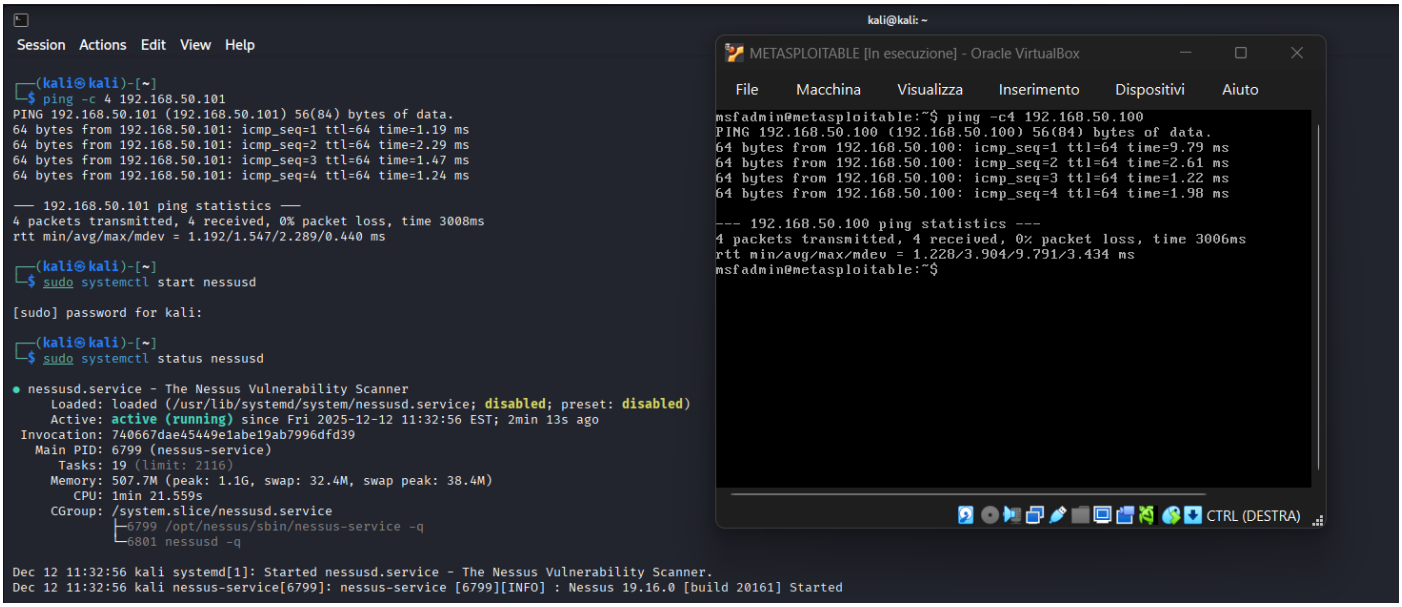
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il presente report riporta i risultati di un'attività di analisi delle vulnerabilità volta al fine di valutarne il livello di esposizione a rischi di sicurezza.
L'analisi è stata condotta utilizzando **Nessus** come strumento principale per l'identificazione automatizzata delle vulnerabilità, **Kali Linux** come piattaforma di verifica tecnica dei servizi esposti e **Metasploitable** come sistema oggetto dell'analisi.
Attraverso l'integrazione di questi strumenti è stato possibile individuare le principali criticità presenti, intervenire sui servizi più a rischio e verificare l'efficacia delle azioni correttive applicate, fornendo una valutazione dello stato di sicurezza del sistema.

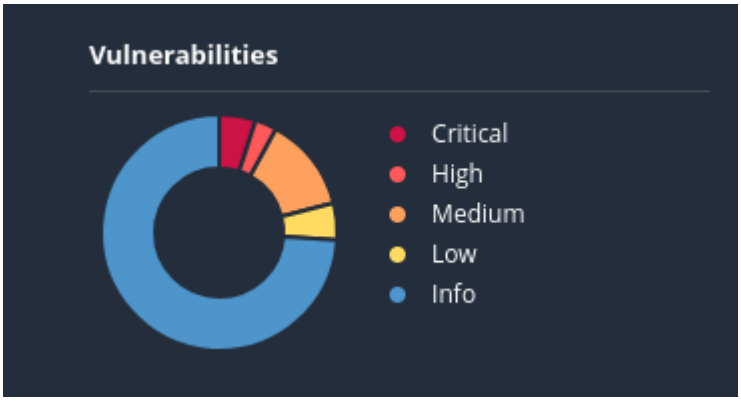
OBIETTIVO: l'obiettivo del presente lavboratorio è individuare e ridurre le vulnerabilità più rilevanti presenti sul sistema, migliorandone il livello di sicurezza complessivo e diminuendo il rischio di accessi non autorizzati o compromissioni dei servizi.

SCANSIONI EFFETTUATE



Prima di avviare le attività di analisi, è stata effettuata una fase preliminare di verifica dell'ambiente operativo al fine di garantire la piena operatività dei sistemi coinvolti.
In questa fase è stata controllata la connettività di rete tra le macchine utilizzate, assicurando che i sistemi fossero correttamente raggiungibili e in grado di comunicare tra loro in modo stabile; i test di connettività hanno confermato l'assenza di perdite di pacchetti e la corretta latenza di rete, indicando che l'infrastruttura era idonea a supportare le successive attività di analisi.
Successivamente è stato avviato **Nessus** (strumento dedicato all'analisi automatizzata delle vulnerabilità) verificandone lo stato operativo per assicurare che il motore di scansione fosse correttamente in esecuzione; il controllo dello stato del servizio ha confermato che Nessus risultava attivo e funzionante, condizione necessaria per garantire l'affidabilità delle analisi successive.
Questa fase di preparazione ha permesso di escludere problematiche infrastrutturali o di servizio, creando le condizioni operative adeguate per l'avvio delle attività di rilevazione delle vulnerabilità sui sistemi target.

Una volta verificata la corretta comunicazione di rete tra i sistemi coinvolti, è stata avviata un'attività strutturata di analisi delle vulnerabilità.
A tal fine è stato utilizzato **Nessus** configurato per eseguire una scansione completa del sistema target e la suddetta scansione è stata condotta sull'host **Metasploitable**, utilizzato come sistema da analizzare, con l'obiettivo di individuare vulnerabilità note e servizi esposti.

