## S5-L3

Vulnerability scanning with Nessus on Meta2

Presented By:

Mattia Di Donato



#### TRACCIA:

Si richiede una scansione tramite l'utilizzo di Nessus di un sistema operativo (abbiamo utilizzato per questa evenienza metasploitable2).

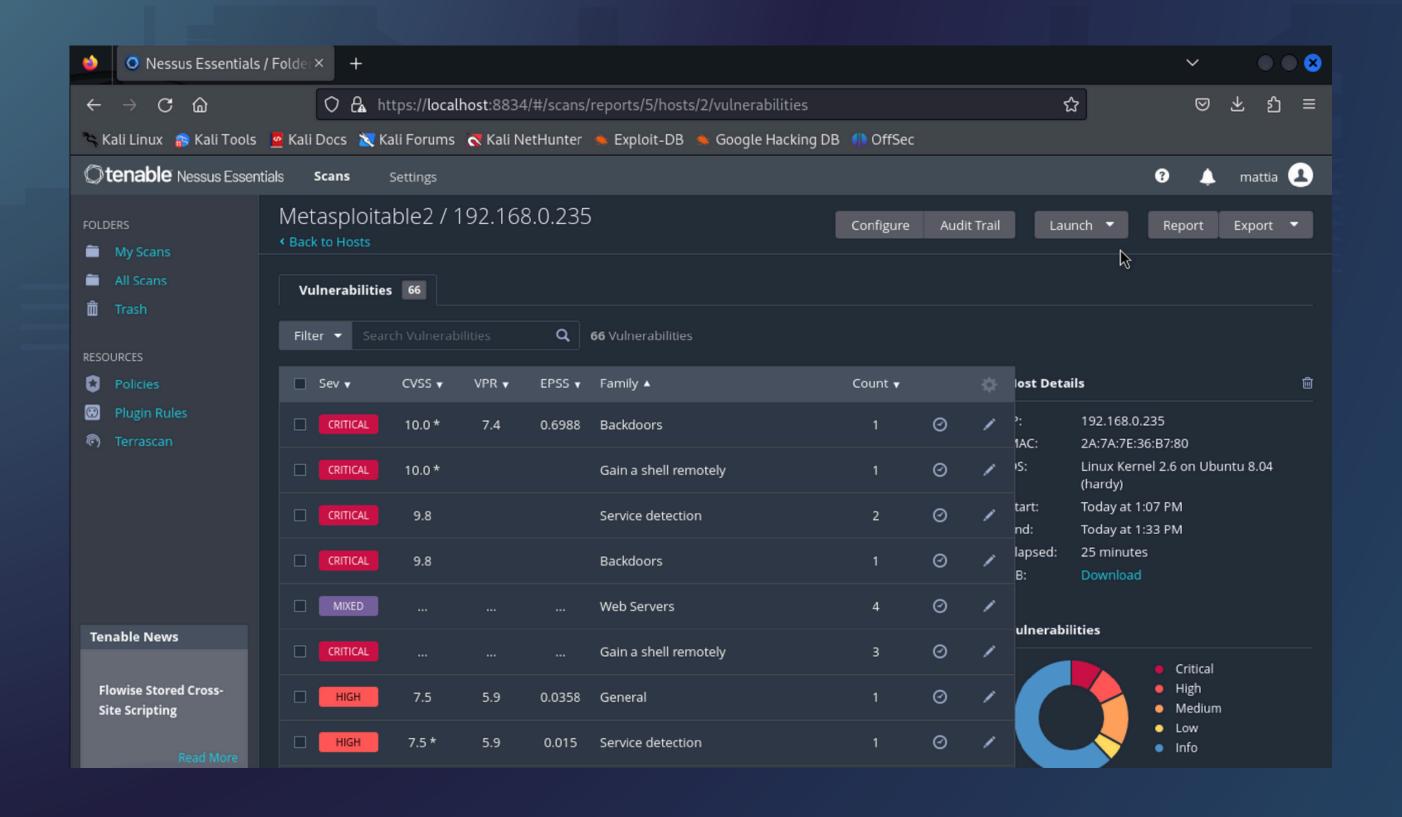
si fornirà poi un report di n.5 vulnerabilità trovate e su come risolverle al meglio.

