GUIDA DI SISTEMI E RETI

PER AUTOSTOPPISTI

Prof. Ing. Simone Zanella

“Guida di Sistemi e Reti per Autostoppisti”

3a Edizione – Giugno 2024

INTRODUZIONE

“La Guida ha già soppiantato la grande Enciclopedia galattica, come l'indiscussa depositaria di tutta la conoscenza e la saggezza, per due importanti ragioni. Primo, costa un po' meno; secondo, reca la scritta DON'T PANIC, niente panico, in grandi e rassicuranti caratteri sulla copertina.“

Così viene definita la “Guida galattica per gli autostoppisti” nell’omonimo romanzo di fantascienza umoristica scritto da Douglas Adams nel 1979, che per un caso curioso è anche l’anno di nascita dell’autore della Guida che state leggendo.

Ho iniziato a scrivere questa Guida nel 2019, per fornire un ausilio ai miei studenti nel ripassare gli argomenti principali di “Sistemi e Reti”, materia che insegno in un Istituto Tecnico a indirizzo “Informatica e Telecomunicazioni”.

Dentro sono presenti brevi sintesi dei principali argomenti d’Esame, corredati di alcuni appunti di esperienze di laboratorio, approfondimenti extra, e consigli per lo svolgimento della II Prova, di cui sul mio sito www.simonezanella.it raccolgo da anni tutti i testi, simulazioni e soluzioni che trovo in rete, o che preparo per la mia scuola.

Questa Guida non è in grado di sostituire il libro, gli appunti e tutto il resto del materiale fornito dai docenti, ovviamente, ma magari può essere un valido aiuto per ripassare quando il tempo stringe e l’Esame si avvicina.

Questa Guida non è d’aiuto se si è ancora indecisi su cosa fare del proprio futuro dopo il Diploma, ma se siete in cerca della risposta alla “Domanda Fondamentale sulla Vita, l'Universo e Tutto Quanto”, allora vi consiglio di consultare il libro di Adams, dove scoprirete che la risposta è molto semplice: 42.

BUON RIPASSO, NON DIMENTICATE L’ASCIUGAMANO E SOPRATTUTTO... NON FATEVI PRENDERE DAL PANICO!

INDICE

TEORIA

QUALCOSA SULLE RETI

Modello ISO/OSI: International Organization for Standardization. È un'organizzazione internazionale non governativa che sviluppa e pubblica standard volontari per una vasta gamma di settori e industrie.

OSI: Open Systems Interconnection è un modello concettuale che descrive come le reti informatiche dovrebbero funzionare e comunicare tra loro. Il modello OSI suddivide il processo di comunicazione di rete in 7 strati distinti, ognuno dei quali svolge un compito specifico, consentendo a dispositivi e applicazioni di comunicare in modo efficace attraverso una rete informatica.

- Strato **fisico**: si occupa dei dettagli fisici della trasmissione, come il cablaggio e i segnali elettrici.
- Strato di **collegamento dati (data link)**: gestisce il trasferimento affidabile dei dati attraverso il collegamento fisico. Si occupa di errori, flusso di dati e indirizzi MAC (Media Access Control).
- Strato di **rete (network)**: instrada i dati attraverso la rete. Questo strato utilizza indirizzi IP per determinare il percorso migliore per inviare i dati.
- Strato di **trasporto**: gestisce la consegna affidabile dei dati. Si occupa di suddividere i dati in pacchetti, numerarli per il corretto ordine di consegna e gestire il controllo del flusso e la correzione degli errori.

- Strato di **sessione**: stabilisce, mantiene e termina le sessioni di comunicazione tra i dispositivi. Gestisce la sincronizzazione e il dialogo tra i processi che comunicano.
- Strato di **presentazione**: si occupa della rappresentazione e della traduzione dei dati in un formato comprensibile per l'applicazione ricevente. Include la cifratura, la compressione e la conversione del formato dei dati.
- Strato di **applicazione**: fornisce interfacce per le applicazioni di rete. Si occupa dell'interazione diretta con l'utente e delle funzionalità specifiche dell'applicazione, come la posta elettronica, la navigazione web o la condivisione di file.

PDU: Protocol Data Unit, ovvero un pacchetto di dati che viene trasmesso attraverso una rete da un dispositivo all'altro, contiene i dati che devono essere inviati, insieme ad altre informazioni necessarie per il corretto instradamento e la consegna dei dati al destinatario, ad esempio l'indirizzo IP del mittente e del destinatario, i numeri di porta, i controlli di errore e altre informazioni di gestione della rete.

Topologie di rete: la topologia **fisica** descrive la struttura fisica delle rete (livelli 1 e 2) ovvero gli apparati utilizzati, la loro collocazione, i tipi di canali trasmissivi, le interfacce; la topologia **logica** descrive le configurazioni degli apparati, l'indirizzamento IP, le classi di indirizzi utilizzate, i nomi degli host. La scelta della topologia dipende dalle esigenze specifiche della rete, tra cui la dimensione, l'affidabilità, la scalabilità e il budget disponibile. Le **topologie fisiche** classiche sono:

- Topologia a **stella**: tutti i dispositivi di rete sono collegati a un hub o a uno switch centrale. Tutti i dati passano attraverso il dispositivo centrale, che coordina il flusso delle informazioni tra i dispositivi.
- Topologia ad **anello**: i dispositivi di rete sono collegati formando un anello chiuso. Ogni dispositivo è collegato a due dispositivi adiacenti e i dati circolano lungo l'anello in una direzione specifica. Ogni dispositivo riceve e inoltra i dati fino a quando non raggiungono la destinazione desiderata.
- Topologia a **bus**: i dispositivi di rete sono collegati a un unico cavo di trasmissione principale, i dati vengono inviati lungo il cavo e tutti i dispositivi sulla rete ricevono i dati. Tuttavia, solo il dispositivo di destinazione specifico elabora effettivamente i dati.
- Topologia a **maglia (mesh)**: ogni dispositivo di rete è collegato direttamente a ogni altro dispositivo. Ciò crea un'elevata ridondanza e una maggiore affidabilità, poiché se un collegamento si interrompe, i dati possono comunque essere instradati tramite percorsi alternativi.
- Topologia ad **albero**: è una combinazione di topologie a stella e a bus. I dispositivi sono organizzati in una struttura ad albero, con un dispositivo centrale che funge da radice e altri dispositivi collegati a esso in modo gerarchico; viene spesso utilizzata nelle reti di grandi dimensioni.

Token-Ring: è un tipo di rete di computer in cui i dispositivi sono collegati a un anello fisico e si scambiano i dati in modo sequenziale.

Si basa su un meccanismo chiamato "token passing". Il processo continua in modo ciclico nell'anello, consentendo a tutti i dispositivi di avere un turno per inviare e ricevere dati sulla rete. Quando un dispositivo detiene il token, può inserire i propri dati nel token e inviarli sulla rete. Il token, con i dati aggiunti, continua a circolare nell'anello, consentendo agli altri dispositivi di ricevere i dati e, se necessario, aggiungere o modificare le informazioni prima di inoltrarle.L'utilizzo del token garantisce che solo un dispositivo possa trasmettere dati alla volta, evitando collisioni di dati e garantendo un accesso equo alla rete per tutti i dispositivi connessi.