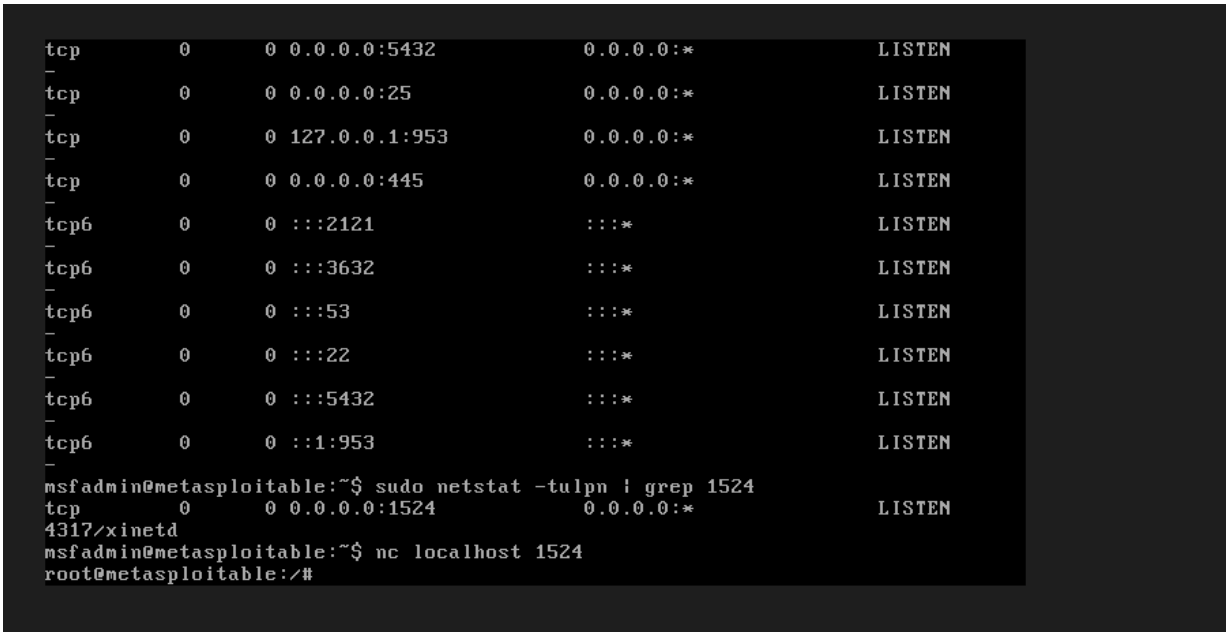


Al termine del processo, Nessus ha prodotto una vista consolidata dello stato di sicurezza del sistema analizzato, classificando le vulnerabilità individuate in base al loro livello di gravità.
I risultati ottenuti evidenziano la presenza di vulnerabilità **critiche** e **ad alta severità**, oltre a segnalazioni di livello medio, basso e informativo; questa distribuzione indica un'esposizione significativa del sistema, con rischi concreti per la riservatezza, l'integrità e la disponibilità delle risorse.
L'analisi ottenuta ha costituito la base per le successive attività di approfondimento e mitigazione, consentendo di identificare in modo prioritario le vulnerabilità più rilevanti e di definire interventi correttivi.

BIND SHELL BACKDOORD DETECTION

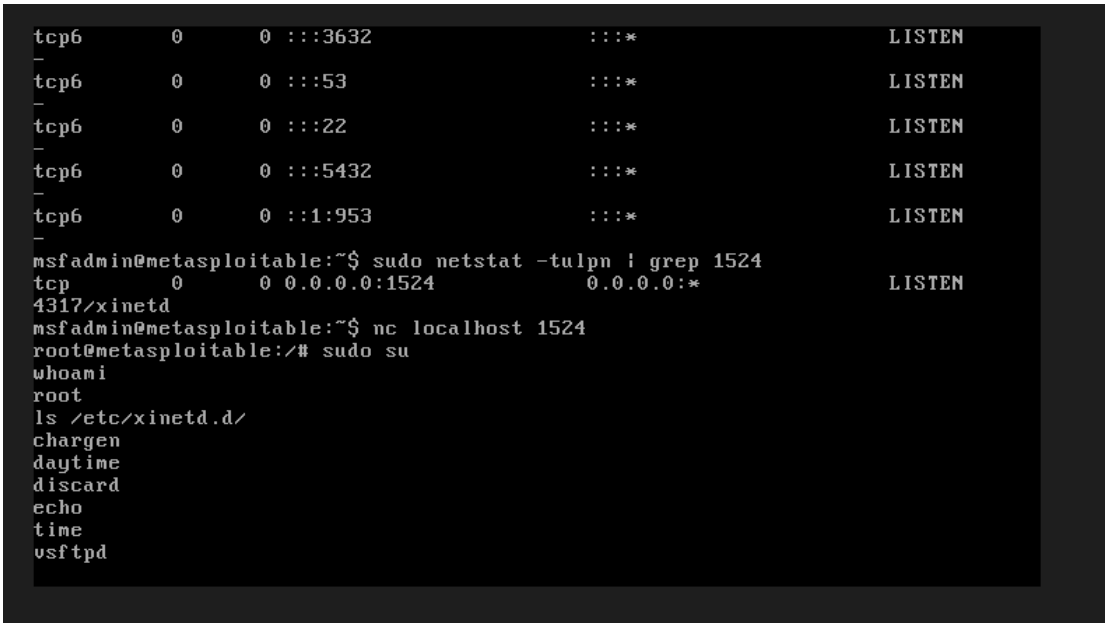
Nel corso dell'attività di analisi delle vulnerabilità è stata individuata una criticità classificata come **Bind Shell Backdoor Detection**.
Tale vulnerabilità indica la presenza di un servizio di rete in ascolto che espone direttamente una shell di sistema su una porta TCP, consentendo potenzialmente l'accesso remoto non autorizzato al sistema.

Attraverso un controllo dei servizi attivi e delle porte di rete in stato di ascolto, è stata confermata la presenza di una porta aperta associata a un processo non coerente con i servizi legittimi del sistema.
Questa verifica ha permesso di individuare con precisione il punto di esposizione utilizzato dalla bind shell.

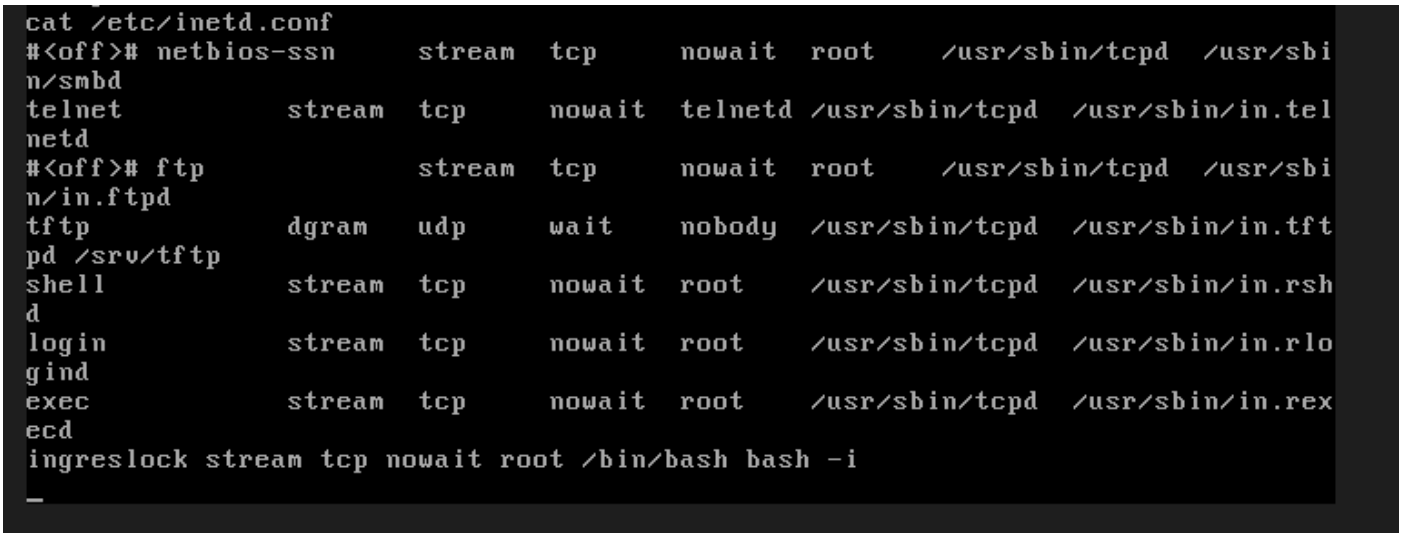


Successivamente, l'analisi è stata approfondita esaminando nel dettaglio le porte di rete attive sul sistema. Il controllo ha evidenziato la presenza di una porta TCP in ascolto, identificata come **1524**, associata al servizio *ingreslock* e gestita dal demone *xinetd*, un comportamento non coerente con le funzionalità operative legittime del sistema.
Un'ulteriore verifica ha confermato che tale porta consentiva una connessione locale senza

alcun meccanismo di autenticazione, configurazione tipica di una *bind shell*, utilizzata per fornire accesso diretto alla shell di sistema.