1 Ambiente Nessus dopo scansione

2 Vulnerabilità trovate

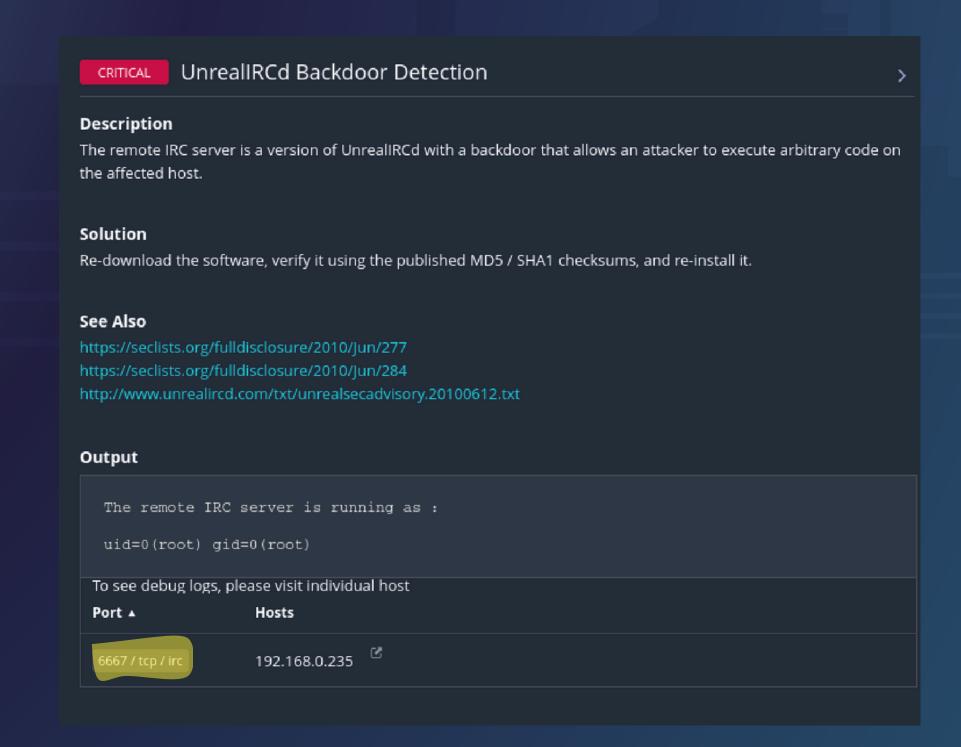
Conclusioni

#### 1. AMBIENTE NESSUS DOPO SCANSIONE



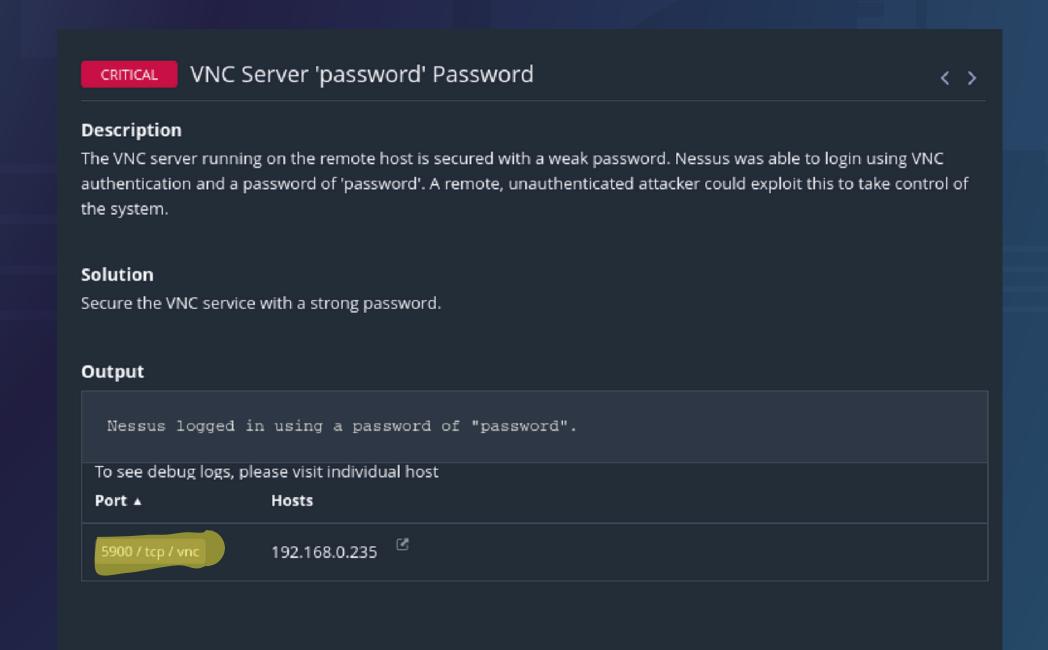
## 2.1 VULNERABILITÀ TROVATE

Da una prima rilevazione abbiamo potuto constatare una vulnerabilità della porta 6667 che è usata per il protocollo IRC (internet relay chat) la quale viene utilizzata per la comunicazione in tempo reale tra più utenti in una chatroom



