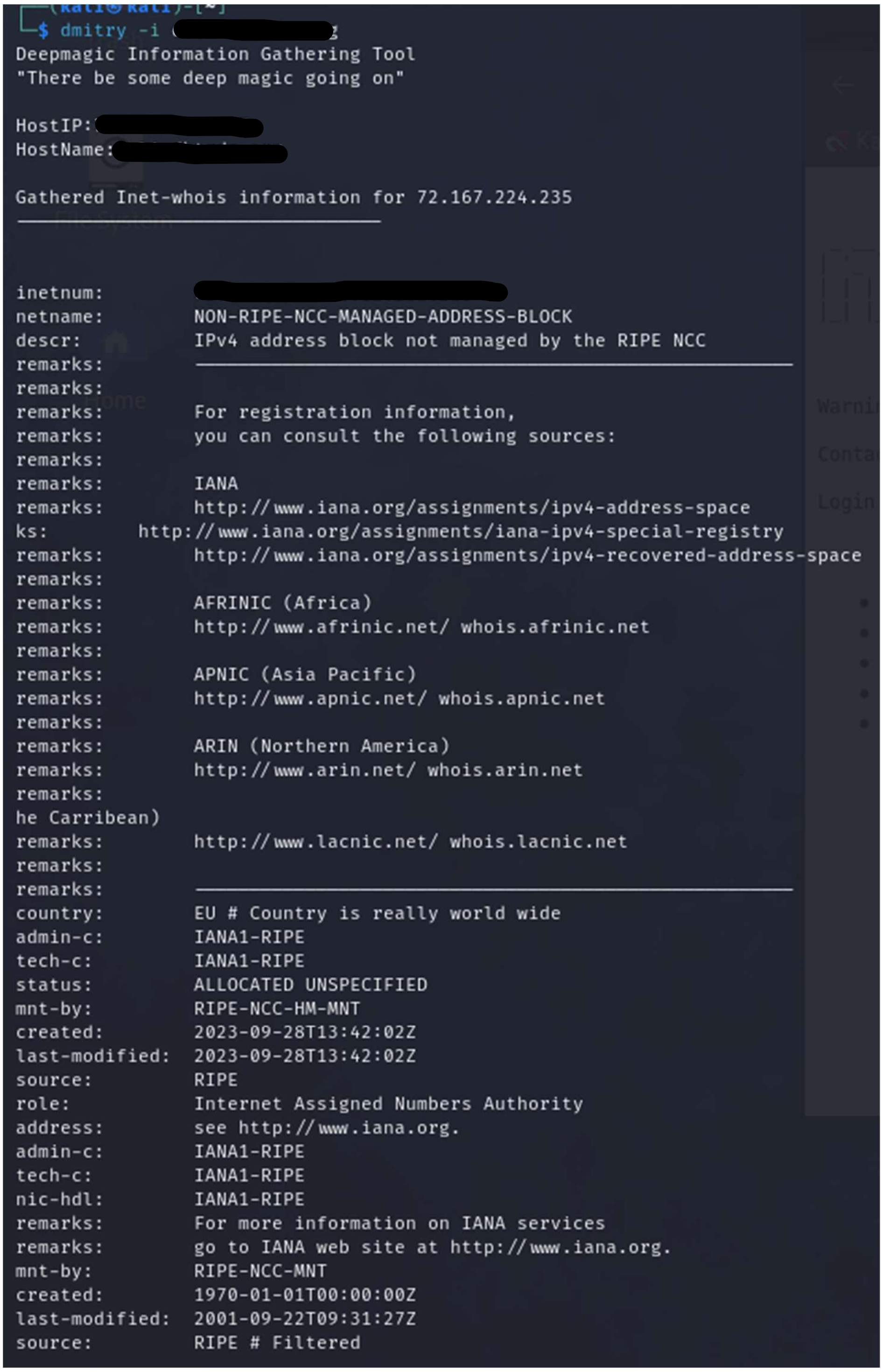




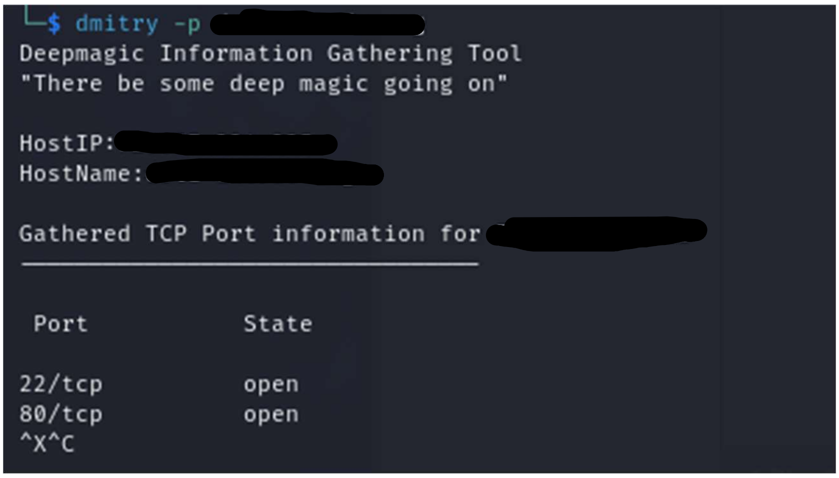
Index of [redacted]

