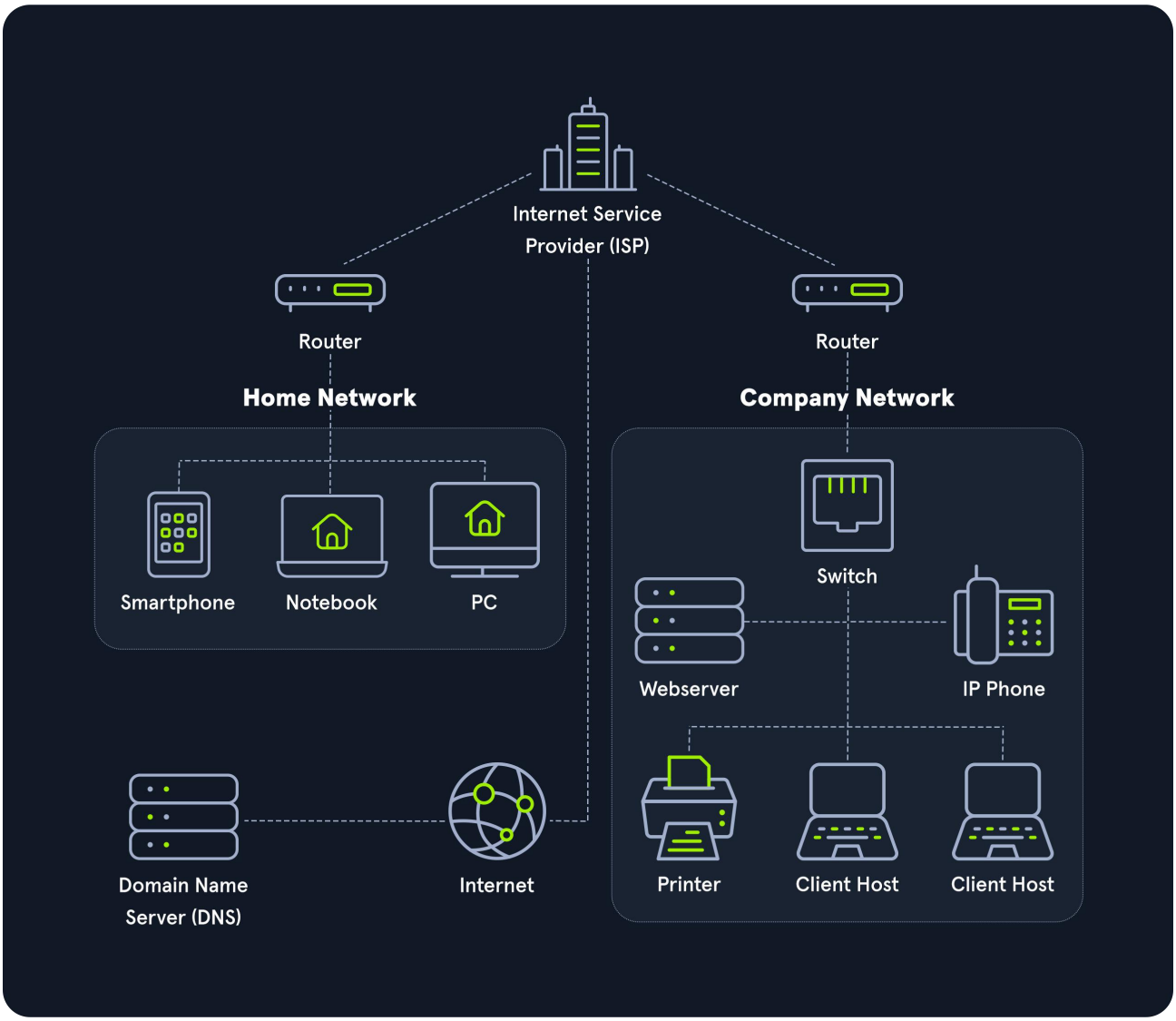
Fondamenti sulle reti

1. Struttura di reti home e company



Switchare le reti permette di isolare i flussi di dati ed evitare attacchi e comunicazioni tra i vari client.

