INDICE

NETCAT

NMAP

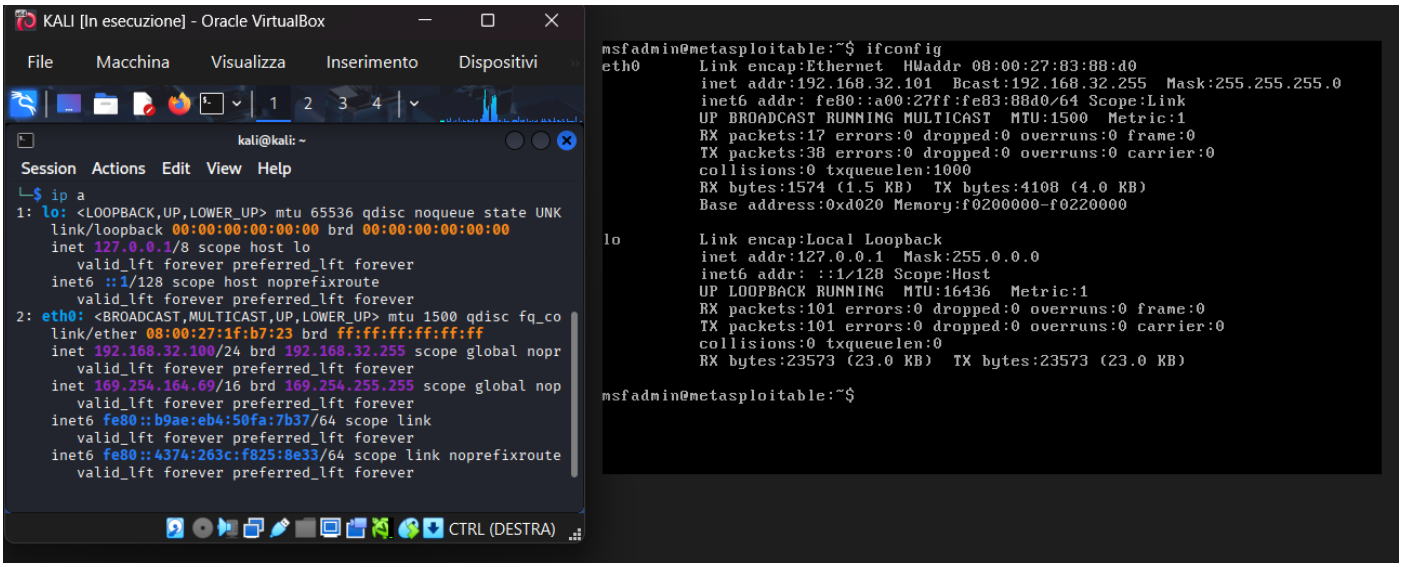
INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio ha l'obiettivo di verificare in modo chiaro e strutturato il funzionamento delle comunicazioni tra due macchine virtuali presenti nello stesso ambiente di rete.
Attraverso l'utilizzo di strumenti standard, l'esercizio permette di osservare come avviene una connessione tra due sistemi, come vengono scambiati i dati e quali risposte restituisce la macchina che riceve la richiesta.
Il lavoro svolto fornisce una visione pratica dei meccanismi di base che regolano l'interazione tra dispositivi collegati, consentendo di comprenderne il comportamento in condizioni controllate.

OBIETTIVO: verificare la comunicazione tra due macchine virtuali, stabilendo un collegamento diretto e osservando le risposte prodotte durante lo scambio di dati. Il fine è documentare in modo semplice e riproducibile i passaggi essenziali che caratterizzano l'interazione tra i due sistemi nella stessa rete.

