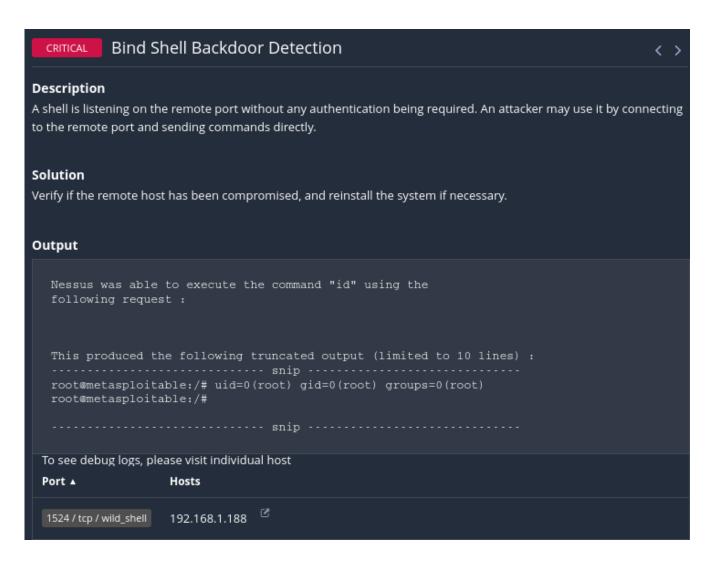
Report S5L5

Sulla base della traccia proposta ho preso in considerazione 4 vulnerabilità critiche del sistema Metasploitable 2 ed in questo report cercherò di descrivere il processo che mi ha portato alla risoluzione del problema.

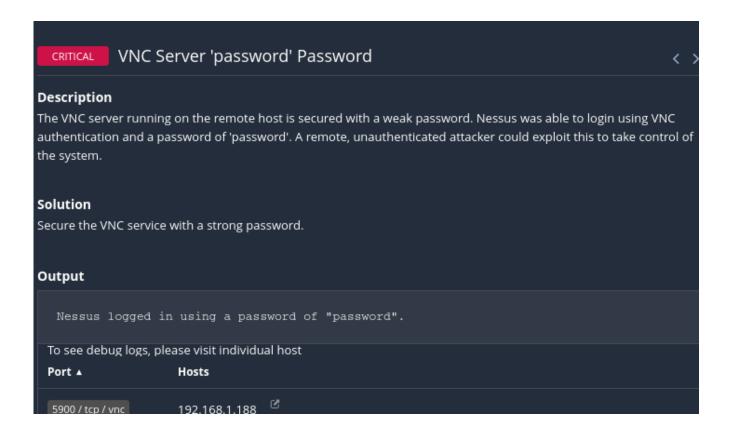
Criticità 1

Nessun ha rilevato la presenza di una backdoor sulla porta 1524. Ho utilizzato iptables per chiudere l'accesso alla backdoor che era in esecuzione sulla porta 1524 della Metasploitable 2. Con il comando "sudo iptables -I INPUT -p tcp --dport 1524 -j REJECT", ho inserito una regola che rifiuta qualsiasi connessione TCP in ingresso su quella porta. Questa regola impedisce efficacemente l'accesso non autorizzato alla backdoor, proteggendo il sistema da potenziali intrusi.



Criticità 2

Qui la scansione Nessun ha rilevato una password insicura, per risolvere il problema ho inserito anche la porta 5900 nelle chain di iptables. Nonostante questo il server VNC dovrebbe poter rimanere accessibile in caso di emergenza, ed è quindi meglio procedere con il cambio della password con una più sicura, per avere la possibilità di riaprire in sicurezza la porta.



