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.

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Solution

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

Soluzione

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

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:/#
```

Con iptablet ho cercato di applicare delle regole. Ho provato anche a mettere input/output/forward in DROP.

Ho provato ad utilizzare un'opzione di iptables che ci permette di filtrare solo i pacchetti di tipo SYN. I pacchetti di tipo SYN vengono inviati da un host a un server per aprire una connessione. A seconda di come risponderà il server potrà avvenire o meno il collegamento.
Questo meccanismo, che È alla base del protocollo TCP, viene chiamato three-way handshake consta di 3 fasi (noi abbiamo analizzato solo la prima), sulle quali non ci soffermiamo, ma che potrebbero essere oggetto di una trattazione futura. Per fare in modo di scartare i pacchetti con la flag SYN attivata potremo usare l'opzione --syn. Ad esempio:

iptables -A INPUT -i ppp0 -p tcp --syn -j DROP

Farà in modo di bloccare tutto il traffico TCP proveniente da Internet e con il quale si richiede di aprire una connessione con la nostra postazione

Con molte di queste opzioni È possibile usare l'operatore ! (NOT) per indicare tutto ciò che non fa riferimento al parametro che stiamo passando. Poniamo ad esempio di volere tener disponibile a chiunque da Internet solo il nostro server Web presente sulla nostra rete locale, mentre vogliamo

impedire che qualcuno acceda a tutti gli altri servizi presenti. Per far questo basterà usare iptables in questo modo:

iptables -A INPUT -i ppp0 -p tcp --syn --dport ! 80 -j DROP

Per quel che riguarda il protocollo ICMP È possibile anche specificare il tipo sul quale vogliamo agire tramite l'opzione --icmp-type tipo. Ad esempio:

iptables -A INPUT -p icmp --icmp-type 0 -j DROP

Per bloccare tutti gli ICMP di tipo echo-reply, e quindi i ping.