2. Tipi di Rete

Tipo di rete	Definizione
Rete geografica (WAN)	Internet
Rete locale (LAN)	Reti interne (es: casa o ufficio)
Rete locale senza fili (WLAN)	Reti interne accessibili tramite Wi-Fi
Rete privata virtuale (VPN)	Connette più siti di rete a unoLAN

2.1 WAN

La WAN (Wide Area Network) è comunemente indicata come The Internet. Quando si tratta di apparecchiature di rete, spesso avremo un indirizzo WAN e un indirizzo LAN. Quello WAN è l'indirizzo a cui si accede generalmente da Internet. Detto questo, non è inclusivo per Internet; una WAN è solo un gran numero di LAN unite insieme. Molte grandi aziende o agenzie governative avranno una "WAN interna" (chiamata anche Intranet, Airgap Network, ecc.). In generale, il modo principale per identificare se la rete è una WAN è utilizzare un protocollo di routing specifico della WAN come BGP e se lo schema IP in uso non è all'interno di RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

2.2 LAN/WLAN

Le LAN (Local Area Network) e le WLAN (Wireless Local Area Network) assegneranno in genere indirizzi IP designati per l'uso locale (RFC 1918, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). In alcuni casi, come alcuni college o hotel, ti potrebbe essere assegnato un indirizzo IP (Internet) instradabile dall'accesso alla loro LAN, ma è molto meno comune. Non c'è niente di diverso tra una LAN o una WLAN, a parte il fatto che le WLAN introducono la possibilità di trasmettere dati senza cavi. È principalmente una designazione di sicurezza.

2.3 VPN

Una VPN o Virtual Private Network (Rete virtuale privata) crea una connessione di rete privata tra dispositivi su Internet. Le VPN sono utilizzate per trasmettere dati sulle reti pubbliche in modo anonimo e sicuro. Funzionano camuffando gli indirizzi IP dell'utente e crittografando i dati in modo che non possano essere letti da chi non è autorizzato a riceverli. Esistono tre tipi principali Virtual Private Networks(VPN), ma tutti e tre hanno lo stesso obiettivo di far sentire l'utente come se fosse collegato a una rete diversa.

2.3.1 Site-to-Site VPN

Sia il client che il server sono dispositivi di rete, in genere o Routerso Firewalls, e condividono interi intervalli di rete. Questo è più comunemente utilizzato per unire le reti aziendali su Internet, consentendo a più sedi di comunicare su Internet come se fossero locali.

2.3.2 Remote access VPN

Ciò comporta la creazione da parte del computer del cliente di un'interfaccia virtuale che si comporta come se si trovasse sulla rete di un cliente. Hack The Box utilizza OpenVPN, che crea un adattatore TUN che ci consente di accedere ai laboratori. Quando si analizzano queste VPN, un elemento importante da considerare è la tabella di routing che viene creata quando si accede alla VPN. Se la VPN crea percorsi solo per reti specifiche (es: 10.10.10.0/24), questo viene chiamato Split-Tunnel VPN, il che significa che la connessione Internet non esce dalla VPN. Questo è ottimo per Hack The Box perché fornisce l'accesso al laboratorio senza la preoccupazione per la privacy di monitorare la tua connessione Internet. Tuttavia, per un'azienda, split-tunnelle VPN in genere non sono l'ideale perché se la macchina è infettata da malware, molto probabilmente i metodi di rilevamento basati sulla rete non funzioneranno poiché il traffico esce da Internet.

2.3.3 VPN SSL

Questa è essenzialmente una VPN che viene eseguita all'interno del nostro browser Web e sta diventando sempre più comune poiché i browser Web stanno diventando in grado di fare qualsiasi cosa. In genere questi trasmettono in streaming applicazioni o

intere sessioni desktop al tuo browser web. Un ottimo esempio di questo sarebbe HackTheBox Pwnbox.

3. Strutture di rete

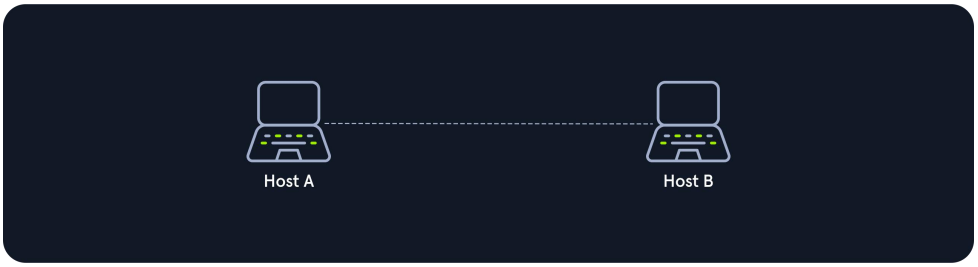
Possiamo immaginare una topologia come una forma virtuale o structure of a network. Questa forma non corrisponde necessariamente all'effettiva disposizione fisica dei dispositivi nella rete. Pertanto queste topologie possono essere physicalo logical. Ad esempio, i computer di un computer LANpossono essere disposti in cerchio in una camera da letto, ma è molto improbabile che abbiano una topologia ad anello reale.

