Analisi di vulnerabilità con Nessus

S5L3

Cosa ho fatto in questa attività

In questo esercizio ho usato Nessus per cercare problemi di sicurezza su una macchina chiamata "Metasploitable". Era una macchina volutamente vulnerabile, utile per fare pratica.

Verifica della rete

Prima di iniziare la scansione, ho controllato che le due macchine riuscissero a comunicare tra loro tramite il comando "ping". Se non si vedono in rete, la scansione non può partire.

Impostazioni in Nessus

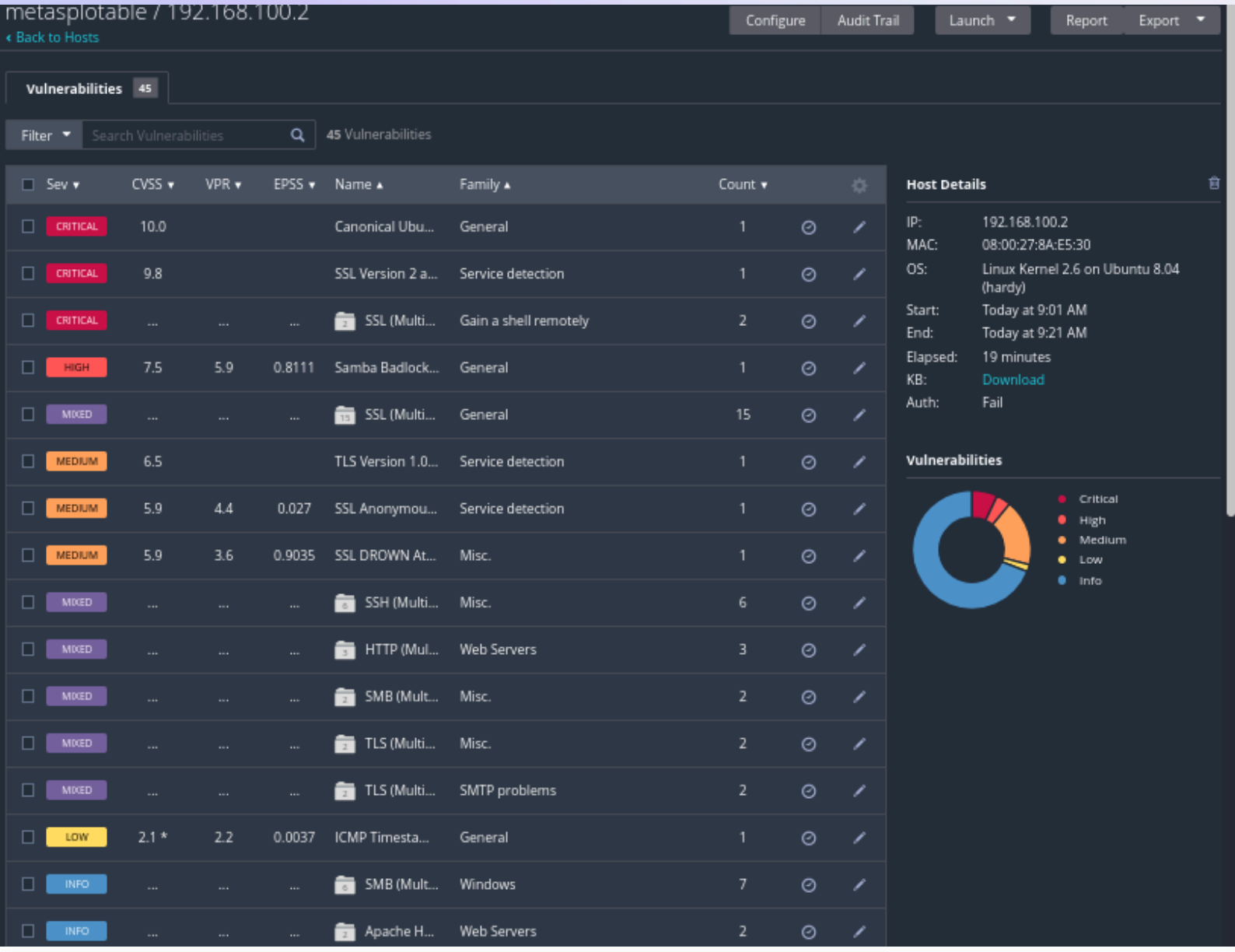
Ho creato una nuova scansione con queste impostazioni:

- Inserito l'indirizzo IP 192.168.100.2
- Porte indicate dal professore
- Brute force attivo
- Scansione UDP abilitata

