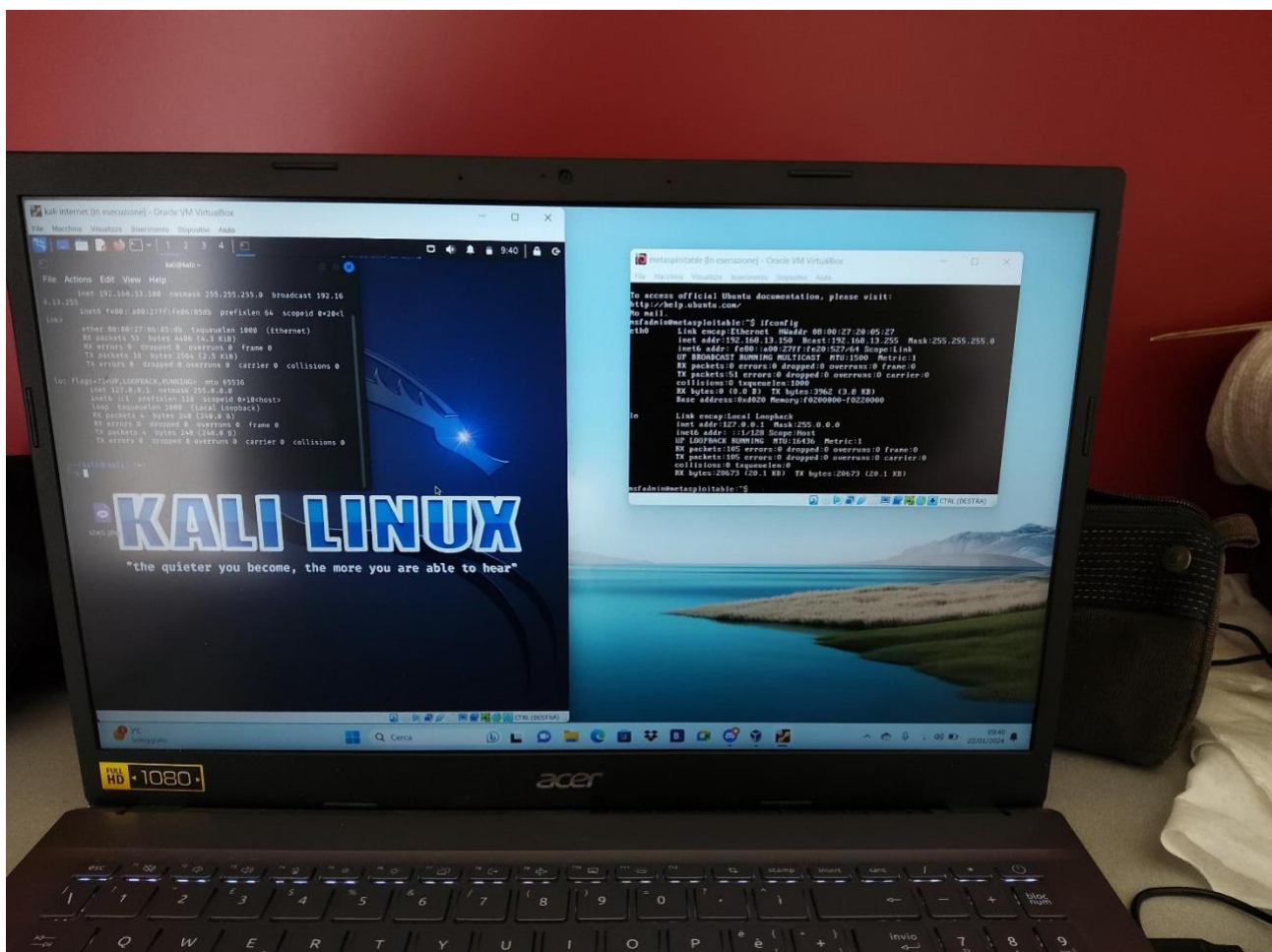


# Scansione delle vulnerabilità sulla macchina e Implementazione delle soluzioni

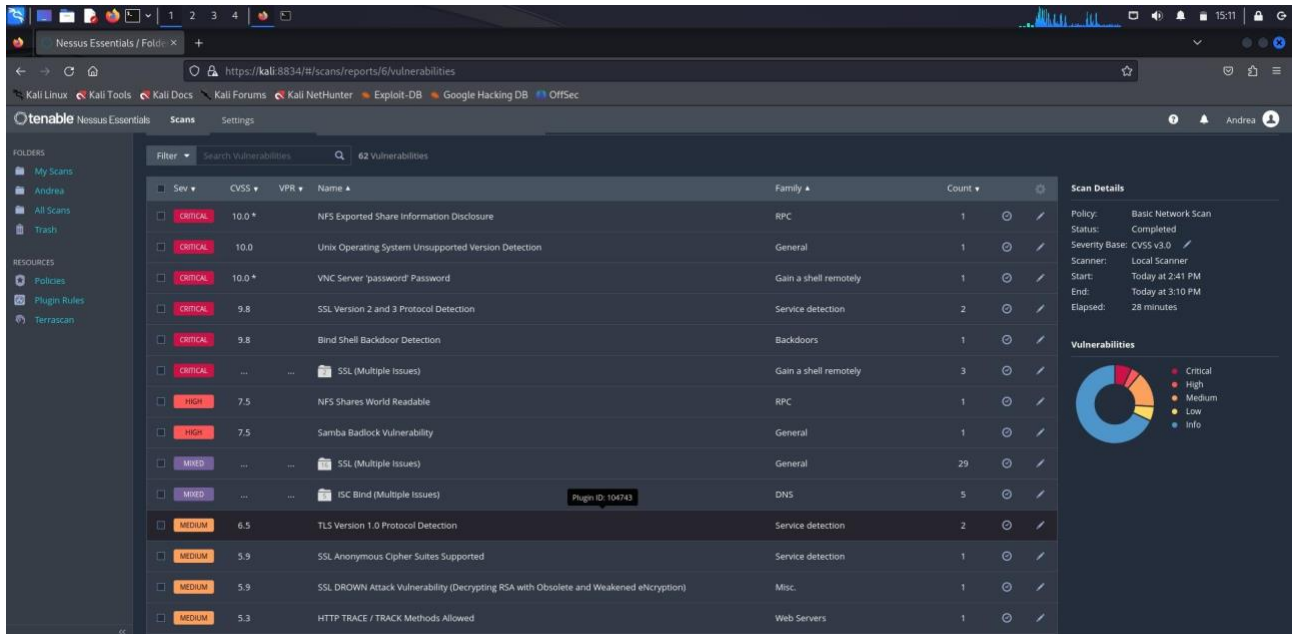
Il progetto di questa settimana ci chiederà di effettuare una scansione completa sul target Metasploitable per poi scegliere da un minimo di due vulnerabilità critiche / high e provare ad implementare delle azioni di rimedio.

Come prima azione bisogna collegare le macchine kali e Metasploitable in modo da effettuare la scansione tramite il Nessus, per effettuare il collegamento utilizzeremo il comando “Ping” seguito dalla indirizzo IP dell'altra macchina.



Una volta collegate le due macchine azioniamo il Nessus tramite il comando “sudo systemctl start nessusd.service” in seguito accediamo alle sue funzioni tramite l’indirizzo “https://kali:8834”.