NETCAT

VERIFICA CONFIGURAZIONE DI RETE

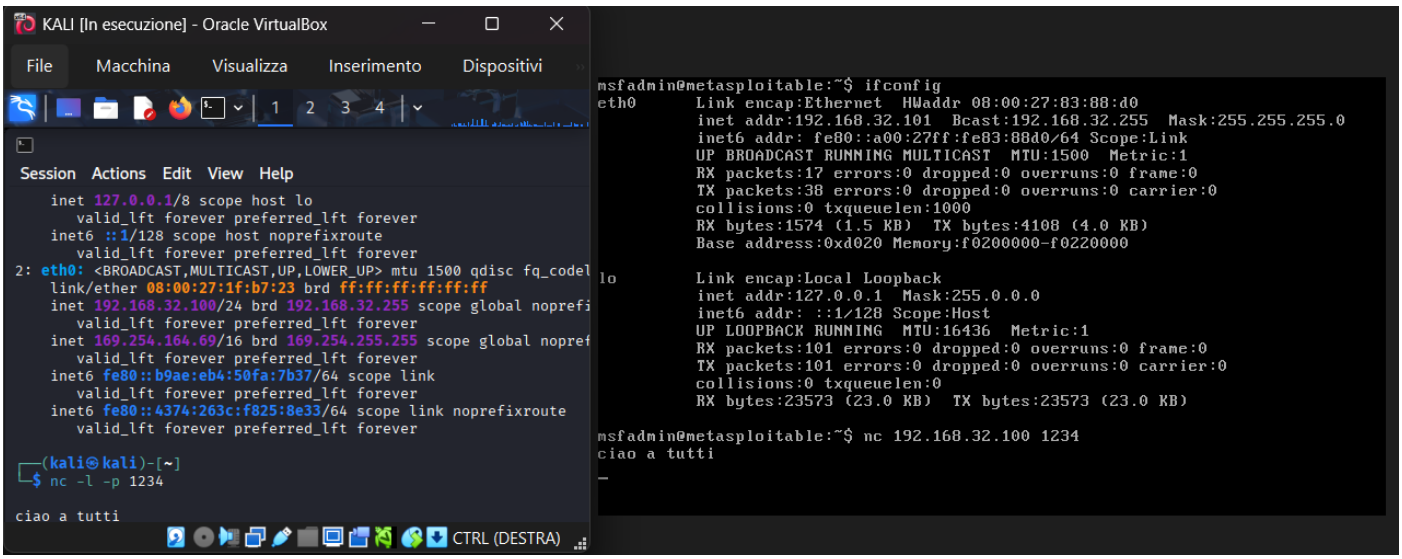


Per avviare il laboratorio è stata verificata la configurazione di rete delle due macchine virtuali coinvolte.

Su *Kali Linux* è stato utilizzato il comando **ip a**, mentre sulla macchina remota è stato eseguito **ifconfig,** così da identificare indirizzi IP, interfacce attive e parametri assegnati. Entrambi i sistemi risultano correttamente collegati alla stessa rete e presentano indirizzi compatibili, condizione necessaria per permettere lo scambio di dati previsto nelle attività successive.

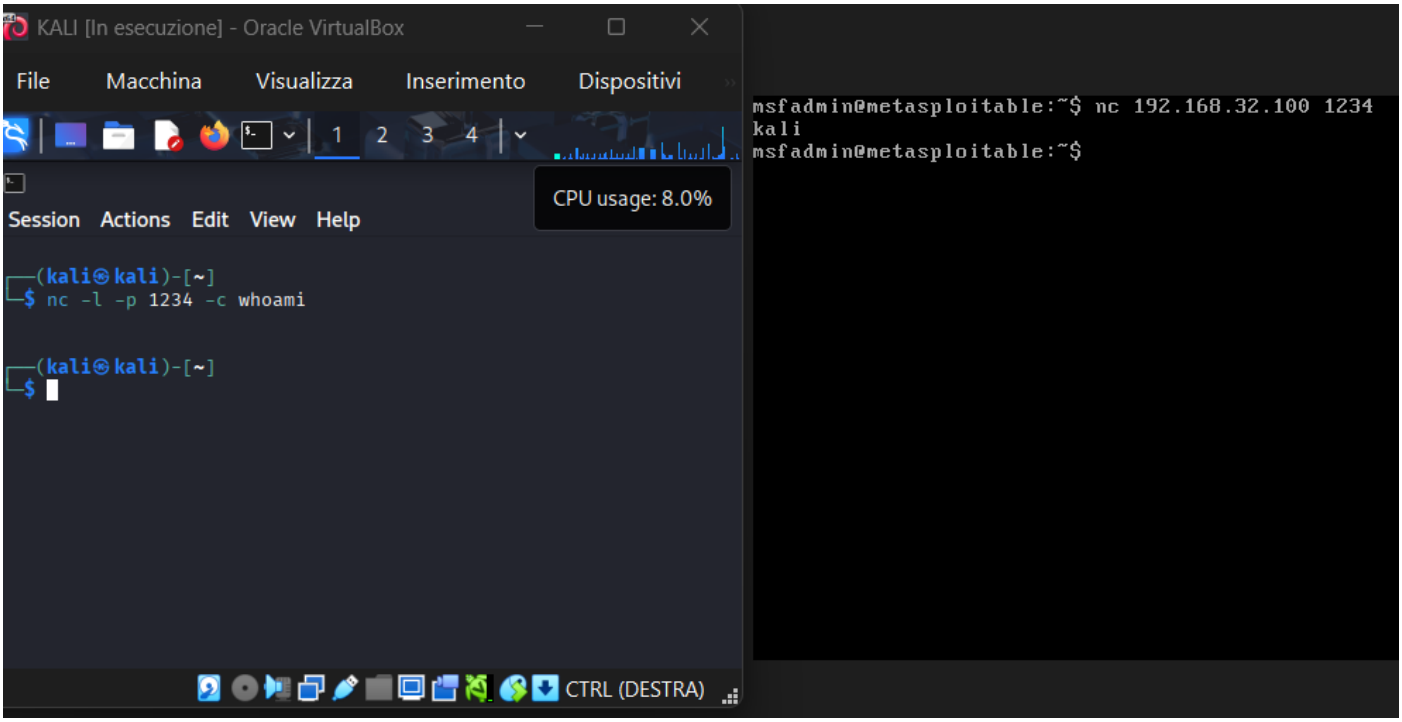
Questa verifica preliminare garantisce che le due postazioni possano comunicare senza interferenze o problemi di connettività.

