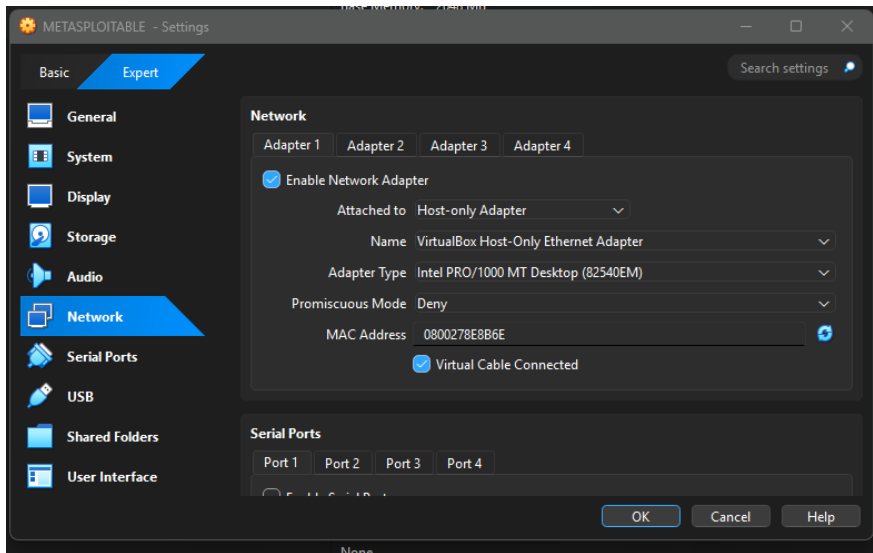


W12D1 – FRANCESCO MONTALTO

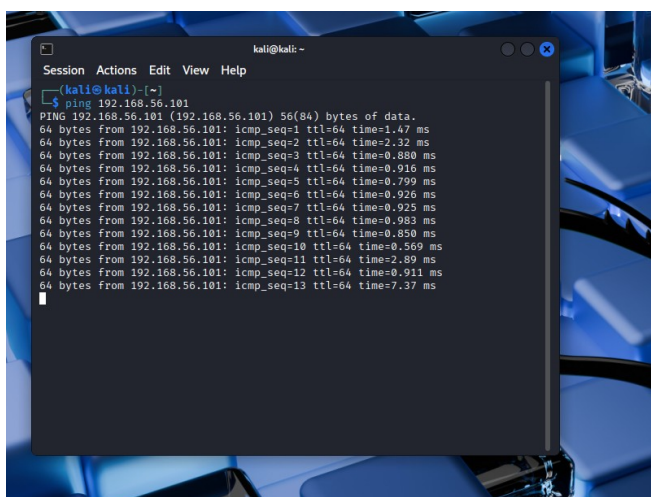
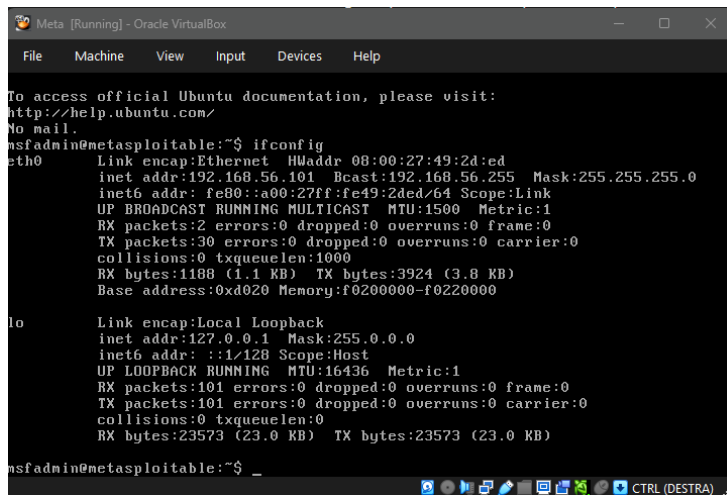
ATTENZIONE, NOTA PER IL PROFESSORE:

Ho caricato questo file di W12D1 solo successivamente perché mi sono reso conto che l'originale (caricato per tempo) era corrotto e non me ne ero accorto.