LAN, MAN, WAN, WLAN, PAN: termini che suddividono le reti (AN: Area Network) in base all'area geografica servita: Local - Metropolitan - Wide - Wireless Local - Personal.

SAN: Storage Area Network, rete dedicata al trasferimento dati tra server e storage, tipicamente basata su fibra e con trasferimenti dati elevati fino a 16Gbit/s.

Pacchetto: indica a livello generale una sequenza di dati trasmessi su una rete. Tecnicamente nel livello 2 si chiama **frame**, nel livello IP/rete si chiama **datagramma** (o **pacchetto IP**), nel livello TCP si chiama **segmento** (ma anche datagramma nel caso di UDP).

Protocollo: insieme di regole che sovrintendono la comunicazione tra entità dello stesso livello. Definisce le PDU che vengono trasferite per comunicare, formate da un **header** (che contiene informazioni di controllo) e un **payload** (che contiene i dati). Nelle reti informatiche, gli strati di protocollo sono suddivisi in diversi livelli (vedi OSI), ognuno dei quali svolge compiti specifici e mette a

disposizione diversi servizi. Un **SAP** (Service Access Point) è il punto di accesso a un servizio all'interno di uno strato di protocollo.

IEEE 802: è una famiglia di standard sviluppato dall'IEEE (Institute of Electrical and Electronics Engineers) per la standardizzazione delle LAN, delle WLAN e delle MAN. Si occupa dei primi 2 livelli OSI attraverso i protocolli LLC (controllo logico del collegamento) e MAC (Media Access Control, controllo dell'accesso al mezzo fisico) che identifica con un indirizzo univoco di 48 bit le stazioni di rete.

Ethernet: è una famiglia di protocolli di rete (standard 802.3) che definisce i metodi di accesso al mezzo trasmissivo e il formato dei frame (struttura dei pacchetti) utilizzati per la trasmissione dei dati all'interno di una rete locale (LAN). Ethernet è ampiamente utilizzata per la sua semplicità, affidabilità e scalabilità. Supporta una vasta gamma di applicazioni, come ad esempio la condivisione di file, l'accesso a Internet, le comunicazioni VoIP. Le principali caratteristiche dello standard Ethernet includono:

- **Metodo di accesso al mezzo**: utilizza il metodo **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection). Ciò significa che i dispositivi sulla rete controllano se il mezzo trasmissivo (ad esempio il cavo) è libero prima di trasmettere i dati. Se più dispositivi trasmettono contemporaneamente e si verificano collisioni, i dispositivi rilevano le collisioni e attendono un breve periodo prima di ritentare la trasmissione.
- **Velocità di trasmissione**: alcune delle velocità comuni includono **Ethernet** 10 Mbps, **Fast Ethernet** 100 Mbps, **Gigabit Ethernet** 1 Gbps e 10 **Gigabit Ethernet** 10 Gbps.

- **Formato dei frame**: un frame Ethernet tipico include campi come indirizzo di destinazione MAC, indirizzo di origine MAC, tipo di protocollo e i dati stessi.
- **Tipi di cablaggio**: può essere implementato su diversi tipi di cablaggio, come il tradizionale cavo in rame (UTP/STP) o il cablaggio in fibra ottica.

PoE: Power over Ethernet, consente l'alimentazione di un apparato tramite cablaggio di rete. E' particolarmente utilizzata per i dispositivi impiegati nelle reti WiFi.

Dominio di broadcast: è l'insieme di tutti i dispositivi che possono ricevere un pacchetto di broadcast. I domini di broadcast sono generalmente delimitati da dispositivi di rete come router, switch o bridge. Questi dispositivi creano segmenti di rete o VLAN (Virtual LAN) che suddividono fisicamente o logicamente la rete in domini di broadcast separati, riducendo l'effetto di broadcast indesiderati su tutta la rete.

Dominio di collisione: insieme di host che accedono allo stesso mezzo trasmissivo su cui vogliono trasmettere dati. in una rete Ethernet in cui due o più dispositivi inviano contemporaneamente dei dati sulla stessa linea di trasmissione, causando una collisione dei segnali. Questo si verifica perché in una rete Ethernet condivisa, tutti i dispositivi sulla stessa rete utilizzano lo stesso canale di comunicazione. Quando una collisione si verifica, i segnali si sovrappongono e i dati trasmessi dai dispositivi coinvolti nella collisione possono risultare corrotti. Quando ciò accade, i dispositivi rilevano la collisione tramite un meccanismo di rilevazione delle

collisioni (CSMA/CD) e attendono un periodo casuale prima di ritentare la trasmissione dei dati.

CSMA/CD: protocollo di accesso multiplo per la risoluzione delle collisioni su reti locali cablate di tipo broadcast. Un host può utilizzare la rete Ethernet soltanto se nessun altro la sta già utilizzando, tramite un meccanismo di ascolto del mezzo.

Dorsale o Backbone: collegamento ad alta velocità tra due server o router di smistamento informazioni, tipicamente collega tronchi di rete con velocità e capacità inferiore grazie a meccanismi di multiplazione.

802.11: standard IEEE per la trasmissione wireless nelle reti WLAN, noto anche come Wi-Fi. Le principali caratteristiche degli standard 802.11 includono:

- **Accesso al mezzo**: utilizzano il metodo di accesso al mezzo condiviso chiamato CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). A differenza di Ethernet, che utilizza CSMA/CD (Collision Detection), 802.11 cerca di evitare le collisioni utilizzando un sistema di prevenzione delle collisioni.
- **Velocità di trasmissione**: supportano una varietà di velocità di trasmissione, tra cui 1 Mbps, 2 Mbps, 11 Mbps, 54 Mbps, 300 Mbps, 450 Mbps, 600 Mbps, 1 Gbps e oltre. Le velocità possono variare a seconda dello standard specifico (ad esempio 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax).
- **Frequenza di operazione**: operano su diverse frequenze di trasmissione, tra cui le bande di 2,4 GHz e 5 GHz. La banda di

2,4 GHz è utilizzata dagli standard **802.11b/g/n**, mentre la banda di 5 GHz è utilizzata dagli standard **802.11a/n/ac/ax**.

- **Sicurezza**: includono meccanismi di sicurezza per proteggere le reti wireless da accessi non autorizzati. Alcuni degli algoritmi di sicurezza utilizzati includono Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) e Wi-Fi Protected Access 2 (WPA2). Quest'ultimo è l'attuale standard di sicurezza consigliato per le reti Wi-Fi.
- **Range di copertura**: dipende da vari fattori, tra cui la potenza del segnale, l'ambiente circostante e l'eventuale presenza di ostacoli. In generale, la copertura di una rete wireless può variare da poche decine di metri a centinaia di metri.
- **Interoperabilità**: sono progettati per consentire l'interoperabilità tra i dispositivi Wi-Fi di diversi produttori. Ciò significa che i dispositivi conformi allo stesso standard dovrebbero essere in grado di comunicare tra loro senza problemi.