CONNESSIONE NETCAT



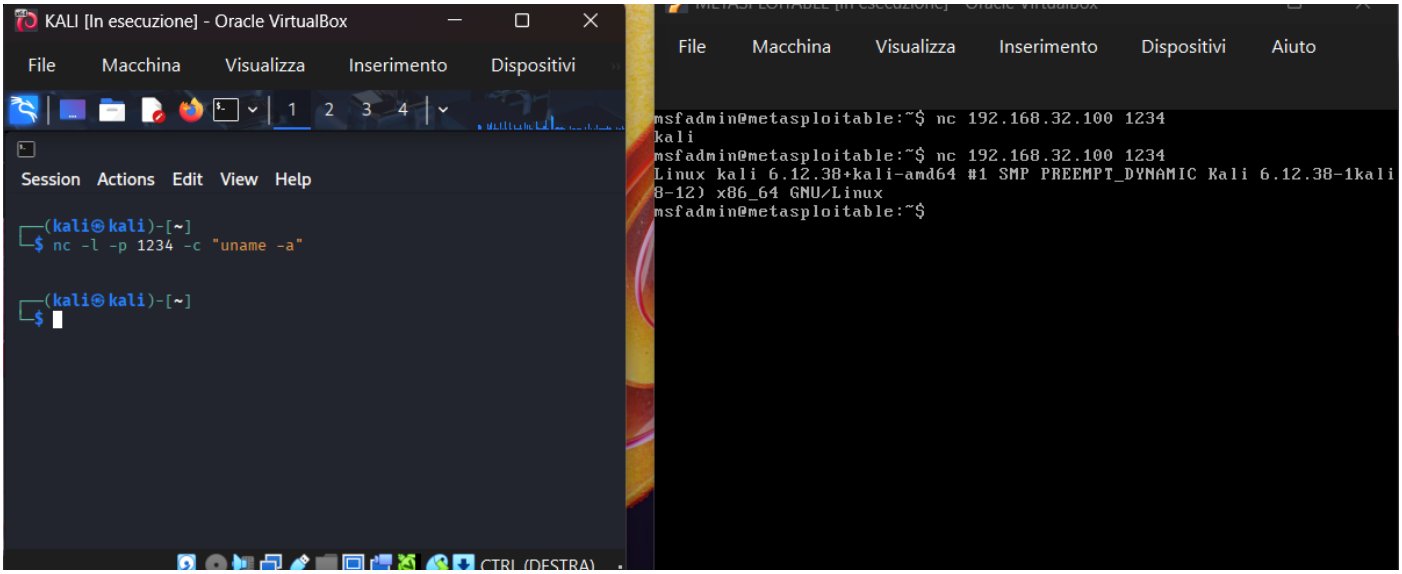
Dopo aver confermato che entrambe le macchine si trovano nella stessa rete, è stata avviata una prima comunicazione diretta tramite **Netcat**.
Sulla macchina Kali è stato aperto un **listener sulla porta 1234**, mentre dalla macchina remota è stata effettuata la connessione verso l'indirizzo di Kali utilizzando la stessa porta.
Alla ricezione del messaggio di prova inviato dalla macchina remota, il *listener* ha risposto correttamente, confermando che la comunicazione tra i due sistemi è attiva e funziona come previsto.
Questo passaggio dimostra che il collegamento è stabilito correttamente e che i messaggi possono essere scambiati senza interruzioni.