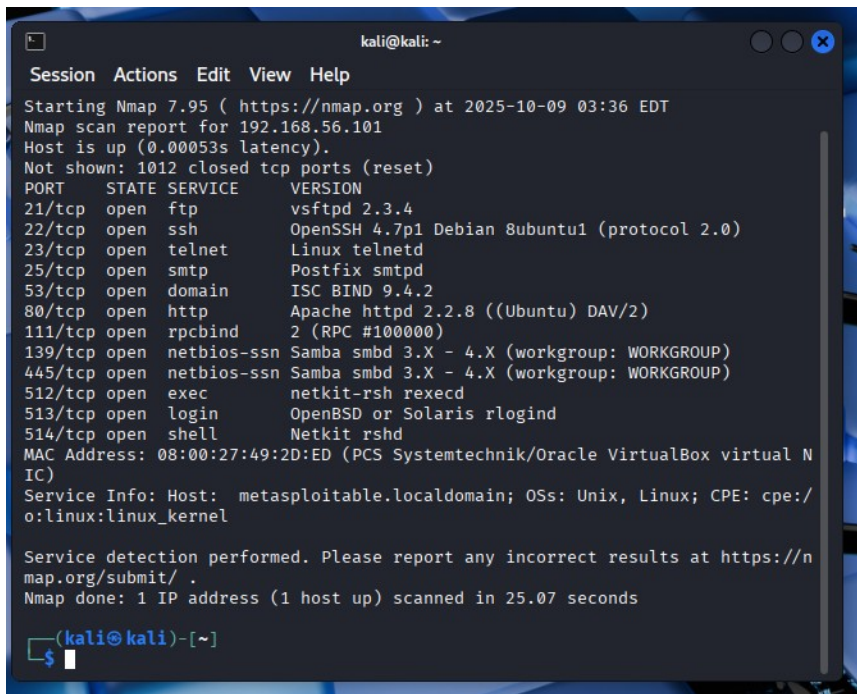
1. Ho innanzitutto settato sia Kali Linux che Metasploitable sulla stessa r (nel mio caso Host Only).



Ho successivamente pingato per conferma.

