

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

metasploitable / 192.168.100.2

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Hosts](#)

Vulnerabilities 45						
Filter	Search Vulnerabilities					45 Vulnerabilities
Sev	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0			Canonical Ubu...	General	1
Critical	9.8			SSL Version 2 a...	Service detection	1
Critical	SSL (Multi...)	Gain a shell remotely	2
High	7.5	5.9	0.8111	Samba Badlock...	General	1
Mixed	SSL (Multi...)	General	15
Medium	6.5			TLS Version 1.0...	Service detection	1
Medium	5.9	4.4	0.027	SSL Anonymou...	Service detection	1
Medium	5.9	3.6	0.9035	SSL DROWN At...	Misc.	1
Mixed	SSH (Multi...)	Misc.	6
Mixed	HTTP (Mul...	Web Servers	3
Mixed	SMB (Mult...	Misc.	2
Mixed	TLS (Multi...)	Misc.	2
Mixed	TLS (Multi...)	SMTP problems	2
Low	2.1 *	2.2	0.0037	ICMP Timesta...	General	1
Info	SMB (Mult...	Windows	7
Info	Apache H...	Web Servers	2

Host Details

IP: 192.168.100.2
MAC: 08:00:27:8A:E5:30
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 9:01 AM
End: Today at 9:21 AM
Elapsed: 19 minutes
KB: Download
Auth: Fail

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

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.

The screenshot shows a web browser window with three tabs open: 'Temp Mail - Disposable T...', 'Nessus Essentials / Folde...', and 'Ubuntu Fridge | Ubuntu 8.x'. The active tab is 'Ubuntu Fridge | Ubuntu 8.x' at the URL <https://fridge.ubuntu.com/2013/03/29/ubuntu-8-04-hardy-heron-reaching-end-of-life-on-may-9-2013/>. The page content discusses the end of life for Ubuntu 8.04 (Hardy Heron) server and 10.04 (Lucid Lynx) desktop. It mentions that support ends on May 9, 2013. The page footer includes links to various Ubuntu resources like OffSec, Kali Linux, and Planet Ubuntu. The right sidebar contains search and navigation sections for the website.

Ubuntu 8.04 (Hardy Heron) server, 10.04 (Lucid Lynx) desktop and 11.10 (Oneiric Ocelot) reaching End of Life on May 9 2013

By pleia2 | Published: 2013-03-29

On behalf of the Ubuntu Release Team, Adam Conrad announces the formal EOL dates of Ubuntu 8.04 (Hardy Heron) server, 10.04 (Lucid Lynx) desktop and 11.10 (Oneiric Ocelot) desktop and server.

8.04 (Hardy Heron) server

Ubuntu announced its 8.04 (Hardy Heron) release almost 5 years ago, on April 24, 2008. As with the earlier LTS releases, Ubuntu committed to ongoing security and critical fixes for a period of 5 years. The support period is now nearing its end and Ubuntu 8.04 will reach end of life on Thursday, May 9th. At that time, Ubuntu Security Notices will no longer include information or updated packages for Ubuntu 8.04.

The supported upgrade path from Ubuntu 8.04 is via Ubuntu 10.04. Users are encouraged to evaluate and upgrade to our latest 12.04 LTS release via 10.04. Instructions and caveats for the upgrades may be found at <https://help.ubuntu.com/community/LucidUpgrades> and <https://help.ubuntu.com/community/PreciseUpgrades>. Ubuntu 10.04 and 12.04 continue to be actively supported with security updates and select high-impact bug fixes.

10.04 (Lucid Lynx) desktop

Ubuntu announced its 10.04 (Lucid Lynx) release almost 3 years ago, on April 29, 2010. As with the earlier LTS releases, Ubuntu committed to ongoing security and critical fixes for a period of 3 years on the desktop. The support period is now nearing its end and Ubuntu 10.04 Desktop will reach end of life on Thursday, May 9th. At that time, Ubuntu Security Notices will no longer include information or updated packages for Ubuntu 10.04 Desktop. Ubuntu 10.04 Server continues to be supported for another 2 years.

The supported upgrade path from Ubuntu 10.04 is via Ubuntu 12.04. Instructions and caveats for the upgrade may be found at <https://help.ubuntu.com/community/PreciseUpgrades>. Ubuntu 12.04 continues to be actively supported with security updates and select high-impact bug fixes.

Vulnerabilità 2

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

The screenshot shows a web browser window with the following details:

- Tab Bar:** Temp Mail - Disposable T X, Nessus Essentials / Folder X, Manual:Ciphers(1) - OpenSSL X
- Address Bar:** https://wiki.openssl.org/index.php/Manual:Ciphers(1)
- Page Content:** The main content area displays the OpenSSL Wiki page titled "Manual:Ciphers(1)". It includes a navigation bar with "manual" selected, and sections on "TLS Ciphers", "SSL Ciphers", and "TLS 1.3 Ciphers".
- Sidebar:** A sidebar on the left contains links to "Main page", "Recent changes", "Random page", "Help about MediaWiki", and a search bar with "Search OpenSSLWiki" and "Go" buttons.
- Footer:** The footer includes links to "OpenSSL License", "Privacy policy", "About OpenSSLWiki", "Disclaimers", and a "Powered by MediaWiki" logo.

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@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