ESECUZIONE COMANDI REMOTI



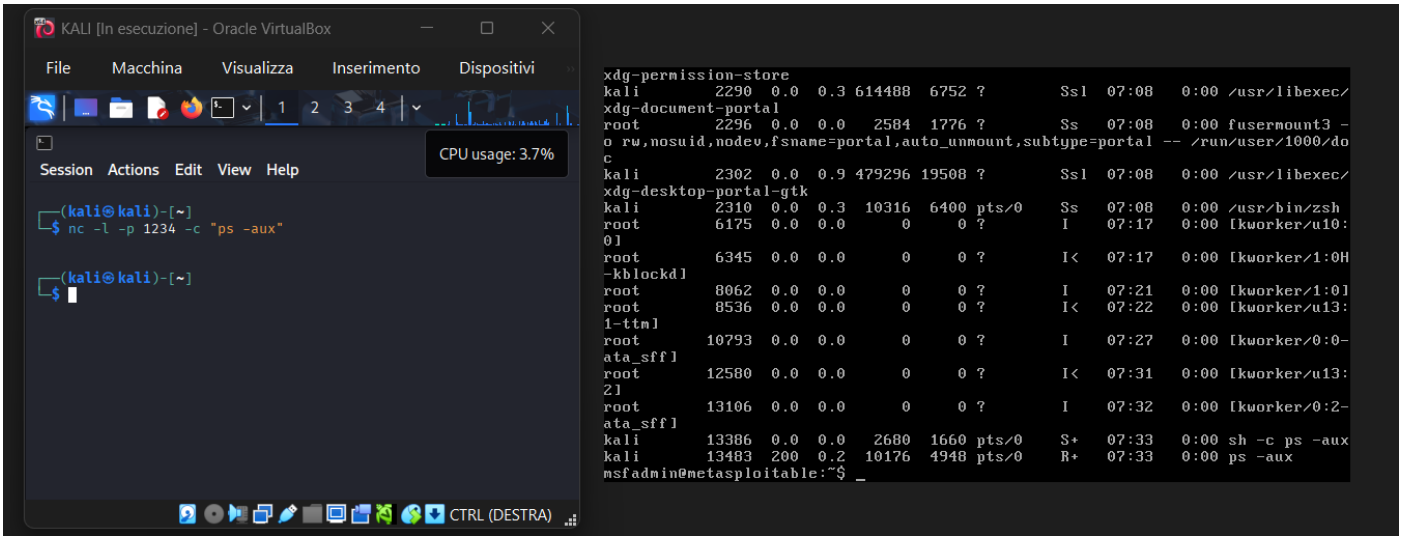
Dopo aver stabilito la connessione, è stato utilizzato Netcat per inviare comandi direttamente alla macchina remota.
In questo passaggio il listener di Kali è stato configurato per eseguire in automatico il comando **whoami** non appena la connessione veniva ricevuta; collegandosi alla porta indicata la macchina remota ha *restituito il proprio nome utente*, confermando che l'esecuzione dei comandi inviati da Kali avviene correttamente.
Ciò dimostra la piena operatività del canale stabilito e la sua capacità di eseguire istruzioni in modo immediato.

RACCOLTA INFO SISTEMA



Proseguendo con la verifica della comunicazione, il listener di Kali è stato configurato per eseguire automaticamente il comando *uname -a* al momento della connessione.
Questo ha permesso di ottenere dalla macchina remota informazioni dettagliate sul sistema in uso, come versione del kernel e architettura; l'output restituito conferma che la connessione stabilita consente non solo l'invio di comandi, ma anche la raccolta immediata di dati utili sul sistema collegato, dimostrando la continuità e l'affidabilità dello scambio.