Le topologie di rete sono suddivise nei seguenti otto tipi di base:

Point-to-Point (Punto a Punto)	Bus
Star (stella)	Ring (anello)
Mesh (maglia)	Tree (albero)
Hybrid (ibride)	Daisy Chain (margherita)

3.1 Punto a punto

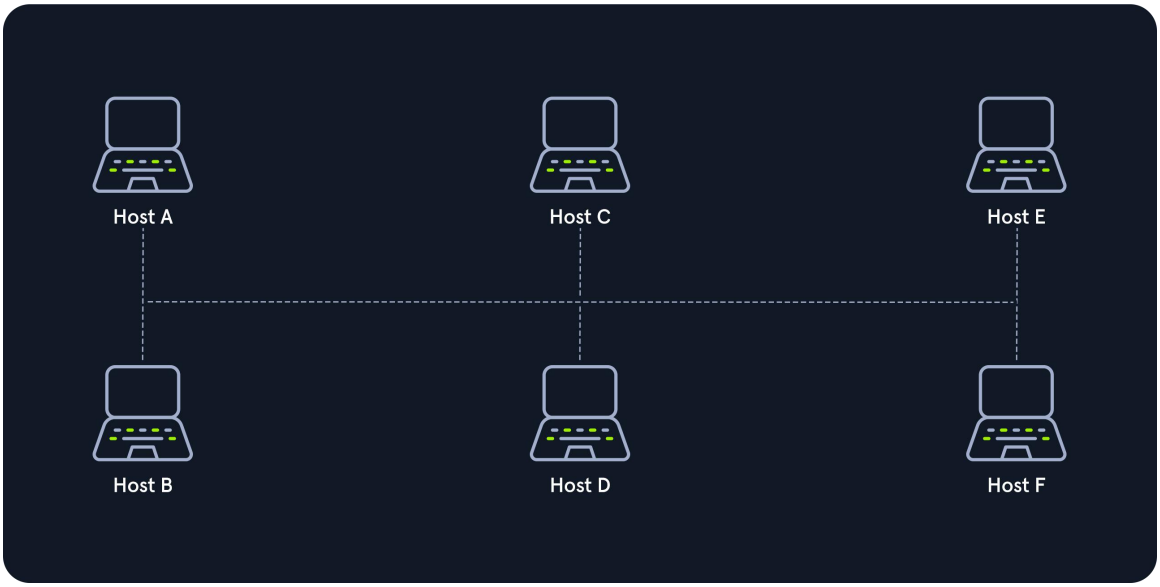
collegamento fisico diretto e diretto solo tra two hosts. Questi due dispositivi possono utilizzare queste connessioni per la comunicazione reciproca. Sono il modello base della telefonia tradizionale e non devono essere confuse con P2P(Peer-to-Peer).



3.2 Bus

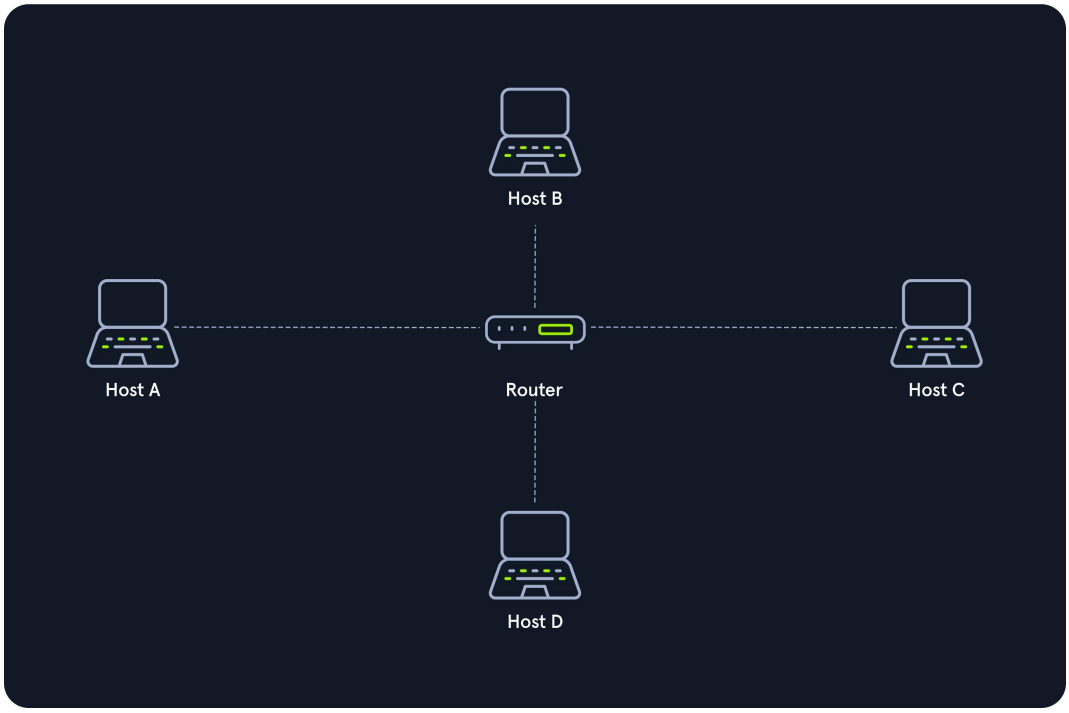
Tutti gli host sono collegati tramite un mezzo di trasmissione nella topologia bus. Ogni host ha accesso al mezzo di trasmissione e ai segnali che vengono trasmessi su di esso. Non esiste un componente di rete centrale che controlla i processi su di esso. Il mezzo di trasmissione per questo può essere, ad esempio, un file coaxial cable.

