

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.

CRITICAL Bind Shell Backdoor Detection < >

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution


Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0 (root) gid=0 (root) groups=0 (root)
root@metasploitable:/#
----- snip -----
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.188 

Criticità 2

Qui la scansione Nessus 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.

CRITICAL VNC Server 'password' Password < >

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.


Solution

Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.188 

Qui sotto vi sono alcuni tentativi di accesso eseguiti con la Metasploit 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 - 192.168.1.188:5900 - LOGIN FAILED: :tunonpuo (Incorrect: Authentication failed)
[+] 192.168.1.188:5900 - 192.168.1.188:5900 - Login Successful: :password
[*] 192.168.1.188:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 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 - 192.168.1.188:5900 - Login Successful: :password
[*] 192.168.1.188:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 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: <BLANK>:tunonpuo (Unable to Connect: The connection (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 connection (192.168.1.188:5900) timed out.)
[*] 192.168.1.188:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 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: <BLANK>:tunonpuo (Unable to Connect: The connection (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 connection (192.168.1.188:5900) timed out.)
[*] 192.168.1.188:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

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.

CRITICAL

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

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 particular, 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

192.168.1.188



25 / tcp / smtp

192.168.1.188



CRITICAL

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 particular, 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.

CRITICAL UnrealIRCd Backdoor Detection >

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/Jun/277>
<https://seclists.org/fulldisclosure/2010/Jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>




Output

```
The remote IRC server is running as :  
  
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

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.

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupport...	General	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Req...	Web Servers	1	🕒 ✎
<input type="checkbox"/>	HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	🕒 ✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🕒 ✎
<input type="checkbox"/>	MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1	🕒 ✎
<input type="checkbox"/>	MIXED	 DNS (Multiple Issues)	DNS	3	🕒 ✎
<input type="checkbox"/>	MIXED	 HTTP (Multiple Issues)	Web Servers	3	🕒 ✎
<input type="checkbox"/>	MIXED	 SMB (Multiple Issues)	Misc.	2	🕒 ✎
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection	1	🕒 ✎