Suite TCP/IP: è un insieme di protocolli di rete che consentono la comunicazione e lo scambio di dati tra dispositivi all'interno di una rete. Fornisce le fondamenta per la comunicazione e la connettività su Internet e su molte reti locali. I protocolli all'interno della suite lavorano insieme per consentire il trasferimento affidabile dei dati, l'instradamento dei pacchetti e la connessione tra dispositivi all'interno di una rete. Prende il nome dai due protocolli principali che la compongono: il protocollo di controllo di trasmissione (TCP) e

il protocollo Internet (IP). I componenti principali della suite TCP/IP sono:

- **Protocollo Internet (IP)**: è responsabile dell'instradamento dei pacchetti di dati attraverso la rete. Assegna un indirizzo IP univoco a ogni dispositivo collegato alla rete e si occupa dell'indirizzamento e dell'instradamento dei pacchetti di dati da una sorgente a una destinazione.
- **Protocollo di controllo di trasmissione (TCP)**: suddivide i dati in segmenti più piccoli, chiamati pacchetti, e li invia in modo affidabile tra i dispositivi. Si assicura che i pacchetti vengano inviati correttamente, controlla gli errori e gestisce la sequenza e il flusso dei dati.
- **Protocollo di trasferimento di posta elettronica (SMTP)**: è utilizzato per l'invio di posta elettronica attraverso la rete. Gestisce la consegna dei messaggi di posta elettronica da un server di posta all'altro, consentendo la comunicazione tra gli utenti tramite la posta elettronica.
- **Protocollo di trasferimento di file (FTP)**: consente il trasferimento di file tra computer collegati alla rete. Permette agli utenti di caricare e scaricare file da un server FTP remoto.
- **Protocollo di risoluzione degli indirizzi (ARP)**: viene utilizzato per mappare gli indirizzi IP dei dispositivi di rete con i rispettivi indirizzi MAC delle schede di rete. Questo permette ai dispositivi di comunicare tra loro all'interno di una rete locale.

- **Protocollo di risoluzione dei nomi (DNS)**: traduce i nomi di dominio (come www.simonezanella.it) negli indirizzi IP corrispondenti. In pratica, consente agli utenti di utilizzare nomi di dominio facili da ricordare per accedere a risorse su Internet invece di dover memorizzare gli indirizzi IP numerici.

Incapsulamento: è la procedura con cui i dati vengono strutturati e organizzati durante la comunicazione tra i dispositivi di rete. Il pacchetto dati viene suddiviso in strati o livelli, ognuno dei quali svolge un compito specifico. Ogni livello aggiunge un header ai dati originali, che contiene informazioni necessarie per il corretto instradamento e la gestione dei dati in quel livello. A destinazione, ogni livello rimuove l'intestazione aggiunta dal livello precedente e recupera i dati originali.

Unicast: comunicazione uno a uno, il mittente invia un pacchetto di dati a un destinatario specifico.

Multicast: comunicazione uno a molti, il mittente invia un pacchetto di dati a un gruppo selezionato di destinatari, che sono interessati a ricevere quei dati specifici. I dati vengono trasmessi una sola volta dal mittente e vengono ricevuti da tutti i destinatari interessati che fanno parte del gruppo multicast.

Broadcast: comunicazione uno a tutti, il mittente invia un pacchetto di dati a tutti i dispositivi presenti nella rete. Il messaggio viene diffuso a tutti i dispositivi, che possono riceverlo e ascoltarlo.

Indirizzo IPv4: indirizzi logici formati da 32 bit suddivisi in 4 gruppi da 8 bit separati da un punto, espressi in decimale (es. 192.168.1.42), costituiti da una parte dedicata al NET-ID (identifica la rete) e una al HOST-ID (identifica il dispositivo).

Classi di indirizzi IPv4: si raggruppano, in base al valore dei bit più significativi, in 5 classi. Per principio identificano l'estensione di una rete in base all'IP di appartenenza. Per trovare la classe di appartenenza occorre convertire in binario il primo ottetto, e vedere il valore dei bit più significativi.

- **Classe A**: l'indirizzo in binario inizia con un bit a "0", la subnet di default è /8, i blocchi di indirizzi iniziano (in decimale) con dei valori da 0 a 127 (0.0.0.0 – 127.255.255.255).
- **Classe B**: inizia con "10", subnet: /16 blocchi: da 128 a 191.
- **Classe C**: inizia con "110", subnet: /24 blocchi: da 192 a 223.
- **Classe D**: inizia con "1110", subnet: non definita, blocchi: da 224 a 239, usata per multicast.
- **Classe E**: inizia con "1111", subnet: non definita, blocchi: da 240 a 255, riservata per usi futuri.

Indirizzi IPv4 riservati: sono indirizzi che hanno una forma specifica e sono stati scelti per utilizzi ben precisi. I principali sono:

- **0.0.0.0**: è utilizzato per indicare un'interfaccia di rete o un host che non è associato a un indirizzo IP specifico. Ha un significato diverso a seconda del contesto in cui viene utilizzato. In alcuni casi, può essere utilizzato come indirizzo IP sull'host locale per indicare **tutte le interfacce di rete disponibili** o come un indirizzo "qualsiasi" o "tutti". Ad esempio, se si configura un server web per "ascoltare" sull'indirizzo IP 0.0.0.0, il server sarà in grado di accettare le connessioni provenienti da tutte le interfacce di rete

disponibili sull'host. Nelle tabelle di routing, l'indirizzo 0.0.0.0 è spesso utilizzato come un indirizzo di rete predefinito, noto come "**default route**". Indica che tutte le destinazioni di rete sconosciute devono essere inviate attraverso l'interfaccia di rete associata a tale indirizzo IP. In alcuni contesti di programmazione di rete, l'indirizzo IP 0.0.0.0 può essere utilizzato per fare il "bind" di un socket. Significa che il socket sarà in ascolto su tutte le interfacce di rete disponibili sull'host.

- **indirizzo di rete**: indirizzo che ha la parte dell'**HOST-ID** con tutti i bit a 0, identifica in modo univoco una rete specifica all'interno di una struttura di rete più ampia.
- **indirizzo di broadcast**: indirizzo che ha la parte dell'**HOST-ID** con tutti i bit a 1, è l'indirizzo che serve a effettuare l'invio a tutti gli host della sottorete di appartenenza;
- **indirizzo di loopback**: sono quelli compresi **tra 127.0.0.1 e 127.255.255.255**, i pacchetti inviati verso un'interfaccia di loopback vengono fatti tornare indietro verso la stessa sorgente da cui hanno avuto origine,
- **255.255.255.255**: è un indirizzo di broadcast che invia i pacchetti a tutti i dispositivi che possono riceverlo in una rete.

Reti private: sono caratterizzate da indirizzi IP che non sono direttamente accessibili dall'esterno della rete stessa, in particolare da Internet. Possono utilizzare indirizzi appartenenti ai seguenti gruppi di indirizzi riservati:

- da 10.0.0.0 a 10.255.255.255 (Classe A)
- da 172.16.0.0 a 172.31.255.255 (Classe B)
- da 192.168.0.0 a 192.168.255.255 (Classe C)

Indirizzi IPv6: sono indirizzi IP formati da 128 bit, suddivisi in 8 campi da 16 bit ciascuno, separati dal simbolo dei "due-punti", espressi in esadecimale (ad esempio hhhh:0000:0000:hhh0:0000:0000:0000:0000), seguono alcune regole di compattazione quali ad esempio: un blocco composto da 4 bit a 0 viene sintetizzato in un solo 0, i bit a 0 più a sinistra di un gruppo e i campi contigui composti da tutti i bit a 0 si possono omettere utilizzando una coppia di "due-punti", che può essere usata una sola volta in un indirizzo e solo per il gruppo che si trova più a sinistra. (ad esempio hhhh::hhh0:0:0:0:0).

