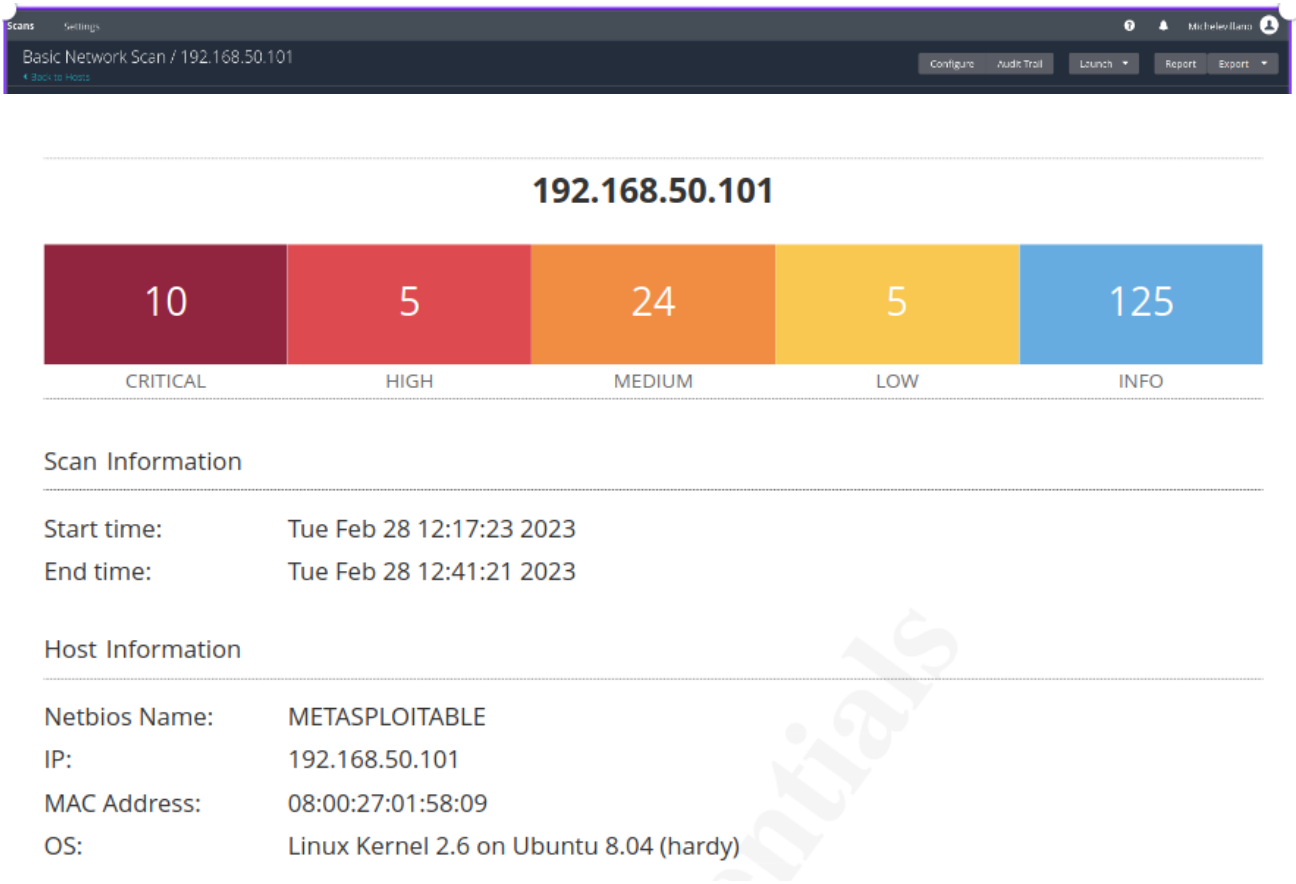
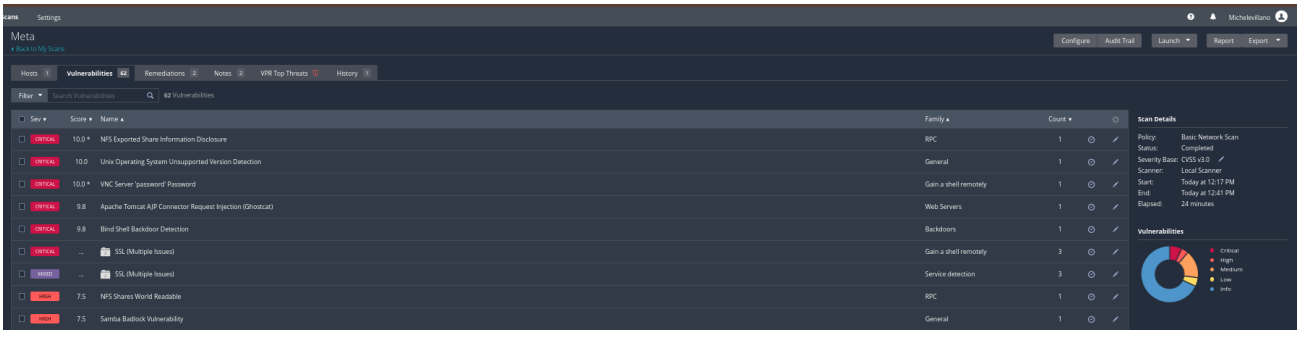
Progetto Week 5 - Scansione inizio su Nessus

