Attacker report

Ethical Hacking

Matteo Bianchi

Vito Stefano Gozzo

Michele Bungaro

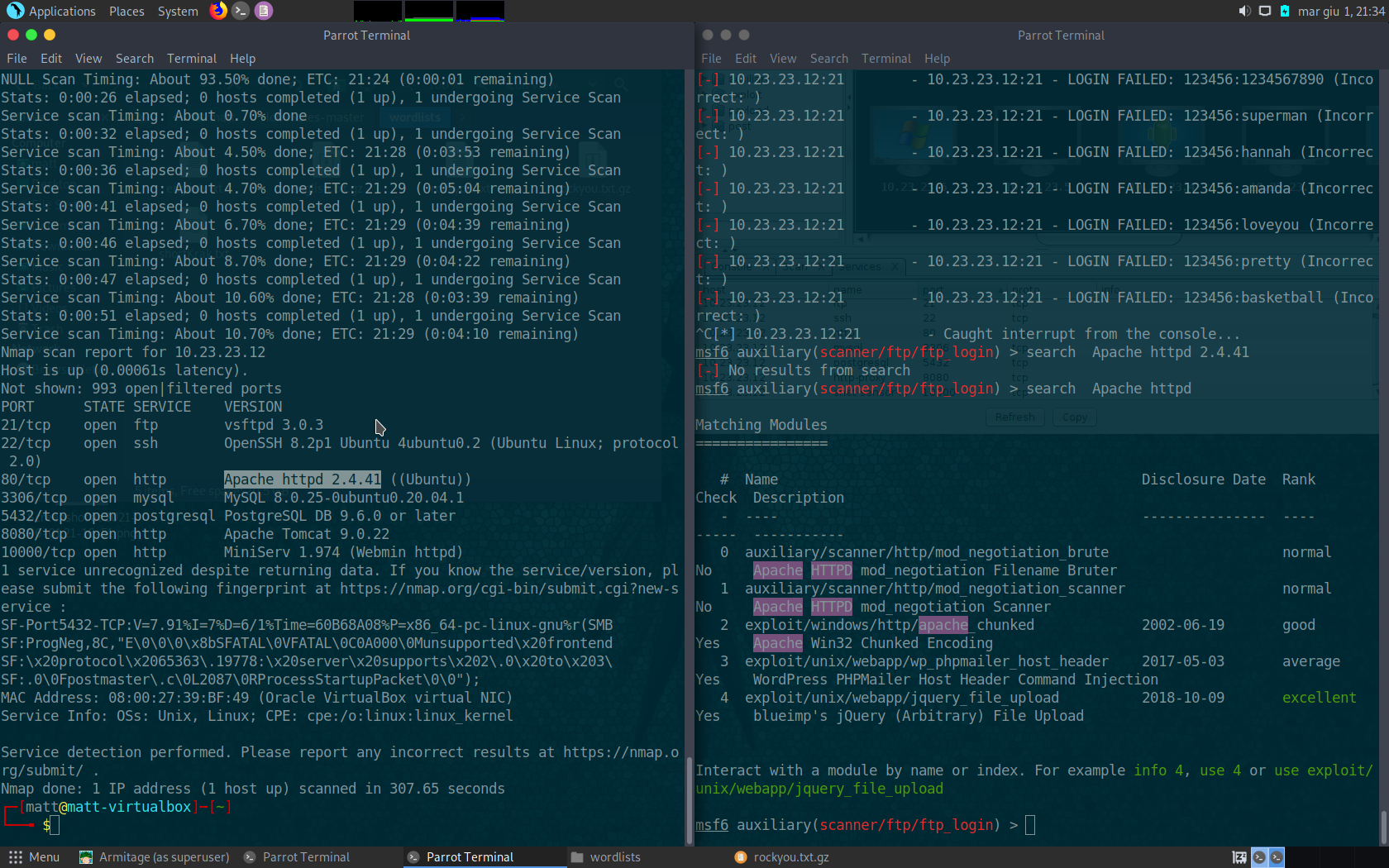
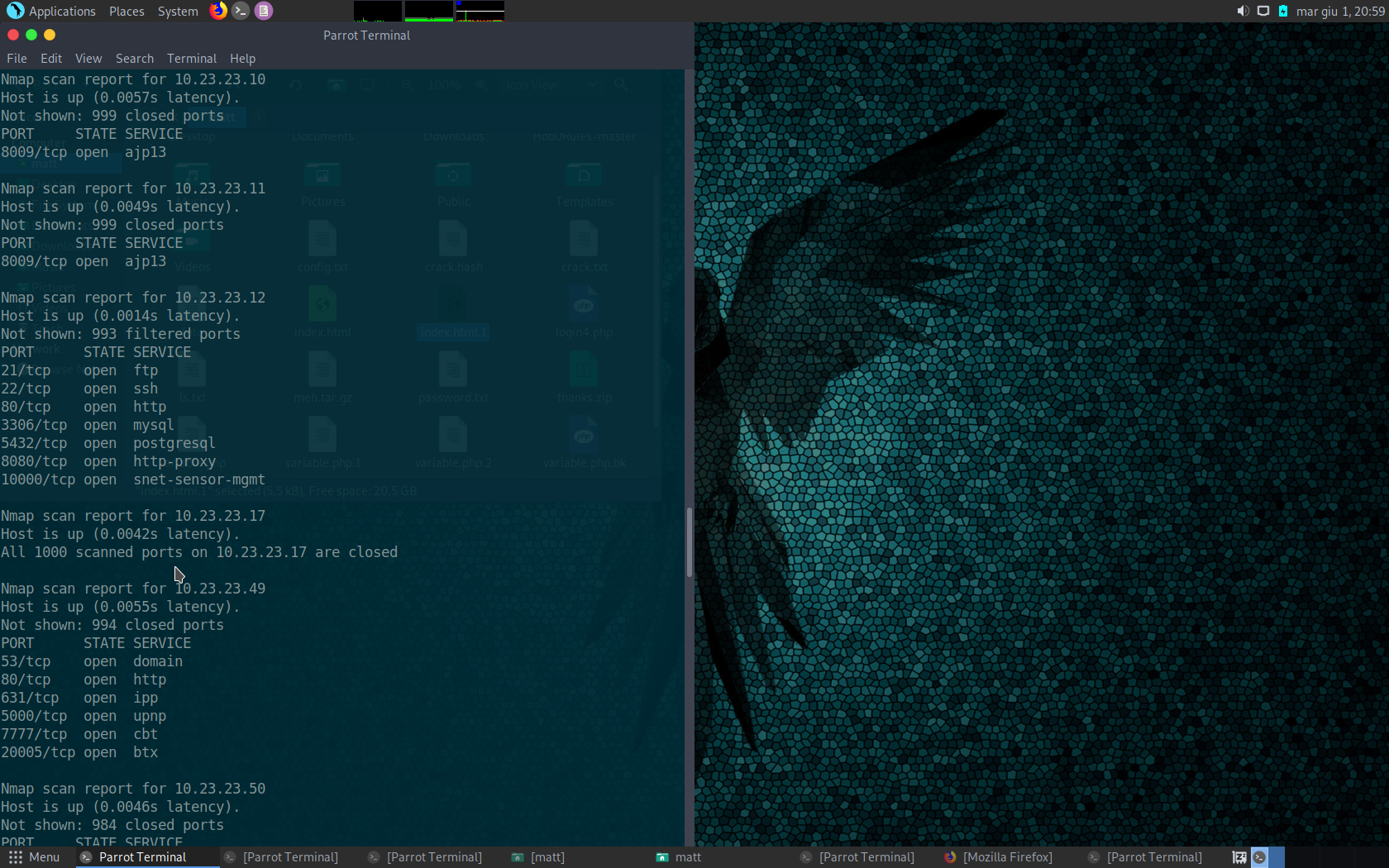
June 20, 2021

