Relazione Tecnica: Vulnerability Scanning su Metasploitable

Studente: Mirko Imbrogno

Corso: Cyber Security & Ethical Hacking - EPICODE **Strumento Utilizzato:** Nessus Professional

---

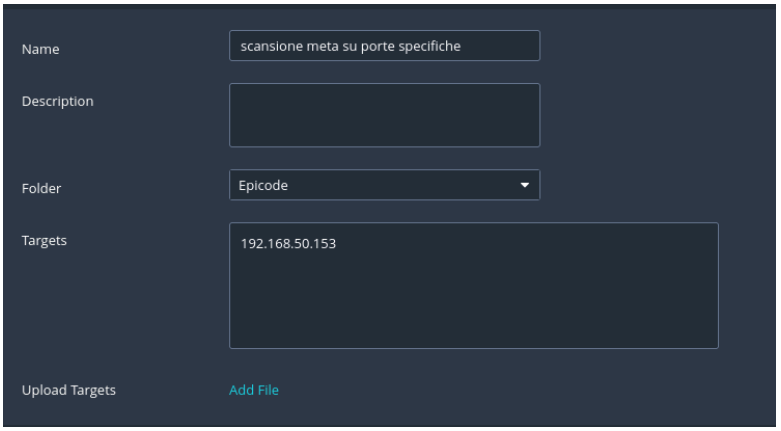
1. Obiettivo dell'Attività

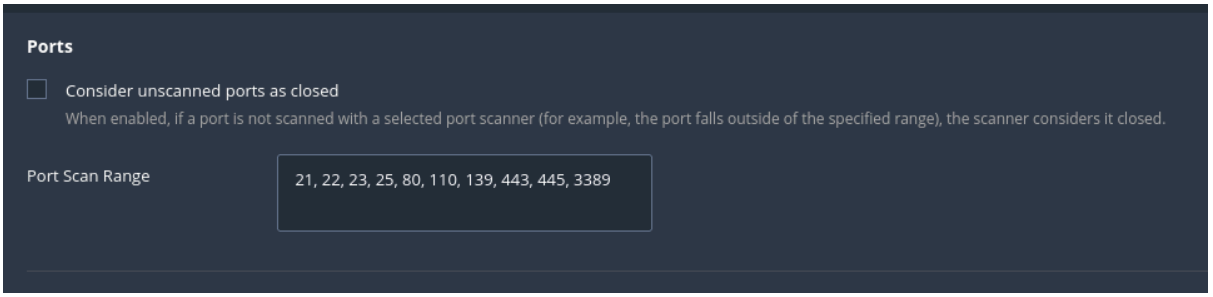
L'obiettivo dell'esercizio è effettuare una scansione di vulnerabilità sulla macchina target **Metasploitable**. L'attività mira a consolidare la pratica con lo strumento **Nessus**, configurare scansioni mirate su porte specifiche e interpretare i report per approfondire le vulnerabilità note.

2. Metodologia e Configurazione

La scansione è stata configurata seguendo i parametri indicati nella traccia:

- **Target:** 192.168.50.153 (Metasploitable 2).
- **Nome Scansione:** "scansione meta su porte specifiche".
- **Selezione Porte:** La scansione è stata ristretta esclusivamente alle porte comuni: **21, 22, 23, 25, 80, 110, 139, 443, 445, 3389**.
- **Tipo di Scansione:** Advanced Scan (configurato per analizzare i servizi specifici sulle porte selezionate).





