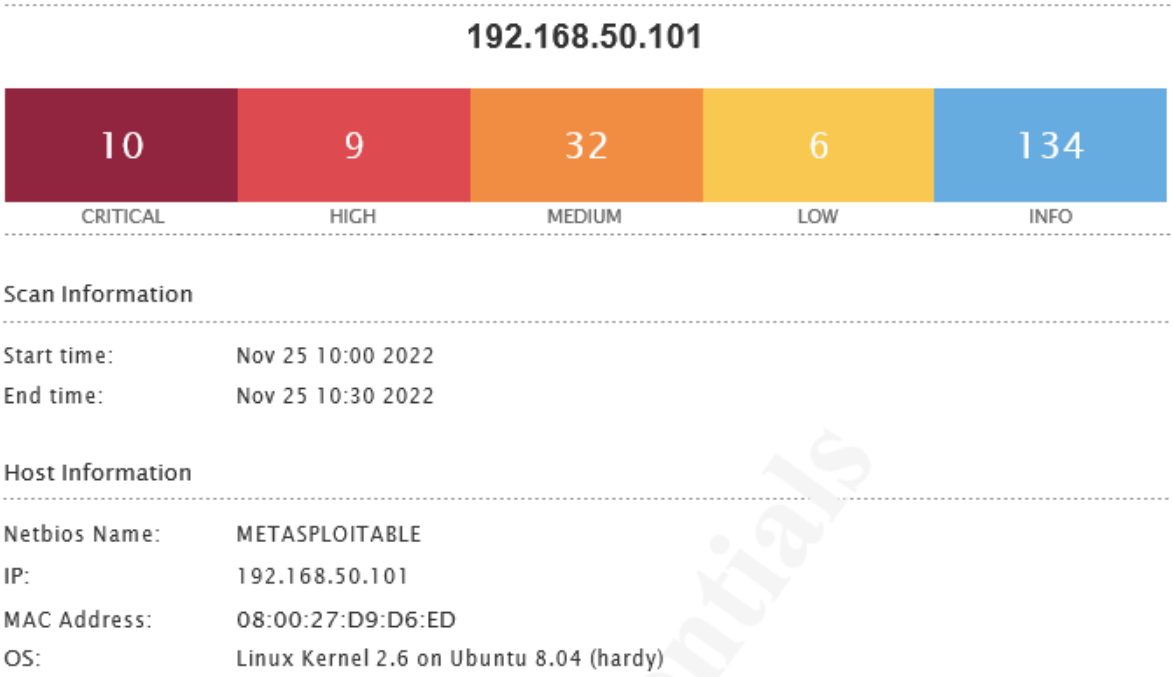
Gabriele Di giampietro **Data 25/11/2022**

Obbiettivo: Effettuare una VA sulla macchina virtuale Metasploitable, analizzare e attuare delle remediation action su un minimo di 2 ad un massimo di 4 vulnerabilità trovate di livello Critical.

Report per il Tecnico

Metasploitable

Report generated by Nessus™ 25/11/2022



11356 - 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.

- Risk Factor: Critical
- Plugin Output: udp/2049/rpc-nfs

61708 - 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.

- Risk Factor: Critical
- Plugin Output: tcp/5900/vnc

51988 – 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.

- Risk Factor: Critical
- Plugin Output: tcp/1524/wild_shell