**INDIVIDUAZIONE DI VULNERABILITà E IMPLEMENTAZIONE DI AZIONI DI RIMEDIO**

**Traccia:** Effettuare una scansione completa sul target Metasploitable.  
 Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

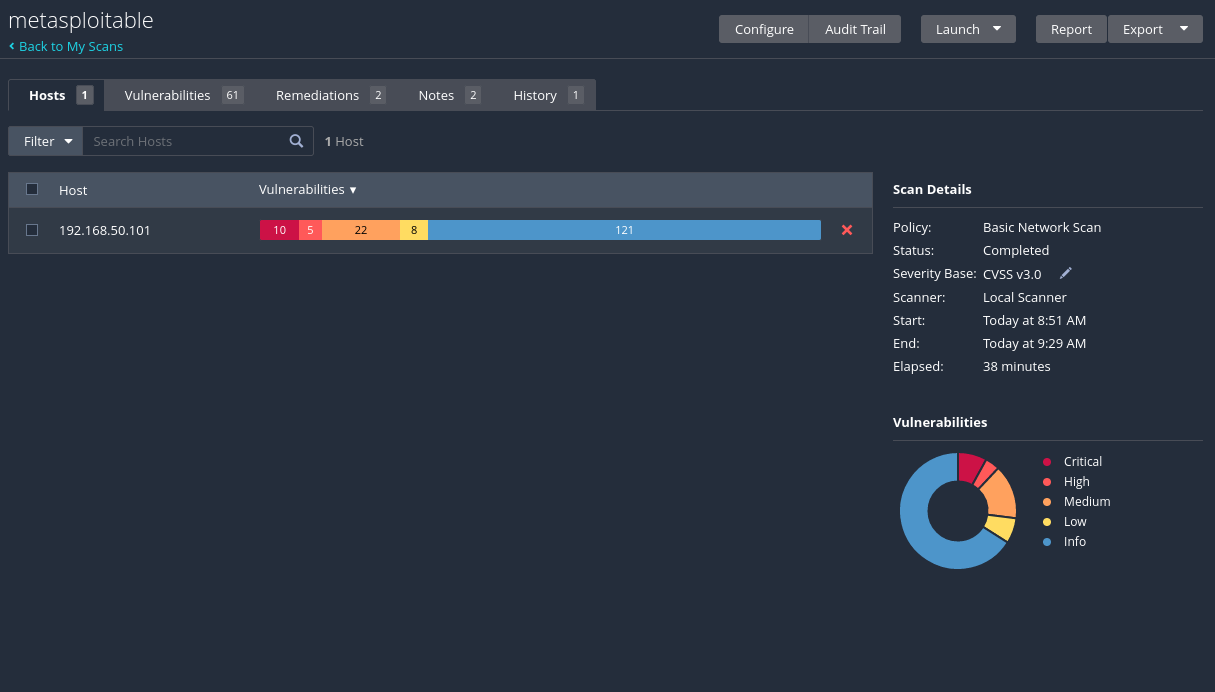
N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l’efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

**Procedimento:**

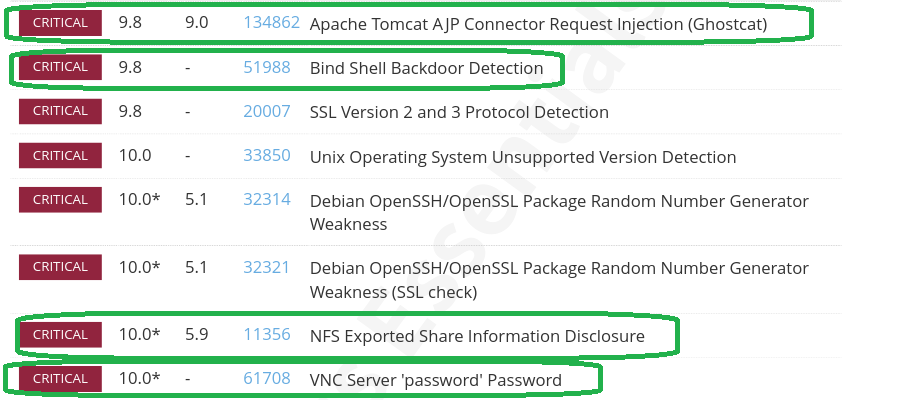
Per la prova di oggi, si effettuerà un Vulnerability Scan della macchina Metasploitable con il programma Nessus. Nessus è un vulnerability scanner che offre una vasta gamma di funzionalità tra cui scansioni automatiche e preimpostate, enumerazione e valutazioni di vulnerabilità note riscontrate e generazione di report dettagliati con link a documentazione apposita per le vulnerabilità trovate.

