

Vulnerability Assessment Report

Target: Metasploitable2

Durata temporale dell'attività:

7 ore

Attività eseguita da:

Leonzio Emanuele

Indice generale Sommario

Screenshot VNC Server 'password' Password e relativa spiegazione.....	2
Screenshot Bind Shell Backdoor Detection e relativa spiegazione.....	4
Screenshot Debian OpenSSH/OpenSSL Package Random Number Generator Weakness e Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) e relativa spiegazione	6

Report Vulnerabilità

1. Screenshot VNC Server 'password'

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo problema per assumere il controllo del sistema. Pertanto possiamo rimediare configurandolo con una password robusta.

Implicazioni di sicurezza

1. **Accesso non autorizzato:** Se il servizio VNC non è protetto da una password robusta o se è configurato per non richiedere alcuna password, un attaccante potrebbe accedere facilmente al sistema remoto.
2. **Man in the middle (MitM):** Se il traffico VNC non è crittografato, un attaccante potrebbe intercettare le credenziali e i dati trasmessi tra il client VNC e il server, sfruttando tecniche di **sniffing** della rete.
3. **Esecuzione di comandi malevoli:** Un attaccante che ottiene l'accesso al sistema tramite VNC potrebbe eseguire comandi, installare software dannoso o compromettere il sistema in altro modo.

Un attaccante, dunque, potrebbe sfruttare la vulnerabilità in diversi modi:

- **Indovinare o forzare la password:** Se la password del VNC è debole o facile da indovinare, un attaccante potrebbe utilizzare tecniche di **brute-force** per ottenere l'accesso.
- **Sfruttare la mancanza di crittografia:** Se il traffico tra il client e il server VNC non è criptato, un attaccante potrebbe usare strumenti come **Wireshark** per intercettare i dati in chiaro, incluse le credenziali di accesso.

Impatto CVSS Base Score: 10.0

Ecco i passi eseguiti da admin:

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$
```

2. Screenshot Bind Shell Backdoor Detection

Descrizione

La vulnerabilità Bind Shell Backdoor Detection indica che una shell di comando è in ascolto su una porta remota senza richiedere autenticazione. Questo potrebbe consentire a un attaccante di eseguire comandi sul sistema senza restrizioni. La presenza di una bind shell è un forte indicatore che il sistema è stato compromesso.

Per prima cosa andiamo a vedere, con Nessus, qual è la porta compromessa. In questo caso è la 1524.

Cos'è una backdoor?

Una **backdoor** è un accesso non autorizzato al sistema che viene lasciato aperto da un attaccante, di solito per permettere future intrusioni. Un processo che espone una backdoor può essere un programma che gira in background e che ascolta su una porta di rete specifica, consentendo a un attaccante di accedere al sistema senza autenticazione o con un metodo non sicuro.

Quando una vulnerabilità backdoor è identificata, l'attaccante può aver eseguito un processo specifico sulla macchina che rimane attivo in attesa di comandi remoti. Questo processo avrà un PID che può essere utilizzato per monitorare o terminare il processo.

Il **PID** (Process ID) è un identificatore unico che il sistema operativo assegna a ciascun processo in esecuzione. Ogni volta che un programma o un servizio viene avviato su una macchina, il sistema operativo gli assegna un PID per tenere traccia di quel processo specifico.

Nel contesto di una **vulnerabilità di backdoor** (come nel caso di **UnrealIRCd Backdoor Detection**), il PID si riferisce all'identificatore del processo malevolo o sospetto che sta eseguendo una backdoor sulla macchina compromessa.

Come identificare un processo backdoor tramite PID

Se una backdoor è stata identificata su un sistema come Metasploitable2 (o qualsiasi altro sistema), dovrai identificare il processo che la sta eseguendo per poterlo fermare o rimuovere.

Impatto CVSS Base Score: 10.0

Una volta identificata la porta, determiniamo quale processo è responsabile:

1. Troviamo il PID del processo;
2. Conferma il binario eseguibile;

```
msfadmin@metasploitable:~$ sudo lsof -i :1524
COMMAND PID USER  FD   TYPE DEVICE SIZE MODE NAME
xinetd  4465 root   12u  IPv4 12162      TCP *:ingreslock (LISTEN)
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ ps -p 4465
  PID TTY          TIME CMD
 4465 ?            00:00:00 xinetd
msfadmin@metasploitable:~$
```


Poi andiamo ad Arrestare il processo sospetto con il comando “sudo kill -9 <PID>”