MAC Address: è un indirizzo univoco di livello 2 di una interfaccia di rete Ethernet, costituito da 48 bit divisi in 6 gruppi da 8 bit espressi in esadecimale (0-9, A-F), separati ognuno da due-punti. I primi 3 gruppi sono assegnati dall'IEEE e identificano il **produttore**, gli altri il **numero di serie** del dispositivo (es. AA:BB:CC:DD:EE:FF). L'indirizzo FF:FF:FF:FF:FF:FF viene utilizzato per il **broadcast**.

Hub: è un dispositivo di livello 1, collega diversi dispositivi tramite porta di rete LAN, crea un unico dominio di collisione, lavora in half-duplex, replica i bit trasmessi. Ha funzione di amplificazione di segnale, pertanto lo si usa spesso su reti con cavi molto lunghi.

Switch: è un dispositivo di livello 2, inoltra i dati sulla porta cui è connesso il destinatario, lavora in full-duplex, mantiene una tabella con l'associazione tra indirizzi MAC e porte, tipicamente può avere

fino a poco più di 100 porte. E' dotato di firmware e spesso è amministrabile, il che lo rende più efficiente e al tempo stesso più vulnerabile rispetto a un hub. Consente di ridurre drasticamente le collisioni, perché crea un dominio di collisione separato per ciascuna porta. Non può interconnettere reti che utilizzano protocolli di comunicazione diversi (ad esempio una rete Token Ring e una Ethernet).

Half-duplex: è un tipo di comunicazione in cui i dati possono essere trasmessi in entrambe le direzioni, ma non contemporaneamente. Un dispositivo può inviare dati mentre l'altro dispositivo ascolta e viceversa, ma non possono trasmettere simultaneamente.

Full-duplex: è un tipo di comunicazione in cui i dati possono essere trasmessi contemporaneamente in entrambe le direzioni. I dispositivi comunicanti dispongono di canali separati per la trasmissione e la ricezione dei dati, consentendo una comunicazione bidirezionale simultanea.

Bridge: è un dispositivo di livello 2, collega segmenti di rete, effettua filtraggio e inoltro dei pacchetti, può avere una decina di porte al massimo, cerca di capire dall'indirizzo del destinatario il segmento di rete cui appartiene mantenendo una tabella di forwarding di indirizzi MAC per ciascuna porta. E' in grado di verificare se su un altro segmento di rete su cui deve trasmettere esiste un problema di collisione, in tal caso utilizza CSMA/CD bufferizzando i dati e inviandoli successivamente a LAN libera. All'accensione le tabelle di forwarding sono vuote e il frame viene inoltrato su tutte le linee ad eccezione di quella di arrivo (**flooding**).

Differenza tra bridge e switch: in passato, il termine “bridge” era utilizzato per descrivere un dispositivo che collegava due segmenti di rete, mentre lo switch era un dispositivo più avanzato in grado di connettere più segmenti di rete contemporaneamente. Rispetto al bridge, lo switch esegue tutte le proprie elaborazioni via hardware e non software, perciò non rallenta il flusso del traffico tra i segmenti di rete. Gli switch sono diventati la scelta comune per il collegamento delle reti locali grazie alle loro funzionalità avanzate e alla maggiore scalabilità.

Gateway: opera tipicamente a livello 4 e 5, trasmette dati tra dispositivi che usano protocolli differenti. Nel routing il **Default Gateway** è il dispositivo utilizzato (tipicamente un router) quando un host richiede il collegamento ad un indirizzo IP esterno alla rete locale (ad esempio per la navigazione su Internet).

Router: è un dispositivo di livello 3, instrada i dati fra reti fisiche diverse. Quando riceve un pacchetto, risolve l’indirizzo logico in fisico e crea un frame diretto verso il router successivo (**next hop**), in caso di instradamento dinamico comunica con gli altri router nella rete. Nel caso in cui un router con instradamento statico debba inviare dati a una rete cui non è connesso direttamente, invia i dati al gateway predefinito. E’ dotato di firmware e tipicamente ha 4 porte.

Uplink: Le porte di uplink sono utilizzate per creare connessioni di backbone o di collegamento principale tra dispositivi di rete. Ad esempio, se si dispone di più switch collegati tra loro per formare una rete più ampia, si può utilizzare una porta di uplink su ciascuno degli switch per connetterli tra loro. In questo modo, il traffico di rete può essere instradato tra gli switch senza passare attraverso le porte standard.

Segmento di rete: una porzione logica o fisica di una rete più ampia che collega un gruppo di dispositivi. Questi dispositivi all'interno del segmento condividono un insieme comune di caratteristiche e spesso comunicano direttamente tra loro senza la necessità di attraversare un router.

Modem: MOdulatore - DEModulatore, è generalmente un dispositivo di collegamento a una rete dati che in trasmissione modula i segnali digitali in analogici (dal computer alla linea telefonica ad esempio) e in ricezione demodula i segnali analogici in digitali.

Access Point (AP): è un dispositivo di rete che permette di accedere a una rete in modalità wireless. Può essere collegato ad altri AP per estendere una rete wireless, consentendo ai dispositivi che la utilizzano di restare connessi anche se spostandosi cambiano AP o canale (**handover**).

Cablaggio Strutturato: è un sistema di cablaggio standardizzato che viene utilizzato per creare una rete di comunicazione affidabile e flessibile all'interno di un edificio. Fornisce l'infrastruttura di rete necessaria per supportare diverse tecnologie di comunicazione, come telefonia, connessione Internet, trasmissione dati e sistemi di automazione degli edifici. Offre numerosi vantaggi, tra cui la flessibilità nell'aggiungere, spostare o modificare i dispositivi di rete, una migliore gestione del cavo e una maggiore affidabilità delle comunicazioni all'interno dell'edificio. Consiste nei seguenti aspetti:

- **Pianificazione e progettazione**: si valutano le esigenze attuali e future dell'edificio, tenendo conto del numero di utenti, delle applicazioni previste e della distribuzione dei

punti di accesso alla rete. Si definiscono i requisiti, si determinano i percorsi dei cavi e si pianifica la disposizione dei punti di distribuzione del segnale.