Nessus ha un’interfaccia user friendly e abbastanza intuitiva. Per lo scan dell’esercitazione, si utilizza la basic network scan: una scansione che andrà a scannerizzare le porte più comuni e utilizzate, insieme ai servizi a loro associate.



Finita la scansione, è possibile vedere tutte le vulnerabilità riscontrate dal programma e classificate secondo il CVSS (Common Vulnerabilities Scoring System), che aiuta lo scanner ad associare un livello di rischio ben specifico a una data vulnerabilità.

Sfruttando la funzione di report di Nessus, andiamo a scegliere le 4 vulnerabilità e proviamo ad implementare delle azioni di rimedio.



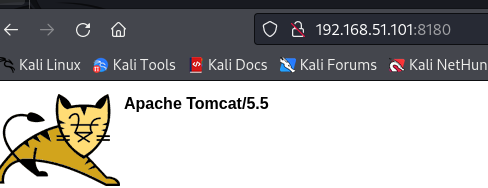
Iniziamo a implementare le azioni di rimedio seguendo un’ordine dall’alto verso il basso:

1. **Apache Tomcat AJP Connector Request Injection (GhostCat)**

Questa vulnerabilità è stata riscontrata sulla porta 8009 della macchina target.

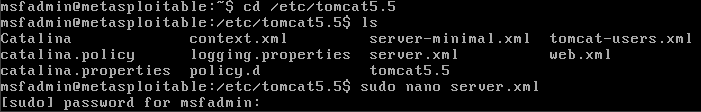
L’AJP Connector del servizio Apache Tomcat, potrebbe permettere ad un attaccante di leggere file di applicazioni web da un server vulnerabile. Se nel malaugurato caso che fosse permesso il caricamento di file da parte del server, l’attaccante potrebbe caricare del software malevolo e ottenere il permesso di eseguire comandi da remoto.

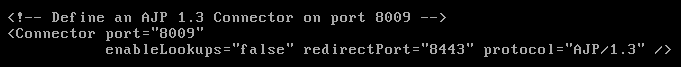
Possiamo verificare la versione di Tomcat attualmente installata digitando l’IP della macchina target:8180 che è la porta a cui viene reindirizzato il servizio Tomcat.



Ci sono varie soluzioni al problema, in questo caso imposteremo l’AJP Connector in modo tale che richieda un'autorizzazione per essere usato.

Su meta ci sposteremo nella directory di tomcat, una volta lì apriremo il file server.xml che contiene le impostazioni di configurazione del servizio.





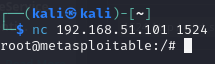


Inserendo i parametri secret Required="true” e secret="microkernel", facciamo in modo che l’AJP connector richieda un’autorizzazione e che la password da inserire equivalga al parametro secret.

Questo andrà a mitigare la vulnerabilità.

1. **Bind Shell Backdoor Detection**

Sulla porta 1524 è presente una backdoor che dà accesso ai comandi di root della macchina target tramite una shell. Per connettersi alla backdoor, basta utilizzare un software come netcat, inserendo l’IP e la porta interessati.

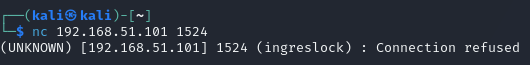


Così abbiamo accesso di root. Per prima cosa dobbiamo individuare il processo che rende possibile il bindshell. Su meta utilizziamo la linea di comando sudo **lsof -i :’1524’** per trovare tutti i processi di rete attivi sulla porta 1524. Il comando lsof viene usato per ottenere informazioni sui file aperti in quel momento dai processi. Con l’opzione -i andiamo a chiedere informazioni riguardo i processi di rete e poi restringiamo ancora di più il campo aggiungendo la porta che ci interessa.



In questo modo vediamo che il processo colpevole è il 4447 che è in ascolto sulla porta.

Usando il comando kill 4447 su meta, riusciamo ad eliminare il processo.



Questo però non basta a eliminare la backdoor definitivamente, ma la blocca per questo ciclo. Al riavvio della macchina, il processo riprenderà perciò dobbiamo creare una regola nel firewall per impedire l’accesso alla porta.



Attivando questa regola nel firewall di PFsense, abbiamo bloccato tutto il traffico verso la porta 1524 della macchina meta.

