LEZIONE 4 – RETI VIRTUALI E SEGMENTAZIONE

- In questa lezione analizziamo come funziona la rete nelle infrastrutture virtualizzate.
- L'obiettivo è capire come collegare le macchine virtuali tra loro e con la rete fisica.
- Impareremo anche i concetti di segmentazione di rete, fondamentali per sicurezza e cybersecurity.

OBIETTIVI DELLA LEZIONE

Comprendere come funziona la rete nelle piattaforme di virtualizzazione.

Configurare diverse modalità di rete per le macchine virtuali.

Capire il concetto di isolamento e segmentazione di rete.

Applicare questi concetti in un laboratorio con KVM o altri hypervisor.

COS'È UNA RETE VIRTUALE

Una rete virtuale è una rete creata tramite software all'interno di un hypervisor.

Le macchine virtuali possono comunicare tra loro come se fossero collegate a uno switch fisico.

Questo permette di costruire infrastrutture di rete complesse senza hardware aggiuntivo.

DIGRESSIONE: VLAN

- Una VLAN (Virtual Local Area Network) è una tecnologia che consente di segmentare una rete fisica in più sottoreti logiche isolate tra loro, operando su switch gestiti.
- **Segmentazione e Sicurezza:** Isola il traffico tra i gruppi (es. Dipartimento A non vede Dipartimento B), aumentando la sicurezza.
- **Gestione del Traffico:** Riduce la congestione della rete limitando i domini di broadcast.
- I dispositivi possono essere raggruppati logicamente indipendentemente dalla loro posizione fisica
- .**VLAN Tagging (802.1Q):** Utilizzato per identificare a quale VLAN appartengono i pacchetti dati quando attraversano più switch tramite una porta

PROTOCOLLO 802.3Q

- Ciascuna VLAN è identificata da un numero, detto VID (Vlan ID), che va da 1 a 4094 (0 e 4095 sono riservati).
- Per realizzare il trunking di VLAN presenti su switch diversi, è necessario che sui collegamenti tra switch si possa identificare a quale VLAN appartiene ciascun pacchetto. Per fare questo, nel frame ethernet IEEE 802.3 viene aggiunto un campo di 12 Bit posto tra il destination address e il campo type/length, questo tag, detto VLAN TAG oppure DOT1Q TAG, contiene il VID relativo a quel pacchetto. Lo switch che riceve questo pacchetto deve quindi sapere che deve interpretare questi 12 Bit come VLAN TAG, ed il resto del pacchetto come un normale pacchetto 802.3.
- Una porta di uno switch su cui viaggiano pacchetti con il VLAN TAG è detta *tagged* o *trunk port*. Viceversa, una su cui viaggiano pacchetti senza VLAN TAG è detta *access port*. Alcuni switch accettano anche un traffico misto di pacchetti tagged e non tagged, e una porta configurata in questo modo è detta *hybrid port*.

SWITCH FISICI

- porte: come nell'esempio sopra descritto, ciascuna porta di uno switch è configurata per appartenere ad una data VLAN. Tutti i pacchetti provenienti da quella porta saranno "taggati" con l'ID della sua VLAN, e su questa porta verranno inviati solo pacchetti provenienti dalla sua VLAN. Questo è il metodo più diffuso e più semplice da implementare, in quanto lo switch deve guardare solo da quale porta viene un pacchetto per attribuirgli un VID.
- autenticazione: i diversi apparati possono essere assegnati automaticamente a determinate VLAN sulla base di credenziali di autenticazione dell'utente o dell'apparato stesso tramite l'impiego del protocollo 802.1x.
- protocollo: l'appartenenza ad una VLAN è dettata dal protocollo incapsulato in 802.3. Ad esempio, i pacchetti IP possono appartenere ad una VLAN diversa da quella usata dai pacchetti IPX.
- MAC Address o indirizzo IP: i pacchetti vengono attribuiti ad una VLAN sulla base dell'indirizzo MAC o IP dell'host da cui provengono. In questo modo, ad una porta di uno switch possono essere collegati diversi host, che però appartengono a VLAN diverse.
- analisi del pacchetto: lo switch che riceve il pacchetto lo esamina in dettaglio, possibilmente fino al livello applicazioni, e sulla base dei risultati decide a quale VLAN attribuirlo sulla base del suo contenuto

SWITCH VIRTUALE

- Uno switch virtuale è un componente software che simula il comportamento di uno switch di rete.
- Serve per collegare le interfacce di rete delle macchine virtuali.
- Nelle piattaforme di virtualizzazione ogni VM ha una scheda di rete virtuale collegata a questo switch.

