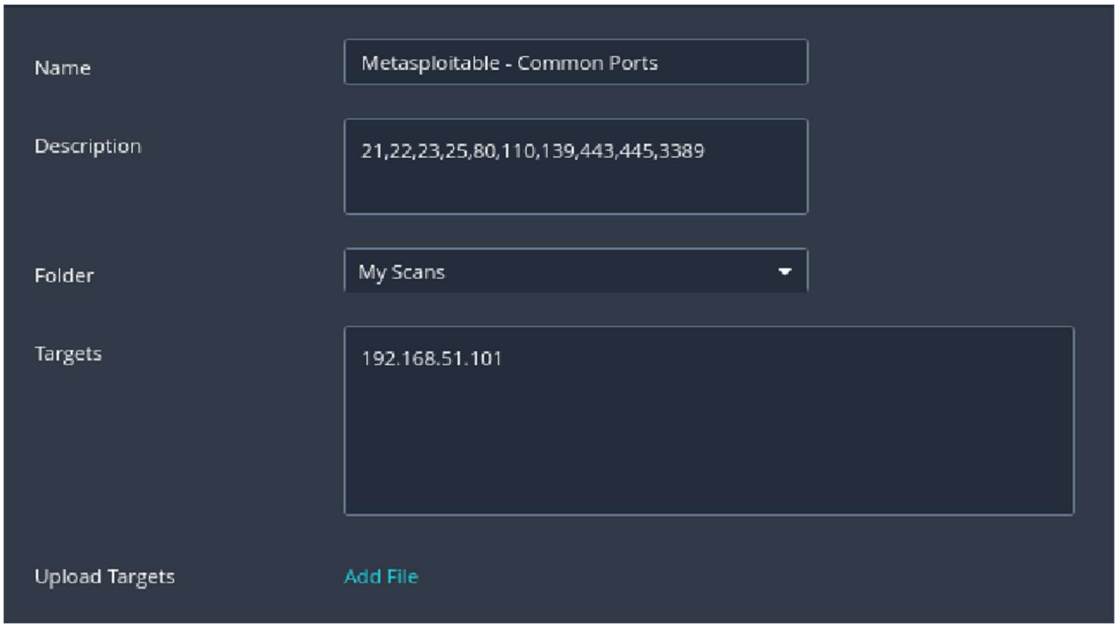
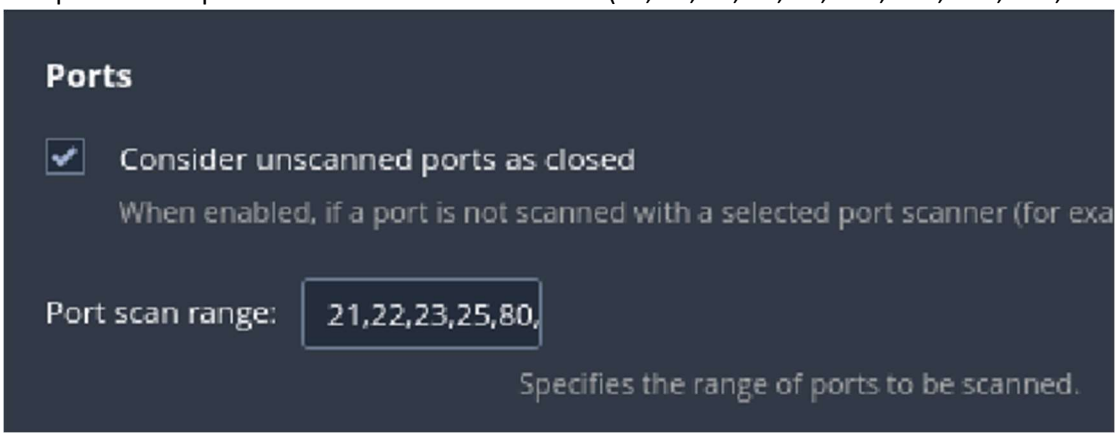
S5-L3

