Protocolli di rete

1. Protocolli comuni

I protocolli Internet sono regole e linee guida standardizzate definite in RFC che specificano come i dispositivi su una rete devono comunicare tra loro. Garantiscono che i dispositivi su una rete possano scambiare informazioni in modo coerente e affidabile, indipendentemente dall'hardware e dal software utilizzati. Affinché i dispositivi possano comunicare su una rete, devono essere connessi tramite un canale di comunicazione, ad esempio una connessione cablata o wireless. I dispositivi si scambiano quindi informazioni utilizzando una serie di protocolli standardizzati che definiscono il formato e la struttura dei dati trasmessi. I due tipi principali di connessioni utilizzate sulle reti sono il protocollo di controllo della trasmissione (TCP) e il protocollo datagramma utente (UDP).

1.1 TCP (Protocollo di controllo della trasmissione)

TCPè un connection-oriented protocol che stabilisce una connessione virtuale tra due dispositivi prima di trasmettere i dati utilizzando un Three-Way-Handshake . Questa connessione viene mantenuta fino al completamento del trasferimento dei dati e i dispositivi possono continuare a inviare dati avanti e indietro finché la connessione è attiva.

Ad esempio, quando inseriamo un URL nel nostro browser Web, il browser invia una richiesta HTTP al server che ospita il sito Web utilizzando TCP. Il server risponde inviando il codice HTML per il sito Web al browser utilizzando TCP. Il browser utilizza quindi questo codice per visualizzare il sito Web sul nostro schermo. Questo processo si basa su una TCPconnessione stabilita tra il browser e il server Web e mantenuta fino al completamento del trasferimento dei dati. Di conseguenza, TCPè affidabile ma più lento di UDP poiché richiede un sovraccarico aggiuntivo per stabilire e mantenere la connessione.

1.2 UDP (Protocollo datagramma utente)

D'altra parte, UDPè un connectionlessprotocollo, il che significa che non stabilisce una connessione virtuale prima di trasmettere i dati. Invece, invia i pacchetti di dati alla destinazione senza controllare se sono stati ricevuti.

Ad esempio, quando riproduciamo in streaming o guardiamo un video su una piattaforma come YouTube, i dati del video vengono trasmessi al nostro dispositivo utilizzando UDP. Questo perché il video può tollerare una certa perdita di dati e la velocità di trasmissione è più importante dell'affidabilità. Se alcuni pacchetti di dati video vengono persi lungo il percorso, ciò non influirà in modo significativo sulla qualità complessiva del video. Ciò rende UDP più veloce del TCP ma meno affidabile perché non vi è alcuna garanzia che i pacchetti raggiungano la loro destinazione.

1.3 ICMP

Internet Control Message Protocol (ICMP) è un protocollo utilizzato dai dispositivi per comunicare tra loro su Internet per vari scopi, inclusa la segnalazione degli errori e le informazioni sullo stato. Invia richieste e messaggi tra dispositivi, che possono essere utilizzati per segnalare errori o fornire informazioni sullo stato.

Una richiesta ICMP è un messaggio inviato da un dispositivo a un altro per richiedere informazioni o eseguire un'azione specifica. Un esempio di richiesta in ICMP è la pingrichiesta, che verifica la connettività tra due dispositivi. Quando un dispositivo invia una richiesta ping a un altro, il secondo dispositivo risponde con un ping reply message.

Un'altra parte cruciale di ICMP per noi è il campo Time-To-Live (TTL) nell'intestazione del pacchetto ICMP che limita la durata del pacchetto mentre viaggia attraverso la rete. Impedisce ai pacchetti di circolare indefinitamente sulla rete in caso di routing loop. Ogni volta che un pacchetto passa attraverso un router, il router decrementa il valore TTL value da 1. Quando il valore TTL raggiunge 0, il router scarta il pacchetto e invia un Time Exceededmessaggio ICMP al mittente.

Possiamo anche usare TTL per determinare il numero di salti che un pacchetto ha effettuato e la distanza approssimativa dalla destinazione. Ad esempio, se un pacchetto ha un TTL di 10 e impiega 5 salti per raggiungere la sua destinazione, si può dedurre che la destinazione è a circa 5 salti di distanza. Ad esempio, se vediamo un ping con il TTL valore di 122, potrebbe significare che abbiamo a che fare con un sistema Windows (TTL 128 per impostazione predefinita) a 6 hop di distanza.