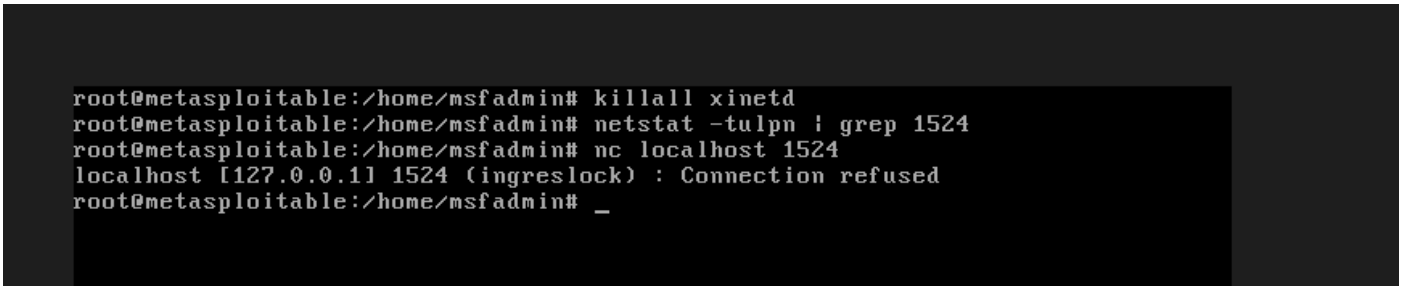


Successivamente è stato verificato il contesto di esecuzione del servizio, accertando che l'accesso ottenuto consentiva l'esecuzione di comandi con privilegi elevati.
L'analisi dei servizi gestiti da *xinetd* ha permesso di circoscrivere ulteriormente l'origine della configurazione insicura, confermando che la *porta 1524* non era riconducibile ad alcun servizio legittimo necessario al funzionamento del sistema.
Questi riscontri hanno consolidato l'evidenza che il sistema fosse esposto ad una vulnerabilità critica in grado di consentire l'accesso remoto non autorizzato e il pieno controllo dell'host compromesso.

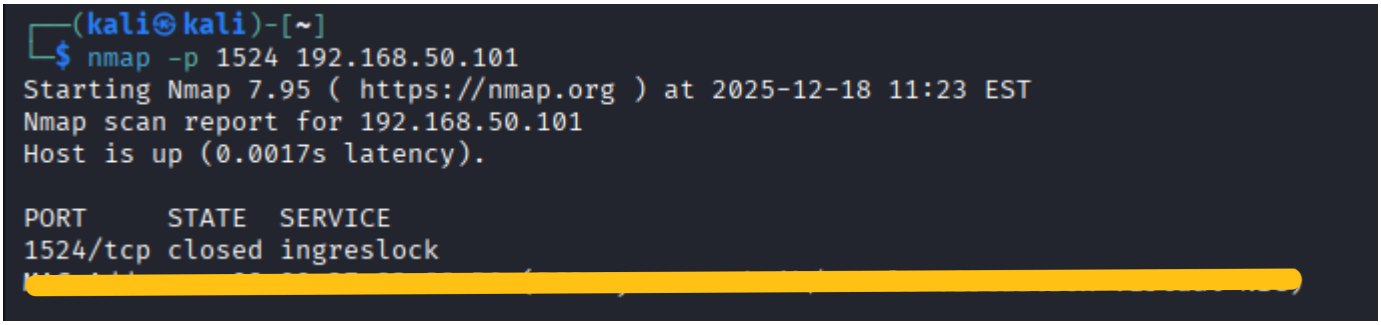


Proseguendo l'analisi, è stato quindi necessario individuare l'origine della porta 1524 e comprenderne la configurazione a livello di servizio.

L’esame dei file di configurazione del superserver di rete ha evidenziato la presenza di una voce specifica che definiva il servizio *ingreslock* come *servizio attivo*; tale servizio risultava configurato per accettare connessioni TCP e avviare direttamente una shell di sistema (/bin/bash) con privilegi elevati, senza prevedere alcun meccanismo di autenticazione o controllo degli accessi.
Questa configurazione conferma che la porta individuata non era riconducibile a un servizio applicativo legittimo, bensì a una funzionalità deliberatamente esposta per fornire accesso diretto alla shell del sistema.
La presenz77a di tale impostazione all’interno della configurazione di rete rappresenta un’evidente condizione di rischio, in quanto consente a un attaccante di ottenere un accesso immediato al sistema semplicemente stabilendo una connessione alla porta in ascolto.
L’analisi del file di configurazione ha quindi permesso di identificare con precisione il meccanismo attraverso cui la *bind shell* veniva resa disponibile, fornendo una conferma definitiva della vulnerabilità segnalata e del relativo vettore di esposizione.



A seguito dell’identificazione del servizio responsabile dell’esposizione, è stato eseguito un intervento di mitigazione mirato mediante l’arresto di xinetd, responsabile dell’attivazione della bind shell associata alla porta 1524.
Successivamente, è stata effettuata una nuova verifica delle porte di rete in stato di ascolto, che ha confermato la chiusura della porta precedentemente esposta e l’impossibilità di stabilire ulteriori connessioni verso il servizio *ingreslock*.
Il rifiuto esplicito della connessione ha evidenziato la corretta disattivazione della bind shell e l’eliminazione del canale di accesso non autorizzato, confermando l’efficacia dell’azione correttiva adottata e la rimozione della vulnerabilità individuata.



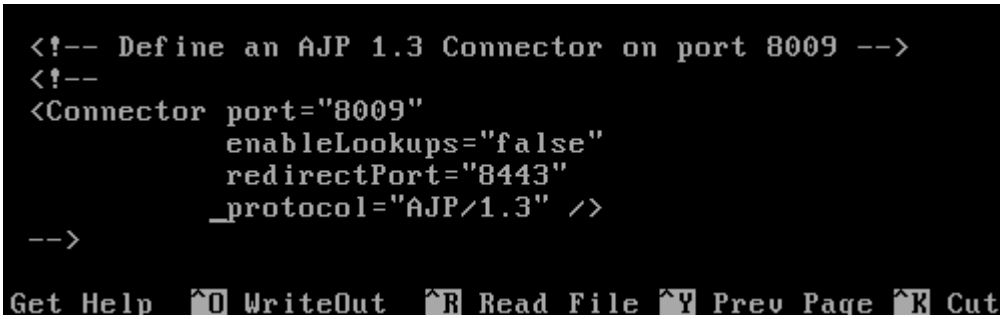
Al termine è stata eseguita una verifica mirata, finalizzata a confermare l'effettiva rimozione del punto di esposizione precedentemente individuato.
Il controllo ha evidenziato che la porta *TCP 1524*, in precedenza in stato di ascolto e associata al servizio *ingreslock*, risulta ora chiusa e non più raggiungibile dall'esterno.
L'esito della scansione conferma che il servizio responsabile non è più attivo e che il sistema non espone più la shell di sistema attraverso tale porta.
Questa verifica conclusiva attesta l'avvenuta mitigazione della vulnerabilità e l'eliminazione del rischio di accesso remoto non autorizzato precedentemente rilevato.

```
root@metasploitable:/home/msfadmin# sudo netstat -tulpn | grep 8009
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
4347/jsvc
root@metasploitable:/home/msfadmin# _
```

