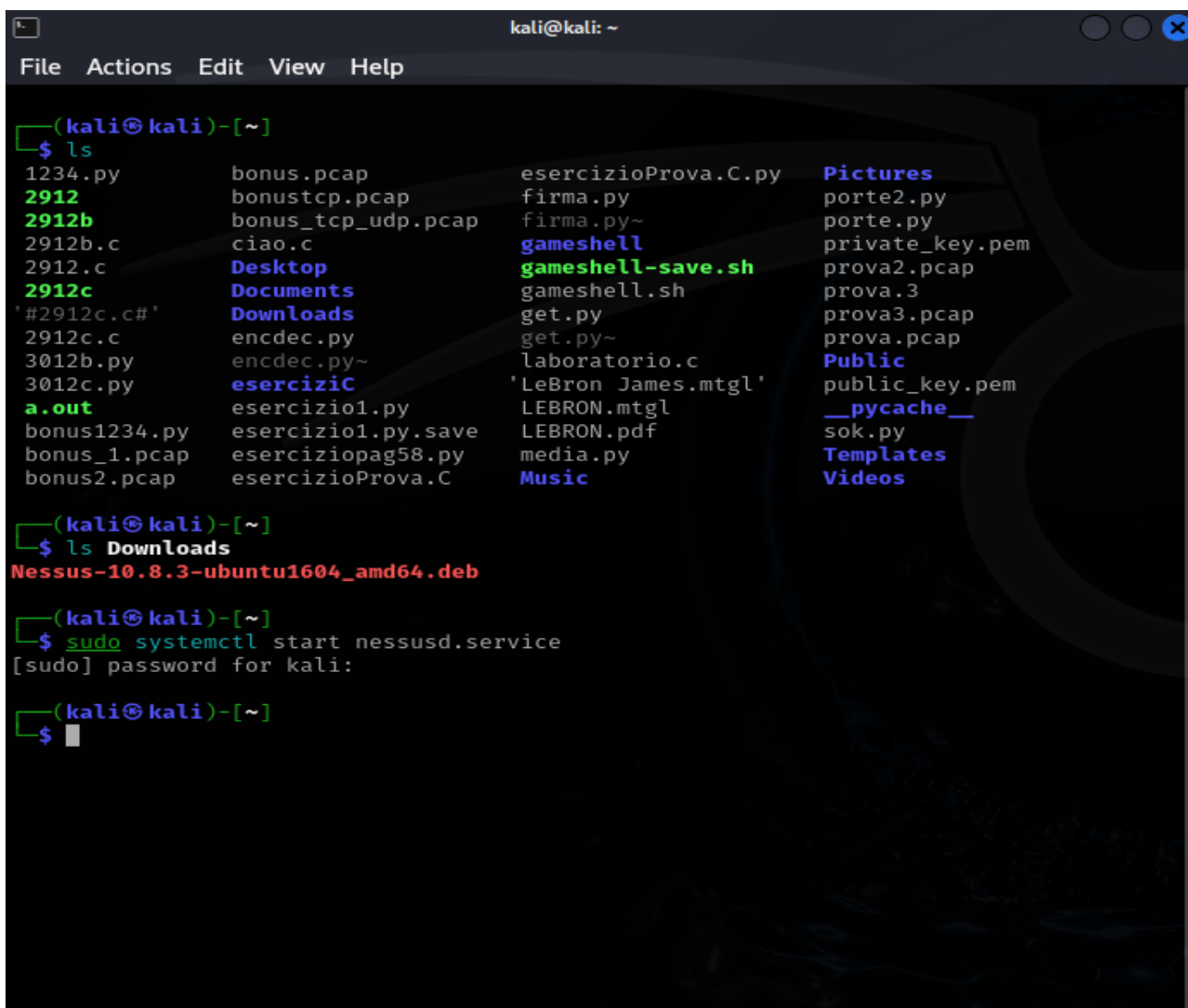


LABORATORIO 09/01/2025 S5-L3

Nel laboratorio odierno andremo ad effettuare un Vulnerability Scanning utilizzando il tool Nessus da Kali.