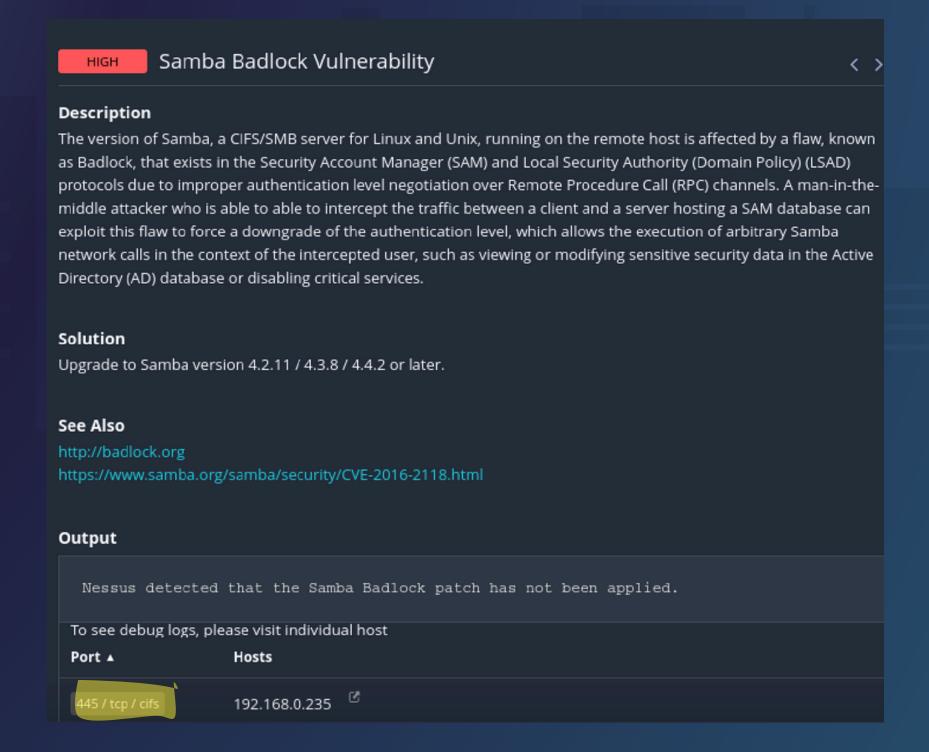
## 2.2 VULNERABILITÀ TROVATE

Da una seconda rilevazione abbiamo potuto constatare una vulnerabilità della porta 5900 che è usata per il protocollo VNC (virtual network computing) la quale consente il controllo remoto di un computer. È una porta esposta a diversi rischi di sicurezza, soprattutto se non configurata e protetta adeguatamente.



