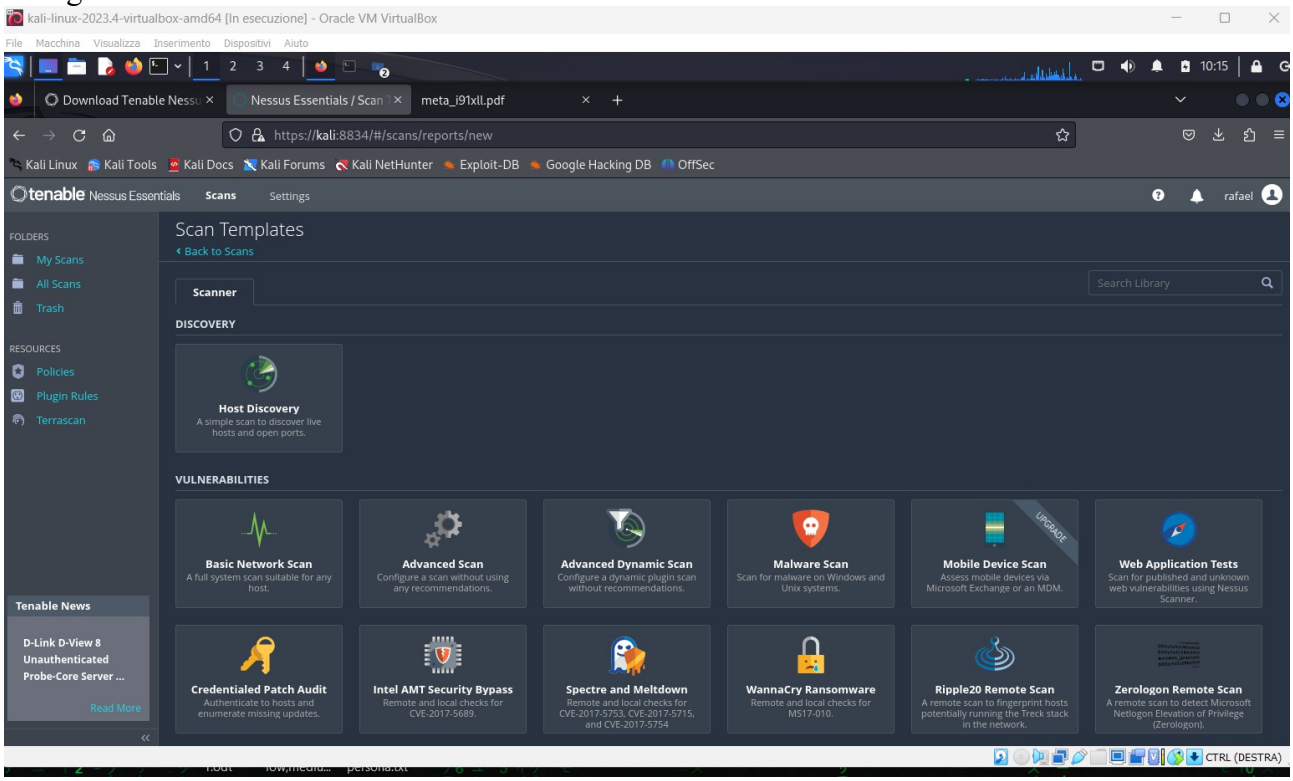
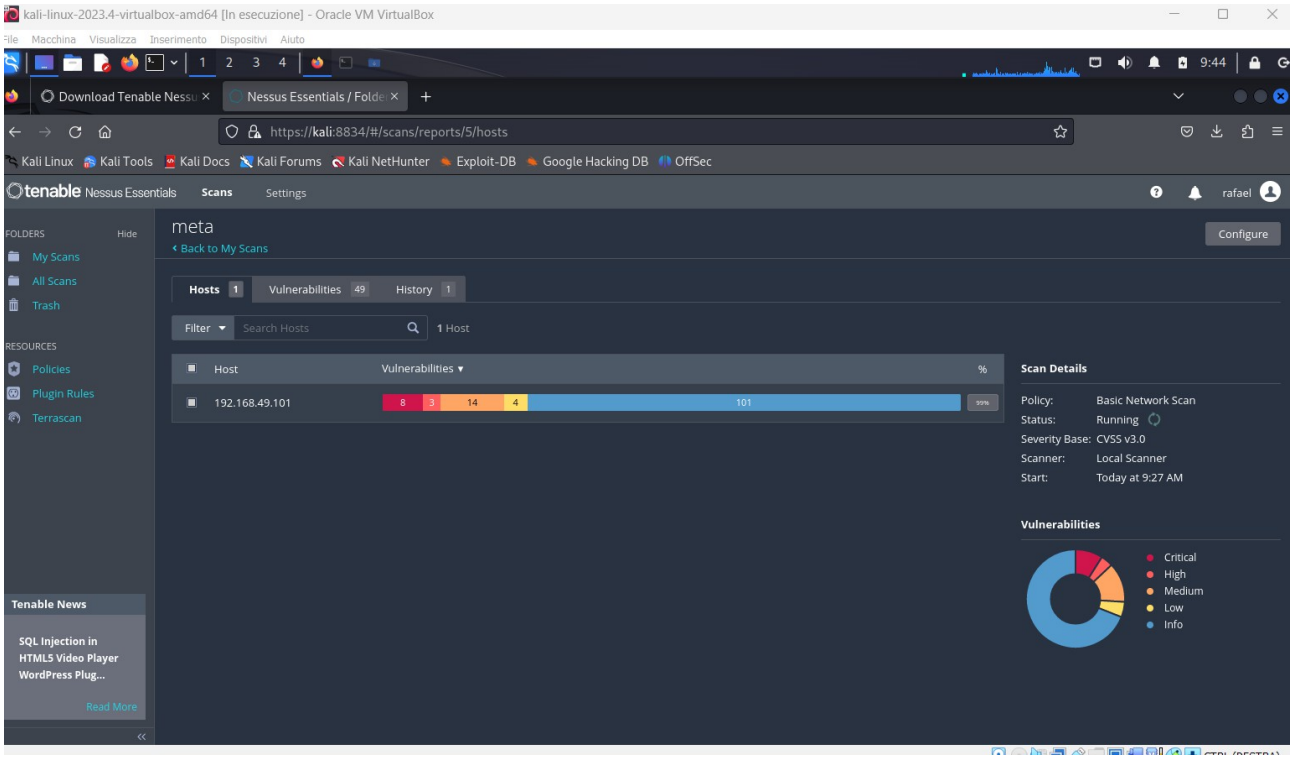
Oggi abbiamo fatto uno scan delle vulnerabilità con nessus

