

## S5 L4 NESSUS

In questo esercizio, abbiamo utilizzato l'applicativo NESSUS.

Abbiamo effettuato una "BASIC NETWORK SCAN", delle well know ports verso l'ip di metasploit.

Ottenendo come risultato delle vulnerabilità, divise per gravità.

Sotto riportiamo 4 delle più gravi.

**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.

Il servizio VNC, permette il controllo remoto di un host. In questo caso, ci indica di utilizzare un password più efficace, poiché un malintenzionato, potrebbe prendere facilmente controllo dell'host in questione.

**CRITICAL** Unix Operating System Unsupported Version Detection

**Description**  
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.  
  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**  
Upgrade to a version of the Unix operating system that is currently supported.

Qui indica, invece, che stiamo utilizzando una versione di Unix non recente, pertanto, consiglia di aggiornarla in modo tale da avere le ultime patch di sicurezza disponibili.

**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.

Bindshell permette di accedere all'host senza bisogno di alcuna autenticazione.

**CRITICAL** NFS Exported Share Information Disclosure

**Description**  
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**  
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

NFS(NETWORK FILE SHARING), riguarda la possibilità, di condividere file e cartelle con altri client linux nella rete. Pertanto rende facile, attivare la condivisioni di file e quindi rubarne il contenuto.