X60 - Lorenzo Santambrogio

Report Esame

Immagine che contiene Elementi grafici, design

Descrizione generata automaticamente

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 Metasplotable1 o facilitare attacchi contro Metaploitable1. 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 Metasplotable1. Eventuali modifiche apportate all'ambiente durante il periodo di test potrebbero influire sui risultati della valutazione.

**Indice**

[**SINTESI**](#_heading=h.2et92p0) **ESECUTIVA [3](#_heading=h.2et92p0)**

[Raccomandazione](#_heading=h.tyjcwt) [4](#_heading=h.1ksv4uv)

[**Metodologia**](#_heading=h.3dy6vkm) **di test**

mappatura versione servizi

accesso alla macchina [6](#_heading=h.44sinio)

altro **Errore. Il segnalibro non è definito.**[**Definizioni**](#_heading=h.1t3h5sf) **di classificazione [8](#_heading=h.1t3h5sf)**

[classificazioni](#_heading=h.4d34og8) del rischio [8](#_heading=h.4d34og8)

Classificazioni della probabilità di sfruttamento [8](#_heading=h.2jxsxqh)

Classificazioni dell'impatto aziendale [9](#_heading=h.z337ya)

Classificazioni della difficoltà di rimedio [9](#_heading=h.3j2qqm3)

[**Risultati**](#_heading=h.1y810tw) del penetration test **[10](#_heading=h.1y810tw)**

[**Appendice**](#_heading=h.4i7ojhp) **A - strumenti utilizzati [13](#_heading=h.4i7ojhp)**

[**appendice**](#_heading=h.17dp8vu) **B - informazioni sull'incarico**  **[14](#_heading=h.17dp8vu)**

[informazioni](#_heading=h.3rdcrjn) sul cliente **Errore. Il segnalibro non è definito.**

# 

# **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.

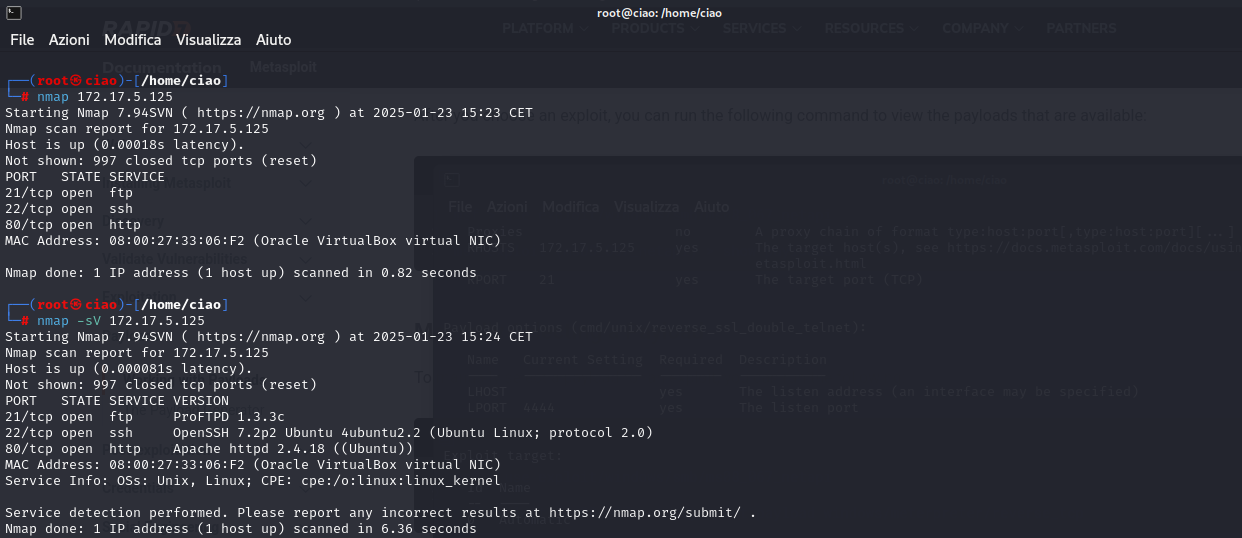
# Durante la fase di ricognizione, abbiamo raccolto informazioni sulla macchina Esame-Nevio. X60 ha utilizzato scansioni delle porte e altri metodi di enumerazione per affinare le informazioni sugli obiettivi e valutare il loro valore.

# 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



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

Immagine che contiene testo, schermata

Descrizione generata automaticamente

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

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

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.