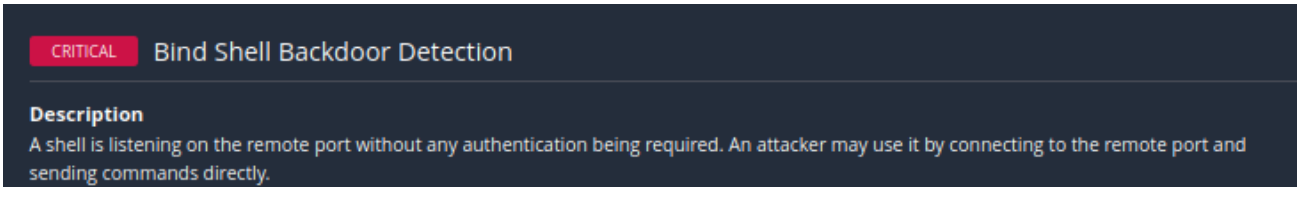


Il report di Nessus, eseguito il 28 Febbraio sulla macchina Metasploitable, evidenzia 10 vulnerabilità di critical level. Vediamo sommariamente le vulnerabilità, che saranno oggetto del nostro studio.



Osserviamo le vulnerabilità, piu nel dettaglio:

1- Bind Shell Backdoor Detection



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 / wild_shell	192.168.50.101

La scansione ha rilevato la presenza di una shell in ascolto su una porta remota, senza alcuna autenticazione richiesta, ovvero una backdoor attiva. Ciò significa che un attaccante potrebbe utilizzare tale shell accedendo alla porta remota e inviando comandi direttamente. Il comando è stato eseguito con l'identità di root e quindi con privilegi da amministratore. Un attaccante potrebbe, pertanto, sfruttare questa vulnerabilità per assumere il controllo del sistema e compromettere i dati. La soluzione raccomandata da Nessus è quella di verificare se la macchina remota è stata compromessa e reinstallare il sistema se necessario. In ogni caso, è importante adottare misure di sicurezza aggiuntive per impedire futuri attacchi di questo tipo, ad esempio inserire un firewall.

2- NFS Exported Share Information Disclosure

CRITICAL NFS Exported Share Information Disclosure

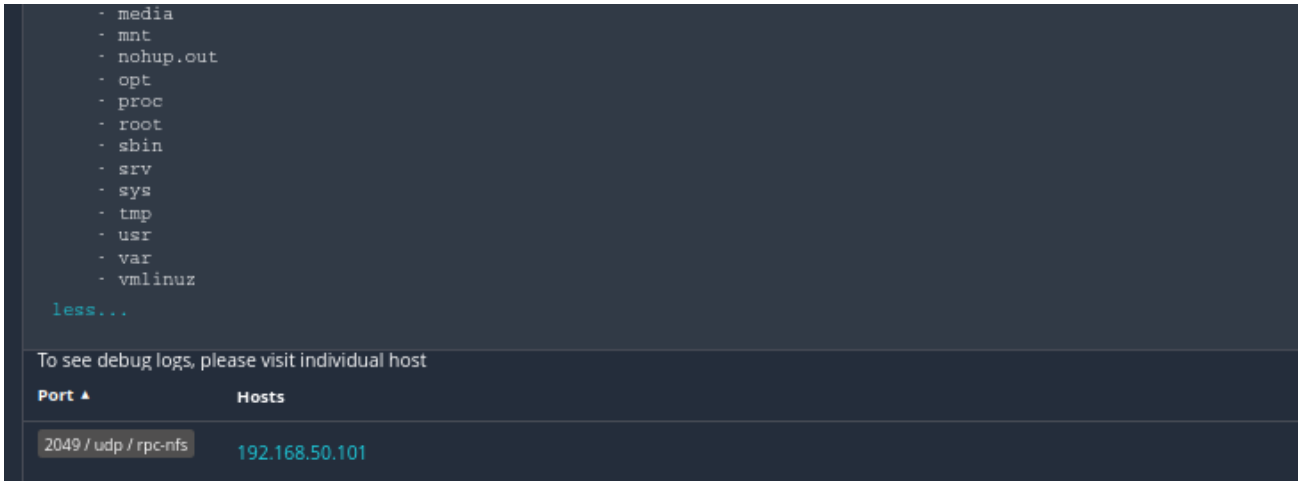
Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