SCHEDA DI RETE VIRTUALE

- Ogni macchina virtuale possiede una o più interfacce di rete virtuali chiamate vNIC.
- Queste schede di rete si comportano come una normale scheda Ethernet.
- Permettono alla VM di inviare e ricevere traffico sulla rete virtuale.

BRIDGE DI RETE

- Un bridge collega la rete virtuale alla rete fisica.
- Questo permette alle macchine virtuali di ottenere un indirizzo IP dalla stessa rete dei computer fisici.
- Il bridge è molto usato nei laboratori e nei server di virtualizzazione.

MODALITÀ NAT

- La modalità NAT (Network Address Translation) permette alle VM di accedere a internet tramite l'host.
- Le VM hanno indirizzi privati e non sono direttamente visibili dalla rete esterna.
- Questa modalità è utile per ambienti isolati e laboratori.

MODALITÀ BRIDGED

- In modalità Bridged la VM si comporta come un computer collegato direttamente alla rete.
- Ottiene un indirizzo IP dalla rete locale.
- Può essere raggiunta da altri dispositivi della LAN.

MODALITÀ HOST-ONLY

- La modalità Host-Only crea una rete privata tra host e VM.
- Le macchine virtuali possono comunicare solo con l'host e tra loro.
- È utile per test isolati e ambienti di laboratorio.

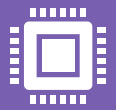
CONFRONTO MODALITÀ RETE

- NAT: accesso internet ma isolamento dalla rete locale.
- Bridged: accesso diretto alla rete locale.
- Host-Only: rete completamente isolata.
- La scelta dipende dal tipo di laboratorio o ambiente di produzione.

INDIRIZZI IP NELLE VM

Le macchine virtuali utilizzano indirizzi IP come qualsiasi altro computer.

Possono ricevere IP tramite DHCP oppure essere configurate con IP statico.



Una corretta configurazione IP è essenziale per il funzionamento della rete.

DHCP NELLE RETI VIRTUALI

- Molte piattaforme di virtualizzazione includono un server DHCP virtuale.
- Questo assegna automaticamente gli indirizzi IP alle VM.
- È molto utile nei laboratori perché semplifica la configurazione.

DNS NELLE INFRASTRUTTURE VIRTUALI

- Il DNS permette di risolvere i nomi delle macchine virtuali in indirizzi IP.
- In ambienti aziendali spesso è gestito da un server DNS centrale.
- Una corretta configurazione DNS facilita la gestione delle infrastrutture.

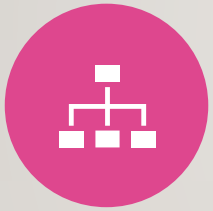
SEGMENTAZIONE DI RETE

- La segmentazione consiste nel dividere la rete in più zone separate.
- Questo riduce la superficie di attacco e migliora la sicurezza.
- In ambienti virtualizzati è molto facile creare reti separate.

PERCHÉ SEGMENTARE LA RETE

- Limitare la comunicazione tra sistemi diversi.
- Ridurre il rischio di propagazione di attacchi.
- Organizzare meglio l'infrastruttura IT.

ZONE DI RETE TIPICHE



RETE DI MANAGEMENT.

RETE SERVER.

RETE UTENTI.

DMZ PER SERVIZI ESPOSTI SU INTERNET.

DMZ

- DMZ significa Demilitarized Zone.
- È una rete separata che ospita servizi accessibili dall'esterno.
- Serve a proteggere la rete interna dell'organizzazione.

FIREWALL VIRTUALI

Un firewall virtuale controlla il traffico tra diverse reti virtuali.

Permette di applicare regole di sicurezza.

È molto usato negli ambienti cloud e virtualizzati.

MICRO-SEGMENTAZIONE

- La micro-segmentazione divide ulteriormente la rete in segmenti molto piccoli.
- Ogni VM può avere regole di sicurezza specifiche.
- Questo approccio è sempre più diffuso nelle architetture Zero Trust.