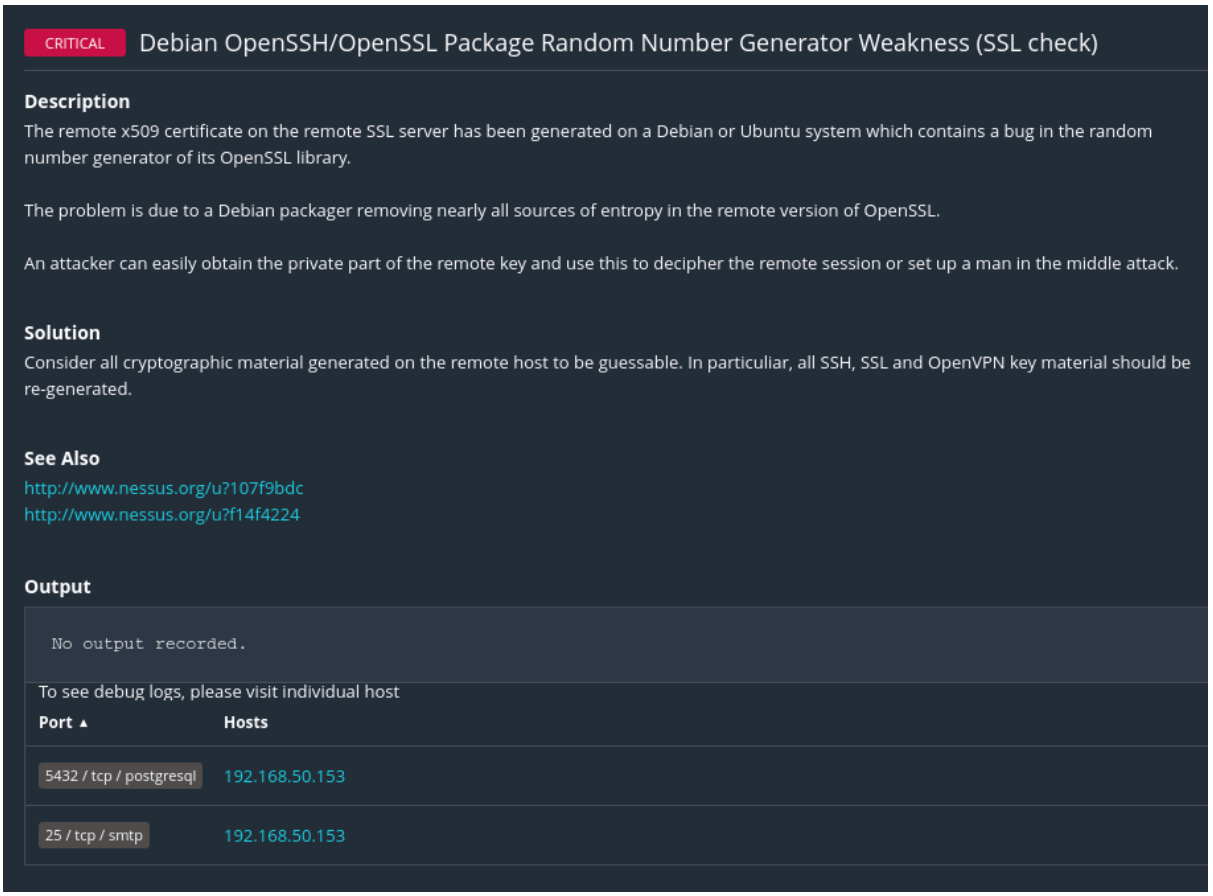
3. Analisi delle Criticità Emerse

Dall'analisi del report sono emerse diverse vulnerabilità di livello **Critical** e **Medium**. Di seguito il dettaglio delle più rilevanti:

A. Vulnerabilità Critiche (CRITICAL)

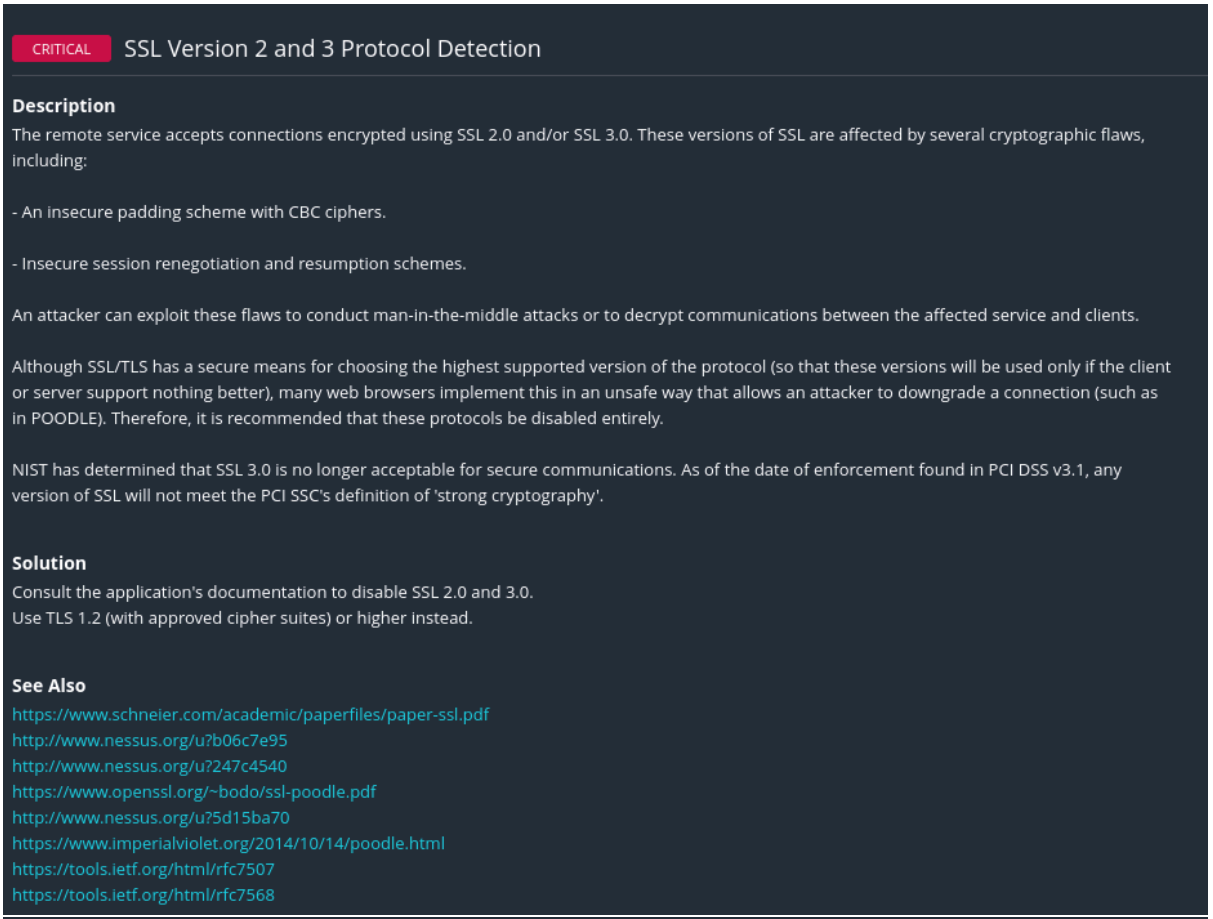
1. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Descrizione:** Il certificato x509 del server remoto è stato generato su un sistema Debian/Ubuntu affetto da un bug nel generatore di numeri casuali della libreria OpenSSL.
- **Impatto:** Un attaccante può facilmente ottenere la parte privata della chiave e utilizzarla per decifrare la sessione o eseguire attacchi Man-in-the-Middle (MitM).
- **Soluzione:** Rigenerare tutto il materiale crittografico (chiavi SSH, SSL, OpenVPN) poiché considerato compromesso.
- **Approfondimento:** Come indicato nei link del report (es. *nessus.org/u?107f9bdc*), questa è la celebre falla del 2008 causata dalla rimozione di righe di codice per la generazione di entropia da parte di un manutentore Debian.



2. SSL Version 2 and 3 Protocol Detection

- **Descrizione:** Il servizio accetta connessioni criptate tramite protocolli obsoleti (SSLv2 e SSLv3), affetti da gravi difetti di progettazione come schemi di padding insicuri.
- **Impatto:** Espone al rischio di attacchi come **POODLE** (*Padding Oracle On Downgraded Legacy Encryption*), permettendo a un attaccante di decifrare le comunicazioni.
- **Soluzione:** Disabilitare SSLv2 e SSLv3 in favore di TLS 1.2 o superiore.
- **Riferimenti:** Il report suggerisce la lettura del paper di Schneier e i dettagli su *imperialviolet.org* riguardo l'attacco POODLE.



CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

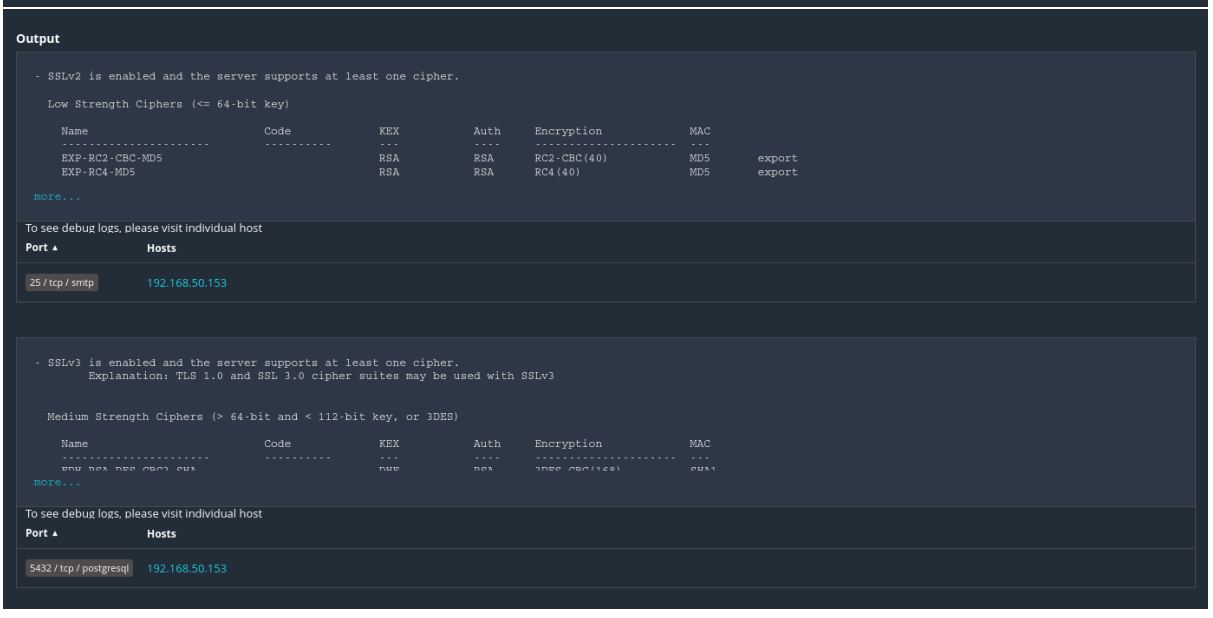
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568