Poiché il mezzo è condiviso con tutti gli altri, solo one host can send, e tutti gli altri possono solo ricevere e valutare i dati e vedere se sono destinati a se stessi.



3.3 Star

mantiene una connessione a tutti gli host. Ogni host è connesso a central network componenttramite un collegamento separato. Di solito si tratta di un router, un hub o uno switch. Questi gestiscono i forwarding functionpacchetti di dati. Per fare ciò, i pacchetti di dati vengono ricevuti e inoltrati alla destinazione. Il traffico dati sul componente di rete centrale può essere molto elevato poiché tutti i dati e le connessioni lo attraversano.



3.4 Anello

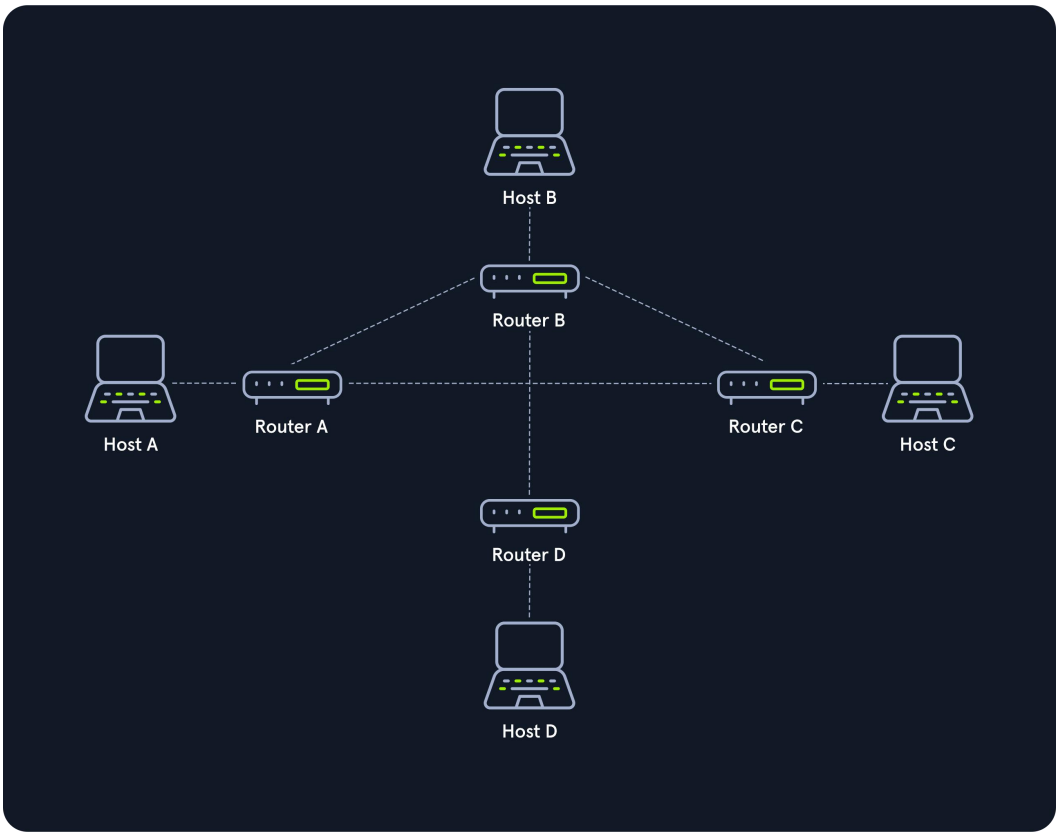
La physicaltopologia ad anello è tale che ogni host o nodo è connesso all'anello con due cavi: 1 per dati in entrata e 1 per dati in uscita.

