LABORATORIO – RETI VIRTUALI E SEGMENTAZIONE CON KVM

In questo laboratorio pomeridiano metteremo in pratica i concetti della lezione sulle reti virtuali.

Utilizzeremo un host Fedora con KVM e diverse macchine virtuali.

L'obiettivo è capire concretamente come funzionano NAT, reti isolate e segmentazione di rete.

Queste tecniche sono fondamentali nei data center virtualizzati e negli ambienti cybersecurity.

OBIETTIVI DEL LABORATORIO

- Configurare e utilizzare una rete NAT con libvirt.
- Verificare la comunicazione tra macchine virtuali.
- Creare una rete completamente isolata.
- Comprendere il concetto di segmentazione di rete.
- Analizzare il traffico di rete tra le VM.

SCENARIO DEL LABORATORIO

L'infrastruttura del laboratorio è composta da un host Fedora con hypervisor KVM.

All'interno dell'host eseguiremo diverse macchine virtuali Linux.

Le VM saranno collegate a diverse reti virtuali per osservare comportamenti differenti.

Questo laboratorio simula un piccolo ambiente di data center virtualizzato.

ARCHITETTURA DEL LABORATORIO

Useremo più macchine virtuali per simulare una piccola rete.

Alcune VM saranno collegate alla rete NAT predefinita.

Altre VM saranno collegate ad una rete isolata.

Questo permetterà di osservare come la segmentazione limita la comunicazione tra sistemi.

VERIFICA DELLE RETI LIBVIRT

- Il primo passo è verificare quali reti virtuali esistono nell'host KVM.
- Libvirt gestisce le reti virtuali e spesso crea automaticamente una rete chiamata 'default'.
- Questa rete è configurata in modalità NAT.
- Utilizzeremo il comando virsh per visualizzare le reti disponibili.

COMANDO VIRSH NET-LIST

- Il comando virsh net-list mostra le reti virtuali gestite da libvirt.
- Questo comando è molto usato dagli amministratori di sistemi virtualizzati.
- Permette di verificare se una rete è attiva oppure disattiva.
- In un laboratorio spesso vedremo la rete 'default' già attiva.

RETE NAT DI LIBVIRT

- La rete default di libvirt utilizza la modalità NAT.
- Le macchine virtuali ricevono un indirizzo IP privato.
- L'host traduce gli indirizzi permettendo alle VM di accedere a internet.
- Questo è molto utile nei laboratori perché non richiede configurazioni complesse.

AVVIO DELLE MACCHINE VIRTUALI

- Nel laboratorio avvieremo due macchine virtuali collegate alla rete NAT.
- Questo ci permetterà di verificare la comunicazione tra sistemi virtuali.
- Le VM si comportano come normali computer collegati alla stessa rete.
- Useremo il comando virsh start oppure virt-manager.

VERIFICA DELL'INDIRIZZO IP

- Una volta avviata la macchina virtuale dobbiamo verificare l'indirizzo IP assegnato.
- In Linux possiamo utilizzare il comando ip a.
- Questo comando mostra tutte le interfacce di rete e gli indirizzi associati.
- Nella rete NAT di libvirt gli indirizzi sono tipicamente nella rete 192.168.122.0.

TEST DI CONNETTIVITÀ CON PING

- Il comando ping permette di verificare se due macchine possono comunicare.
- È uno strumento fondamentale per diagnosticare problemi di rete.
- Nel laboratorio proveremo a pingare una VM dall'altra.
- Se il ping funziona significa che la comunicazione di rete è corretta.

ACCESSO A INTERNET DALLE VM

- Le VM collegate alla rete NAT possono accedere a internet.
- Questo è possibile grazie alla traduzione degli indirizzi effettuata dall'host.
- Possiamo testare questa funzionalità pingando un indirizzo pubblico come 8.8.8.8.
- Se il ping funziona significa che il NAT è configurato correttamente.

INTRODUZIONE ALLE RETI ISOLATE

- Dopo aver verificato la rete NAT creeremo una rete isolata.
- Una rete isolata permette la comunicazione solo tra macchine virtuali.
- Non esiste accesso alla rete esterna o a internet.
- Questo tipo di rete è molto usato per test di sicurezza e simulazioni.

CREAZIONE DI UNA RETE ISOLATA

- Libvirt permette di creare facilmente nuove reti virtuali.
- Definiremo una rete isolata tramite un file di configurazione XML.
- Questo file descrive il bridge virtuale e la configurazione DHCP.
- Successivamente attiveremo la rete tramite virsh.

FILE XML DI CONFIGURAZIONE RETE

- Il file XML definisce i parametri della rete virtuale.
- Possiamo definire nome della rete, bridge virtuale e indirizzi IP.
- È possibile anche configurare un server DHCP interno.
- Questo metodo è molto comune nella gestione delle infrastrutture virtualizzate.