```
msfadmin@metasploitable:~$ sudo kill -9 4465
msfadmin@metasploitable:~$
```



Inoltre per una prevenzione futura configuriamo un firewall per bloccare connessioni non autorizzate o un firewall più moderno come ufw.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rules updated
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```



3. Screenshot Debian OpenSSH/OpenSSL Package Random Number Generator Weakness / Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

La vulnerabilità "**Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**" deriva da un problema nella generazione di numeri casuali su alcune versioni di OpenSSL distribuite con Debian e Ubuntu. Questo problema può compromettere la sicurezza dei certificati SSL/TLS utilizzati dal server, consentendo a un attaccante di calcolare la chiave privata associata e decifrare la comunicazione.

Descrizione della vulnerabilità

Nel **2008**, un grave difetto è stato introdotto nel pacchetto OpenSSL presente su Debian a causa di una modifica effettuata da un manutentore del pacchetto. Questo difetto ha compromesso la qualità della generazione di numeri casuali nel sistema, in particolare nella libreria di OpenSSL. La vulnerabilità è nota come:

- **Debian OpenSSL Weakness.**
- **CVE-2008-0166** (Common Vulnerabilities and Exposures).

Il problema è stato causato dal fatto che il manutentore di Debian aveva **rimosso quasi tutte le fonti di entropia** (casualità) durante la creazione delle chiavi crittografiche e dei numeri casuali usati da OpenSSL. Di conseguenza, **OpenSSL** utilizzava una sequenza di numeri casuali **prevedibili** anziché numeri realmente casuali e sicuri. In altre parole, il generatore di numeri casuali di OpenSSL su Debian (e su sistemi basati su Debian) è diventato vulnerabile a un attacco, in quanto i numeri generati erano facilmente prevedibili.

Come funziona il problema

Un generatore di numeri casuali è cruciale per la sicurezza di molti algoritmi crittografici, inclusi quelli usati in **SSL/TLS** e in **OpenSSH**. Durante la creazione di chiavi crittografiche, certificati SSL o nella generazione di chiavi SSH, viene utilizzato un generatore di numeri casuali per produrre valori imprevedibili.

Nel caso della vulnerabilità, **OpenSSL** su Debian non era in grado di generare numeri veramente casuali. A causa della debolezza nel generatore di numeri casuali, le chiavi

crittografiche generate erano vulnerabili a **attacchi di brute-force** o a **attacchi basati sulla previsione della chiave**.

Questo significa che se un attaccante otteneva accesso a una chiave criptata, sarebbe stato in grado di calcolare facilmente la chiave privata associata, permettendo così di decifrare il traffico protetto da SSL/TLS o SSH.

Implicazioni di sicurezza

Le principali implicazioni di questa vulnerabilità sono:

1. **Compromissione delle chiavi private:** Se un attaccante riesce a prevedere i numeri casuali generati per creare una chiave SSH o un certificato SSL, può derivare facilmente la chiave privata e decifrare o compromettere le comunicazioni protette.
2. **Attacchi di man-in-the-middle:** Con una chiave privata compromessa, un attaccante potrebbe impersonare il server e intercettare o manipolare il traffico cifrato. Questo è particolarmente pericoloso in contesti come SSH o HTTPS, dove la protezione delle comunicazioni è essenziale.
3. **Rischio di compromissione di sistemi critici:** Se il sistema utilizza le chiavi compromesse per autenticarsi o cifrare comunicazioni sensibili (come il traffico tra server, o la gestione di dati sensibili), l'attaccante potrebbe sfruttare la vulnerabilità per ottenere l'accesso ai sistemi e ai dati.

Impatto CVSS Base Score: 9.8

Ecco come risolvere la vulnerabilità:

1. Identificare la versione vulnerabile di OpenSSL

Verifica la versione di OpenSSL installata e se fosse necessario aggiornarla:

```
msfadmin@metasploitable:~$ openssl version -a
OpenSSL 0.9.8g 19 Oct 2007
built on: Tue Apr 24 15:22:46 UTC 2012
platform: debian-i386-i686/cmov
options: bn(64,32) md2(int) rc4(idx,int) des(ptr,risc1,16,long) blowfish(idx)
compiler: gcc -fPIC -DOPENSSL_PIC -DZLIB -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -DL_ENDIAN -DTERMIO -O3 -march=i686 -Wa,--noexecstack -g -Wa,--noexecstack -DOPENSSL_BN_ASM_PART_WORDS -DOPENSSL_IA32_SSE2 -DSHA1_ASM -DMD5_ASM -DRMD160_ASM -DAES_ASM
OPENSSLDIR: "/usr/lib/ssl"
```


2. Rigenerare i certificati SSL vulnerabili

I certificati SSL generati con versioni vulnerabili di OpenSSL devono essere rigenerati.

Elimina il certificato e la chiave attuali e Rigenera nuovi certificati:

```
msfadmin@metasploitable:~$ sudo rm /etc/ssl/private/ssl-cert-snakeoil.key
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo rm /etc/ssl/certs/ssl-cert-snakeoil.pem
msfadmin@metasploitable:~$ sudo dpkg-reconfigure ssl-cert
sudo: dpkg-reconfigure: command not found
msfadmin@metasploitable:~$ sudo dpkg-reconfigure ssl-cert
msfadmin@metasploitable:~$
```

Dopo aver aggiornato OpenSSL e rigenerato i certificati, riavviamo tutti i servizi che utilizzano SSL/TLS per garantire che carichino i nuovi certificati.

```
msfadmin@metasploitable:~$ sudo /etc/init.d/apache2 restart
[sudo] password for msfadmin:
* Restarting web server apache2 [ OK ]
msfadmin@metasploitable:~$ _
```

```
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh restart
* Restarting OpenBSD Secure Shell server sshd [ OK ]
msfadmin@metasploitable:~$
```