Vulnerabilità rilevate

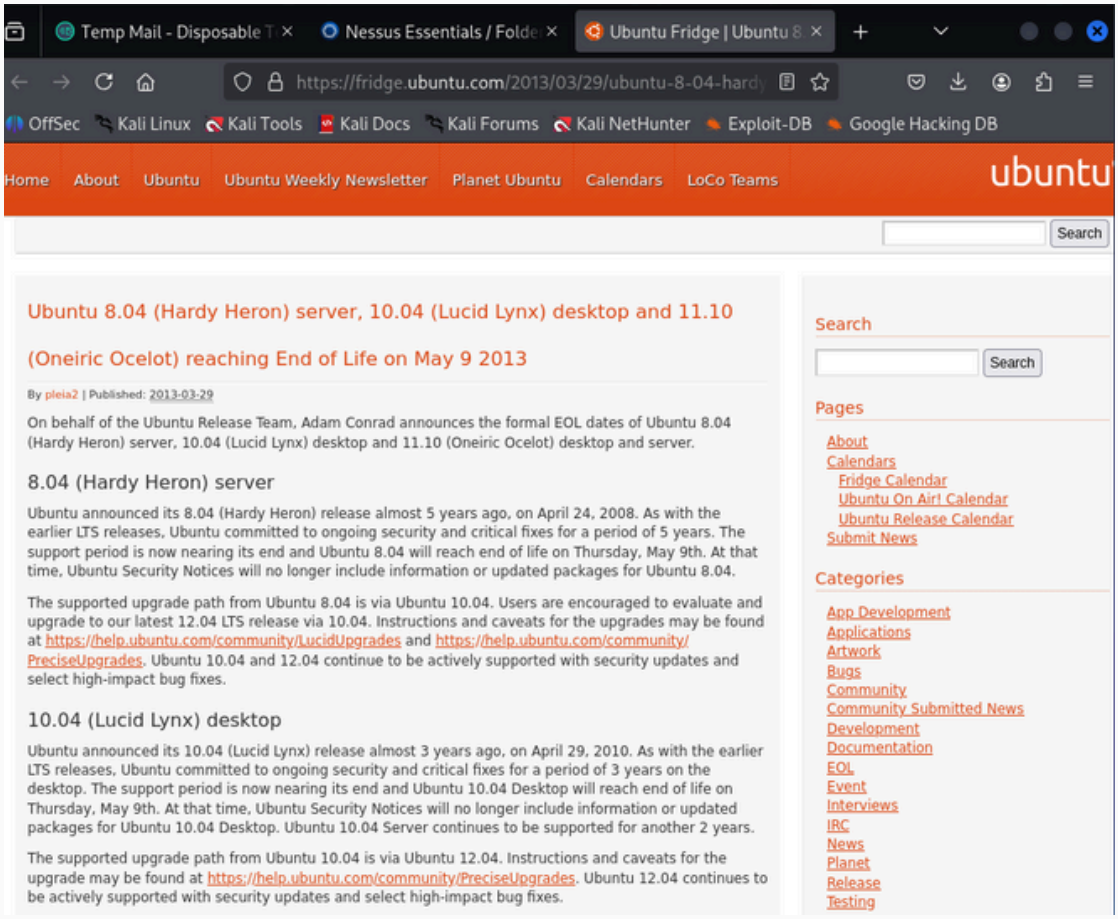
Dopo aver atteso 20 minuti circa, mi ha riscontrato diverse vulnerabilità, ne elenco alcune

1. Sistema operativo vecchio e non aggiornato (Ubuntu 8.04)
2. Protocolli SSL obsoleti e insicuri
3. Algoritmi di cifratura deboli
4. Servizi HTTP e SMB esposti