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

Output

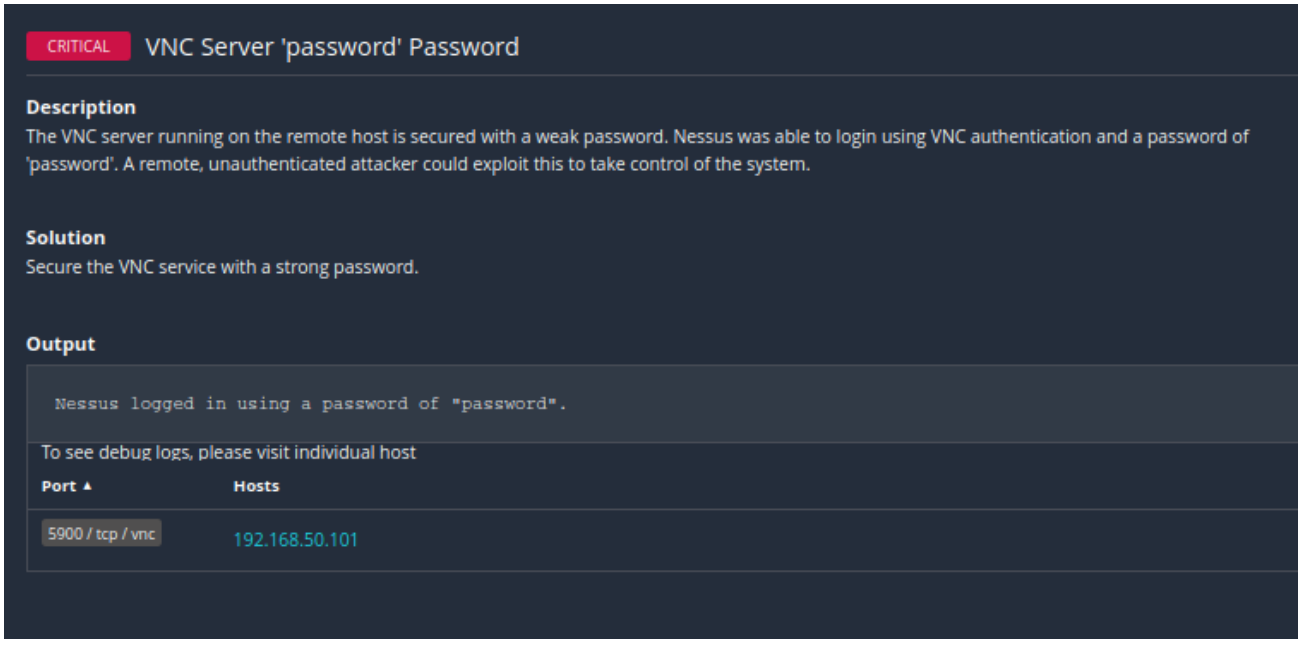
```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
```



La seconda vulnerabilità rileva la presenza di una condivisione NFS (Network File System) esportata tramite il servizio UDP sulla porta 2049 (rpc-nfs). Ciò significa che è possibile accedere alla condivisione NFS sul server remoto e che un attaccante potrebbe sfruttare questa vulnerabilità per leggere e scrivere file sul server remoto.
La soluzione raccomandata da Nessus è di riconfigurare NFS sul terminale Meta, in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