Le informazioni vengono trasmesse in una direzione di trasmissione predeterminata. Tipicamente, si accede al mezzo di trasmissione in sequenza da stazione a stazione utilizzando un sistema di recupero dalla stazione centrale o un file token. Un token è un modello di bit che passa continuamente attraverso una rete ad anello in una direzione, che funziona secondo il claim token process.

3.5 Mesh

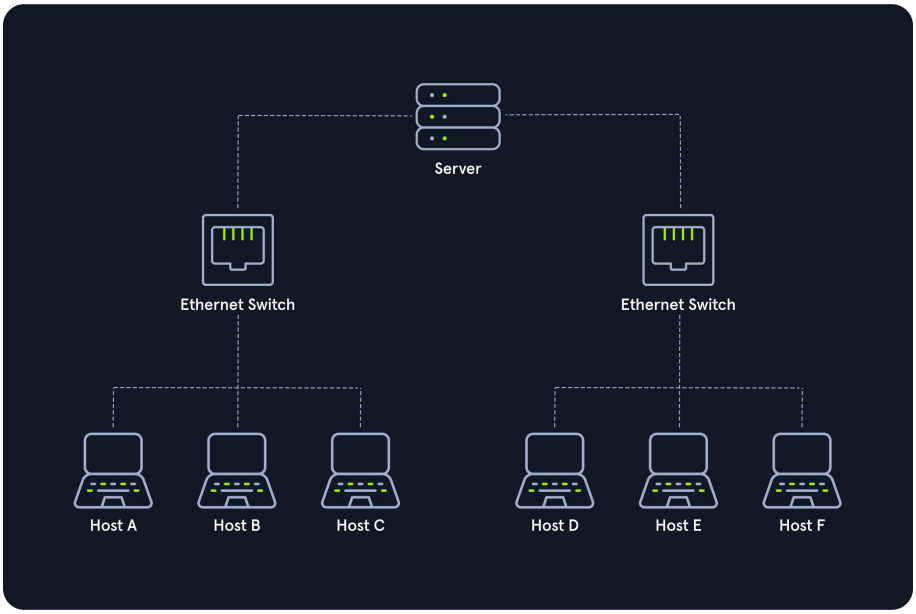
Le strutture mesh non hanno una topologia fissa, Ci sono due strutture di base dal concetto di base: il fully meshed e la partially meshed struttura. Gli host sono collegati tra loro. Questa tecnica viene utilizzata principalmente in WAN o MAN per garantire un'elevata affidabilità e larghezza di banda. In questa configurazione, importanti nodi di rete come i router potrebbero essere collegati in rete insieme. Se un router si guasta, gli altri possono continuare a funzionare senza problemi e la rete può assorbire il guasto dovuto alle numerose connessioni. In partially meshed structure, gli endpoint sono connessi da una sola connessione. In questo tipo di topologia di rete, nodi specifici sono

connessi esattamente a un altro nodo e alcuni altri nodi sono connessi a due o più altri nodi con una connessione punto a punto.