ATTIVAZIONE DELLA RETE ISOLATA

- Una volta creato il file XML possiamo registrare la rete con virsh net-define.
- Successivamente la rete viene attivata con virsh net-start.
- È possibile configurarla per l'avvio automatico con virsh net-autostart.
- Da questo momento la rete isolata è disponibile per le VM.

COLLEGARE UNA VM ALLA NUOVA RETE

- Ora modificheremo la configurazione di una macchina virtuale.
- La VM verrà collegata alla rete isolata appena creata.
- Questo si può fare modificando il file XML della macchina virtuale.
- Oppure utilizzando l'interfaccia grafica virt-manager.

VERIFICA DELL'INDIRIZZO IP NELLA RETE ISOLATA

- Dopo aver collegato la VM alla nuova rete la riavvieremo.
- La macchina virtuale riceverà un indirizzo IP dalla nuova rete.
- Ad esempio potremmo vedere indirizzi come 192.168.200.x.
- Questo conferma che la VM è collegata alla rete isolata.

TEST DI ISOLAMENTO

- Ora testeremo l'isolamento della rete.
- Proveremo a pingare un indirizzo internet come 8.8.8.8.
- Il ping non funzionerà perché la rete isolata non ha accesso esterno.
- Questo dimostra il concetto di isolamento di rete.

CREARE PIÙ VM NELLA STESSA RETE ISOLATA

- Per capire meglio il comportamento della rete isolata creeremo due VM.
- Entrambe saranno collegate alla stessa rete virtuale.
- Le VM potranno comunicare tra loro ma non con altre reti.
- Questo è un esempio di segmentazione.

SEGMENTAZIONE DI RETE

- La segmentazione consiste nel dividere la rete in più zone separate.
- Ogni segmento può avere regole di sicurezza diverse.
- In ambienti aziendali questo riduce il rischio di propagazione degli attacchi.
- Nelle infrastrutture virtuali è molto semplice creare segmenti diversi.

ANALISI DEL TRAFFICO DI RETE

- Ora analizzeremo il traffico di rete tra le macchine virtuali.
- Useremo strumenti come tcpdump.
- Questo strumento permette di vedere i pacchetti che attraversano l'interfaccia di rete.
- È uno strumento molto utilizzato anche nella cybersecurity.

INSTALLAZIONE DI TCPDUMP

- Per utilizzare tcpdump dobbiamo installarlo nel sistema.
- Su Fedora possiamo usare il comando dnf install tcpdump.
- Una volta installato possiamo monitorare il traffico di rete.
- Questo ci aiuterà a capire come comunicano le macchine virtuali.

OSSERVARE IL TRAFFICO ICMP

- Avviamo tcpdump su una macchina virtuale.
- Successivamente eseguiamo un ping da un'altra VM.
- Vedremo comparire i pacchetti ICMP nel terminale.
- Questo dimostra che il traffico passa attraverso la rete virtuale.

PROBLEMI COMUNI NEL LABORATORIO

- Durante il laboratorio potrebbero verificarsi alcuni problemi.
- Ad esempio configurazione IP errata o firewall attivo.
- Un altro problema comune è una rete virtuale non avviata.
- Imparare a diagnosticare questi problemi è una competenza importante.

DEBUG DELLA RETE

- Quando una rete non funziona dobbiamo seguire un metodo.
- Controllare indirizzo IP.
- Verificare la rete virtuale con virsh net-list.
- Controllare firewall e connettività con ping.

COLLEGAMENTO CON LA CYBERSECURITY

- La segmentazione di rete è una tecnica fondamentale nella sicurezza.
- Se un sistema viene compromesso l'attaccante non può muoversi facilmente.
- Questo limita il cosiddetto movimento laterale.
- Le reti virtuali rendono molto semplice applicare questa strategia.

APPLICAZIONI REALI

- Nei data center aziendali esistono spesso centinaia di macchine virtuali.
- La segmentazione permette di separare server web, database e sistemi interni.
- Questo aumenta la sicurezza dell'infrastruttura.
- Le stesse tecniche vengono usate nei cloud pubblici.

RIEPILOGO DEL LABORATORIO

- In questo laboratorio abbiamo configurato diverse reti virtuali.
- Abbiamo osservato la differenza tra NAT e rete isolata.
- Abbiamo creato segmentazione tra macchine virtuali.
- Abbiamo anche analizzato il traffico di rete tra le VM.

PREPARAZIONE ALLA PROSSIMA LEZIONE

- Nella prossima lezione analizzeremo infrastrutture VDI.
- Vedremo come fornire desktop virtuali agli utenti.
- Useremo KVM e sistemi di accesso remoto.
- Questo completerà il percorso sulla virtualizzazione.