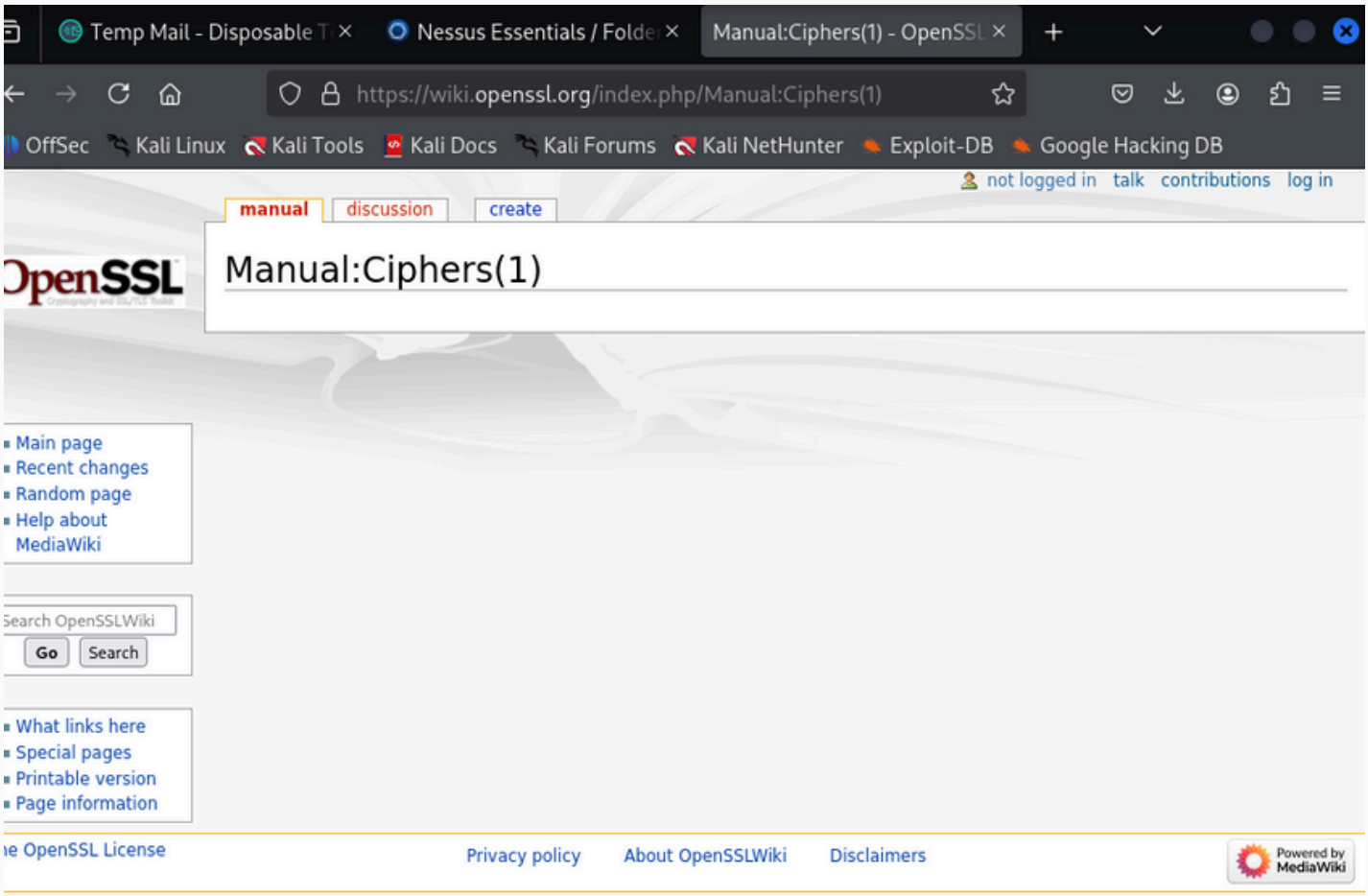
Vulnerabilità 1

La macchina usa Ubuntu 8.04, una versione non più aggiornata dal 2013. Questo la rende vulnerabile, perché non riceve patch di sicurezza.



Vulnerabilità 2

Nessus ha rilevato l'utilizzo di protocolli vecchi come SSLv2 e cipher "anonimi", che rendono facile per un attaccante intercettare i dati.



Approfondimenti

Per capire meglio le vulnerabilità, ho cercato informazioni su siti ufficiali come Ubuntu, OpenSSL e Microsoft.

[USN-605-1] Thunderbird vulnerabilities

Jamie Strandboge jamie at canonical.com
Tue May 6 19:26:11 UTC 2008

- Previous message (by thread): [USN-608-1] KDE vulnerability
- Next message (by thread): [USN-609-1] OpenOffice.org vulnerabilities
- **Messages sorted by:** [date] [thread] [subject] [author]

```
===========================================================
Ubuntu Security Notice USN-605-1              May 06, 2008
mozilla-thunderbird, thunderbird vulnerabilities
CVE-2008-1233, CVE-2008-1234, CVE-2008-1235, CVE-2008-1236,
CVE-2008-1237
===========================================================

A security issue affects the following Ubuntu releases:

Ubuntu 6.06 LTS
Ubuntu 7.04
Ubuntu 7.10
Ubuntu 8.04 LTS

This advisory also applies to the corresponding versions of
Kubuntu, Edubuntu, and Xubuntu.

The problem can be corrected by upgrading your system to the
following package versions:

Ubuntu 6.06 LTS:
  mozilla-thunderbird             1.5.0.13+1.5.0.15~prepatch080417a-0ubuntu0.6.06.1

Ubuntu 7.04:
  mozilla-thunderbird             1.5.0.13+1.5.0.15~prepatch080417a-0ubuntu0.7.04.1

Ubuntu 7.10:
  thunderbird                     2.0.0.14+nobinonly-0ubuntu0.7.10.0

Ubuntu 8.04 LTS:
  thunderbird                     2.0.0.14+nobinonly-0ubuntu0.8.04.1

After a standard system upgrade you need to restart Thunderbird to effect
the necessary changes.

Details follow:
```

Conclusioni

Con questo esercizio ho imparato tante cose interessanti come:

- A creare e lanciare una scansione con Nessus
- A leggere un report di sicurezza
- A riconoscere vulnerabilità comuni