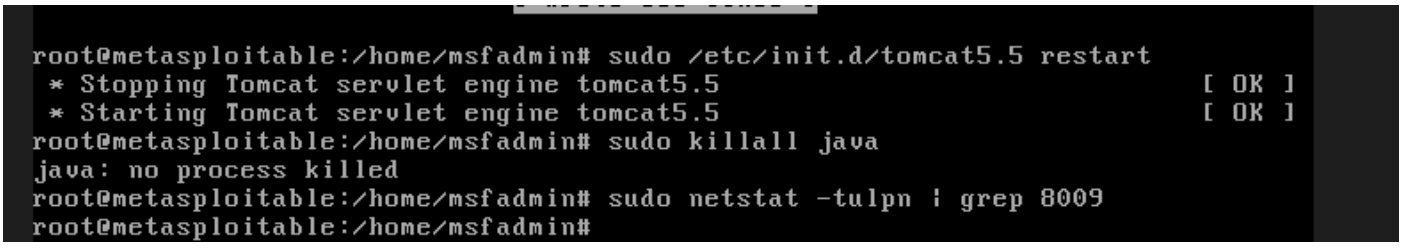
Nel corso dell'analisi delle vulnerabilità condotta tramite Nessus, è stata rilevata una vulnerabilità classificata come **Apache Tomcat AJP Connector Request Injection**.
Questa vulnerabilità è dovuta all'esposizione del connettore *AJP* (Apache JServ Protocol) di *Tomcat*, un componente progettato per la comunicazione interna tra il web server e l'application server, che non dovrebbe essere direttamente accessibile dalla rete.
A seguito della segnalazione è stata effettuata una verifica diretta sul sistema per identificare l'effettiva esposizione del servizio; l'analisi delle porte di rete ha confermato la presenza di *una porta TCP in stato di ascolto sulla 8009*.

```
root@metasploitable:/home/msfadmin# grep -R "8009" /etc/tomcat5.5/
/etc/tomcat5.5/server.xml:    <!-- Define an AJP 1.3 Connector on port 8009 -->
/etc/tomcat5.5/server.xml:    <Connector port="8009"
grep: warning: /etc/tomcat5.5/tomcat5.5: recursive directory loop

/etc/tomcat5.5/server-minimal.xml:    <Connector port="8009" protocol="AJP/1.3"
/>
```

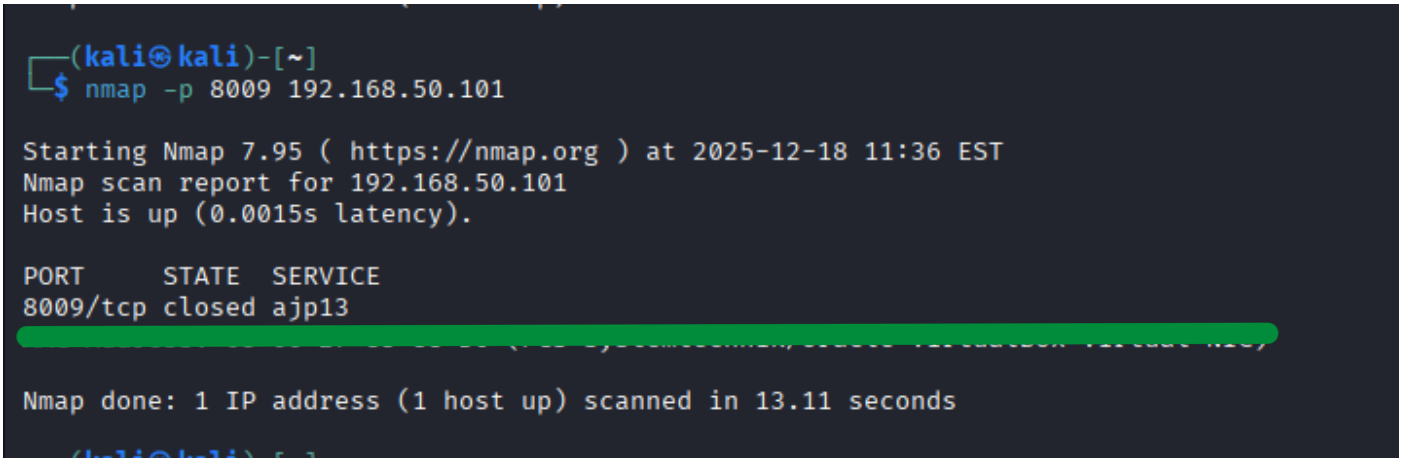
Per approfondire l'origine dell'esposizione del servizio, l'analisi è stata estesa ai file di configurazione di Apache Tomcat: l'ispezione dei file di configurazione ha evidenziato la presenza esplicita del connettore AJP 1.3 (configurato sulla porta 8009) definito all'interno dei file *server.xml* e *server-minimal.xml*.
La configurazione individua un *Connector* attivo che utilizza il protocollo AJP/1.3, senza restrizioni di accesso e senza meccanismi di autenticazione o limitazione dell'origine delle richieste.
Questa impostazione conferma che il servizio non solo era in ascolto a livello di rete, ma risultava anche abilitato e operativo a livello applicativo, rendendo il sistema vulnerabile a richieste arbitrarie dirette al backend di Tomcat.
La presenza di tale configurazione costituisce l'elemento tecnico che giustifica la rilevazione della vulnerabilità da parte di Nessus, in quantoi l'esposizione del connettore AJP consente l'inoltro diretto di richieste verso le risorse interne dell'application server, aggirando i controlli previsti per il traffico HTTP standard.



A qusto punto si è intervenuti direttamente sul file di configurazione *server.xml* di Apache Tomcat, andando a commentare la stringa che definisce il connettore AJP 1.3 sulla porta 8009.
In particolare, il blocco *<Connector port="8009" protocol="AJP/1.3" /> è* stato racchiuso tra *commenti XML,* disabilitando di fatto il servizio AJP.
Questa modifica è stata effettuata con l'obiettivo di *interrompere l'esposizione del connettore AJP*, che rappresenta il prerequisito tecnico alla base della vulnerabilità trattata; commentando il connettore, Tomcat smette di accettare connessioni AJP sulla porta 8009, impedendo qualsiasi interazione diretta tramite questo protocollo.
In questo modo viene eliminata la possibilità di sfruttare la fiducia implicita del protocollo AJP per inoltrare richieste manipolate o accedere a risorse interne; qquesto intervento conferma che la vulnerabilità non è legata all'applicazione in sé, ma alla presenza e all'esposizione del connettore AJP e dimostra come la sua disabilitazione rappresenti una misura di mitigazione efficace per ridurre il rischio associato.