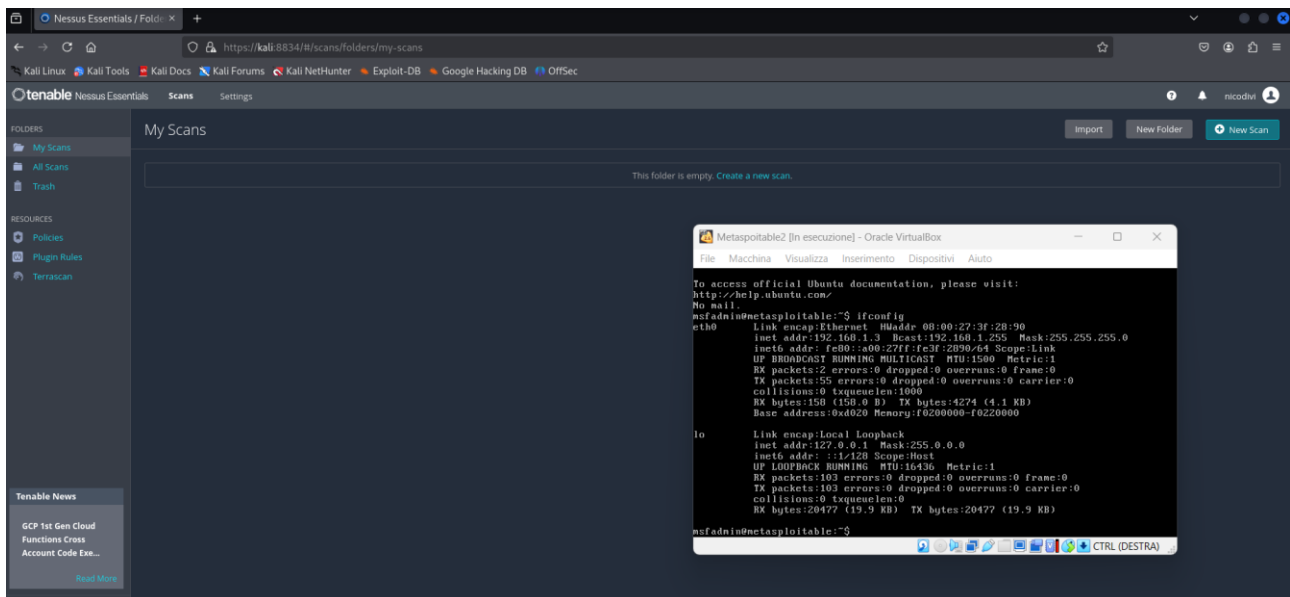
In primo luogo avviamo la macchina virtuale e successivamente apriamo il terminale. Dopo esserci spostati nella Directory Downloads (contenente Nessus) avviamo il demone col comando: `sudo systemctl start nessusd.service`.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ls  
1234.py          bonus.pcap      esercizioProva.C.py  Pictures  
2912            bonustcp.pcap   firma.py             porte2.py  
2912b          bonus_tcp_udp.pcap  firma.py~           porte.py  
2912b.c        ciao.c          gameshell            private_key.pem  
2912.c         Desktop         gameshell-save.sh   prova2.pcap  
2912c         Documents      gameshell.sh        prova.3  
'#2912c.c#'  
2912c.c        encdec.py      get.py              prova3.pcap  
3012b.py       encdec.py~    get.py~            prova.pcap  
