

## Nessus

A seguito di una scansione delle vulnerabilità di un sistema Metasploitable sono state trovate svariate vulnerabilità alcune più critiche altre meno

Nel documento successivo analizzeremo 3 di queste criticità e cercheremo di mitigare il rischio di questecriticità

La prima criticità in questione è legata al Server VNC

**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	192.168.64.10 

Come è possibile notare attraverso nessus è stato molto semplice exploitare la password del server.

La soluzione a questo tipo di criticità è l'utilizzo di una password più sicura.

Nel report viene evidenziata un'altra criticità importante, una backdoor.

Questa porta potrebbe essere inutilizzata, se questo è il caso per limitare il rischio di un possibile exploit attraverso questa porta l'ideale sarebbe disattivarla.

Questo tipo di criticità è possibile evidenziarla anche attraverso il software nmap, individuando esattamente la backdoor aperta ovvero la 1524.

**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 / wlld_shell	192.168.64.10 

[illegible]

Questo tipo di vulnerabilità è dovuta al fatto che la comunicazione attraverso questa porta non è criptata quindi è preferibile disattivarla oppure utilizzare una porta criptata come la SSH. Non essendo una porta criptata trasmette tutte le informazioni in chiaro, quindi è possibile che vengano trasmessi dati sensibili in chiaro.