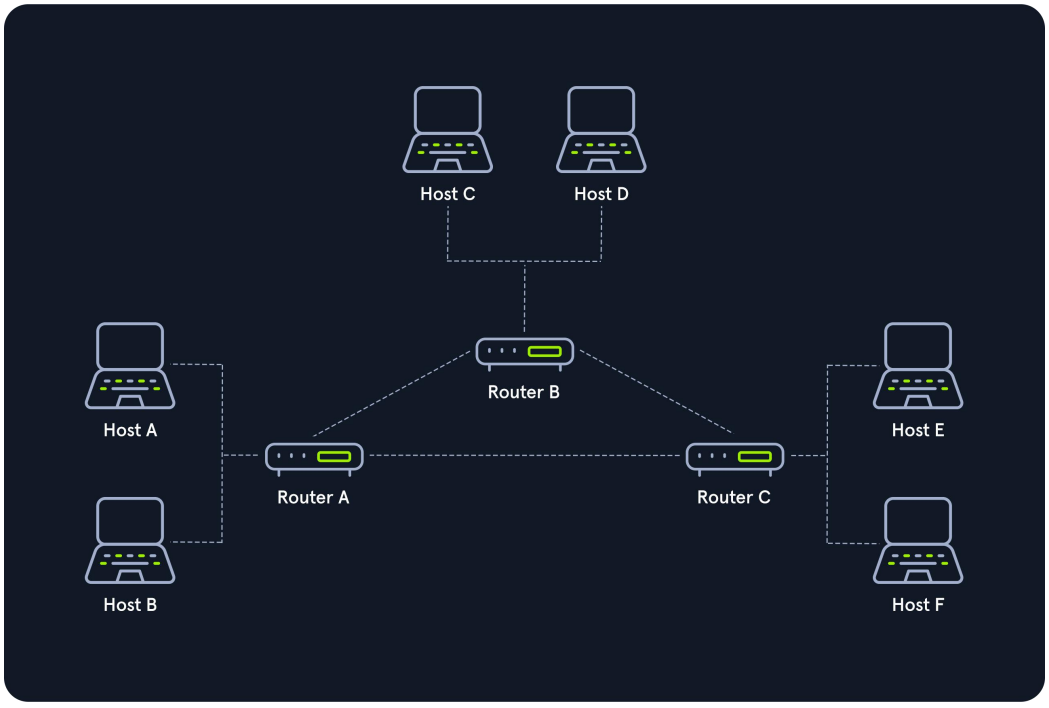
3.6 Albero

Una topologia ad albero include più topologie a stella, che coinvolgono una varietà di singoli nodi collegati a un nodo centrale. Più stelle coinvolgono una serie o nodi terziari collegati a due o più nodi secondari, che sono collegati al nodo principale del tronco dell'albero. Gli esperti possono definire una topologia ad albero come una combinazione di topologie a stella e bus, in cui più elementi sono collegati attraverso una singola connessione laterale. Ogni nodo in un livello gerarchico ha collegamenti punto-punto con ciascun nodo adiacente al suo livello inferiore. Tutti i nodi secondari hanno allegati punto-punto ai nodi terziari nella loro giurisdizione e il nodo primario ha una connessione punto-punto a ciascun nodo secondario. Se visualizzati in modo visivo, questi sistemi appaiono simili a una struttura ad albero. Uno svantaggio di una topologia ad albero è che un intero sistema può essere paralizzato da qualsiasi danno o malfunzionamento del nodo primario.



3.7 Ibrido

Le reti ibride combinano due o più topologie in modo che la rete risultante non presenti topologie standard. Ad esempio, una rete ad albero può rappresentare una topologia ibrida in cui le reti a stella sono collegate tramite reti di bus interconnesse. Tuttavia, una rete ad albero collegata a un'altra rete ad albero è ancora topologicamente una rete ad albero. Una topologia ibrida viene sempre creata quando two differentle topologie di rete di base sono interconnesse.

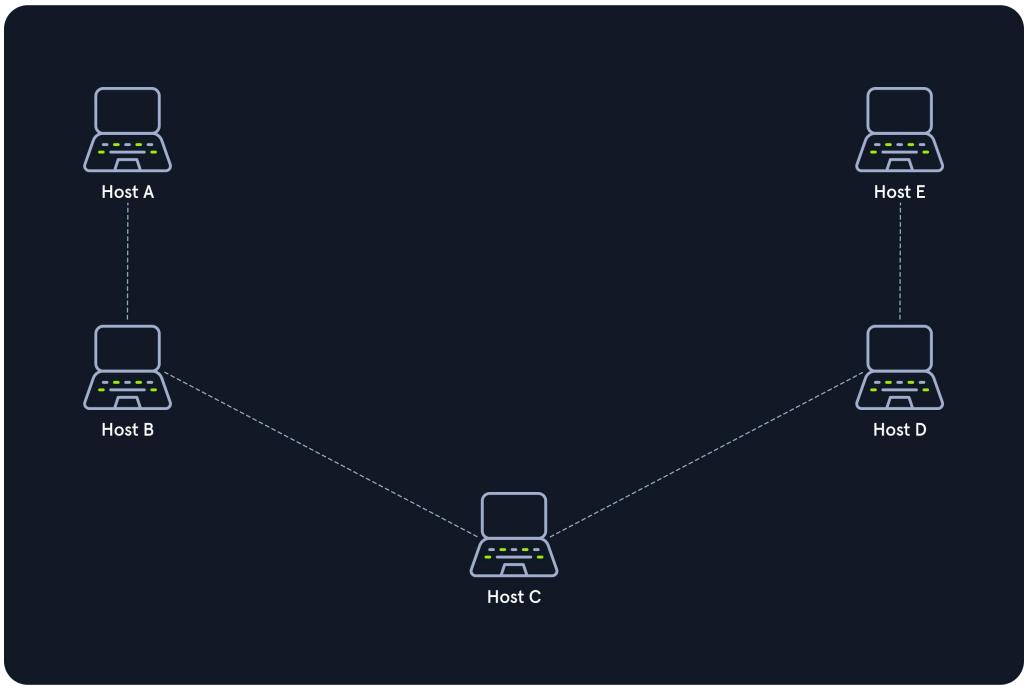


3.8 Margherita

Nella topologia daisy chain, più host sono collegati posizionando un cavo da un nodo all'altro.