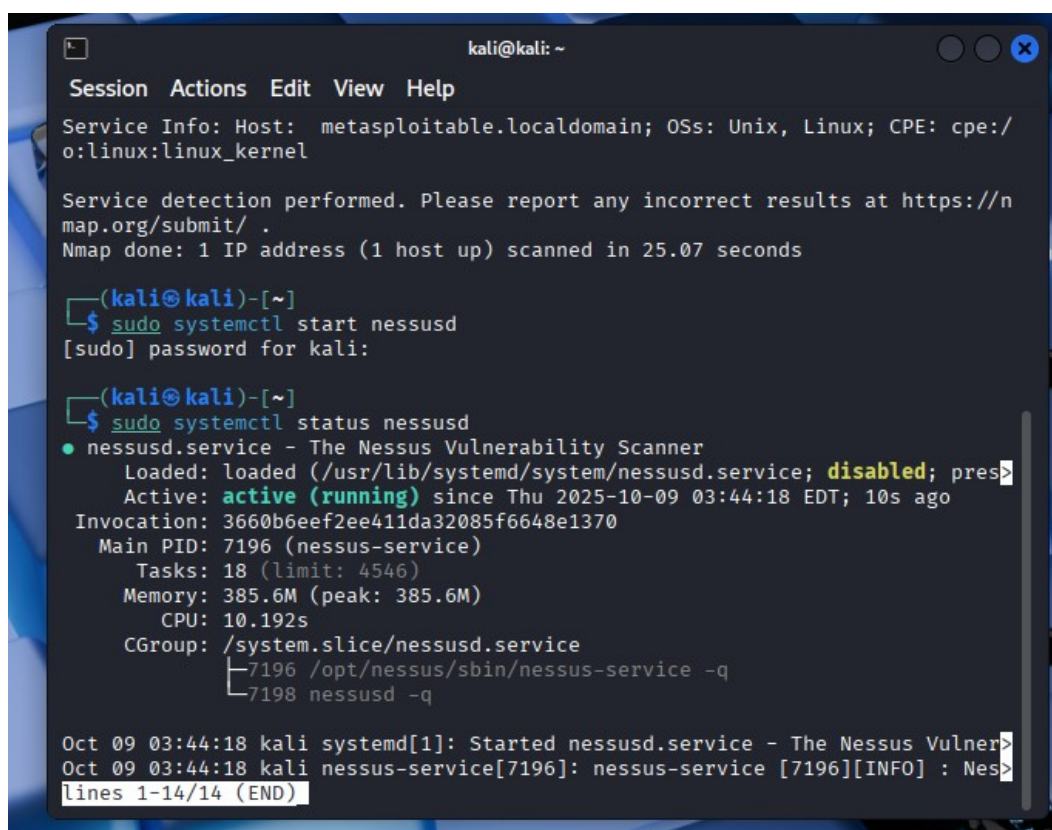


2. Prima dell'avvio effettivo di Nessus ho ritenuto utile una scansione veloce con nmap per vedere le porte aperte, per poterle confrontare dopo.



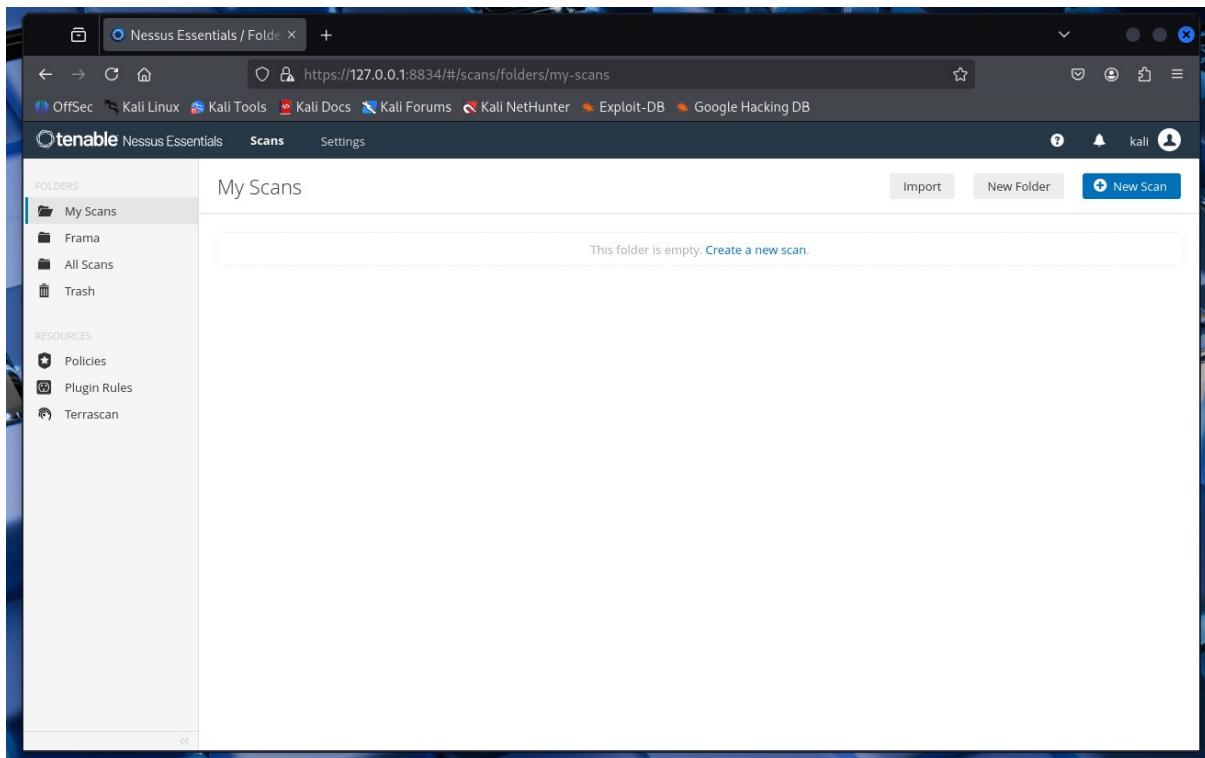
```
kali@kali: ~  
Session Actions Edit View Help  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 03:36 EDT  
Nmap scan report for 192.168.56.101  
Host is up (0.00053s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
MAC Address: 08:00:27:49:2D:ED (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/  
o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 25.07 seconds  
  
(kali@kali)-[~]  
$
```