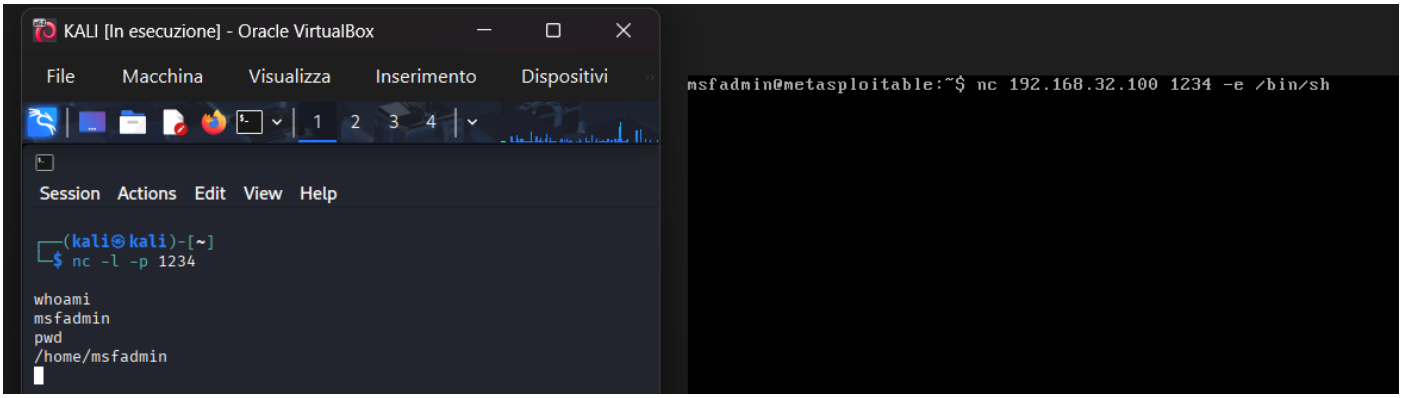
ESECUZIONE COMANDI REMOTI



Durante questa fase è stato stabilito un collegamento diretto dalla macchina remota verso il listener in esecuzione su Kali. L'utilizzo del comando "nc -l -p 1234 -c "ps -aux" ha permesso di inviare, al momento della connessione, l'elenco completo dei processi attivi sul sistema Kali.

La macchina remota, collegandosi all'indirizzo e alla porta indicati, ha ricevuto immediatamente l'output del comando e lo ha visualizzato nel proprio terminale; ciò conferma la corretta esecuzione di comandi remoti e la piena funzionalità del canale di comunicazione stabilito tra le due macchine.