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

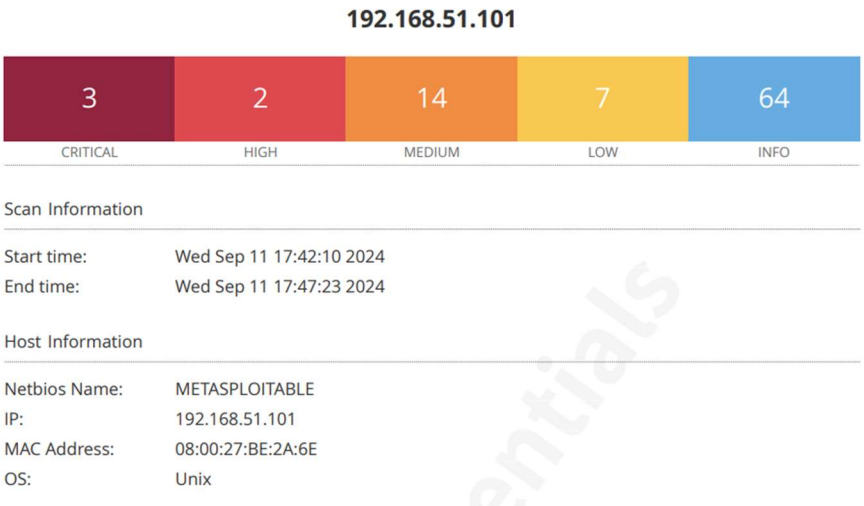
Creiamo una nuova scansione su Nessus:



E impostiamo le porte come richiesto dal esercizio (21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)



Generiamo il report dettagliato per vulnerabilità e otteniamo il PDF in allegato.



Le prime pagine ci forniscono un breve recap di cosa abbiamo trovato e i dati della macchina analizzata.

Di seguito una breve analisi dei 3 risultati critical e 2 high:

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Questi errori ci informano che le chiavi del host SSH sono deboli, a causa di un bug di Ubuntu e nel RNG della libreria OpenSSL. Ci informa che per un attaccante è facilmente recuperabile la parte privata della chiave remota e decifrare la sessione come man in the middle.
Come soluzione ci informano di considerare tutto il materiale generato fin ora come "indovinabile" e di rigenerare le chiavi SSH SSL e OpenVPN

20007 - SSL Version 2 and 3 Protocol Detection

Veniamo informati che questo servizio encrypta il traffico usando un protocollo con debolezze conosciute.
Ci informa che queste versioni di SSL hanno delle falle ben conosciute, che un attaccante potrebbe decriptare le comunicazioni o fare da man in the middle. Ci avvisa che in caso di utilizzo, il protocollo viene usato nella versione più aggiornata tra le due macchine che comunicano, ma ci avvisa che in alcuni casi potrebbe non essere così.
Come soluzione ci consiglia di disabilitare SSL 2.0 e 3.0 seguendo la documentazione e abilitare TLS 1.2.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Questo servizio supporta l'utilizzo di cifrari SSL di media forza, cioè secondo Nessus, chiavi che vanno da 64 a 112 bit o ciò che usa 3DES come metodo di cryptazione. Ci suggerisce di riconfigurare l'applicazione in modo da non usare queste chiavi.

90509 - Samba Badlock Vulnerability

Veniamo informati di una backdoor in questa versione di Samba, tramite una vulnerabilità chiamata Badlock. Un man in the middle potrebbe infiltrarsi e intercettare il traffico, e usare questo exploit per forzare un downgrade nel livello di autenticazione.

Dopo ogni scansione ci viene dato una descrizione, una serie di link a delle documentazioni, soluzione al problema,fattore di rischio e altri dati fino alla porta interrogata

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server 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 decipher the remote session or set up a man in the middle attack.

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 particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.0967

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)

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

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/25/smtp