3012c.py       eserciziC      laboratorio.c        Public  
a.out          esercizio1.py  'LeBron James.mtgl' public_key.pem  
bonus1234.py   esercizio1.py.save  LEBRON.mtgl        __pycache__  
bonus_1.pcap  esercizio1pag58.py  LEBRON.pdf         sok.py  
bonus2.pcap   esercizioProva.C  media.py           Templates  
              Music              Videos  
  
(kali@kali)-[~]  
$ ls Downloads  
Nessus-10.8.3-ubuntu1604_amd64.deb  
  
(kali@kali)-[~]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$
```

Apriamo il nostro browser e ci colleghiamo all' URL di Nessus su Kali: <https://kali:8834>

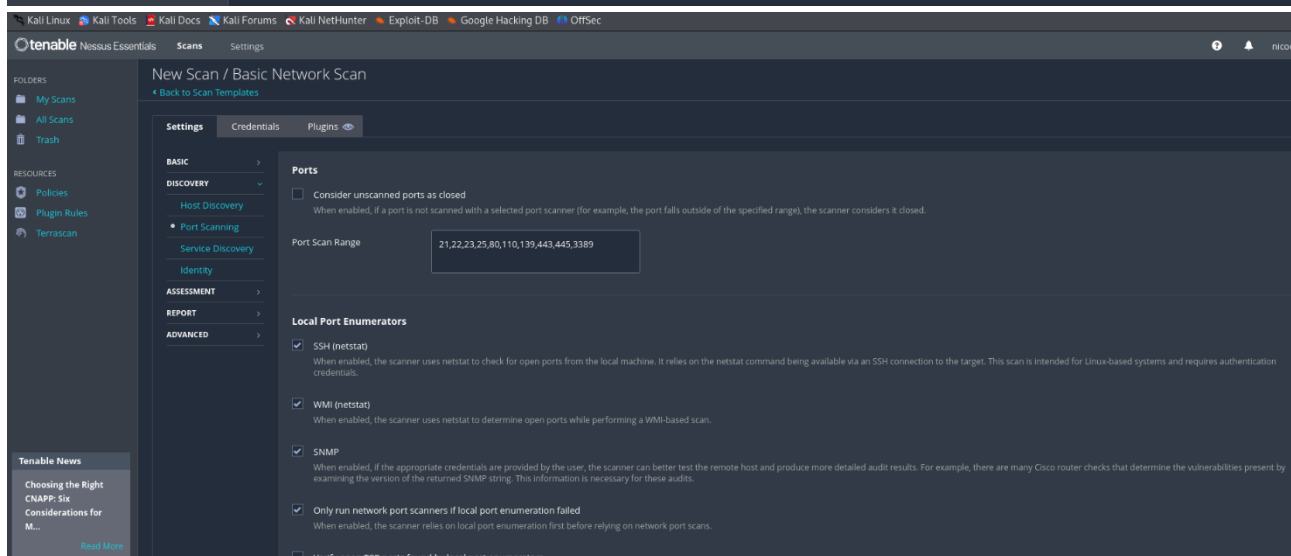
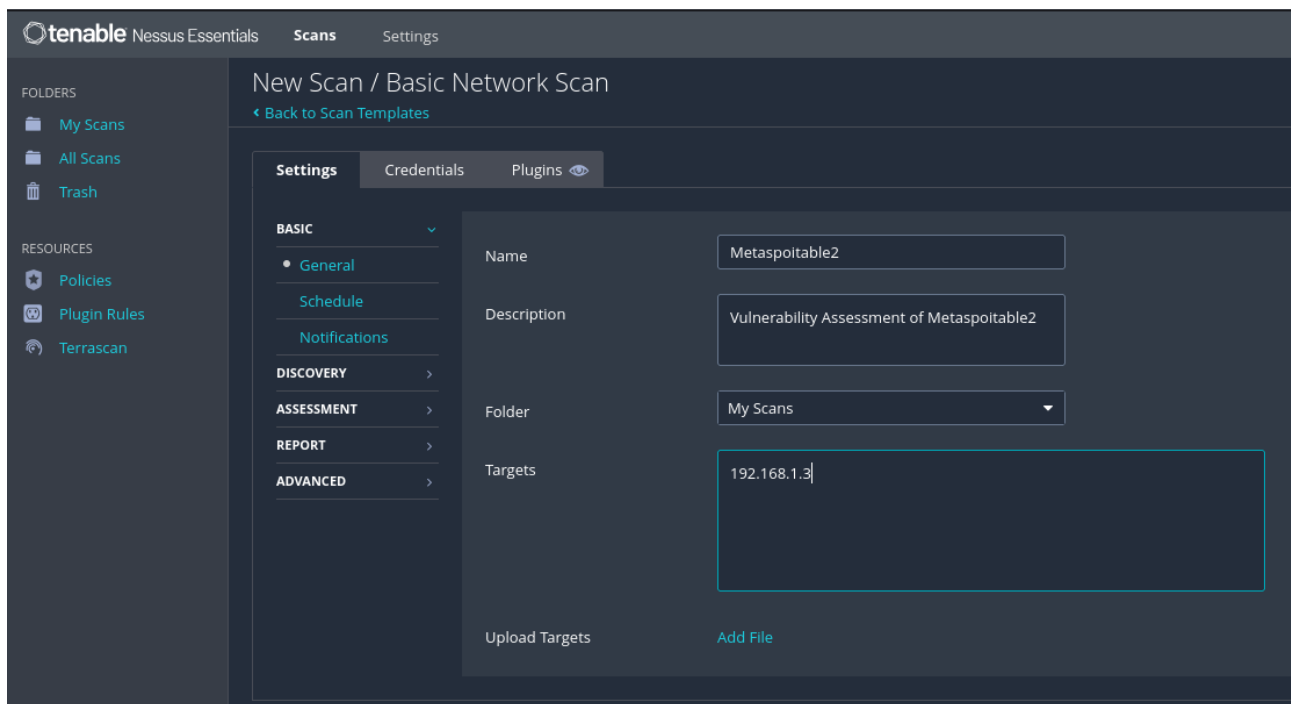
Avviamo quindi la VM di Metasploitable2 che sarà il nostro target. Ricaviamo il suo indirizzo IP col comando ifconfig.