lo abbiamo fatto sulla macchina virtuale meta da kali.(per funzionare le macchine devono essere collegate



abbiamo impostato lo scan per l'IP di meta e abbiamo scelto una basic network scan



Nessus andrà a fare lo scan. Cominceremo a vedere le varie vulnerabilità che ci sono in metasploit. Finita la scansione non vedremo solo le vulnerabilità ma anche i livelli di criticità .con Nessus possiamo avere anche un repor delle varie vulnerabilità che possiamo scaricare in formato pdf .

192.168.49.101

0	1	6	1	7
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported

* indicates the v3.0 score was not available; the v2.0 score is shown

Come vediamo nel report delle vulnerability by host vediamo che ci sono 1 di grato alto ,6 di media vulnerabilità ,1 low è 7 info.

Nella vulnerabilità high SSL Medium Strength Cipher Suites Supported (SWEET32)

vediamo che offre un crittografia di media potenza quindi più semplice da aggirare la crittografia se l'attaccante è sulla stesa rete

la soluzione per questo problema potrebbe essere riconfigurare la crittografia senza 'uso di cifrari a media potenza .

Nella SSL Self-Signed Certificate vediamo che il plugin non controlla la presenza di catene di certificati quindi abbiamo una firma crittografica non verificabile .

Una soluzione può essere acquistare o generare una firma certificata SSL appropriato per questo servizio.

Nella SSL Cipher Block Chaining Cipher Suites Supported vediamo che ci da le informazioni L'host remoto che supporta l'uso di cifrari SSL . E ci dice che queste suite di cifratura offrono pi sicurezza rispetto alla modalità ECB .