1.4 VoIP

Voice over Internet Protocol (VoIP) è un metodo di trasmissione di comunicazioni vocali e multimediali. Ad esempio, ci consente di effettuare telefonate utilizzando una

connessione Internet a banda larga anziché una linea telefonica tradizionale, come Skype, Whatsapp, Google Hangouts, Slack, Zoom e altri.

Tuttavia, SIP è un protocollo di segnalazione per avviare, mantenere, modificare e terminare sessioni in tempo reale che coinvolgono video, voce, messaggistica e altre applicazioni e servizi di comunicazione tra due o più endpoint su Internet. Pertanto, utilizza richieste e metodi tra gli endpoint.

SIP ci consente di enumerare gli utenti esistenti per potenziali attacchi. Questo può essere fatto per vari scopi, come determinare la disponibilità di un utente, trovare informazioni sulle capacità o sui servizi dell'utente o eseguire successivamente attacchi di forza bruta sugli account utente.

Uno dei modi possibili per enumerare gli utenti è la OPTIONS richiesta SIP. È un metodo utilizzato per richiedere informazioni sulle capacità di un server SIP o agenti utente, come i tipi di media che supporta, i codec che può decodificare e altri dettagli. La OPTIONS richiesta può sondare un server SIP o un agente utente per informazioni o testarne la connettività e la disponibilità.

2. Terminologia dei protocolli

Protocollo	Acronimo	Descrizione
Privacy equivalente cablata	WEP	WEP è un tipo di protocollo di sicurezza comunemente utilizzato per proteggere le reti wireless.
Guscio sicuro	SSH	Un protocollo di rete sicuro utilizzato per accedere ed eseguire comandi su un sistema remoto
File Transfer Protocol	FTP	Un protocollo di rete utilizzato per trasferire file da un sistema all'altro
Protocollo di trasferimento della posta semplice	SMTP	Un protocollo utilizzato per inviare e ricevere e-mail
Protocollo di trasferimento ipertestuale	HTTP	Un protocollo client-server utilizzato per inviare e ricevere dati su Internet
Blocco messaggio del server	SMB	Un protocollo utilizzato per condividere file, stampanti e altre risorse in una rete
Sistema di file di rete	NFS	Un protocollo utilizzato per accedere ai file su una rete
Protocollo di gestione della rete semplice	SNMP	Un protocollo utilizzato per gestire i dispositivi di rete
Accesso Wi-Fi protetto	WPA	WPA è un protocollo di sicurezza wireless che utilizza una password per proteggere le reti wireless da accessi non autorizzati.
Protocollo di integrità della chiave temporale	TKIP	TKIP è anche un protocollo di sicurezza utilizzato nelle reti wireless ma meno sicuro.
Protocollo orario di rete	NTP	Viene utilizzato per sincronizzare i tempi dei computer su una rete.
Rete locale virtuale	VLAN	È un modo per segmentare una rete in più reti logiche.
Protocollo di trunking VLAN	VTP	VTP è un protocollo di livello 2 utilizzato per stabilire e mantenere una LAN virtuale (VLAN) che si estende su più switch.
Protocollo di informazioni di instradamento	RIP	RIP è un protocollo di routing del vettore di distanza utilizzato nelle reti locali (LAN) e nelle reti geografiche (WAN).
Apri prima il percorso più breve	OSPF	Si tratta di un protocollo di gateway interno (IGP) per l'instradamento del traffico all'interno di un singolo sistema autonomo (AS) in una rete IP (Internet Protocol).