Output

```
- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    Name                        Code            KEX          Auth     Encryption            MAC
    --------------------        ----------      ---          ----     --------------------  ---
    EXP-RC2-CBC-MD5                             RSA          RSA      RC2-CBC(40)           MD5      export
    EXP-RC4-MD5                                 RSA          RSA      RC4(40)               MD5      export

  more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
25 / tcp / smtp	192.168.50.153

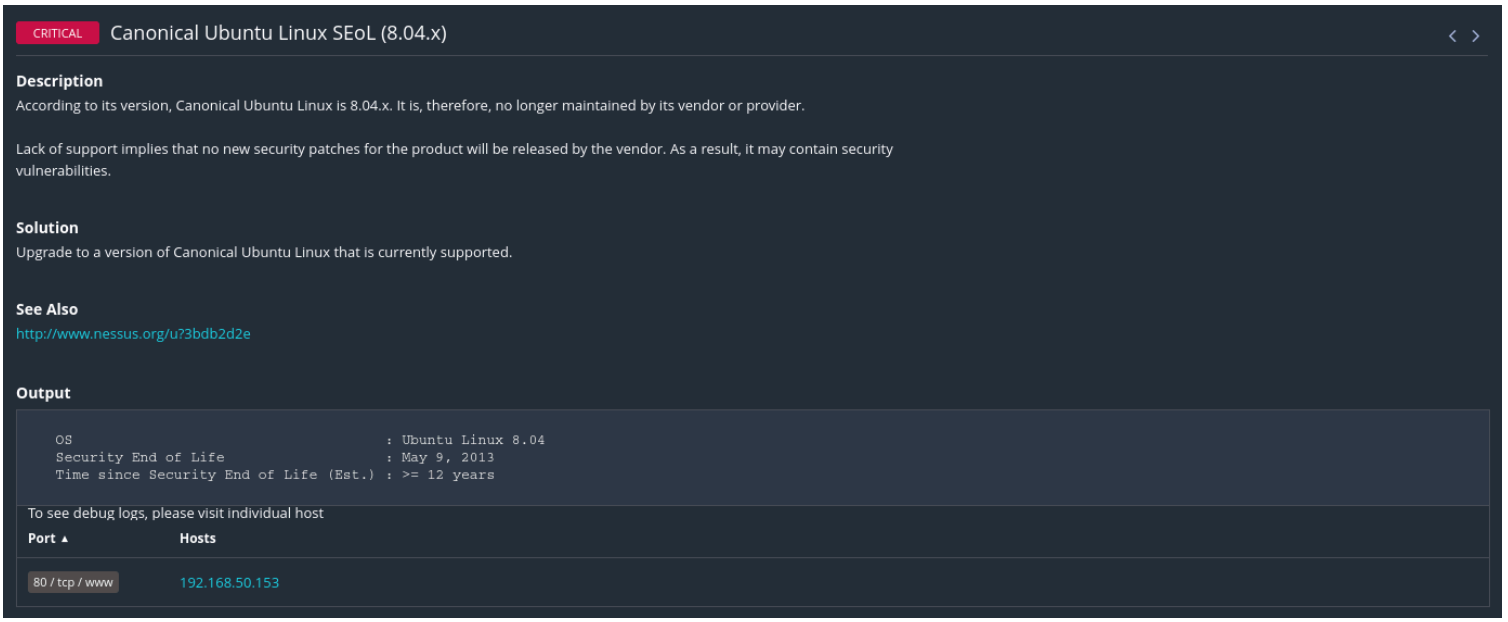
```
- SSLv3 is enabled and the server supports at least one cipher.
        Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code            KEX          Auth     Encryption            MAC
    --------------------        ----------      ---          ----     --------------------  ---
    EDH-RSA-DES-CBC3-SHA                        DHE          RSA      3DES-CBC(168)         SHA1
  more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.50.153

