

## **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:/#
```