3. Ho avviato Nessus, verificandone lo stato.



```
kali@kali: ~  
Session Actions Edit View Help  
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/  
o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 25.07 seconds  
  
(kali@kali)-[~]  
$ sudo systemctl start nessusd  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ sudo systemctl status nessusd  
● nessusd.service - The Nessus Vulnerability Scanner  
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; pres  
   Active: active (running) since Thu 2025-10-09 03:44:18 EDT; 10s ago  
   Invocation: 3660b6eef2ee411da32085f6648e1370  
   Main PID: 7196 (nessus-service)  
     Tasks: 18 (limit: 4546)  
    Memory: 385.6M (peak: 385.6M)  
       CPU: 10.192s  
    CGroup: /system.slice/nessusd.service  
            └─7196 /opt/nessus/sbin/nessus-service -q  
              └─7198 nessusd -q  
  
Oct 09 03:44:18 kali systemd[1]: Started nessusd.service - The Nessus Vulner  
Oct 09 03:44:18 kali nessus-service[7196]: nessus-service [7196][INFO] : Nes  
lines 1-14/14 (END)
```

4. Ho creato una nuova scansione, forzando Nessus a scansionare le porte “standard” dal 1 al 1024.



New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

CredentialsPlugins

BASIC

GeneralScheduleNotifications

DISCOVERYASSESSMENTREPORTADVANCED

NameVA Meta

DescriptionVulnerability Assessment su Metasploitable – porte comuni

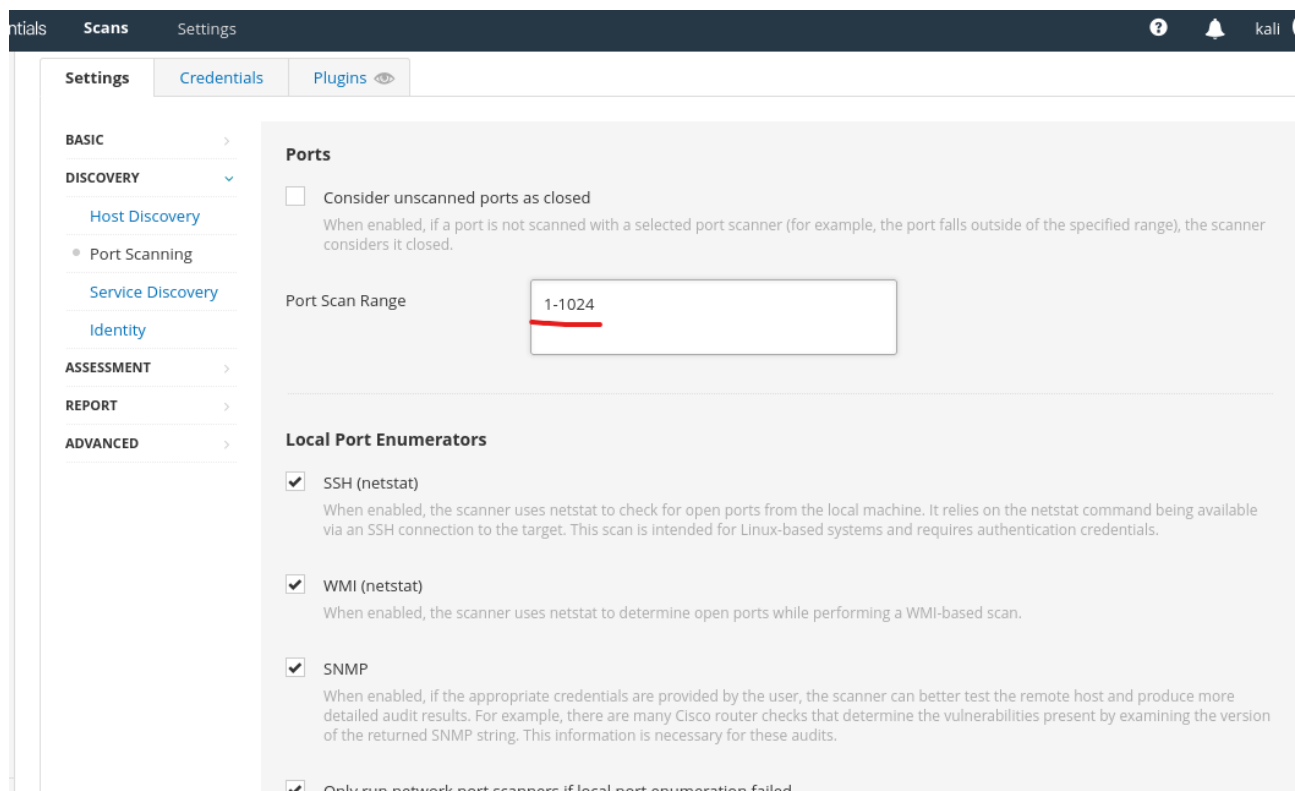
FolderMy Scans