Protocollo	Acronimo	Descrizione
Protocollo di instradamento del gateway interno	IGRP	IGRP è un protocollo di gateway interno proprietario di Cisco progettato per il routing all'interno di sistemi autonomi.
Protocollo di routing del gateway interno migliorato	EIGRP	Si tratta di un protocollo di routing avanzato del vettore di distanza utilizzato per instradare il traffico IP all'interno di una rete.
Privacy abbastanza buona	PGP	PGP è un programma di crittografia utilizzato per proteggere e-mail, file e altri tipi di dati.
Protocollo di trasferimento di notizie di rete	NNTP	NNTP è un protocollo utilizzato per la distribuzione e il recupero dei messaggi nei newsgroup su Internet.
Protocollo di rilevamento Cisco	CDP	È un protocollo proprietario sviluppato da Cisco Systems che consente agli amministratori di rete di rilevare e gestire i dispositivi Cisco connessi alla rete.
Protocollo router hot standby	HSRP	HSRP è un protocollo utilizzato nei router Cisco per fornire ridondanza in caso di guasto di un router o di un altro dispositivo di rete.
Protocollo di ridondanza del router virtuale	VRRP	È un protocollo utilizzato per fornire l'assegnazione automatica dei router IP (Internet Protocol) disponibili agli host partecipanti.
Protocollo Spanning Tree	STP	STP è un protocollo di rete utilizzato per garantire una topologia senza loop nelle reti Ethernet Layer 2.
Terminal Access Controller Sistema di controllo degli accessi	TACACS	TACACS è un protocollo che fornisce autenticazione, autorizzazione e contabilità centralizzate per l'accesso alla rete.
Protocollo di Inizializzazione Sessione	SIP	È un protocollo di segnalazione utilizzato per stabilire e terminare sessioni vocali, video e multimediali in tempo reale su una rete IP.
Voce su IP	VOIP	VOIP è una tecnologia che consente di effettuare chiamate telefoniche tramite Internet.
Protocollo di autenticazione estensibile	EAP	EAP è un framework per l'autenticazione che supporta più metodi di autenticazione, come password, certificati digitali, password monouso e autenticazione a chiave pubblica.
Protocollo di autenticazione estensibile leggero	LEAP	LEAP è un protocollo di autenticazione wireless proprietario sviluppato da Cisco Systems. Si basa sull'Extensible Authentication Protocol (EAP) utilizzato nel Point-to-Point Protocol (PPP).

Protocollo	Acronimo	Descrizione
Protocollo di autenticazione estensibile protetto	PEAP	PEOP è un protocollo di sicurezza che fornisce un tunnel crittografato per reti wireless e altri tipi di reti.
Server di gestione dei sistemi	SMS	SMS è una soluzione di gestione dei sistemi che aiuta le organizzazioni a gestire reti, sistemi e dispositivi mobili.
Analizzatore di sicurezza di base Microsoft	MBSA	È uno strumento di sicurezza gratuito di Microsoft che viene utilizzato per rilevare potenziali vulnerabilità di sicurezza in computer, reti e sistemi Windows.
Controllo di supervisione e acquisizione dati	SCADA	È un tipo di sistema di controllo industriale utilizzato per monitorare e controllare i processi industriali, come quelli di produzione, generazione di energia e trattamento delle acque e dei rifiuti.
Rete privata virtuale	VPN	VPS è una tecnologia che consente agli utenti di creare una connessione sicura e crittografata a un'altra rete su Internet.
Sicurezza del protocollo Internet	IPsec	IPsec è un protocollo utilizzato per fornire comunicazioni sicure e crittografate su una rete. Viene comunemente utilizzato nelle VPN, o reti private virtuali, per creare un tunnel sicuro tra due dispositivi.
Protocollo di tunneling punto-punto	PPTP	È un protocollo utilizzato per creare un tunnel sicuro e crittografato per l'accesso remoto.
Traduzione dell'indirizzo di rete	NAT	NAT è una tecnologia che consente a più dispositivi su una rete privata di connettersi a Internet utilizzando un singolo indirizzo IP pubblico. NAT funziona traducendo gli indirizzi IP privati dei dispositivi sulla rete in un unico indirizzo IP pubblico, che viene quindi utilizzato per connettersi a Internet.
Avanzamento riga ritorno a capo	CRLF	Combina due caratteri di controllo per indicare la fine di una riga e l'inizio di una nuova riga per determinati formati di file di testo.
JavaScript e XML asincroni	AJAX	Tecnica di sviluppo Web che consente di creare pagine Web dinamiche utilizzando JavaScript e XML/JSON.
Interfaccia di programmazione dell'applicazione server Internet	ISAPI	Consente di creare estensioni Web orientate alle prestazioni per i server Web utilizzando un set di API.
Identificatore di risorsa uniforme	URI	È una sintassi utilizzata per identificare una risorsa su Internet.
Localizzatore uniforme	URL	Sottoinsieme di URI che identifica una pagina Web o un'altra risorsa

Protocollo	Acronimo	Descrizione
di risorse		su Internet, inclusi il protocollo e il nome di dominio.
Scambio di chiavi Internet	IKE	IKE è un protocollo utilizzato per impostare una connessione sicura tra due computer. Viene utilizzato nelle reti private virtuali (VPN) per fornire l'autenticazione e la crittografia per la trasmissione dei dati, proteggendo i dati da intercettazioni e manomissioni esterne.
Incapsulamento del routing generico	GRE	Questo protocollo viene utilizzato per incapsulare i dati trasmessi all'interno del tunnel VPN.
Guscio remoto	RSH	È un programma sotto Unix che permette di eseguire comandi e programmi su un computer remoto.