Poiché questo crea una catena di connessioni, è anche nota come configurazione daisy-chain in cui più componenti hardware sono collegati in serie. Questo tipo di collegamento in rete si trova spesso nella tecnologia di automazione (CAN).

Il collegamento a margherita si basa sulla disposizione fisica dei nodi, a differenza delle procedure token, che sono strutturali ma possono essere rese indipendenti dalla disposizione fisica. Il segnale viene inviato da e verso un componente tramite i suoi nodi precedenti al sistema informatico.



4. Proxy

Un proxy è quando un dispositivo o un servizio si trova nel mezzo di una connessione e funge da mediatore e deve essere in grado di ispezionare il contenuto del traffico. Senza la possibilità di essere un mediator, il dispositivo è tecnicamente un gateway, non un proxy.

Se hai problemi a ricordarlo, i proxy funzioneranno quasi sempre al livello 7 del modello OSI. Esistono molti tipi di servizi proxy, ma i principali sono:

- Dedicated Proxy/Forward Proxy
- Reverse Proxy
- Transparent Proxy

4.1 Proxy dedicato / Proxy di inoltro

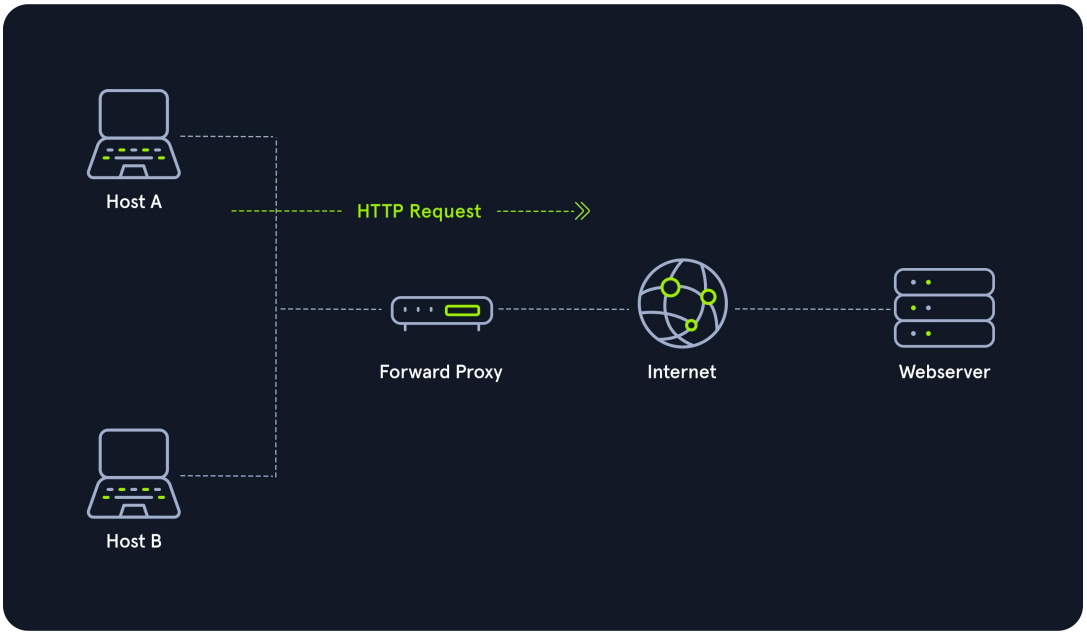
Il Forward Proxy, è ciò che la maggior parte delle persone immagina sia un proxy. Un proxy di inoltro si verifica quando un client effettua una richiesta a un computer e quel computer esegue la richiesta.

Ad esempio, in una rete aziendale, i computer sensibili potrebbero non avere accesso diretto a Internet. Per accedere a un sito web, devono passare attraverso un proxy (o filtro web). Questa può essere una linea di difesa incredibilmente potente contro il malware, poiché non solo deve aggirare il filtro web (facile), ma dovrebbe anche essere o utilizzare proxy awareun C2 non tradizionale (un modo in cui il malware riceve informazioni sulle attività). Se l'organizzazione utilizza solo FireFox, la probabilità di ottenere malware proxy-aware è improbabile.

I browser Web come Internet Explorer, Edge o Chrome obbediscono tutti alle impostazioni "Proxy di sistema" per impostazione predefinita. Se il malware utilizza WinSock (Native Windows API), sarà probabilmente a conoscenza del proxy senza alcun codice aggiuntivo. Firefox non utilizza WinSocke utilizza invece libcurl, che gli consente di utilizzare lo stesso codice su qualsiasi sistema operativo. Ciò significa che il malware dovrebbe cercare Firefox ed estrarre le impostazioni del proxy, cosa che è altamente improbabile che il malware faccia.