In this document we will describe the method used to analyze the VM and the steps that allow us to exploit its vulnerabilities.

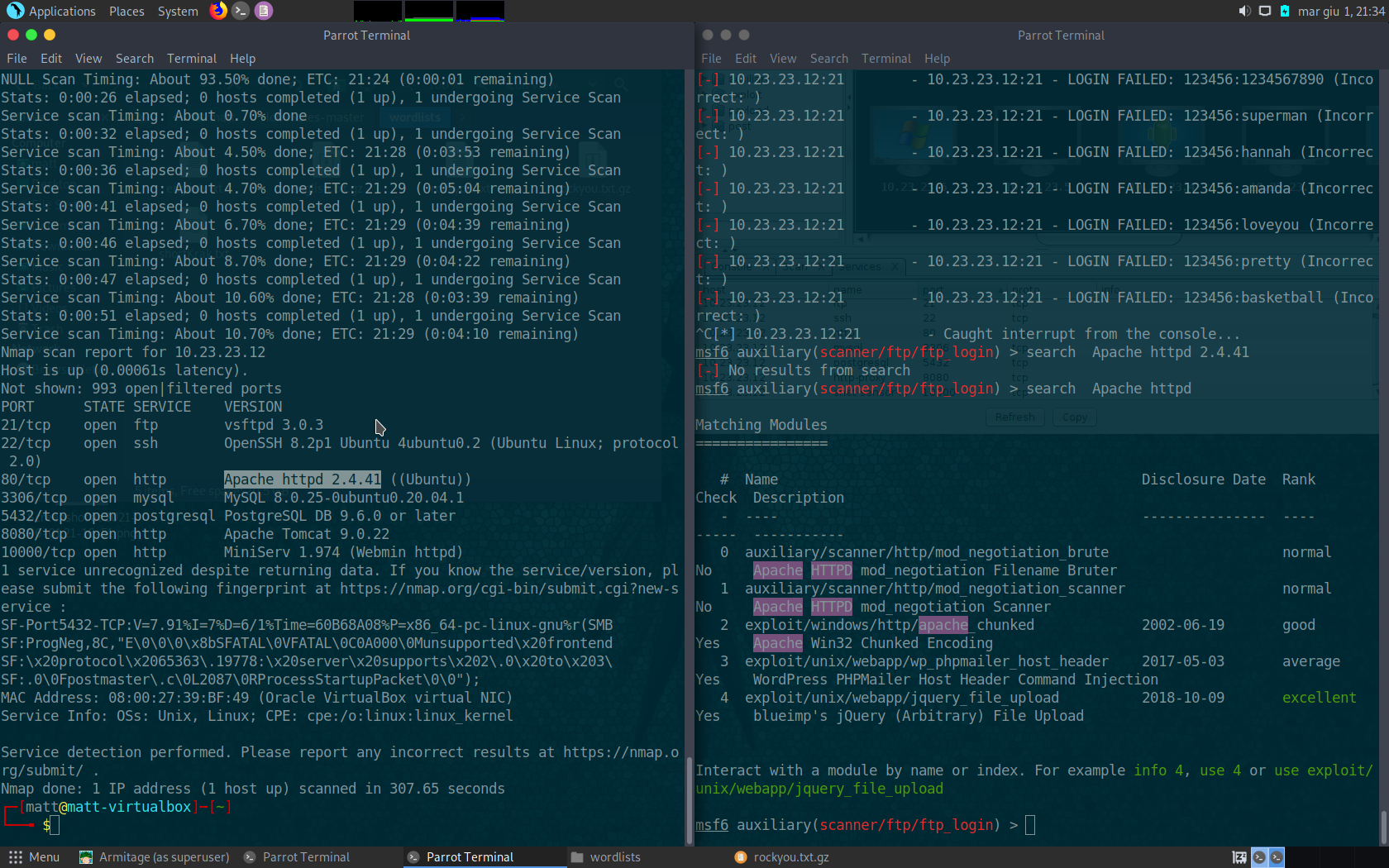
# Host Discovery and Service Scanning

We made the VM as a network subnet host, setting the network card in bridged mode.

Then we proceed to scan the active hosts in subnet in order to obtain info:



Thank to nmap scan we obtained IP address of the host and its open ports of active services.



As we can see there are 7 active services with its version running on the host with open ports:

* ftp, 21
* ssh,22
* http, 80
* mysql, 3306
* postgresql, 5432
* http-proxy, 8080
* snet-sensor-mgmt (Webmin httpd), 10000

# Vulnerabilities

## Local access

### Postgresql

We use a Metasploit module (multi/postgres/postgres\_copy\_from\_program\_cmd\_exec) passing as payload “cmd/unix/reverse\_perl/ and setting metasploit like:

Immagine che contiene testo, monitor, computer, screenshot

Descrizione generata automaticamente

Using it we obtained a reverse PERL TCP postgres shell of postgres user.