ZERO TRUST
«MAI FIDARSI, VERIFICARE SEMPRE»

- **Verifica Esplicita:** Ogni richiesta di accesso è autenticata e autorizzata in base a identità, posizione, dispositivo e contesto, non solo dalla rete di provenienza.
- **Accesso con Privilegi Minimi (Least Privilege):** Agli utenti viene concesso solo l'accesso necessario per svolgere il proprio lavoro, limitando il movimento laterale in caso di violazione
- **Ipotizzare la Violazione (Assume Breach):** Il sistema agisce assumendo che le minacce siano onnipresenti, segmentando le reti per limitare i danni.
- **Microsegmentazione:** La rete viene divisa in zone più piccole e sicure per isolare i carichi di lavoro e prevenire la propagazione di attacchi.

RETE NEI DATA CENTER VIRTUALIZZATI

- Nei data center moderni la maggior parte della rete è definita via software.
- Questo approccio è chiamato Software Defined Networking.
- Permette grande flessibilità nella gestione delle infrastrutture.

SOFTWARE DEFINED NETWORKING

- SDN separa il controllo della rete dall'hardware.
- La configurazione può essere gestita centralmente.
- È molto utilizzato nei cloud pubblici e privati.

RETI VIRTUALI CON KVM

- Nel mondo Linux, KVM utilizza spesso libvirt per gestire le reti virtuali.
- Le reti possono essere NAT, bridge o isolate.
- La configurazione può essere fatta tramite virt-manager o da terminale.

COMANDO VIRSH PER LE RETI

- Il comando virsh permette di gestire le reti virtuali da terminale.
- È possibile creare, attivare e configurare reti.
- Questo approccio è molto utile nei server senza interfaccia grafica.

ESEMPIO DI RETE NAT CON LIBVIRT

- Libvirt crea automaticamente una rete NAT chiamata 'default'.
- Questa rete permette alle VM di accedere a internet tramite l'host.
- È la configurazione più comune nei laboratori.

CREARE UNA RETE BRIDGE

- Per collegare le VM alla LAN si crea una rete bridge.
- Il bridge collega l'interfaccia fisica dell'host con la rete virtuale.
- Le VM ricevono IP dalla rete reale.

RETI ISOLATE

- Una rete isolata permette la comunicazione solo tra VM.
- Non c'è accesso alla rete esterna.
- È molto utile per simulazioni e test di sicurezza.

LABORATORIO DI RETE VIRTUALE

- In laboratorio creeremo più VM collegate alla stessa rete virtuale.
- Verificheremo la comunicazione tramite ping.
- Analizzeremo il traffico di rete tra le macchine virtuali.

VERIFICA CON PING

- Il comando ping permette di verificare la connettività tra macchine.
- È uno strumento semplice ma molto utile.
- Viene spesso usato come primo test di rete.

ANALISI CON TRACEROUTE

- Traceroute mostra il percorso dei pacchetti nella rete.
- È utile per diagnosticare problemi di routing.
- Può essere usato anche nelle reti virtuali.

MONITORAGGIO TRAFFICO

- Strumenti come tcpdump o Wireshark permettono di analizzare il traffico.
- Questo aiuta a comprendere come comunicano le VM.
- È anche un esercizio utile per gli studenti di cybersecurity.

PROBLEMI COMUNI

- Configurazione IP errata.
- Firewall che blocca il traffico.
- Rete virtuale non attiva.

DEBUG DELLA RETE

- Controllare configurazione IP.
- Verificare che la rete virtuale sia attiva.
- Controllare le regole firewall.

SICUREZZA DELLE RETI VIRTUALI

- Anche le reti virtuali possono essere attaccate.
- È importante applicare le stesse buone pratiche delle reti fisiche.
- Segmentazione e firewall sono strumenti fondamentali.

ATTACCHI POSSIBILI

- Scanning della rete.
- Movimento laterale tra macchine.
- Attacchi man-in-the-middle.

PROTEZIONE DELLA RETE

- Usare firewall.
- Segmentare la rete.
- Monitorare il traffico.

CASO REALE AZIENDALE

- In un'azienda possono esistere centinaia di VM.
- La rete virtuale permette di gestire queste infrastrutture.
- La sicurezza diventa un elemento fondamentale.

PREPARAZIONE AL LABORATORIO

- Nella prossima attività creeremo una rete virtuale con KVM.
- Configureremo più macchine virtuali.
- Testeremo la comunicazione tra di loro.

RIEPILOGO DELLA LEZIONE

- Abbiamo studiato come funzionano le reti nelle infrastrutture virtualizzate.
- Abbiamo analizzato NAT, bridge e reti isolate.
- Abbiamo introdotto il concetto di segmentazione e sicurezza di rete.