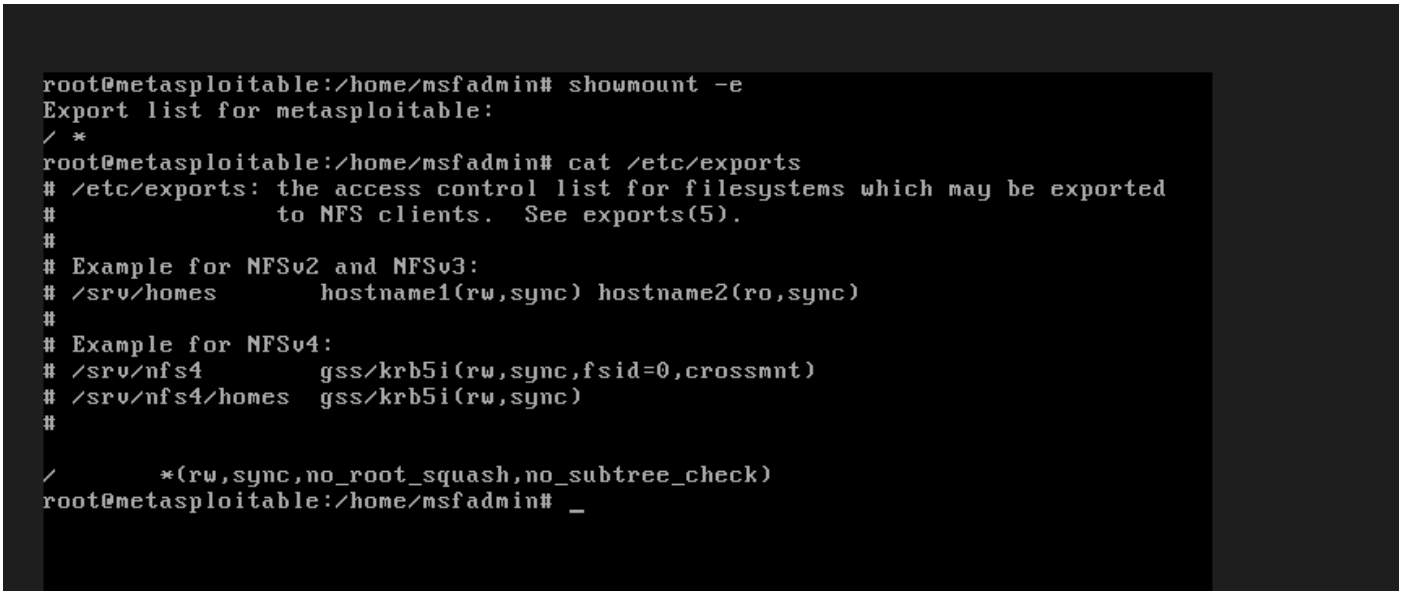


Dopo aver commentato il connettore AJP nel file di configurazione, il servizio è stato riavviato per rendere operative le modifiche, come confermato dai messaggi di arresto e avvio corretti.
È stato quindi effettuato un controllo aggiuntivo per assicurarsi che non fossero presenti processi residui che potessero mantenere attiva una configurazione; La verifica finale è stata eseguita a livello di rete tramite il comando *netstat -tulpn | grep 8009*, utilizzato per individuare eventuali servizi in ascolto sulla porta AJP.
L'assenza di qualsiasi output conferma che la porta 8009 non risulta più aperta e che il connettore AJP è stato effettivamente disabilitato.



A completamento è stata effettuata anche una validazione tramite Nmap per confermare l'effettiva chiusura del servizio .
La scansione mirata sulla porta 8009/TCP mostra che la porta risulta chiusa indicando che non è più presente alcun servizio in ascolto su tale porta.
Questo risultato conferma che il connettore AJP non è raggiungibile dalla rete e che la modifica applicata a livello di configurazione ha avuto l'effetto desiderato.

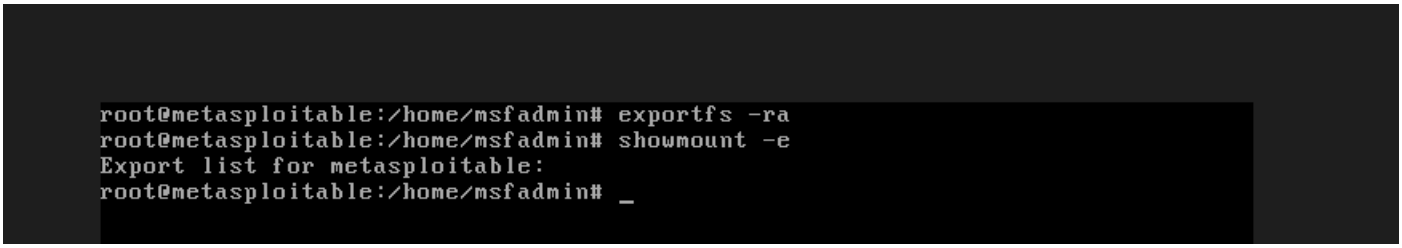
NFS SHARES WORLD READABLE



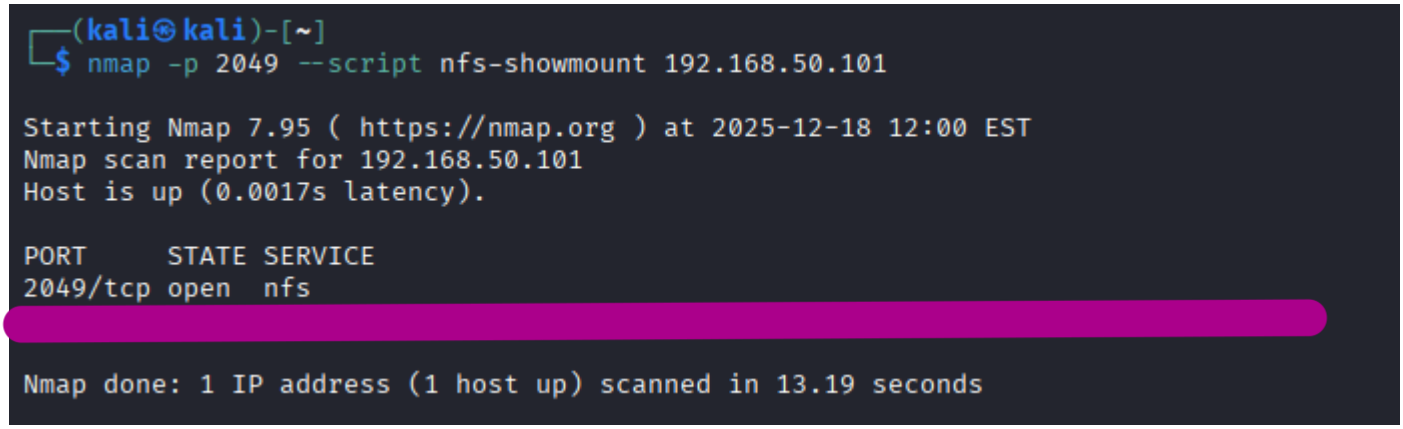
Un'altra vulnerabilità riscontrata durante l'analisi con Nessus riguarda la presenza di NFS Shares World Readable, una configurazione che consente l'accesso non autorizzato a directory esportate dal sistema.
Questa condizione comporta un rischio significativo in quanto permette a host remoti di enumerare e potenzialmente montare filesystem condivisi, accedendo a file e dati sensibili senza adeguati controlli di autenticazione o restrizione.
La risoluzione di questa vulnerabilità è necessaria per prevenire la divulgazione di informazioni, l'accesso improprio alle risorse di sistema e possibili escalation di privilegio derivanti da configurazioni permissive.
Nel passaggio mostrato, l'analisi viene avviata direttamente sul sistema target tramite il comando *showmount -e* utilizzato per interrogare il servizio NFS e ottenere l'elenco delle *esportazioni attive*; l'output conferma che il server risponde correttamente alle richieste di enumerazione, indicando che il servizio NFS è operativo e accessibile.
Successivamente viene esaminato il *file di configurazione /etc/exports*, il quale definisce le directory esportate e le relative opzioni di accesso; il contenuto del file evidenzia una configurazione in cui le condivisioni risultano esportate con permessi ampi, come l'accesso in lettura e scrittura e l'assenza di restrizioni sui client autorizzati.
Questo passaggio dimostra concretamente la causa tecnica della vulnerabilità segnalata da Nessus, mostrando come la configurazione del servizio NFS consenta l'accesso generalizzato alle risorse condivise, rendendo necessario un intervento di mitigazione per limitare l'esposizione e ridurre il rischio di compromissione del sistema.

```
#_      *(rw,sync,no_root_squash,no_subtree_check)
```