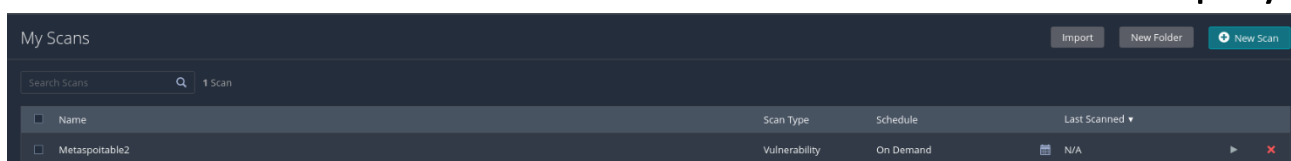
Avviamo con il pulsante “New Scan” una nuova scansione e scegliamo tra le varie opzioni una “Basic Network Scan”.

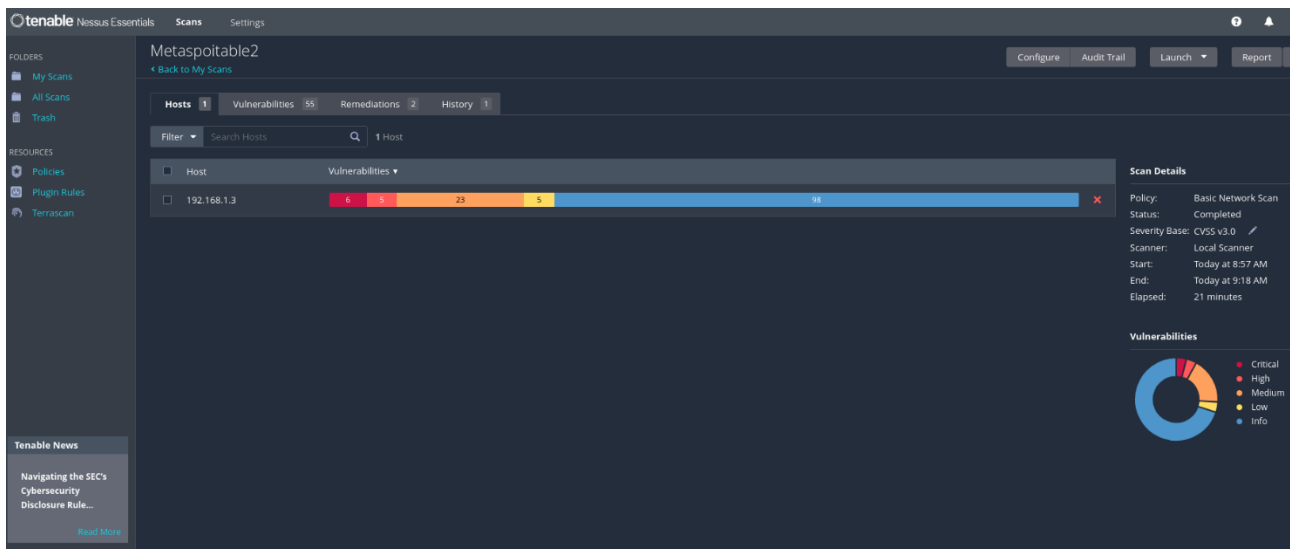
A questo punto compiliamo i campi richiesti nella campo “Setting” ed assegnamo il nome, la descrizione e l' indirizzo IP target della nostra scansione.

Nel campo “Discovery” invece selezioneremo le porte che vogliamo controllare.



Salviamo le nostre preferenze e facciamo partire la scansione con il comando play.