Targets192.168.56.101

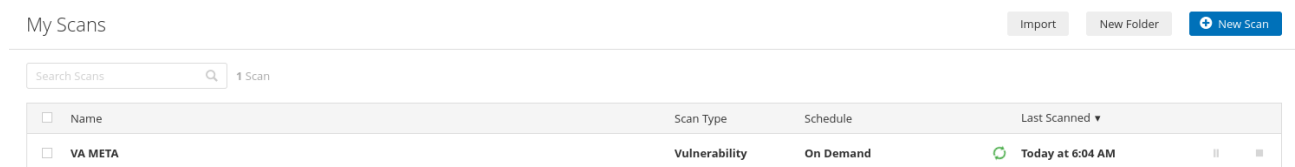
Upload TargetsAdd File

Save

Cancel



5. Ho poi chiaramente lanciato lo scan.



6. Ho aperto la scansione (una volta finita) dalla lista (l’ho anche esportata, per precauzione); da questa schermata ho potuto vedere le vulnerabilità.

ntials	Scans	Settings							
<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1	🔄	✎
<input type="checkbox"/>	CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghosc...	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	CRITICAL	📁 2 SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/>	HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1	🔄	✎
<input type="checkbox"/>	HIGH	7.5			NFS Shares World Readable	RPC	1	🔄	✎
<input type="checkbox"/>	MIXED	📁 15 SSL (Multiple Issues)	General	28	🔄	✎
<input type="checkbox"/>	MIXED	📁 5 ISC Bind (Multiple Issues)	DNS	5	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	3.6	0.9035	SSL DROWN Attack Vulnerability (Decrypting RSA with O...	Misc.	1	🔄	✎
<input type="checkbox"/>	MIXED				📁 SSL (Multiple Issues)	Misc.	6	🔄	✎

https://127.0.0.1:8834/#/scans/reports/6/hosts

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DB

There's an error with your feed. [Click here to view your license info](#)

VA META_9r3mpo.nessus
Completed — 2.1 MB
[Show all downloads](#)

ScansSettings

VA META
[Back to My Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities64Remediations2Notes2History1