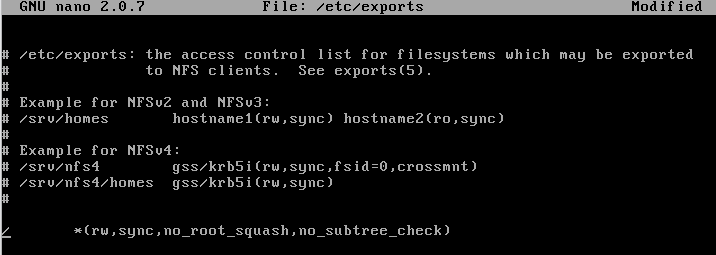


1. **NFS Exported Share Information Disclosure**

Network File Sharing permette di condividere directory e file con altri su una rete.

NFS è mal configurata sulla porta 2049 e permetterebbe a un potenziale attaccante di accedere alle directory condivise, leggerle e addirittura scriverci. Configureremo due file di NFS per restringere le cartelle condivise e la rete su cui queste saranno disponibili.

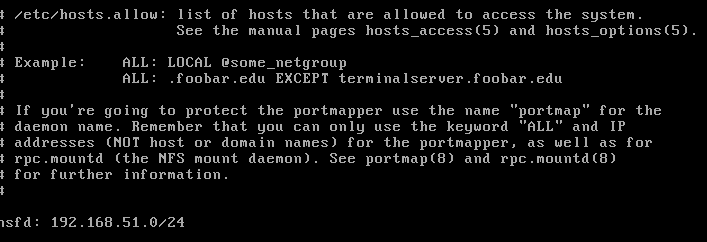
1 - Exports: File dove vengono specificate quali directories sono condivise dall’host con gli altri client e quali permessi vengono dati ai client. In questo caso specifico, vediamo che tutte le directories sono condivise, indicato con il segno /.



Vediamo come siano disponibili i permessi di lettura e scrittura, la sincronizzazione dei dati, il no\_root\_squash che permette al root del client NFS di accedere a tutto ciò che viene condiviso senza bisogno di privilegi e il no\_subtree\_check che permette l’accesso anche a sottocartelle che non sono state esplicitamente esportate o condivise. In questo file, specifichiamo che solo la directory /srv/nfs possa essere montata.



2 - Hosts.allow = File dove vengono specificati i client autorizzati ad accedere. Di default, chiunque può accedere all’NFS ma noi andremo a specificare che solo gli IP del network 192.168.51.0/24 possono accedere.



Con le nostre modifiche, il file sharing ora avviene solo tra i dispositivi nella rete interna 192.168.51.0/24.

**4) VNC Server 'password' Password**

Virtual Network Computing (VNC) è un servizio di accesso remoto usato principalmente per scopi amministrativi. La vulnerability scan ci segnala che sulla porta 5900, il servizio è protetto da una password debole e facilmente vulnerabile ad attacchi di tipo bruteforce.

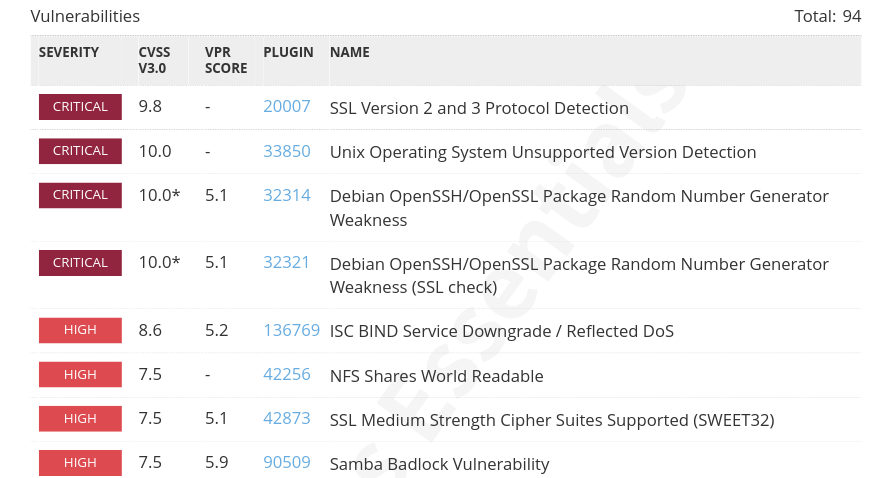
Andremo a modificare la password per renderla più forte e più sicura, usando il comando vncpasswd.



Una volta cambiata la password, il sistema dovrebbe essere più sicuro.

**Conclusione:**

Effettuiamo una nuova scansione con Nessus, per vedere se le vulnerabilità sono state effettivamente sanate.



Le vulnerabilità segnalate prima non sono più riportate quindi le azioni di rimedio e mitigazione implementate hanno avuto esito positivo.