In alternativa, il malware potrebbe utilizzare il DNS come meccanismo c2, ma se un'organizzazione sta monitorando il DNS (cosa facilmente eseguibile utilizzando Sysmon), questo tipo di traffico dovrebbe essere catturato rapidamente.

Un altro esempio di Forward Proxy è Burp Suite, poiché la maggior parte delle persone lo utilizza per inoltrare richieste HTTP. Tuttavia, questa applicazione è il coltellino svizzero dei proxy HTTP e può essere configurata per essere un proxy inverso o trasparente!

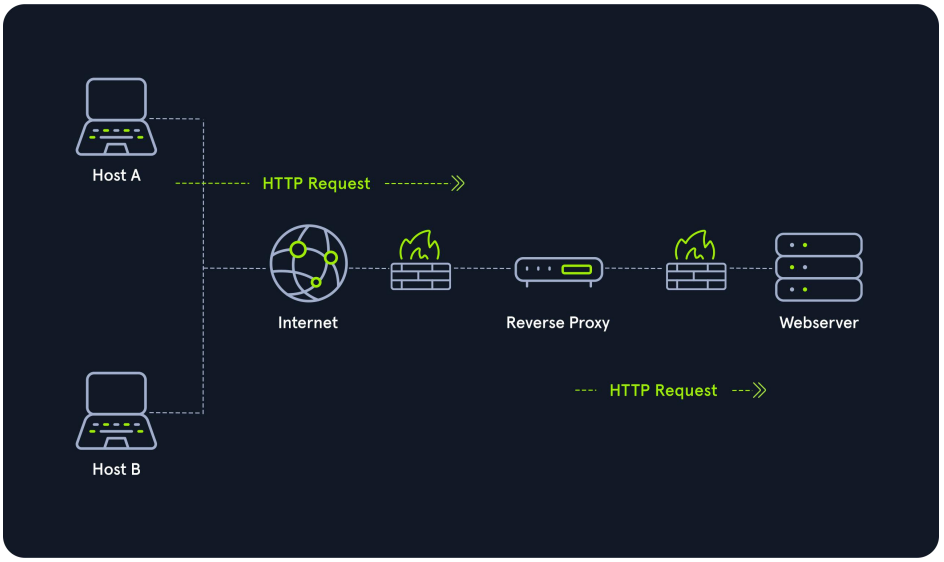


4.2 Proxy inverso

Come avrai intuito, a reverse proxy, è il contrario di a Forward Proxy. Invece di essere progettato per filtrare le richieste in uscita, filtra quelle in entrata. L'obiettivo più comune con un Reverse Proxy, è ascoltare un indirizzo e inoltrarlo a una rete chiusa.

I Penetration Tester configureranno i proxy inversi sugli endpoint infetti. L'endpoint infetto resterà in ascolto su una porta e invierà qualsiasi client che si connette alla porta all'aggressore attraverso l'endpoint infetto. Questo è utile per aggirare i firewall o eludere la registrazione. Le organizzazioni possono avere IDS(Intrusion Detection Systems), che controllano le richieste web esterne. Se l'attaccante ottiene l'accesso all'organizzazione tramite SSH, un proxy inverso può inviare richieste Web attraverso il tunnel SSH ed eludere l'IDS.

Un altro proxy inverso comune è ModSecurity, a Web Application Firewall(WAF). I firewall per applicazioni Web ispezionano le richieste Web alla ricerca di contenuti dannosi e bloccano la richiesta se è dannosa.



4.3 Proxy invers

Tutti questi servizi proxy agiscono con Proxy trasparente o no.

Con a transparent proxy, il client non sa della sua esistenza. Il proxy trasparente intercetta le richieste di comunicazione del client a Internet e funge da istanza sostitutiva. All'esterno, il proxy trasparente, come il proxy non trasparente, funge da partner di comunicazione.

Se è un non-transparent proxy, dobbiamo essere informati della sua esistenza. A tale scopo, a noi e al software che vogliamo utilizzare viene assegnata una speciale configurazione proxy che garantisce che il traffico verso Internet sia prima indirizzato al proxy. Se questa configurazione non esiste, non possiamo comunicare tramite il proxy. Tuttavia, poiché il proxy di solito fornisce l'unico percorso di comunicazione verso altre reti, la comunicazione con Internet viene generalmente interrotta senza una configurazione proxy corrispondente.