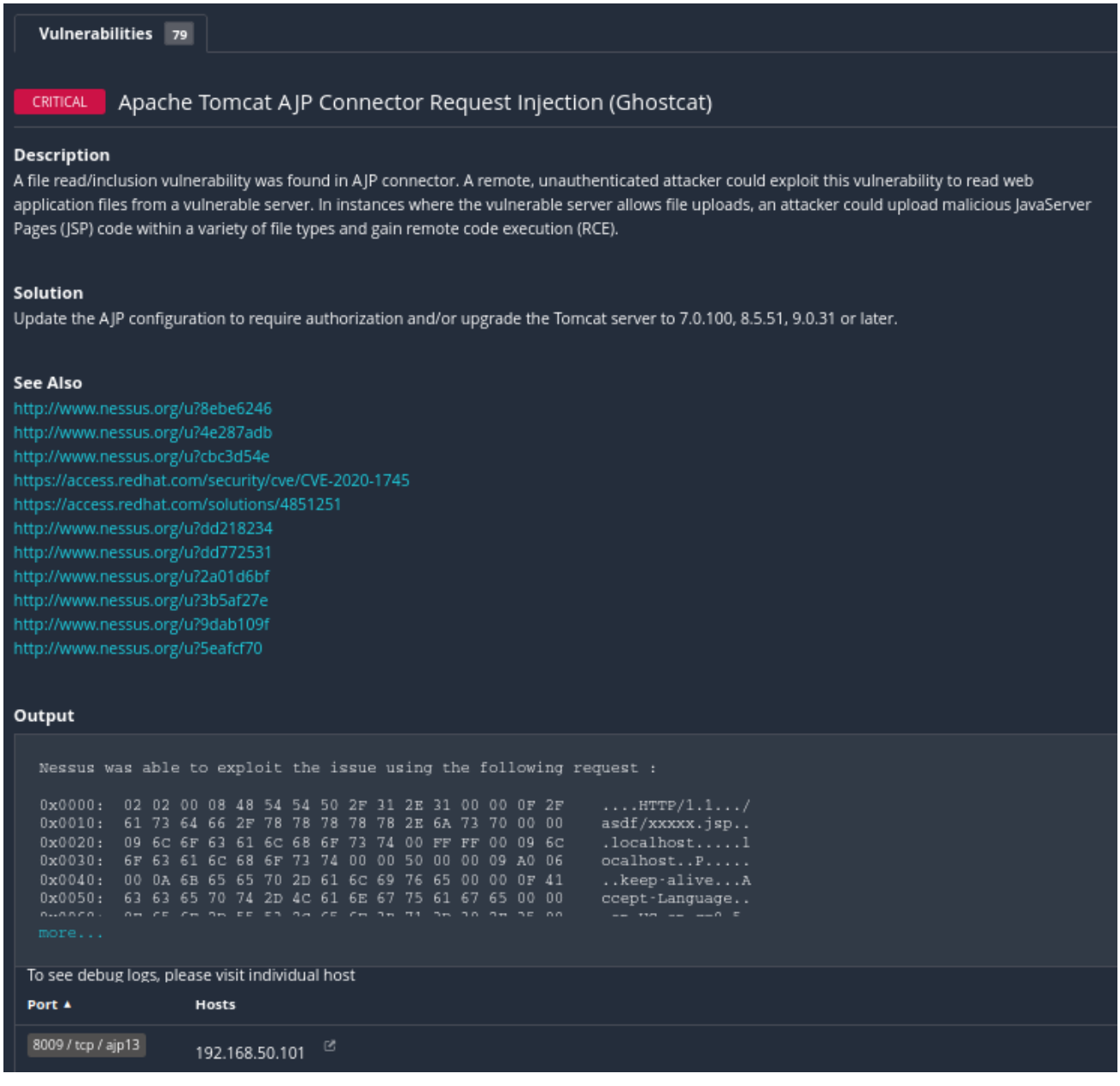
3- VNC Server 'password' Password



La scansione qui ha rivelato che il server VNC (Virtual Network Computing) è protetto da una password debole. Piu precisamente, Nessus è stato in grado di effettuare il login tramite l'autenticazione VNC, utilizzando una password predefinita, ovvero "password". Ciò indica che un attaccante esterno potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.
La soluzione raccomandata è di proteggere il servizio VNC con una password forte e sicura.
In sintesi, la scansione eseguita da Nessus ha individuato una vulnerabilità critica di sicurezza, relativa al livello di protezione che offre la password per il servizio VNC sulla macchina

Metasploitable, il che potrebbe consentire ad un attaccante non autenticato di prendere il controllo del sistema. Difatti, "password" è la pass piu utilizzata: è bene cambiarla.

4- Apache Tomcat AJP Connector Request Injection (Ghostcat)



La vulnerabilità rilevata riguarda una versione vulnerabile di Apache Tomcat AJP Connector, che potrebbe consentire ad un attaccante esterno di leggere e modificare i file di un'applicazione web o addirittura eseguire codice malevolo a distanza.
La soluzione proposta da Nessus è di aggiornare la configurazione AJP. Se autorizzati, si può procedere con un aggiornamento ulteriore del server Tomcat ad una versione successiva alla 7.0.100, ad esempio la 8.0.53.