FilterSearch Hosts1 Host

HostAuthVulnerabilities

192.168.56.101Fail86239109

Scan Details

Policy:Basic Network Scan

Status:Completed

Severity Base:CVSS v3.0

Scanner:Local Scanner

Start:Today at 6:03 AM

End:Today at 6:12 AM

Elapsed:8 minutes

Vulnerabilities

Critical

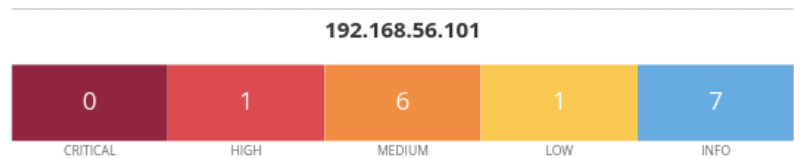
High

Medium

Low

Info

Scans	Settings
<input type="checkbox"/> MEDIUM 5.9 3.6 0.9035 SSL DROWN Attack Vulnerability (Decrypting RSA with O... Misc. 1	
<input type="checkbox"/> MIXED SSH (Multiple Issues) Misc. 6	
<input type="checkbox"/> MIXED HTTP (Multiple Issues) Web Servers 3	
<input type="checkbox"/> MIXED SMB (Multiple Issues) Misc. 2	
<input type="checkbox"/> MIXED TLS (Multiple Issues) Misc. 2	
<input type="checkbox"/> MIXED TLS (Multiple Issues) SMTP problems 2	
<input type="checkbox"/> LOW 3.7 3.9 0.9403 SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) Misc. 1	
<input type="checkbox"/> LOW 2.6 * X Server Detection Service detection 1	
<input type="checkbox"/> LOW 2.1 * 2.2 0.0037 ICMP Timestamp Request Remote Date Disclosure General 1	
<input type="checkbox"/> INFO SMB (Multiple Issues) Windows 7	
<input type="checkbox"/> INFO TLS (Multiple Issues) General 4	
<input type="checkbox"/> INFO DNS (Multiple Issues) DNS 3	
<input type="checkbox"/> INFO Apache HTTP Server (Multiple Issues) Web Servers 2	
<input type="checkbox"/> INFO FTP (Multiple Issues) Service detection 2	
<input type="checkbox"/> INFO PHP (Multiple Issues) Web Servers 2	
<input type="checkbox"/> INFO RPC (Multiple Issues) RPC 2	



Vulnerabilities

Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	6.1	0.4002	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	7.3	0.9032	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	0.9402	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

REPORT TECNICO:

VULNERABILITA' CRITICHE

VULNERABILITA'	PORTA	SOLUZIONE SINTETICA
Ubuntu Linux SLoL 8.04: Ubuntu 8.04 è fuori supporto dal 2013. Non riceve più patch di sicurezza ed è vulnerabile a exploit pubblici.	80/tcp	Aggiornare a versione supportata
VNC Server-password debole: Il servizio VNC accetta la password di default "password". Nessus ha confermato l'accesso remoto con credenziali deboli.	5900/tcp	Cambiare password o disabilitare servizio
Tomcat Ghostcat (AJP Injection): Consente lettura/esecuzione di file JSP malevoli su server Tomcat vulnerabili.	8009/tcp	Aggiornare Tomcat / disabilitare AJP
SSLv2/3 Protocol Enabled: Il servizio remoto accetta SSLv2/3, protocolli vulnerabili	443/tcp	Disabilitare SSLv2/SSLv3 e abilitare TLS1.2
Debian OpenSSH/OpenSSL RNG Weakness SSL: Il bug nei pacchetti OpenSSL di Debian riduce l'entropia del generatore di numeri casuali, rendendo prevedibili le chiavi crittografiche. Tutte le chiavi generate sono vulnerabili.	22/tcp, 5543/tcp	Rigenerare chiavi SSL e SSH
Debian OpenSSH RNG Weakness (SSH): Il servizio SSH utilizza chiavi generate con entropia ridotta. Gli aggressori possono derivare la chiave privata del server.	22/tcp	Rigenerare chiavi SSH host/server

VULNERABILITA' ELEVATE

VULNERABILITA'

rlogin Service Detection:

Il servizio rlogin consente autenticazioni non cifrate, rendendo vulnerabili username e password ad attacchi di intercettazione.

Samba Badlock Vulnerability:

La vulnerabilità Badlock consente attacchi man-in-the-middle e downgrade dell'autenticazione SMB. _

NFS Shares World Readable:

Il servizio NFS esporta directory senza restrizioni, permettendo accesso completo a qualsiasi host in rete.

PORTA

513/tcp

445/tcp

2049/tcp

SOLUZIONE SINTETICA

Disabilitare rlogin, usare SSH

Aggiornare Samba >= 4.4.2

Limitare accesso NFS nel file /etc/exports

VULNERABILITA' MEDIE

VULNERABILITA'	PORTA	SOLUZIONE SINTETICA
<u>TLS Version 1.0 Protocol</u> <u>Detection:</u> Il servizio remoto accetta connessioni tramite TLS 1.0, un protocollo obsoleto con debolezze note.	5432/tcp, 25/tcp	Abilitare TLS 1.2 e disabilitare TLS 1.0
<u>Unencrypted Telnet Server:</u> Il servizio Telnet trasferisce credenziali e comandi in chiaro, consentendo intercettazione.	23/tcp	Disabilitare Telnet e usare SSH
<u>SSL Anonymous Cipher Suites</u> <u>Supported:</u> Il servizio supporta cifrari SSL anonimi che non garantiscono autenticazione.	25/tcp	Disabilitare cifrari anonimi
<u>SSL DROWN Attack</u> <u>Vulnerability:</u> Il server supporta SSLv2, consentendo attacco DROWN	25/tcp	Disabilitare SSLv2 e SSLv3