Il Vulnerability Scanner ci ha restituito varie vulnerabilità di cui 6 critiche, 5 alte, 23 medie e 5 di livello basso, oltre a 98 informazioni utili.

Nella parte delle vulnerabilità possiamo vederle in maniera più specifica.

The screenshot shows a detailed view of the vulnerabilities found during the scan. The table lists various issues, their severity levels, and remediation steps. The 'Vulnerabilities' panel on the right shows a donut chart visualizing the severity distribution.

Severity	CVSS	Plugin	Description	Remediation	Count	Details
CRITICAL	10.0 *	10407	VNC Server 'password' Password	Gain a shell remotely	1	Details
CRITICAL	9.8	10407	SSL Version 2 and 3 Protocol Detection	Service detection	2	Details
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	Details
HIGH	7.5	5.9	0.0489 Samba Badlock Vulnerability	General	1	Details
HIGH	7.5	...	NFS Shares World Readable	RPC	1	Details
MIXED	SSL (Multiple Issues)	General	29	Details
MIXED	ISC Bind (Multiple Issues)	DNS	5	Details
MEDIUM	6.5	...	TLS Version 1.0 Protocol Detection	Service detection	2	Details
MEDIUM	5.9	4.4	0.003 SSL Anonymous Cipher Suites Supported	Service detection	1	Details
MEDIUM	5.9	3.6	0.935 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	Details
MIXED	DNS (Multiple Issues)	DNS	6	Details
MIXED	HTTP (Multiple Issues)	Web Servers	3	Details
MIXED	SMB (Multiple Issues)	Misc.	2	Details
MIXED	TLS (Multiple Issues)	Misc.	2	Details
MIXED	TLS (Multiple Issues)	SMTP problems	2	Details
LOW	2.6 *	...	X Server Detection	Service detection	1	Details

A questo punto possiamo andare a consultare il report della scansione.

Abbiamo la possibilità di consultarlo o di esportarlo in vari formati, tra cui in PDF.

Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Buttons: Generate Report, Cancel, Save as default

Il primo report è piuttosto breve e fornisce un grafico con la panoramica delle vulnerabilità riscontrate come possiamo vedere nell' immagine seguente.

192.168.1.3					
4	4	17	4	68	
CRITICAL	HIGH	MEDIUM	LOW	INFO	

Vulnerabilities					Total: 97
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0053	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0489	90509	Samba Badlock Vulnerability
MEDIUM	6.8	6.0	0.2471	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoni

Gli altri, molto più lunghi e dettagliati, forniscono numerose informazioni utili come:

- Lista completa delle vulnerabilità e relativo punteggio
- Informazioni sul target come IP e sistema operativo
- Nome e descrizione della vulnerabilità
- Link utili per informarsi riguardo tali problemi
- Eventuali soluzioni per mitigarli o risolverli
- Punteggio di rischio della vulnerabilità
- Porta che ha restituito in output tale problematica

192.168.1.3



Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.1.3
MAC Address: 08:00:27:3F:28:90
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up and decipher the remote

See Also

<http://www.nessus.org/u?107f9bdc>
<http://www.nessus.org/u?f14f4224>

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.1994

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

In questo specifico caso preso in esempio la vulnerabilità riguarda la debolezza del generatore di numeri casuali utilizzato da OpenSSL, che può compromettere la sicurezza dei servizi come OpenSSH se i numeri casuali sono prevedibili o insufficienti. Questo problema è stato evidenziato in precedenti vulnerabilità relative alla generazione di numeri casuali in OpenSSL e rappresenta un rischio critico.

Se un attaccante può prevedere i numeri casuali utilizzati nella generazione di chiavi, ciò riduce drasticamente la sicurezza delle connessioni SSL/TLS e delle chiavi SSH, poiché potrebbero essere in grado di indovinare le chiavi private o decifrare dati sensibili.

Su un server compromesso, l'utilizzo di numeri casuali deboli o prevedibili nella generazione delle chiavi aumenta il rischio di riutilizzo delle chiavi o di attacchi di brute force facili.

Si consiglia quindi di aggiornare OpenSSL/OpenSSH in quanto gli aggiornamenti correggono spesso problemi legati al processo di generazione dei numeri casuali e altre vulnerabilità scoperte.