- **Cavi e connettori**: si scelgono le tipologie di cavi per trasportare i segnali di comunicazione. I cavi sono installati in modo strutturato lungo le vie prestabilite, come corridoi o condotti, per collegare le diverse aree dell'edificio.
- **Punti di distribuzione**: si piazzano i punti di distribuzione, basati su **patch panel**, che consentono la connessione dei cavi di rete alle prese di rete nelle varie stanze o uffici. I cavi provenienti dalle diverse aree dell'edificio vengono terminati ai patch panel per facilitare la gestione e la manutenzione.
- **Prese di rete**: vengono installate le prese di rete nelle aree di lavoro o negli ambienti in cui gli utenti avranno accesso alla rete. A seconda dello standard di riferimento può essere indicato il numero di prese previste.
- **Armadi di distribuzione**: vengono utilizzati armadi di distribuzione per alloggiare i dispositivi di rete, come switch di rete, router e altri apparecchi necessari per indirizzare e gestire il traffico di rete. Gli armadi di distribuzione sono dotati di un sistema di organizzazione dei cavi e di componenti di connessione Vengono identificati come **Floor Distributor**, FD, utilizzati nel cablaggio orizzontale, collegati a un a **Building Distributor**, BD, tramite cavi in rame o in fibra ottica per il cablaggio verticale. Allo stesso modo, se

sono presenti diversi edifici i BD vengono collegati a un **Campus Distributor**, CD.

- **Test e certificazione**: una volta completata l'installazione del cablaggio, vengono eseguiti test per verificare la corretta connessione e il funzionamento dei cavi. Questi test assicurano che il cablaggio soddisfi gli standard di prestazione richiesti, come la velocità di trasmissione e l'affidabilità.

FTTx: indica dove arriva l'architettura di una rete in fibra ottica "Fiber To The" per l'accesso alla rete rispetto all'utente finale, le principali sono **FTTN** (fino al "nodo", a diversi km dall'utilizzatore), **FTTC** (fino all'armadio, "cabinet") e **FTTS** (fino alla strada, "street"), FTTB (fino al palazzo, "building"), **FTTH** (fino a casa, "home").

ISP: Internet Service Provider, ente o azienda che fornisce servizi legati ad Internet.

Nodo: ogni elemento hardware di una rete in grado di comunicare. Può essere un elemento di smistamento del traffico (ad esempio un hub, uno switch) o un elemento terminale come un client o un server.

Host: nodo terminale della rete. Significa "ospite", può essere ad esempio un client o un server.

QUALCOSA SUI SERVIZI DI RETE

Servizi di rete: consistono nelle diverse funzionalità e risorse fornite da una rete informatica per consentire la comunicazione, la condivisione delle risorse e l'accesso a informazioni e applicazioni tra i dispositivi connessi. Questi servizi sono progettati per migliorare l'efficienza, la sicurezza e la produttività delle reti e degli utenti che le utilizzano.

Client/Server: è un modello costituito da processi in esecuzione su diversi host. I processi che gestiscono e mettono a disposizione risorse sono detti **server** mentre quelli che ne richiedono l'accesso sono detti **client**.

Architettura distribuita: è un sistema in cui l'elaborazione delle informazioni è distribuita su diversi computer, i cui componenti cooperano comunicando in rete e coordinando le proprie azioni tramite lo scambio di messaggi. Sono caratterizzate da elevata **scalabilità** (possibilità di aggiungere risorse per migliorare le prestazioni e sostenere meglio i carichi di lavoro) e da tolleranza ai guasti grazie alla possibilità di replicare le risorse. Lo sviluppo di sistemi software distribuiti avviene attraverso l'uso del **middleware**, uno strato software che si pone a metà tra sistema operativo e programmi applicativi: agisce come intermediario tra diverse applicazioni o componenti di un sistema distribuito e consente la comunicazione e la gestione dei dati tra di esse.

DHCP: è un protocollo che consente agli host di ricevere una configurazione IP completa per accedere a una rete cui sono

connessi. Il servizio viene fornito da un apposito server (o da un router che offre questo servizio). Tipicamente funziona in tre modalità:

- **statico**: l'amministratore di rete configura nel server le associazioni tra indirizzo IP e MAC Address;
- **automatico**: l'amministratore imposta un range di indirizzi assegnabili dal server, e l'IP viene poi associato all'host senza scadenza prefissata;
- **dinamico**: l'amministratore imposta un range di indirizzi assegnabili dal server, e l'IP viene poi associato all'host per un tempo prefissato per la scadenza (**lease time**).

La procedura di assegnazione dell'indirizzo IP e della configurazione avviene attraverso lo scambio di 4 messaggi:

- **DHCP DISCOVER** (l'host invia un pacchetto dall'indirizzo 0.0.0.0 con destinazione broadcast su tutta la rete 255.255.255.255 in cerca di un server DHCP)
- **DHCP OFFER** (viene inviato dal/dai server, tipicamente in unicast, offrendo un collegamento)
- **DHCP REQUEST** (viene inviato dal client in broadcast indicando il server scelto, eventualmente richiedendo un indirizzo IP posseduto in precedenza)
- **DHCP ACK** (viene inviato dal server all'host confermando i parametri di configurazione offerti, dopo aver effettuato un ping sulla rete per verificare che qualche altro host non si sia collegato con lo stesso indirizzo IP nel frattempo).

Il rinnovo dell'indirizzo IP in caso di lesse time è effettuato dall'host con una nuova DHCP REQUEST. Il DHCP presenta alcune vulnerabilità: la **Address Starvation**, che consiste nell'inoltrare false DHCP REQUEST per saturare i range di indirizzi IP a disposizione, impedendo a nuovi host leciti di connettersi alla rete, e la tecnica del **Rogue Server**, con la quale si inserisce un falso server DHCP cui far connettere le macchine della rete dirottandovi il traffico.

ARP: è il protocollo che si occupa di gestire le corrispondenze tra indirizzi IP e Mac Address in una rete. Ogni host incapsularlo i pacchetti inviati in trame in cui deve inserire l'indirizzo Mac del destinatario, che viene ricavato da apposite tabelle che contengono le associazioni IP-Mac dette ARP Table. Tipicamente la tabella ARP è aggiornata in tre modi: monitorando il traffico di rete ricavando le associazioni dalle trame in transito; emettendo una **ARP REQUEST** in broadcast che chiede quale host abbia un determinato IP, ricevendo una risposta **ARP REPLY** e aggiornando la tabella, con una durata tipica del record di 120 secondi negli switch; oppure memorizzando coppie IP-MAC manualmente senza scadenza (opzione rara). Il protocollo ha due problematiche:

- poiché le ARP REQUEST sono effettuate in broadcast, possono verificarsi delle situazioni di intenso traffico quando molti dispositivi accedono contemporaneamente alla rete;
- è vulnerabile ad attacchi di tipo **ARP Spoofing** (o **ARP Poisoning**) in cui un host immette false ARP REPLY sulla rete per variare opportunamente le tabelle ARP, consentendo una situazione di **MITM** (Man In The Middle) intercettando il traffico tra gli host. L'host A comunica con B, ma in realtà

l'host C attaccante si trova nel mezzo e quello che realmente avviene è che A comunica con C, che ritrasmette a B.

NAT: il Network Address Translation è un servizio che consente di trasformare un indirizzo IP della LAN in un indirizzo IP pubblico, modificando l'header IP dei pacchetti di dati. Viene utilizzato tipicamente all'interno di una rete privata, in cui il dispositivo che si occupa del NAT (in genere un router) associa ai computer che ne fanno richiesta un indirizzo pubblico (tra quelli messi a disposizione dall'ISP che fornisce connettività esterna) per poter comunicare sulla rete esterna. Il NAT consente di risparmiare indirizzi pubblici, e migliora sensibilmente la sicurezza delle reti private, delle quali esternamente non è possibile ricavare informazioni. Presenta una vulnerabilità di tipo **NAT-injection**, con la quale vengono immesse nelle reti delle false associazioni NAT, che reinstradano il traffico della rete secondo i voleri dell'attaccante.