3. Canonical Ubuntu Linux SEoL (8.04.x)

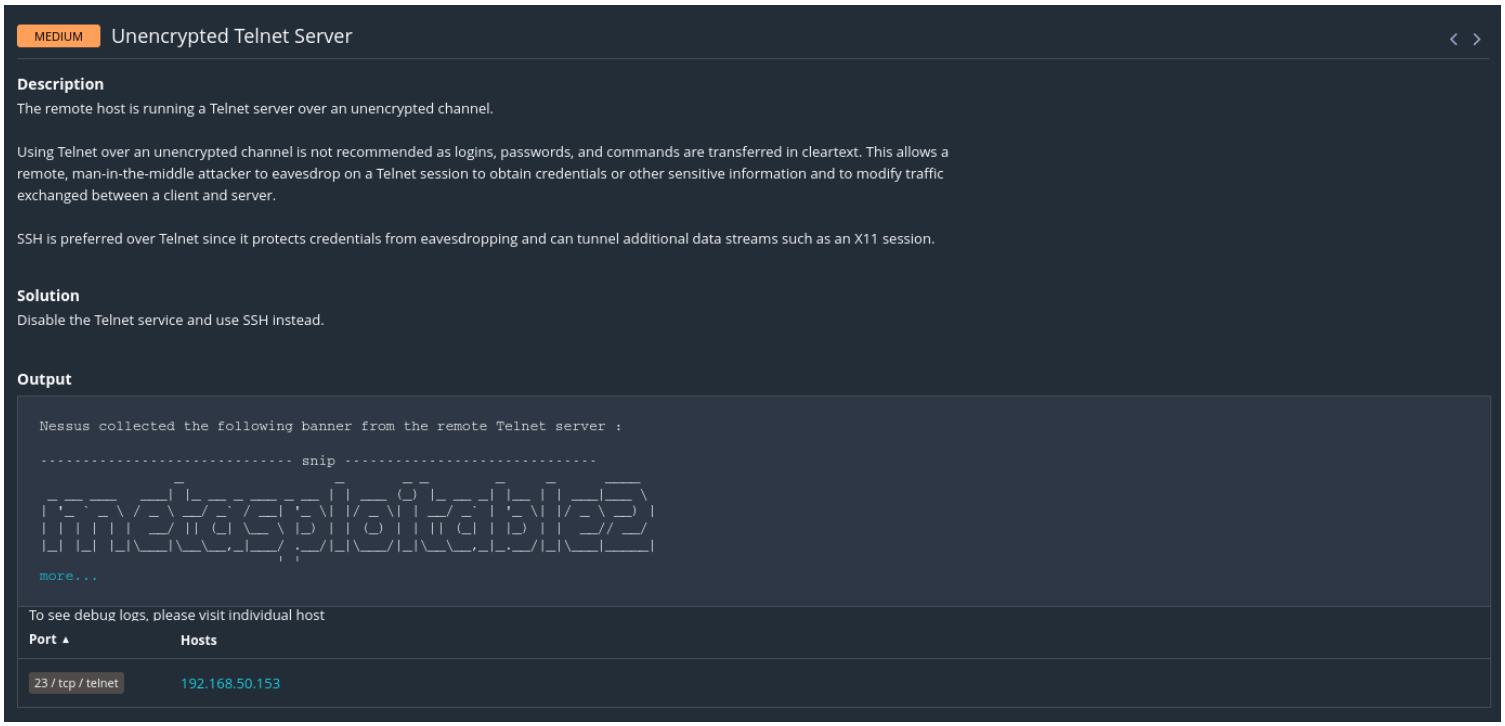
- **Descrizione:** Il sistema operativo rilevato (Ubuntu 8.04) ha raggiunto la fine del supporto (End of Life) nel maggio 2013.
- **Impatto:** Mancanza totale di patch di sicurezza da oltre 12 anni, rendendo il sistema vulnerabile a qualsiasi exploit pubblico rilasciato nell'ultimo decennio.
- **Soluzione:** Aggiornamento immediato del sistema operativo.