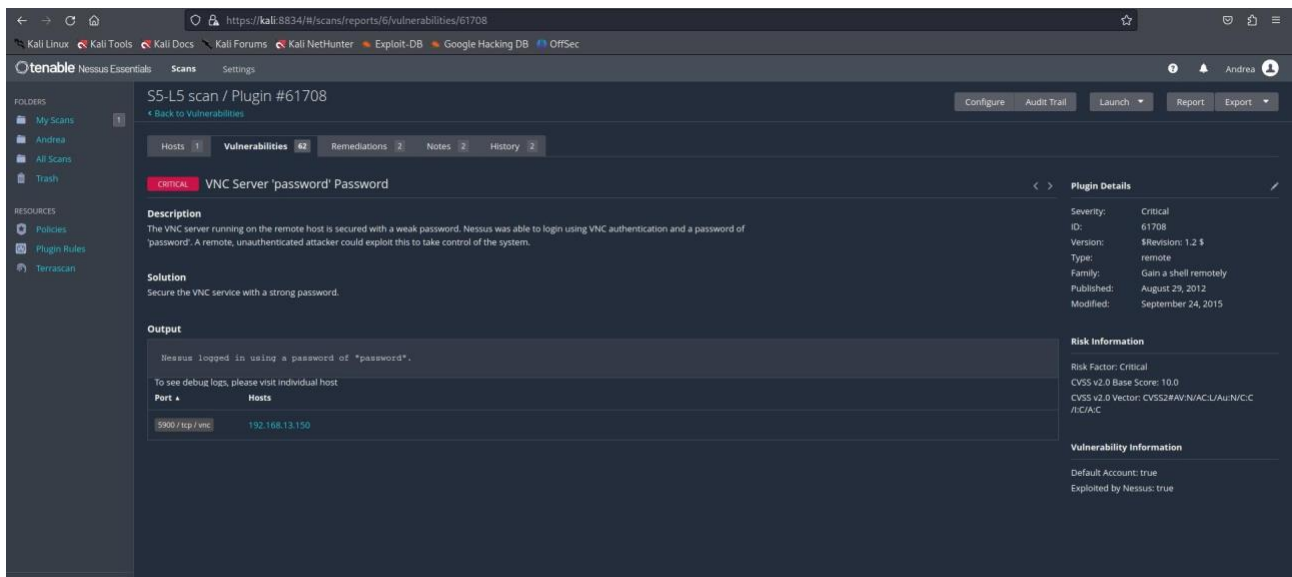
Una volta avviata la scansione ci apparirà una schermata con tutte le vulnerabilità presenti sulla macchina Metasploitable.



Le vulnerabilità che prenderemo in considerazione ai fini dell’esercizio sono due:

- VNC Server “password” Password (Critical Vulnerability)
- Samba Badlock Vulnerability (high Vulnerability)

Cliccando sulle vulnerabilità in questione possiamo capire come risolvere il problema in particolare per il VNC Server “password” Password il Vulnerability scanner mostra come sia troppo semplice accedere al server da remoto in quanto la password: “Password” è troppo banale e rende il sistema vulnerabile ad attacchi di potenziali malintenzionati



Infine per il Samba Badlock Vulnerability il Nessus ci mostra come sia troppo obsoleto e che ormai esistono versioni più recenti e sicure dello stesso, infatti, una fragilità in questo campo permetterebbe una più facile penetrazione da parte di attacchi Man in the middle.

The screenshot displays the Tenable Nessus interface for a scan titled "S5-L5 scan / Plugin #90509". The left sidebar shows a navigation menu with "FOLDERS" (My Scans, Andrea, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). The main content area is titled "S5-L5 scan / Plugin #90509" and includes tabs for "Hosts", "Vulnerabilities", "Remediations", "Notes", and "History". The "Vulnerabilities" tab is active, showing a "HIGH" severity vulnerability titled "Samba Badlock Vulnerability".

**Description**  
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

**Solution**  
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

**See Also**  
<http://badlock.org>  
<https://www.samba.org/samba/security/CVE-2016-2118.html>

**Output**  
Nessus detected that the Samba Badlock patch has not been applied.  
To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.13.150

**Plugin Details**

Severity:	High
ID:	90509
Version:	1.8
Type:	remote
Family:	General
Published:	April 13, 2016
Modified:	November 20, 2019

**Risk Information**

Risk Factor:	Medium
CVSS v3.0 Base Score:	7.5
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PRN/UI/R/S/UC/HA/H/SH
CVSS v3.0 Temporal Vector:	CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score:	6.5
CVSS v2.0 Base Score:	6.8
CVSS v2.0 Temporal Score:	5.0
CVSS v2.0 Vector:	CVSS2#AV:N/AC:M/Au:N/C:P/I/P/A/P
CVSS v2.0 Temporal Vector:	CVSS2#E:U/RL:O/RC:C

**Vulnerability Information**