ICMP: Internet Control Message Protocol è un protocollo di controllo, utilizzato dai nodi per lo scambio di messaggi di errore e informazioni sullo stato della rete. Il più noto è il comando **PING** che serve a inviare dei pacchetti di tipo ECHO REQUEST e ricevere delle ECHO REPLY per stabilire se un host è attivo, calcolando anche il tempo di risposta. Il protocollo può risultare vulnerabile agli attacchi di tipo **Ping of Death**, in cui un eccesso di ECHO REQUEST comporta un sovraccarico della rete e in alcuni casi il crash degli host vulnerabili.

DNS: Domain Name System, serve a tradurre i nomi di dominio (ad esempio www.google.it) in indirizzi IP. Il DNS è organizzato con una struttura ad albero, il punto di origine è indicato con un punto "." e

viene detto **root**, al di sotto vengono indicati i nomi dei **rami** dell'albero e ogni "." rappresenta una diramazione.

Esempio: www.google.it

- .it è il **Top Level Domain** (lo IANA ne mantiene l'elenco: https://www.iana.org/domains/root/db), può rappresentare una nazione (es. .it) o un'organizzazione (es. .com, usato originariamente per i domini commerciali).
- google è il 2° livello (o sottodominio), rappresenta il proprietario del nome a dominio.
- www è il 3° livello, può essere scelto dal proprietario e in genere serve a identificare un servizio offerto (www.google.it per il servizio di navigazione web, mail.google.it per il servizio di posta in uscita, ecc…)

URI: Uniform Resource Identifier, identifica una risorsa in maniera univoca su internet. Ad esempio: google.it/pagina.html

URL: Uniform Resource Locator è una specificazione di un URI con cui si indica la locazione precisa di una risorsa su internet e il protocollo per accedervi. Esempio https://www.google.it/pagina.html

FTP: File Transfer Protocol, è un protocollo per il trasferimento di file tra client e server sulla rete. E' basato su TCP e ha una architettura client/server, con accesso tramite nome utente e password. Utilizza la porta 21 per creare una connessione per lo scambio di messaggi di controllo, in seguito viene aperta una porta per lo scambio dei dati: in **modalità attiva** la porta viene scelta dal client, in **modalità passiva** viene scelta casualmente dal server.

POP3: Post Office Protocol è un protocollo per la consultazione della posta elettronica, utilizzato per ricevere mail da un server remoto verso un client locale, su cui leggere le mail offline (ad esempio Outlook, Mac Mail, Mozilla Thunderbird). Utilizza la porta 110 (995 in modalità sicura tramite SSL/TLS, di base non fornisce cifratura).

IMAP: Internet Message Access Protocol è un protocollo per la consultazione della posta elettronica, utilizzato per l'accesso diretto a una casella email su un server remoto da un client locale (ad esempio tramite un browser web), senza richiedere lo scaricamento dei messaggi. La posta viene consultata direttamente sul server. Utilizza la porta 143 (993 se presente la modalità sicura, tramite protocollo SSL/TLS).

SMTP: Simple Mail Transfer Protocol è il protocollo per l'invio della posta elettronica. Utilizza la porta 25 (465 in modalità sicura, tramite SSL/TLS).

TLS ed SSL: Transport Layer Security e Secure Socket Layers, sono protocolli crittografici per criptare e autenticare una connessione durante il trasferimento di dati su Internet, tramite l'impiego di certificati. TLS è una versione recente di SSL. Il funzionamento si basa sui seguenti passaggi:

- **Handshake**: ìil client e il server negoziano la versione del protocollo, stabiliscono i parametri di crittografia e si scambiano i certificati digitali.
- **Scambio dei certificati**: il server invia al client il suo certificato digitale. Il certificato contiene la chiave pubblica del server, informazioni sul certificato stesso e la firma

digitale di un'autorità di certificazione (CA) di fiducia. Il client verifica la validità del certificato del server, inclusa l'autenticità della firma e la corrispondenza con il nome di dominio richiesto.

- **Generazione di una chiave di sessione**: dopo aver verificato il certificato del server, il client genera una chiave di sessione segreta. Questa chiave viene utilizzata per crittografare i dati trasmessi durante la sessione.
- **Scambio delle chiavi**: utilizzando il certificato del server, il client crittografa la chiave di sessione generata e la invia al server. Solo il server può decifrare la chiave utilizzando la sua chiave privata corrispondente.
- **Criptaggio dei dati**: una volta che la chiave di sessione è condivisa tra il client e il server, i dati trasmessi tra di loro vengono crittografati e decrittografati utilizzando questa chiave.

Certificati digitali: attestano l'identità di un'entità online, come un sito web, sono rilasciati da **autorità di certificazione (CA)** di fiducia e contengono informazioni come il nome di dominio, la chiave pubblica del server, la data di scadenza e la firma digitale della CA. I browser e gli altri client utilizzano i certificati per verificare l'autenticità del server e stabilire una connessione sicura tramite SSL o TLS.

QUALCOSA SU SOTTORETI, ROUTING E VLAN

Subnetting: tecnica che consente di suddividere una rete in sottoreti attraverso l'uso di una **subnet mask**. Per prima cosa si determina la classe di rete e il blocco di indirizzi IP da utilizzare, scelto in maniera opportuna per poter assegnare indirizzi IP distinti a tutti gli host e interfacce della rete. Determinata la classe si prende la netmask di default, e si sceglie il numero di bit dell'HOST-ID che verranno utilizzati per l'identificazione della subnet all'interno dell'indirizzo IP, partendo da quelli più a sinistra. Sommando i bit della maschera di default ai bit presi dall'HOST-ID si ottiene la subnet mask. Ad esempio nel caso di un indirizzo di classe C 192.168.0.0, la net-mask di default è /24, utilizzando i primi 2 bit dell'HOST-ID si ottiene /26, che consente di indirizzare 4 sottoreti distinte ($2^{\text{n° bit sottorete}} = 2^2 = 4$):

192.168.0.0-192.168.0.63 (64 indirizzi IP)

192.168.0.64-192.168.0.127 (64 indirizzi IP)

192.168.0.128-192.168.0.191 (64 indirizzi IP)

192.168.0.192-192.168.0.255 (64 indirizzi IP)

Gli indirizzi utilizzabili sono sempre pari al numero di bit dell'HOST-ID subnettato -2, poiché vanno esclusi l'indirizzo di rete e l'indirizzo di broadcast.

VLSM: tecnica che consente di utilizzare subnet di lunghezza diversa all'interno dello stesso indirizzo di rete. Ad esempio con un blocco di

indirizzi 192.168.0.0/24 si possono avere una sottorete 192.168.0.0./25 e una sottorete 192.168.0.128/26.

Classless: indica l'indirizzamento senza fare riferimento a classi IP di appartenenza, e quindi consente di scegliere liberamente le subnet mask garantendo maggiore flessibilità.