B. Vulnerabilità Medie (MEDIUM)

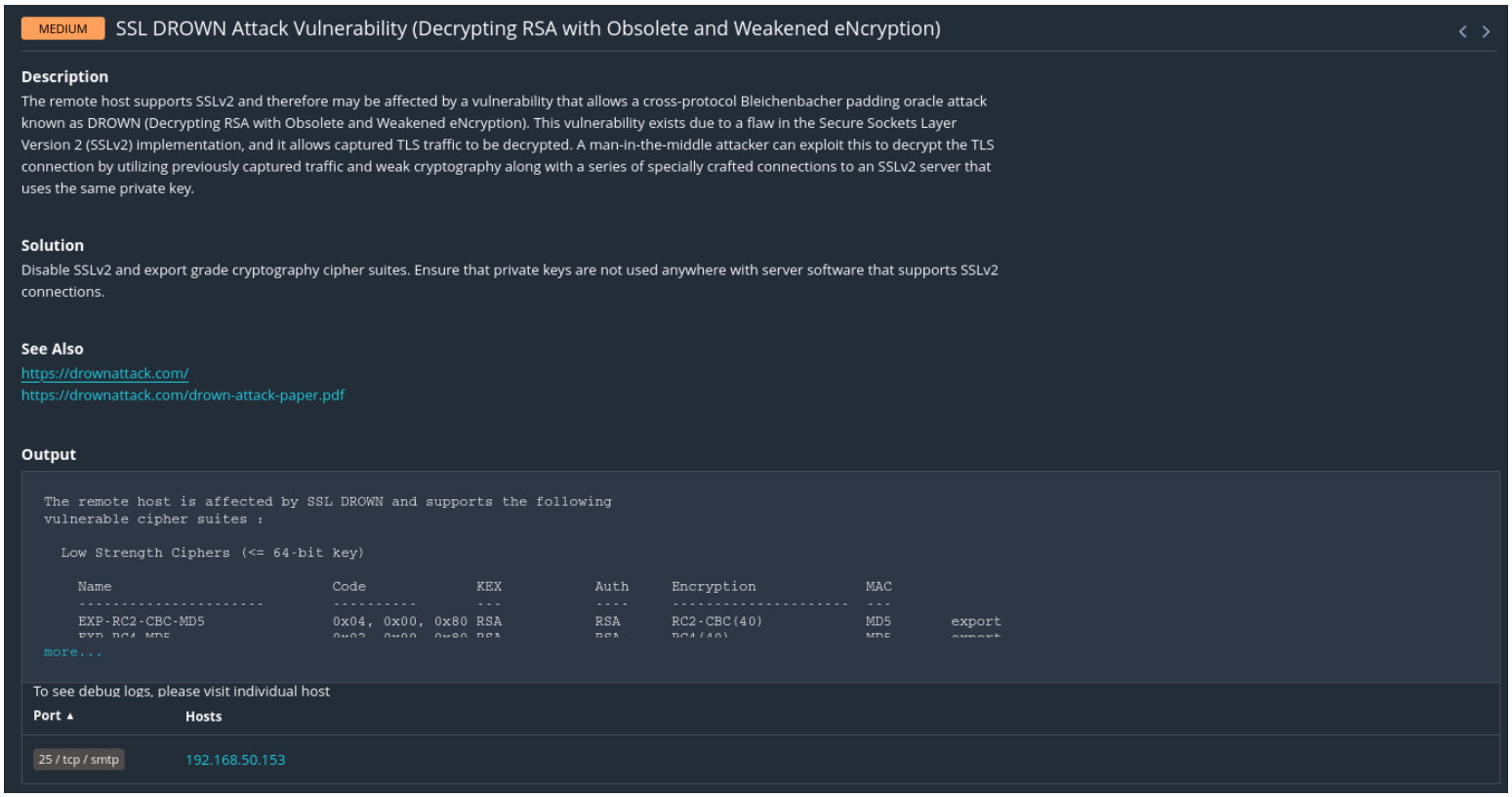
1. Unencrypted Telnet Server (Porta 23)

- **Descrizione:** È attivo un server Telnet che comunica in chiaro.
- **Impatto:** Credenziali e comandi possono essere intercettati tramite sniffing di rete (Man-in-the-Middle).
- **Soluzione:** Disabilitare Telnet e sostituirlo con SSH per garantire la cifratura.



2. SSL DROWN Attack Vulnerability

- **Descrizione:** Il supporto a SSLv2 permette l'attacco **DROWN**, che consente di decifrare il traffico TLS sfruttando debolezze in SSLv2 se la chiave privata è condivisa tra i servizi.
- **Riferimento:** Come menzionato su *drownattack.com*. circa il 33% di tutti i server HTTPS era vulnerabile a questo attacco al momento della sua scoperta.



---

4. Conclusioni e Risultati Attesi

L'attività ha permesso di verificare come la macchina Metasploitable sia intenzionalmente configurata con servizi obsoleti e protocolli di cifratura deboli.

Attraverso questo esercizio, ho acquisito le seguenti competenze:

- Capacità di **restringere il perimetro di scansione** a porte specifiche per ottimizzare le risorse.
- Competenza nell'**interpretare i report di Nessus**, distinguendo tra vulnerabilità software (Debian bug) e configurazioni errate (SSLv2/v3).
- Capacità di **ricerca autonoma** tramite le risorse suggerite dal software per valutare l'effettiva sfruttabilità delle falle.