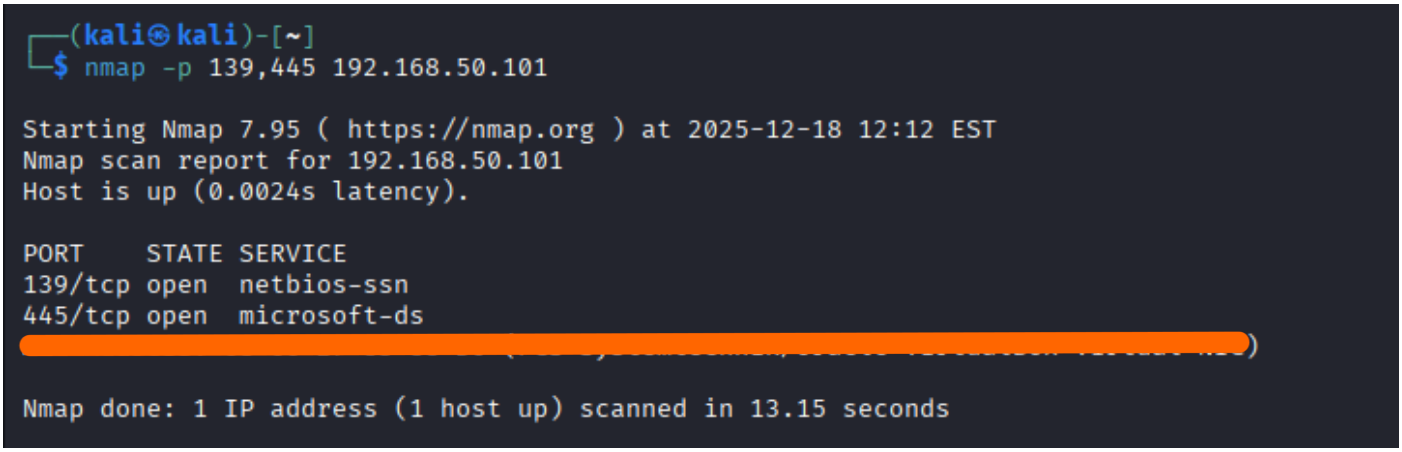
In seguito all'individuazione della configurazione insicura del servizio NFS, si è intervenuti sul *file /etc/exports* andando a commentare la riga che definiva l'esportazione delle condivisioni verso qualsiasi host con permessi eccessivamente permissivi.
La stringa **(rw,sync,no_root_squash,no_subtree_check)* è stata commentata per *disabilitare l'esportazione del filesystem*, impedendo che il servizio rendesse accessibili le directory condivise a client non autorizzati.
Questa scelta consente di eliminare immediatamente il vettore di attacco associato alla vulnerabilità *NFS Shares World Readable* mantenendo traccia della configurazione precedente a fini di verifica e controllo.



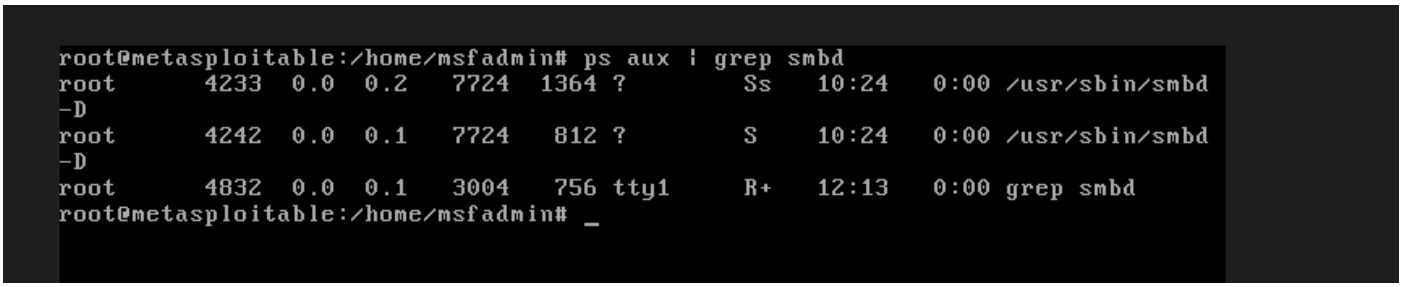
Questo passaggio dà continuità logica e tecnica all'intervento descritto in precedenza e serve a rendere effettiva la modifica applicata al *file /etc/exports*.
Dopo aver commentato la riga di configurazione che esportava il filesystem in modo non sicuro, viene eseguito il comando *exports -ra*, utilizzato per ricaricare la configurazione del servizio NFS senza riavviare l'intero sistema.
Questo comando forza il servizio a rileggere il file /etc/exports e ad applicare immediatamente le nuove impostazioni; successivamente viene nuovamente eseguito il comando *showmount -e* per verificare lo stato delle esportazioni attive.
L'assenza di directory elencate nell'output conferma che non risultano più filesystem esportati, dimostrando che la configurazione precedente è stata correttamente disabilitata.
Questo riscontro operativo evidenzia che l'intervento di mitigazione ha avuto successo, eliminando l'esposizione delle condivisioni NFS e rimuovendo la configurazione alla base della vulnerabilità.



Nel corso della verifica esterna è stato osservato che il servizio NFS risulta attivo e raggiungibile a livello di rete, come indicato dallo stato *open* della porta dedicata.
Questo comportamento è atteso e corretto, in quanto l'intervento di mitigazione non ha previsto la disattivazione del servizio NFS ma la rimozione delle esportazioni non autorizzate.
Mantenere il servizio in stato *open* consente al sistema di continuare a fornire funzionalità NFS, evitando impatti operativi.
L'elemento rilevante ai fini della sicurezza non è quindi la chiusura della porta, ma l'assenza di filesystem esportati e accessibili dall'esterno.
In questo contesto, la verifica conferma che il servizio NFS è correttamente operativo ma non espone più risorse condivise, dimostrando che la vulnerabilità NFS Shares World Readable è stata mitigata attraverso una restrizione della configurazione e non mediante l'interruzione del servizio.



In questa fase del laboratorio l'attenzione è rivolta esclusivamente allo stato di esposizione del servizio, senza entrare ancora nell'analisi della vulnerabilità.
La verifica mostra che le *porte 139/TCP e 445/TCP* risultano *open*, indicando che il servizio Samba è attivo e raggiungibile dalla rete.
Questo controllo preliminare viene effettuato per confermare la presenza del servizio e la sua esposizione, che rappresentano il punto di partenza necessario prima di qualsiasi intervento correttivo.