CIDR: Classless Inter-Domain Routing, identifica l'aggregazione di sottoreti (operazione detta anche di **supernetting**), ovvero l'unione di sottoreti per aumentarne la capacità. I bit di sottorete sono scelti in maniera libera, senza fare riferimento alle classi di appartenenza. Introduce la notazione "indirizzo IP/numero di bit della subnet mask" per l'identificazione delle reti. E' possibile quindi utilizzare, ad esempio, un indirizzo di classe C 192.168.1.0 con subnet /23 per ottenere una rete da 512 indirizzi.

Piano di indirizzamento completo: consiste nella progettazione e all'organizzazione di un sistema di indirizzamento IP per una intera rete. Per definirsi completo include la definizione dei seguenti aspetti:

- Spazio di indirizzamento: determina l'intervallo di indirizzi IP disponibili per la rete, attraverso l'indicazione di indirizzo di rete/subnet mask (notazione CIDR).
- Segmentazione di rete (tramite subnetting): determina la suddivisione del blocco di indirizzi IP in segmenti o sottoreti più piccole per ragioni di gestione e sicurezza. Questa segmentazione consente di creare reti logiche separate all'interno della rete principale.

- Assegnazione degli indirizzi: definizione di come gli indirizzi IP vengono assegnati ai dispositivi di rete (quali computer, stampanti, server, interfacce dei router e altri dispositivi).
- Maschere di sottorete: definizione delle subnet mask da utilizzare per ogni segmento di rete.
- Routing: definizione di come avviene il routing dei pacchetti all'interno della rete, attraverso protocolli dinamici o tabelle di routing per il routing statico.

Routing: è l'operazione di instradamento dei messaggi effettuata dai router. Prevede 2 fasi:

- calcolo (**routing**) del percorso ottimale, basato sulle informazioni presenti nelle tabelle di routing, definite in maniera statica o dinamica;
- inoltro (**forwarding**) del pacchetto verso l'interfaccia di output del router scelta attraverso la tabella di routing (operazione detta di "**matching**"). Appena acquisito l'indirizzo IP del pacchetto, il router controlla la propria netmask e determina se è relativo a un host della propria rete (ovvero direttamente raggiungibile da una delle proprie interfacce), in tal caso utilizzerà i servizi del livello 2 dell'OSI per inoltrare il pacchetto direttamente all'host destinatario (**routing diretto**). Altrimenti, se è destinato ad un'altra rete, consulta la propria **Routing Table** per determinare dove inviare il pacchetto (**routing indiretto**).

Routing Table (Tabella di Routing): è un elemento chiave all'interno di un router per determinare il percorso migliore da seguire per

inoltrare i pacchetti verso la loro destinazione. Contiene informazioni sulle reti connesse direttamente al router e sulle rotte remote raggiungibili tramite altri router. Ogni voce nella tabella di routing indica una destinazione di rete specifica e la prossima interfaccia di uscita, o il prossimo router, verso cui inviare i pacchetti per raggiungere quella destinazione. Contiene:

- Un record per ciascuna rete collegata direttamente al router, con l'indicazione della relativa interfaccia di rete (**routing diretto**); generalmente le interfacce, nel caso del classico router a 4 porte, si indicano con i punti cardinali N,S,O,E.
- Un record per (alcune) reti non collegate direttamente al router, insieme con l'indicazione del router a cui inoltrare i pacchetti (indicato come "**Next Hop**" oppure "**Gateway**");.
- Un record per un router vicino, raggiungibile direttamente, detto di **default**, a cui inoltrare i pacchetti destinati a reti sconosciute (ad esempio quelli destinati alla rete Internet).
- Nel caso l'instradamento sia diretto, nella tabella viene inserito un asterisco come "**Next Hop**", mentre nel caso di reti sconosciute, nella tabella si indica la rete di destinazione con la dicitura "**default**" oppure con l'indirizzo "0.0.0.0", e con /0 la subnet mask.

Longest prefix matching: è la tecnica con cui vengono individuate le destinazioni all'interno della tabella di routing. Dato che nella tabella sono generalmente presenti varie sottoreti, l'indirizzo IP di destinazione di un pacchetto può generare un match per più record: verrà scelta come destinazione quella con la maschera di sottorete più specifica, ovvero con più bit a 1 nella subnet:

- ad esempio con la tabella di routing in figura un pacchetto con destinazione 192.168.1.42 realizza un match su entrambe le reti 192.168.1.0/25 e 192.168.1.32/28 (fa parte di entrambi blocchi), ma poiché la rotta con maschera /28 è più specifica verrebbe inoltrato sull'interfaccia Nord (N) del router.

Routing statico: i percorsi per l'inoltro dei pacchetti sono determinati dall'amministratore di rete, che configura manualmente le tabelle di routing. E' semplice da realizzare su reti di piccole dimensioni e con bassa ridondanza di collegamenti, al crescere della dimensione della rete diventa difficile da gestire. Per sua natura presenta scarsa tolleranza ai guasti , e ad ogni variazione della topologia della rete impone la riconfigurazione delle tabelle nei nodi interessati da parte dell'amministratore di rete.

Routing dinamico: i percorsi per l'inoltro dei pacchetti sono determinati da un protocollo di routing, che aggiorna automaticamente e periodicamente le tabelle di instradamento, in particolare in caso di modifiche della topologia o di variazioni del traffico di rete. E' particolarmente efficace in caso di inserimento di nuovi nodi o collegamenti e in caso di guasti su porzioni della rete.

Routing gerarchico: viene utilizzato su larga scala sulla rete Internet, prevede la realizzazione di una gerarchia di aree di routing, strutturate in regioni chiamate **Autonomous System** (AS), che possono essere ulteriormente suddivise in porzioni dette **Routing Area** (RA) interconnesse da dorsali (**backbone**). I vari enti di gestione si accordano su quali protocolli utilizzare per il dialogo tra i router che interconnettono AS diversi. I protocolli di routing all'interno di un AS sono detti **Interior Gateway Protocol** (IGP),

mentre quelli fra i vari AS sono detti **Exterior Gateway Protocol** (EGP). Ogni router mantiene le informazioni per tutte le destinazioni all'interno dell'AS in cui si trova, mentre per tutte le altre destinazioni si inviano i pacchetti a un router alla periferia dell'AS, che si occupa dell'instradamento verso altri AS. Serve a mantenere ridotte le tabelle di routing in reti di dimensioni levate.

Principali algoritmi di routing dinamico:

- **Routing Information Protocol (RIP)**: è un protocollo a vettore di distanza (**distance vector**) che si basa sul conto delle metriche, come il numero di hop (salti) tra i router, per determinare le rotte migliori. Utilizza un proprio protocollo di aggiornamento per scambiare informazioni di routing tra i router e aggiornare le loro tabelle di routing. Viene ampiamente utilizzato nelle reti aziendali di medie e grandi dimensioni, ma ha alcune limitazioni, come un limite massimo di 15 hop e un tempo di convergenza relativamente lento. Il **tempo di convergenza** è il tempo richiesto affinché i router di una rete si adattino a un cambiamento nella topologia di rete o a una modifica delle informazioni di routing.
- **Open Shortest Path First (OSPF)**: è basato sullo stato dei collegamenti. Utilizza l'**algoritmo di Dijkstra** per calcolare il percorso più breve verso una destinazione utilizzando informazioni dettagliate sulla topologia di rete, come la larghezza di banda del collegamento e la congestione. Supporta reti di grandi dimensioni e offre ridondanza di percorso, in modo che se un percorso primario fallisce, il router possa instradare i pacchetti

attraverso un percorso alternativo. Per queste caratteristiche trova impiego sia nelle reti di medie e grandi dimensioni sia in quelle di telecomunicazioni.