Name	Last modified	Size	Description
Parent Directory		-	
COPYING	2016-03-10 17:41	34K	
COPYRIGHT	2018-12-07 19:49	5.2K	
ChangeLog	2019-01-05 21:11	267K	
INSTALL	2016-03-10 17:49	91	
build/	2019-01-05 21:20	-	
composer.json	2018-12-01 18:07	2.0K	
composer.lock	2017-12-16 16:39	62K	
dev/	2019-01-05 21:12	-	
doc/	2018-12-07 19:49	-	
documents/	2023-10-05 11:50	-	
htdocs/	2018-12-16 19:30	-	
robots.txt	2016-03-10 17:41	95	
scripts/	2018-06-02 00:21	-	

```
──(kali㉿kali)-[~]
└─$ sudo nmap -sS [redacted]
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 16:34 EST
Nmap scan report for [redacted]host.secureserver.net [redacted])
Host is up (0.043s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
5060/tcp open  sip
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
```



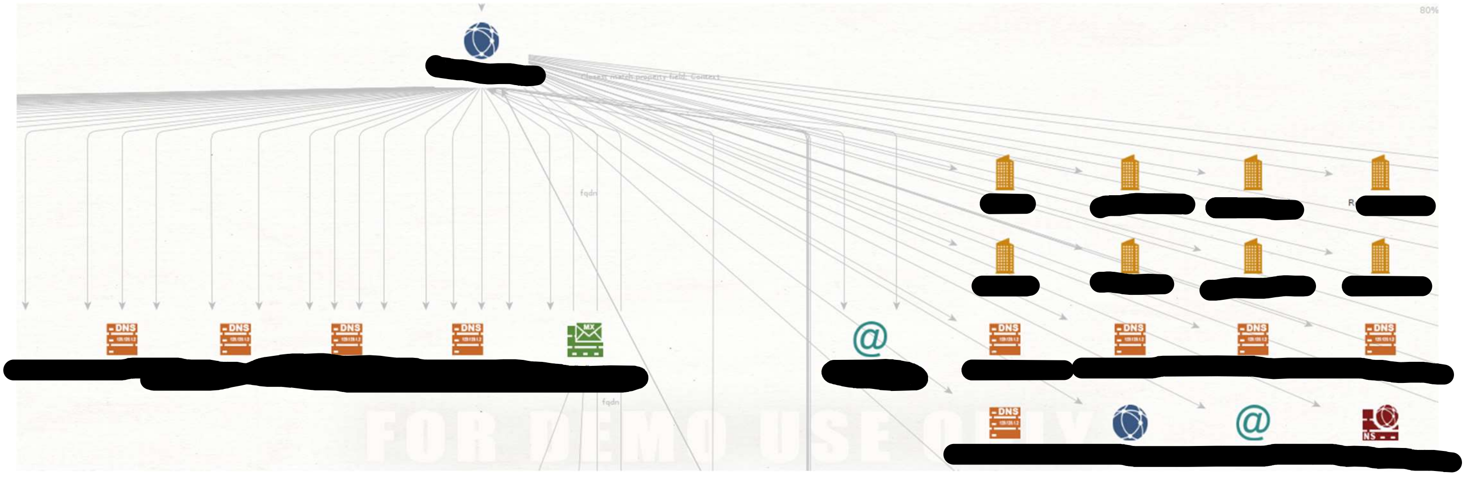
```
└─$ dmitry -i [redacted]
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:[redacted]
HostName:[redacted]

Gathered Inet-whois information for 72.167.224.235
─────────────────────────────────


inetnum:        [redacted]
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ──────────────────────────────────────────────────────
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
ks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
he Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ──────────────────────────────────────────────────────
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2023-09-28T13:42:02Z
last-modified:  2023-09-28T13:42:02Z
source:         RIPE
role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered
```



```
└─$ dmitry -p [redacted]
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:[redacted]
HostName:[redacted]

Gathered TCP Port information for [redacted]
─────────────────────────────────

 Port           State

22/tcp          open
80/tcp          open
^X^C
```

-La ricerca con Recon-ng non ha prodotto nessun risultato.

-Risultato ricerca con Maltego:



Cybersecurity Analyst 2023