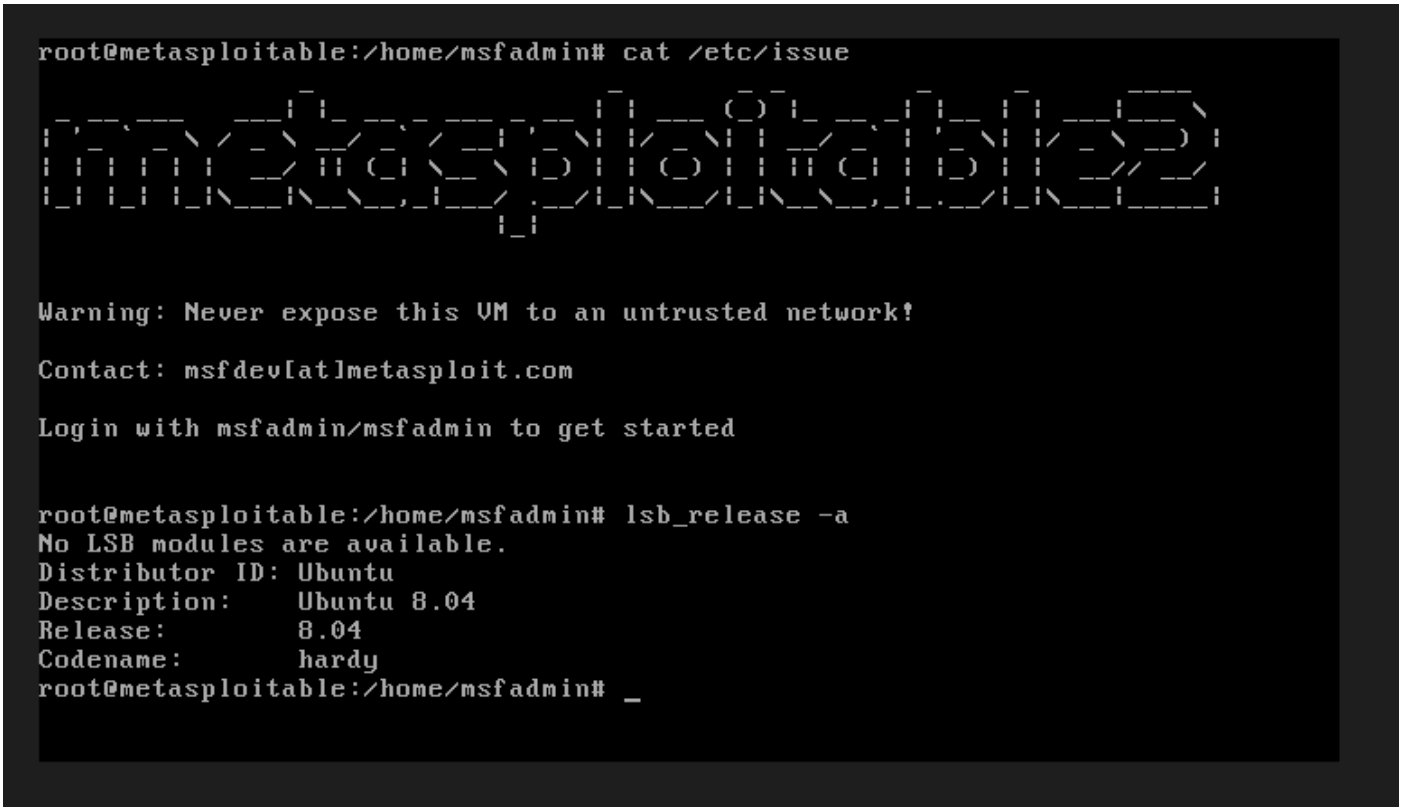
Questo passaggio documenta l'individuazione del processo responsabile dell'esposizione del servizio Samba.
L'analisi dei processi in esecuzione evidenzia la presenza del *demone smbd*, che risulta attivo con più istanze, confermando che il servizio Samba è effettivamente in funzione sul sistema.
Questo riscontro è coerente con quanto osservato in precedenza a livello di rete, dove le porte 139 e 445 risultavano aperte.
L'obiettivo di questa verifica è identificare con precisione il servizio da cui dipende l'esposizione delle porte, così da poter intervenire in modo mirato. La conferma dell'esecuzione del processo smbd consente quindi di stabilire un collegamento diretto tra il servizio attivo e la superficie di attacco rilevata, ponendo le basi tecniche per l'intervento successivo volto alla disattivazione o alla messa in sicurezza del servizio Samba.

```
root@metasploitable:/home/msfadmin# killall smbd
root@metasploitable:/home/msfadmin# _
```

Questo passaggio rappresenta l'intervento diretto sul servizio responsabile dell'esposizione. Dopo aver identificato il demone smbd come processo attivo associato al servizio Samba, si è proceduto alla sua terminazione, con l'obiettivo di interrompere immediatamente il servizio e bloccare l'ascolto sulle porte dedicate.
Questa azione consente di eliminare l'esposizione del servizio Samba dalla rete, riducendo la superficie di attacco e prevenendo l'accesso remoto tramite le porte 139 e 445; l'arresto del processo smbd costituisce quindi una misura di mitigazione immediata, utile per verificare l'impatto della disattivazione del servizio sull'esposizione delle porte e per confermare il legame diretto tra il servizio Samba in esecuzione e la vulnerabilità in fase di analisi.

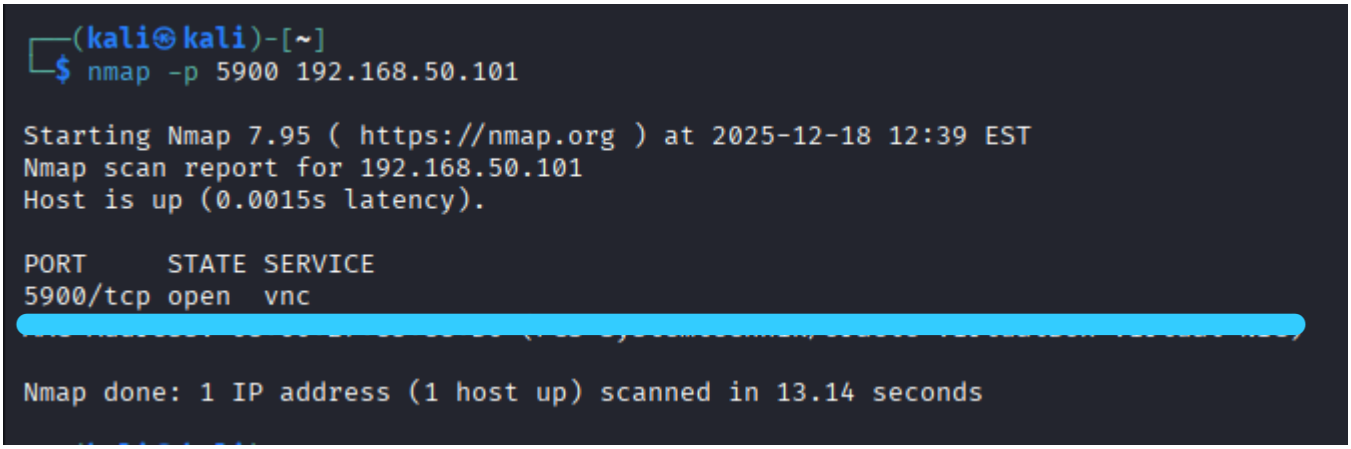
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 139,445 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 12:15 EST
Nmap scan report for 192.168.50.101
Host is up (0.0023s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
[redacted]

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

Questa verifica ha lo scopo di confermare l'efficacia dell'intervento eseguito sul servizio Samba.
L'analisi mostra che le porte precedentemente esposte risultano ora closed, indicando che il servizio non è più raggiungibile dalla rete.
Questo risultato è coerente con l'azione intrapresa e dimostra che la disattivazione del processo responsabile ha avuto l'effetto previsto, eliminando l'ascolto sulle porte associate al servizio.



L'analisi del sistema operativo evidenzia un'ulteriore criticità legata alla versione di Ubuntu installata sulla macchina.
Le informazioni di sistema mostrano infatti che l'host utilizza Ubuntu 8.04 (Hardy Heron), una versione che ha raggiunto da tempo lo stato di *End of Life*, ciò significa che il sistema non riceve più aggiornamenti di sicurezza né patch correttive da parte del fornitore ufficiale.
Questa condizione rappresenta un rischio significativo, poiché eventuali vulnerabilità note presenti nel sistema operativo rimangono esposte e potenzialmente sfruttabili da un attaccante.
L'assenza di supporto implica che nuove falle di sicurezza, così come quelle già documentate, non vengono corrette, aumentando progressivamente la superficie di attacco dell'host.
In questo contesto, la compromissione del sistema può avvenire anche senza la presenza di servizi applicativi vulnerabili, sfruttando direttamente debolezze a livello di sistema operativo.
La risoluzione di questa vulnerabilità richiede un intervento strutturale, che consiste nell'aggiornamento della macchina a una versione di Ubuntu attualmente supportata, in grado di ricevere aggiornamenti di sicurezza regolari e garantire un livello di protezione adeguato agli standard attuali.