VULNERABILITA' BASSE

VULNERABILITA'	PORTA	SOLUZIONE RAPIDA
<u>DH Modulus <= 1024 (Logjam):</u> Il server supporta Diffie-Hellman con modulus <= 1024 bit, vulnerabile all'attacco Logjam.	25/tcp	Usare DH params >= 2048 bit
<u>X Server Detection (X11):</u> È attivo un server X11 che ascolta TCP (non cifrato), esponendo traffico grafico alla rete.	6000/tcp	Disabilitare TCP listen o usare ssh -X
<u>ICMP Timestamp Disclosure:</u> Il sistema risponde a richieste ICMP Timestamp, fornendo l'ora di sistema e favorendo attacchi basati sul tempo.	0/icmp	Bloccare ICMP timestamp request

Porta	Descrizione	Evidenza	Sfruttabilità	Impatto	Risoluzione
80/tcp	Sistema operativo fuori supporto.	Compromissione totale possibile	Alta	Compromissione totale possibile.	Migrare a versione LTS supportata.
5900/tcp	Accesso riuscito con password 'password'	Accesso remoto non autorizzato.	Molto alta	Accesso remoto non autorizzato.	Cambiare password
8009/tcp	Richiesta exploit rilevata da Nessus.	Lettura file sensibili, RCE.	Alta	Lettura file sensibili, RCE.	Aggiornare Tomcat
443/tcp,23/tcp,993/tcp	SSLv2 attivo, cifrari deboli.	Decifrabilità del traffico.	Alta	Decifrabilità del traffico.	Disabilitare SSLv2/v3, abilitare TLS
5543/tcp,22/tcp	Rilevata generazione di chiavi deboli	Compromissione chiavi private	Molto alta	Compromissione chiavi private	Rigenerare chiavi e aggiornare
22/tcp	Rilevato uso di chiavi con entropia ridotta.	Possibile impersonificazione dell'host.	Alta	Possibile impersonificazione dell'host.	Rigenerare chiavi SSH e aggiornare
513/tcp	Connessione non protetta rilevata	Intercettazione credenziali.	Alta	Intercettazione credenziali.	Disabilitare rlogin e usare SSH.
445/tcp	Patch non applicata	Accesso a condivisioni SMB.	Media-alta	Accesso a condivisioni SMB.	Aggiornare Samba
2049/tcp	Shares esportate pubblicamente.	Fuga di dati o alterazione file.	Alta	Fuga di dati o alterazione file.	Limitare accesso in /etc/exports.
5432/tcp,25/tcp	TLSv1 abilitato e in uso.	Rischio di downgrade attack.	Media	Rischio di downgrade attack	Disabilitare TLS1.0, usare TLS1.2.
23/tcp	Banner 'metasploitable2' rilevato.	Intercettazione credenziali.	Alta	Intercettazione credenziali	Disabilitare Telnet, usare SSH.
25/tcp	EXP-ADH-DES-CBC-SHA, RC4-MD5	Attacco MITM possibile.	Media	Attacco MITM possibile.	Disabilitare cifrari anonimi.
25/tcp	Cifrari deboli RC2, RC4 rilevati.	Decifrabilità cross-protocol.	Alta	Decifrabilità cross-protocol.	Disabilitare SSLv2/3
25/tcp	DH size 512 bit.	Traffico decrittabile.	Media	Traffico decrittabile.	Generare dhparam 2048+
6000/tcp	Versione 11.0 rilevata.	Possibile intercettazione grafica.	Bassa	Possibile intercettazione grafica.	Disabilitare TCP o usare SSH -X.
0/icmp	Differenza orologio: 5874s.	Rivelazione informazioni temporali.	Bassa	Rivelazione informazioni temporali.	Bloccare ICMP timestamp