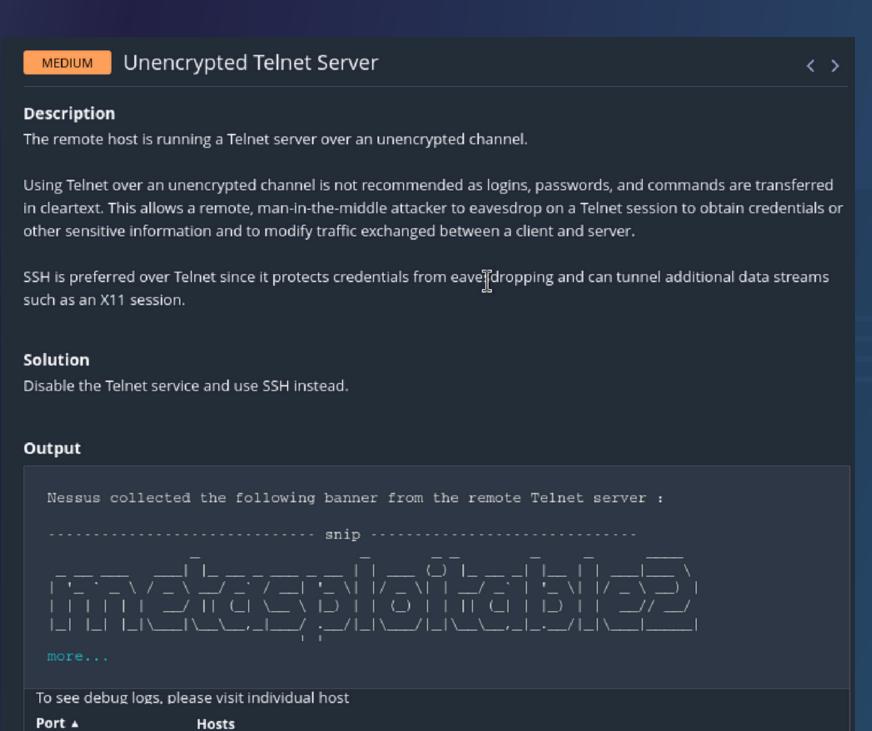
## 2.3 VULNERABILITÀ TROVATE

Da una terza rilevazione abbiamo potuto constatare una vulnerabilità della porta 445 che è usata per il protocollo SMB (server message Block) che consente la condivisione di file, stampanti e altre risorse su reti Windows.



### 2.4 VULNERABILITÀ TROVATE

Da una quarta rilevazione abbiamo potuto constatare una vulnerabilità della porta 23 che è usata per il protocollo telnet che consente l'accesso remoto a dispositivi e server. Tuttavia, Telnet è noto per essere insicuro, poiché trasmette dati, inclusi i dettagli di autenticazione, in chiaro senza crittografia



### 2.5 VULNERABILITÀ TROVATE

Da una quinta e ultima rilevazione abbiamo potuto constatare una vulnerabilità nelle e 25 che 5432 rispettivamente per i protocolli PostgreSQL e SMTP (simple mail transfer protocol). La prima è utilizzata per la gestione di database. È una porta target per attacchi quando il database è accessibile tramite Internet senza adeguate misure di sicurezza. La seconda è utilizzataprincipalmente per l'invio di e-mail. È una delle porte maggiormente bersagliate per attacchi legati allo spam e al phishing, oltre che per l'accesso non autorizzato.

#### 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.

#### 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.

#### See Also

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

#### Output

No output recorded.	
To see debug logs, please visit individual host	
Port ▲	Hosts
5432 / tcp / postgresql	192.168.0.235
25 / tcp / smtp	192.168.0.235 <sup>©</sup>

#### 3. CONCLUSIONI

Per la risoluzione delle vulnerabilità fornite vi consigliamo di utilizzare le seguenti soluzioni:

**Porta 6667** (**IRC**): Disabilitare la porte se non necessaria, limitare l'accesso al firewall, aggiornare software IRC, usare crittografia forte e crittografia TLS.

**Porta 5900** (**VNC**): Usare password complesse, limitare l'accesso al firewall, utilizzare una VPN o SSH per crittografie, aggiornare il software VNC e monitorare le connessioni.

**Porta 445** (**SMB**): Disabilitare SMBv2 o 3 e fare un upgrade, bloccare la porta su reti pubbliche, usare autenticazione forte, aggiornare il sistema operativo, abilitare TLS, e limitare l'accesso tramite firewall.

**Porta 23** (**telnet**): Disabilitare Telnet e usare SSH, limitare l'accesso tramite firewall, usare VPN per l'accesso remoto, e aggiornare i dispositivi.

**Porta 5432** (**PostgreSQL**): Limitare l'accesso tramite firewall, usare password complesse, abilitare SSL, aggiornare PostgreSQL, e monitorare i log di accesso.

**Porta 25** (**SMTP**): Disabilitare open relay, abilitare STARTTLS, richiedere autenticazione, impostare limiti sulle connessioni, abilitare filtri anti-spam, e monitorare i log SMTP.

# THANKYOU MATTIA DI DONATO