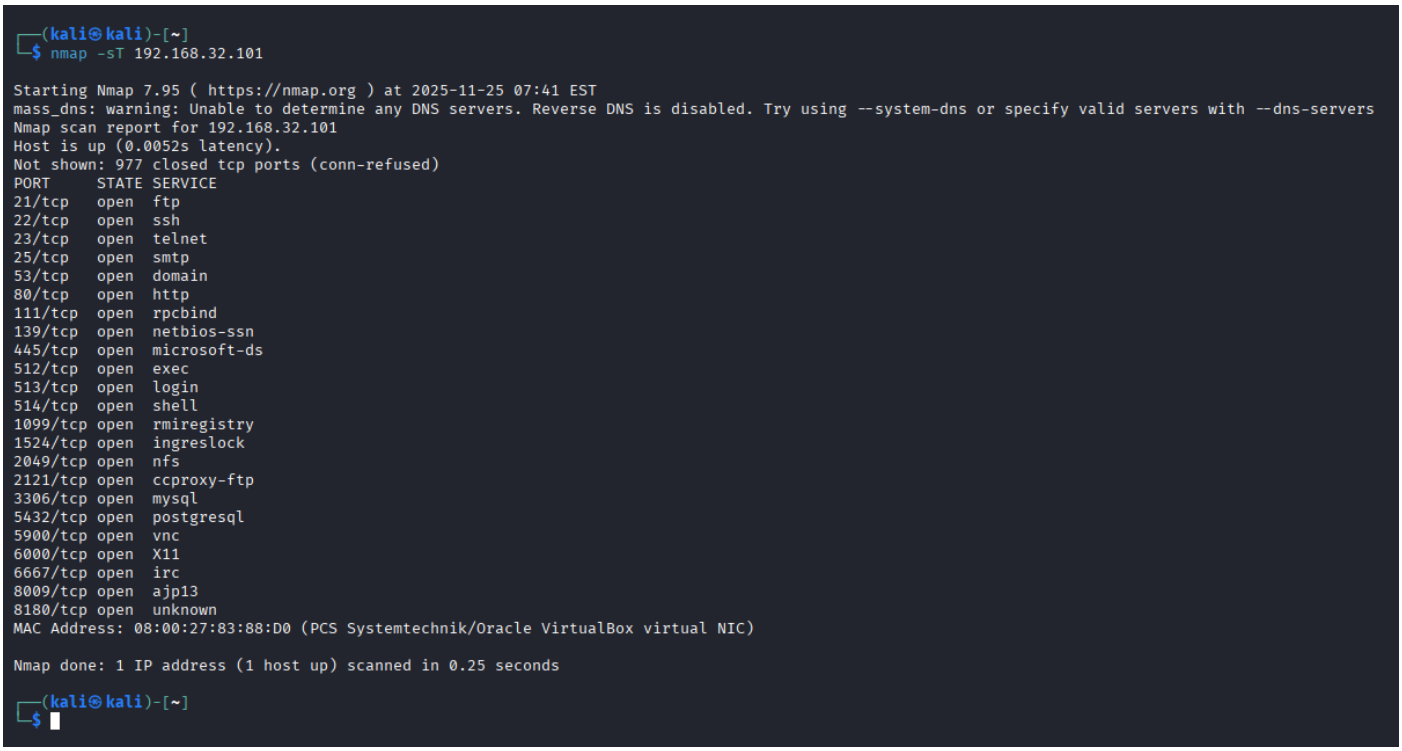
REVERSE SHELL



In questa ultima fase del laboratorio è stato stabilito un collegamento inverso tra due macchine virtuali allo scopo di verificare il comportamento di un sistema quando riceve comandi eseguiti in remoto.
La macchina bersaglio ha aperto una connessione verso l'indirizzo indicato, mentre l'altra macchina era in ascolto sulla porta dedicata e pronta a ricevere l'interazione.
Una volta instaurato il collegamento è stato possibile inviare comandi direttamente alla macchina remota e osservarne le risposte in tempo reale, confermando la corretta instaurazione della sessione.
I test eseguiti hanno dimostrato che la comunicazione avviene in maniera stabile e che la macchina destinataria elabora correttamente le istruzioni ricevute.
La procedura ha permesso di evidenziare in modo concreto come un sistema possa essere controllato attraverso un canale di comunicazione inverso, offrendo una visione chiara delle modalità con cui due dispositivi interagiscono quando la connessione parte dal nodo remoto anziché da quello locale.