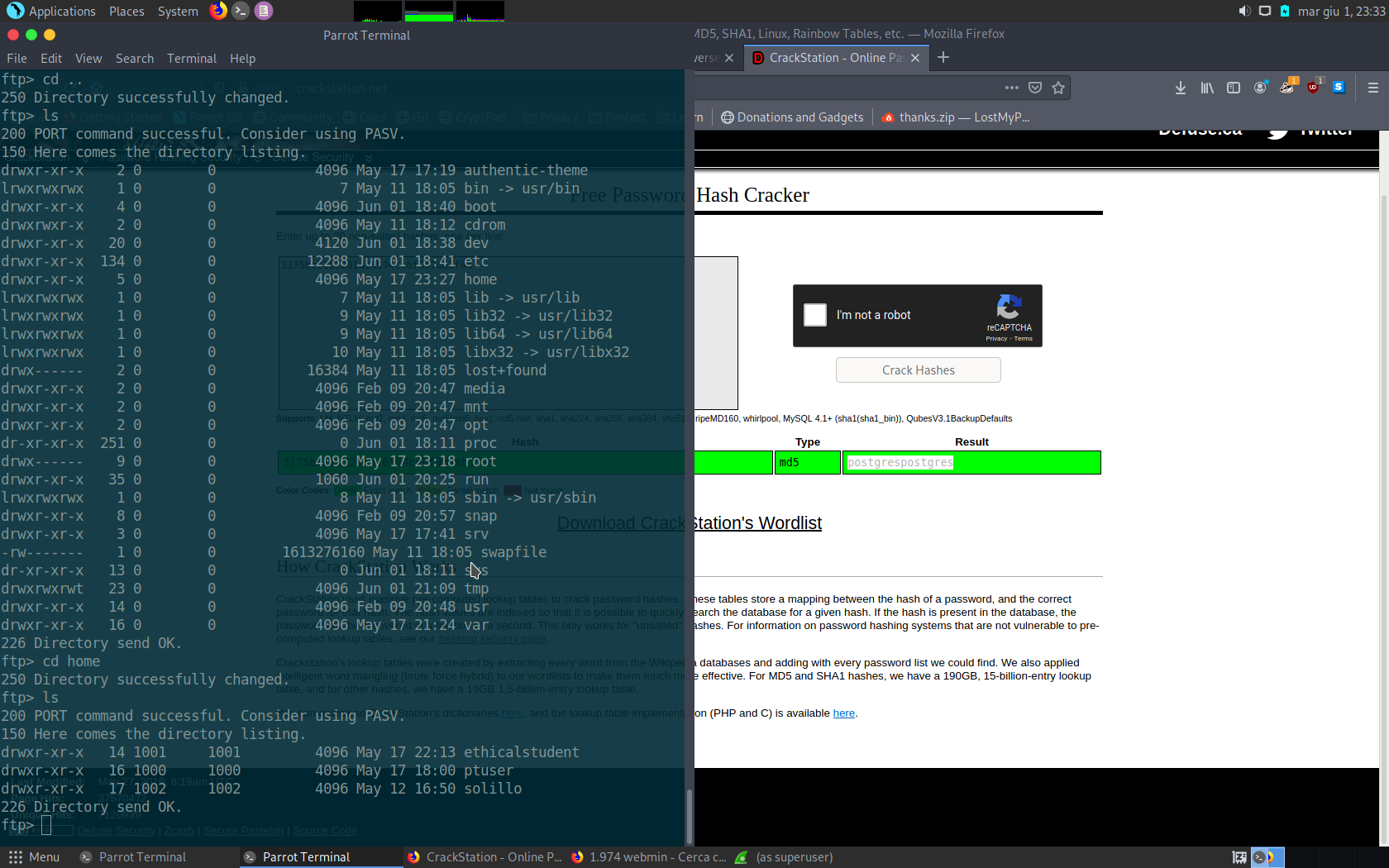
Immagine che contiene testo, monitor, interni, scrivania

Descrizione generata automaticamente

Using postgres user on ftp, moving between directories we discovered the “home/x” folder of other users:

* ethicalstudent
* solillo
* ptuser

Immagine che contiene testo

Descrizione generata automaticamente x

### Mysql

# Privileges Escalation

Crontab