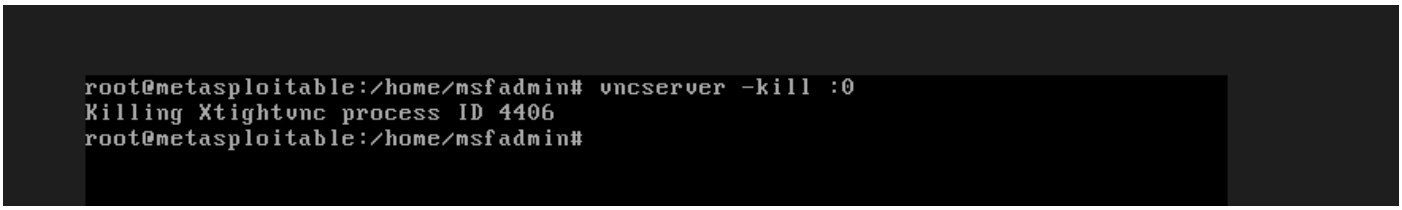
VNC SERVER WITHOUT PASSWORD



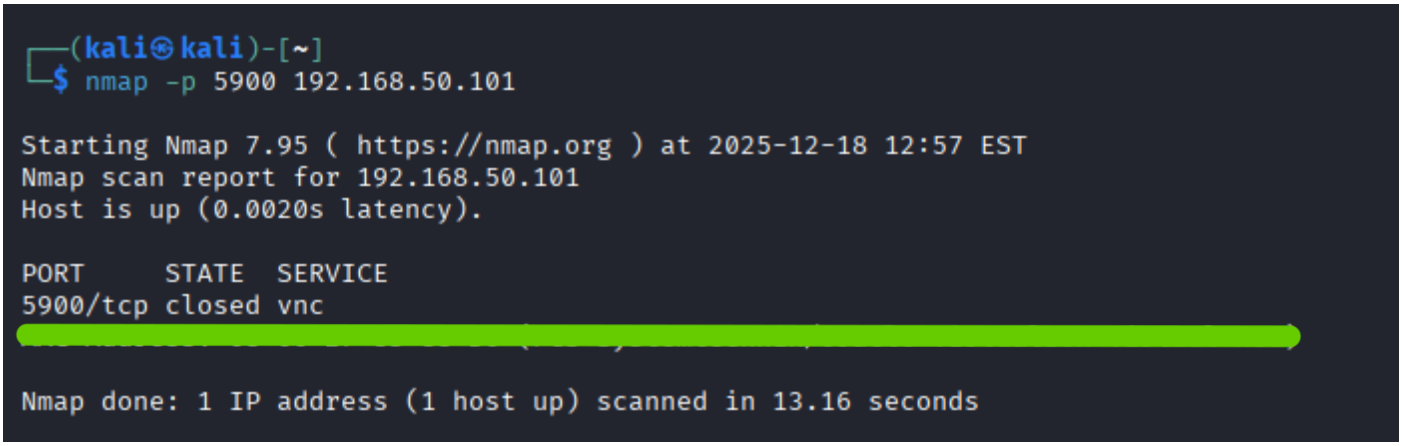
In questa fase viene analizzata l'esposizione del servizio VNC, concentrandosi inizialmente sullo stato della porta associata.
La verifica mostra che la porta 5900/TCP risulta open, indicando che il servizio VNC è attivo e raggiungibile dalla rete.
Questo riscontro conferma la presenza di un servizio di accesso remoto grafico esposto, che consente la connessione diretta all'interfaccia del sistema, la rilevazione dello stato *open* rappresenta il prerequisito tecnico per la vulnerabilità segnalata, poiché un servizio VNC accessibile costituisce un potenziale punto di ingresso se non adeguatamente protetto.

In continuità con quanto verificato a livello di rete, questo passaggio consente di identificare il processo responsabile dell'esposizione del servizio VNC sul sistema.
L'analisi dei processi in esecuzione mostra infatti la presenza del server *Xtightvnc*, confermando che il servizio VNC è attivo e correttamente avviato sull'host.

Questo riscontro collega in modo diretto lo stato *open* della porta 5900 alla presenza effettiva del servizio in esecuzione, escludendo che l'esposizione sia dovuta a configurazioni residue o a servizi non intenzionali.
La verifica dei processi ha quindi lo scopo di individuare con precisione il componente attivo su cui intervenire, ponendo le basi tecniche per l'azione successiva di mitigazione volta alla disattivazione o alla messa in sicurezza del servizio VNC.



Questo passaggio documenta l'intervento diretto sul servizio VNC individuato in precedenza.
Dopo aver confermato che il server Xtightvnc era attivo e responsabile dell'esposizione del servizio sulla porta dedicata, si è proceduto alla terminazione del servizio VNC, con l'obiettivo di interrompere immediatamente l'accesso remoto grafico.
Questa azione consente di eliminare l'esposizione del servizio dalla rete, prevenendo connessioni non autorizzate e rimuovendo il prerequisito tecnico alla base della vulnerabilità VNC Password Authentication Disabled.
L'arresto del servizio rappresenta una misura di mitigazione immediata, finalizzata a ridurre la superficie di attacco e a verificare l'impatto della disattivazione del servizio sull'esposizione della porta associata.



Questo passaggio fornisce la conferma finale dell'efficacia dell'intervento.
La verifica mostra che la porta 5900/TCP risulta ora *closed,* indicando che il servizio VNC non è più raggiungibile dalla rete.
Questo risultato è coerente con l'azione intrapresa e conferma che la disattivazione del server VNC ha avuto l'effetto previsto, eliminando l'esposizione del servizio.
La chiusura della porta dimostra che il vettore di accesso remoto associato alla vulnerabilità VNC Password Authentication Disabled è stato correttamente rimosso, riducendo la superficie di attacco e completando il processo di mitigazione.

CONCLUSIONE

L’attività di vulnerability assessment ha consentito di individuare e analizzare in modo sistematico diverse criticità presenti sull’host, evidenziando come l’esposizione di servizi non adeguatamente configurati e l’utilizzo di componenti obsoleti rappresentino un rischio concreto per la sicurezza del sistema.
Attraverso l’analisi delle evidenze e le successive verifiche tecniche, è stato possibile correlare ciascuna vulnerabilità a una specifica condizione di configurazione o di esposizione, intervenendo in modo mirato per ridurne l’impatto.
Le azioni di mitigazione applicate hanno dimostrato come, anche senza modifiche strutturali complesse, sia possibile ridurre significativamente la superficie di attacco intervenendo su servizi inutilmente esposti, condivisioni non protette e componenti non più supportati.
Le verifiche successive hanno confermato l’efficacia degli interventi, mostrando la corretta rimozione delle condizioni che rendevano sfruttabili le vulnerabilità individuate.
Nel complesso, l’analisi mette in evidenza l’importanza di una gestione consapevole dei servizi di rete, dell’aggiornamento costante del sistema operativo e di un controllo regolare delle configurazioni, elementi fondamentali per garantire un livello di sicurezza adeguato e prevenire potenziali compromissioni future.

GLOSSARIO

Vulnerability Assessment

Processo sistematico finalizzato all'identificazione, analisi e valutazione delle vulnerabilità presenti in un sistema informatico, con l'obiettivo di ridurre i rischi di sicurezza attraverso interventi di mitigazione appropriati.

Servizio esposto

Servizio di rete attivo e raggiungibile da host esterni, che può costituire un rischio se non adeguatamente configurato o protetto.

End of Life (EOL)

Stato di un software o sistema operativo non più supportato dal fornitore, che non riceve aggiornamenti di sicurezza e patch correttive.

Mitigazione

Insieme di azioni tecniche volte a ridurre l'impatto o la sfruttabilità di una vulnerabilità, senza necessariamente eliminarne completamente la causa strutturale.

Backdoor

Meccanismo di accesso nascosto o non documentato che consente di bypassare i normali controlli di autenticazione e autorizzazione di un sistema. Una backdoor può essere inserita intenzionalmente da un attaccante o derivare da configurazioni insicure, software vulnerabili o componenti obsoleti. La sua presenza permette l'accesso remoto persistente al sistema compromesso, spesso senza essere rilevata, rappresentando un rischio elevato per la riservatezza, l'integrità e la disponibilità delle informazioni.

Hardening

Insieme di attività volte a ridurre la superficie di attacco di un sistema, disabilitando servizi non necessari e rafforzando le configurazioni di sicurezza.