NMAP

RILEVAZIONE PORTE

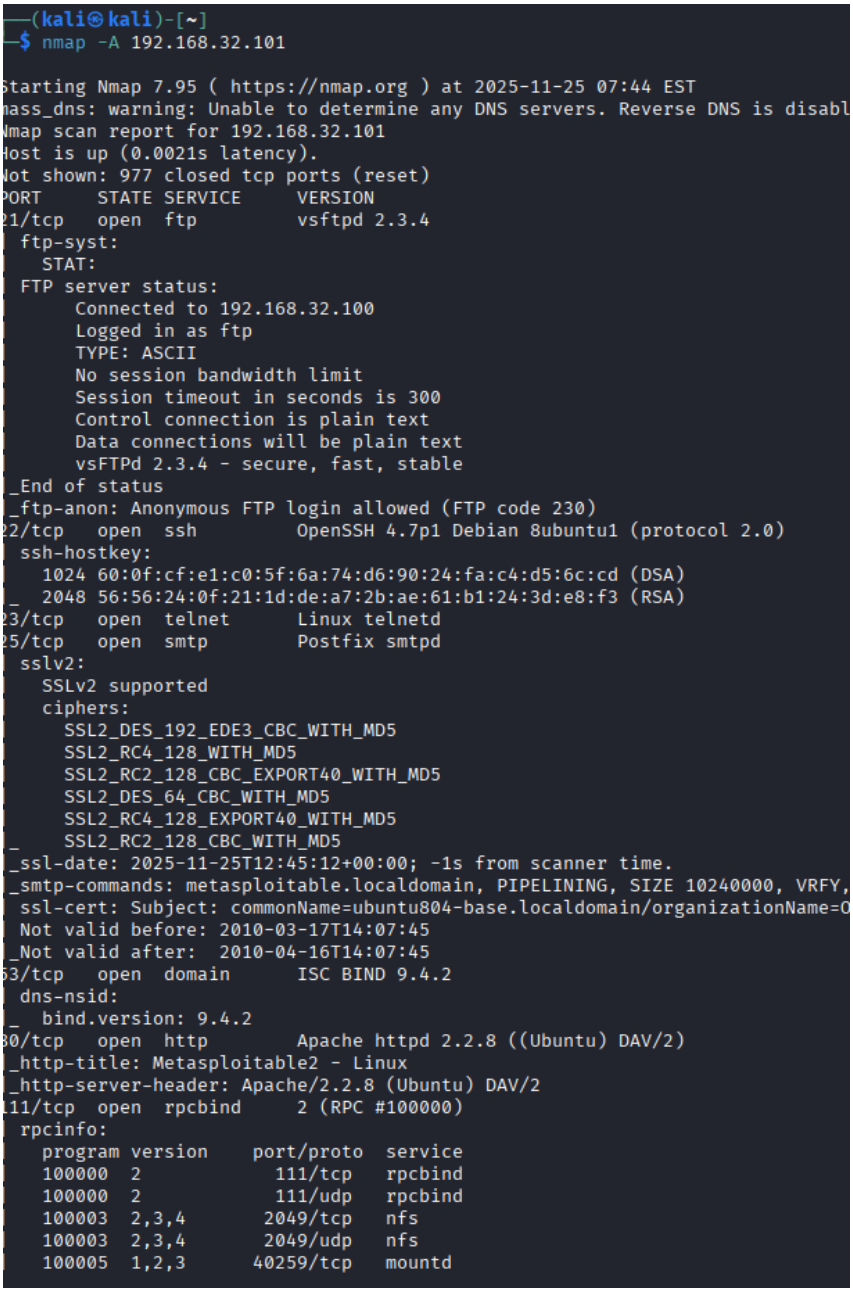


La scansione è stata eseguita per identificare i servizi attivi sulla macchina remota e verificare quale comportamento presentasse il sistema in risposta a una richiesta di connessione standard.
L'analisi effettuata consente di osservare in modo chiaro quali porte risultano aperte, quali servizi sono associati e come la macchina gestisce le comunicazioni in ingresso.
Il risultato fornisce una panoramica immediata dell'esposizione del sistema all'interno della rete e permette di comprendere il livello di accessibilità dei vari servizi, offrendo così una base concreta per ulteriori verifiche o per successive attività di configurazione.

SCANSIONE SYN

La scansione SYN del sistema remoto è stata eseguita per identificare rapidamente le **porte TCP aperte** senza stabilire una connessione completa.
Questa modalità di analisi permette di rilevare i servizi attivi inviando soltanto *pacchetti SYN* e valutando la risposta del sistema, riducendo l'impatto sulla macchina analizzata e il rischio di generare traffico eccessivo.
Il risultato mostra in modo immediato quali porte sono in ascolto e quali servizi risultano disponibili, offrendo una visione affidabile della superficie di comunicazione esposta dal dispositivo.

SCANSIONE



La scansione eseguita con Nmap ha permesso di ottenere una panoramica completa dei servizi attivi sulla macchina analizzata.
Questa modalità integra diverse tecniche di rilevazione, consentendo di identificare con precisione le porte aperte, le versioni dei servizi esposti e ulteriori informazioni utili per comprendere la superficie di comunicazione del sistema.
L'analisi ha evidenziato la presenza di numerosi servizi in esecuzione, confermando che la macchina ospita diversi componenti di rete, tra cui server FTP, SSH, HTTP, SMTP, database e altri servizi applicativi. La scansione fornisce quindi una mappatura dettagliata dello stato del sistema e rappresenta un passaggio fondamentale per documentarne le caratteristiche operative in un ambiente controllato.