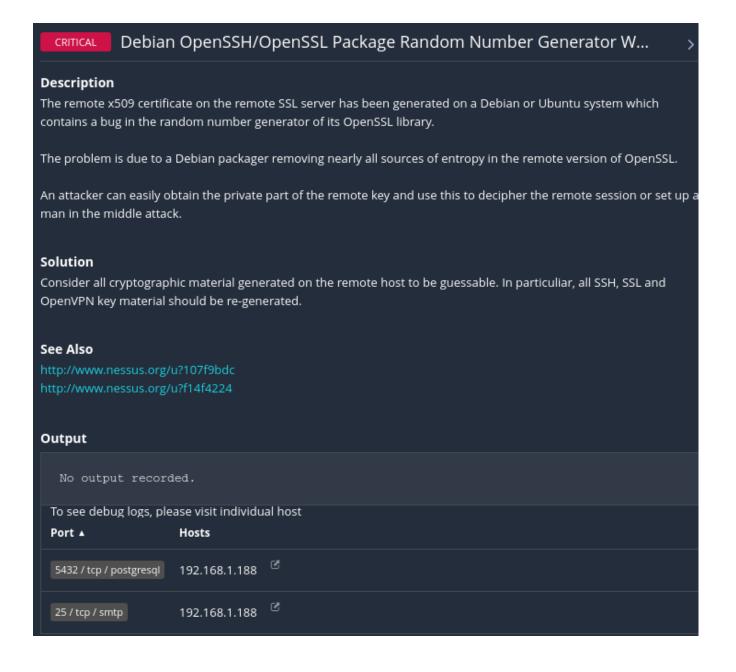
Qui sotto vi sono alcuni tentativi di accesso eseguiti con la Matasploit per avere una conferma rapida della messa in sicurezza della porta.

```
192.168.1.188:5900
                         - 192.168.1.188:5900 - Starting VNC login sweep
  192.168.1.188:5900
                       - No active DB -- Credential data will not be saved!
                         - 192.168.1.188:5900 - LOGIN FAILED: :tunonpuo (Incorrect: Authentication failed)
- 192.168.1.188:5900 - Login Successful: :password
   192.168.1.188:5900
  192.168.1.188:5900
                       - Scanned 1 of 1 hosts (100% complete)
  192.168.1.188:5900
*] Auxiliary module execution completed
                               <mark>logim</mark>) > exploit
nsf6 auxiliary(
*] 192.168.1.188:5900
                        - 192.168.1.188:5900 - Starting VNC login sweep
!] 192.168.1.188:5900
                       - No active DB -- Credential data will not be saved!
   192.168.1.188:5900
                         - 192.168.1.188:5900 - LOGIN FAILED: :tunonpuo (Incorrect: Authentication failed)
                         - 192.168.1.188:5900 - Login Successful: :password
+] 192.168.1.188:5900
                       - 192.108.1.166.19700
- Scanned 1 of 1 hosts (100% complete)
  192.168.1.188:5900
Auxiliary module execution completed
<u>ısf6</u> auxiliary(
                                   ) > exploit
                         - 192.168.1.188:5900 - Starting VNC login sweep
*] 192.168.1.188:5900
                       - No active DB -- Credential data will not be saved!
!] 192.168.1.188:5900
   192.168.1.188:5900
                         - 192.168.1.188:5900 - LOGIN FAILED: <BLANK>:tunonpuo (Unable to Connect: The conr
th (192.168.1.188:5900) timed out.)
                        - 192.168.1.188:5900 - LOGIN FAILED: <BLANK>:password (Unable to Connect: The conn
   192.168.1.188:5900
th (192.168.1.188:5900) timed out.)
*] Auxiliary module execution completed
                               <mark>login</mark>) > exploit
<u>nsf6</u> auxiliary(:
- No active DB -- Credential data will not be saved!
  192.168.1.188:5900
                       - No active bb -- Credentiat data witt not be sure.
- 192.168.1.188:5900 - LOGIN FAILED: <BLANK>:tunonpuo (Unable to Connect: The conn
   192.168.1.188:5900
th (192.168.1.188:5900) timed out.)
   192.168.1.188:5900 - 192.168.1.188:5900 - LOGIN FAILED: <BLANK>:password (Unable to Connect: The conn
th (192.168.1.188:5900) timed out.)
   192.168.1.188:5900 - Scanned 1 of 1 hosts (100% complete)
  Auxiliary module execution completed
<u>sf6</u> auxiliary(
```

Criticità 3 e 4

Qui c'è un bug nella generazione del materiale crittografato, che permette ad un eventuale intruso di risalire alle chiavi. Anche queste porte sono state rese inaccessibili tramite iptables.

Per risolvere il problema del generatore di numeri casuali compromesso è necessario generare e installare un nuovo certificato SSL/TLS sul server remoto.



Debian OpenSSH/OpenSSL Package Random Number Generator W...

<

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 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

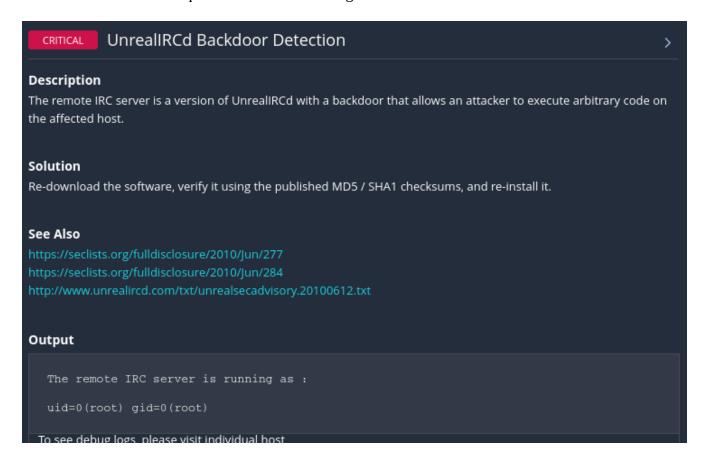
Port ▲ Hosts

22 / tcp / ssh 192.168.1.188

Criticità 5

Anche sulla porta 6667 è stata rilevata una backdoor molto pericolosa, Anche in questo caso la porta è stata messa in sicurezza tramite regola di firewall.

In questo caso Nessus consiglia di reinstallare il software.



Scan finale di nessus

In somma grazie ad una corretta configurazione del firewall è stato possibile eliminare la maggior parte delle criticità, per le ultime due criticità rimanenti è necessario aggiornare i software Unix e Tomcat.

☐ Sev	▼ CVS	VPR ▼	Name ▲	Family ▲	Count ▼		₽
CRI	ITICAL 10.	0	Unix Operating System Unsupport	General		Ø	1
CRI	ITICAL 9.8	9.0	Apache Tomcat AJP Connector Req	Web Servers		0	1
	IIGH 7.5	5.9	Samba Badlock Vulnerability	General		0	1
	IIGH 7.5	j	NFS Shares World Readable	RPC		0	1
☐ ME	DIUM 6.5	;	Unencrypted Telnet Server	Misc.		0	1
	IIXED		DNS (Multiple Issues)	DNS	3	0	1
	IIXED		3 HTTP (Multiple Issues)	Web Servers	3	0	1
	IIXED		SMB (Multiple Issues)	Misc.	2	0	1
	.0W 2.6		X Server Detection	Service detection		Ø	1