- **Border Gateway Protocol (BGP)**: è utilizzato principalmente nelle reti di Internet. È un protocollo di **vettore di percorso** che consente ai router di scambiarsi informazioni sulle rotte e di prendere decisioni di instradamento basate su politiche definite dagli amministratori di rete. È utilizzato dagli ISP per instradare i pacchetti tra diversi domini autonomi (AS), consentendo una connettività globale su Internet.
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**: è un protocollo proprietario sviluppato da Cisco Systems. Combina caratteristiche di routing a vettore di distanza e routing basato sullo stato dei collegamenti. Calcola il percorso ottimale utilizzando informazioni sulla larghezza di banda, il ritardo, la congestione del collegamento e altre metriche. È noto per la sua rapida convergenza e la capacità di supportare reti complesse.
- **Intermediate System to Intermediate System (IS-IS)**: è basato sullo stato dei collegamenti, utilizzato principalmente nelle reti di grandi dimensioni, come le reti di telecomunicazioni. Utilizza l'**algoritmo di Dijkstra** per calcolare il percorso più breve e scambia informazioni sullo stato dei collegamenti tra i router per determinare le rotte migliori.

Costo di una rotta: dipende dalla metrica utilizzata per calcolare il costo di un percorso. La metrica può variare a seconda dell'algoritmo di routing utilizzato e delle specifiche esigenze della rete. Alcune delle metriche comuni prevedono il conteggio degli hop , la larghezza di banda (che tiene conto della capacità di trasmissione disponibile sul collegamento), il ritardo (inteso come tempo richiesto per attraversare un collegamento), il carico e la congestione sul collegamento.

Distance Vector Routing: è un algoritmo utilizzato nel routing dinamico, in cui ogni router invia periodicamente la propria tabella di routing a tutti i router vicini sotto forma di vettore contenente i costi di collegamento. Ad esempio un vettore [A-0, B-2, C-4, D-2] indica che il router A è raggiungibile con instradamento diretto (infatti il costo è zero), il router B ha un costo di 2, e così via.

Black hole: è una problematica che si verifica quando in un punto della rete i pacchetti vengono scartati perché non viene trovata una destinazione.

Count to infinity: è una problematica che si verifica quando il costo per raggiungere una destinazione non più raggiungibile viene progressivamente incrementato all'infinito.

VLAN: è una tecnica utilizzata per suddividere una rete locale fisica in più reti logiche separate. I dispositivi possono comunicare tra loro come se fossero collegati a una rete fisica dedicata, anche se in realtà sono connessi a uno stesso switch di rete. Lo switch di rete mantiene traccia di quali porte appartengono a quali VLAN e inoltra il traffico di rete di conseguenza. I dispositivi in VLAN diverse non possono comunicare direttamente tra loro, per farlo è necessario la

funzionalità detta **routing inter-VLAN**, che può essere realizzato utilizzando un router con interfacce fisiche connesse a ciascuna VLAN o tramite uno switch di rete dotato di funzionalità di routing inter-VLAN integrate. È possibile limitare l'accesso tra VLAN diverse utilizzando regole di filtraggio del traffico o impedire la comunicazione tra determinate porte o dispositivi all'interno della stessa VLAN. Le VLAN presentano molti vantaggi soprattutto in termini di scalabilità della rete. Le VLAN consentono di separare logicamente i dispositivi in gruppi o reparti diversi all'interno di un'organizzazione, fornendo una maggiore sicurezza e isolamento tra i gruppi. Le VLAN consentono di limitare il traffico di rete a un determinato gruppo di dispositivi, il che può essere utile per gestire il flusso di dati e garantire una larghezza di banda adeguata per ciascuna VLAN.

Tipologie di VLAN:

- **Port-based VLAN**: le porte dello switch di rete vengono assegnate a VLAN specifiche. I dispositivi collegati alle porte assegnate appartengono automaticamente alla VLAN corrispondente. È la forma più semplice e comune di VLAN.
- **Tag-based VLAN**: si basano sul protocollo **802.1Q**, consentono di assegnare VLAN a livello di frame Ethernet utilizzando tag VLAN aggiuntivi. I frame di rete vengono contrassegnati con un tag VLAN che indica la VLAN di destinazione. Consente di gestire fino a 4096 VLAN diverse. Questo permette a un singolo collegamento fisico di trasportare il traffico di più VLAN, consentendo una maggiore flessibilità nella configurazione delle VLAN.

- **Protocol-based VLAN**: utilizzano il tipo di protocollo di rete come criterio per assegnare i dispositivi alla VLAN corrispondente. Ad esempio, si può creare una VLAN per il traffico VoIP e assegnare i telefoni IP a quella VLAN specifica.
- **Subnet-based VLAN**: consentono di assegnare i dispositivi alle VLAN in base alla loro appartenenza a una determinata sottorete IP. Ciò consente di creare VLAN che corrispondono alle diverse sottoreti di una rete.
- **Management VLAN**: viene utilizzata per separare il traffico di gestione dei dispositivi di rete, come gli switch, dai dati utente. Questa VLAN è generalmente utilizzata per accedere e gestire gli switch e i dispositivi di rete.

Inter-VLAN routing: per poter far comunicare VLAN diverse tra loro è necessario un dispositivo di routing. È necessario utilizzare un router che abbia interfacce fisiche o logiche connesse a ciascuna VLAN che si desidera far comunicare tra loro. Il router può essere un dispositivo dedicato o un dispositivo multifunzione, come uno switch di rete con funzionalità di routing inter-VLAN.

Porta trunk: è una porta di uno switch di rete che viene utilizzata per trasmettere il traffico di più VLAN attraverso un singolo collegamento fisico. La porta trunk consente di collegare due switch o un switch a un router o a un server che supporta l'inter-VLAN routing.

Router-on-a-stick: è una configurazione di rete che utilizza un unico collegamento fisico tra uno switch e un router per consentire la comunicazione tra VLAN diverse. Questa configurazione è spesso

utilizzata quando è necessario implementare l'inter-VLAN routing in una rete con uno switch che non supporta direttamente il routing inter-VLAN. Sul router, viene configurata un'interfaccia logica (detta **sottointerfaccia**) collegata a una porta dello switch configurata come trunk. La porta trunk consente di trasmettere il traffico di tutte le VLAN attraverso il collegamento fisico tra lo switch e il router.

QUALCOSA SUI PROTOCOLLI DI TRASPORTO

TCP: è un protocollo di trasporto affidabile e orientato ai flussi di dati che gestisce la comunicazione tra mittente e destinatario. Fornisce connessioni affidabili, controllo del flusso, controllo della congestione e rilevamento degli errori per garantire la consegna corretta dei dati su una rete.

UDP: è un protocollo di trasporto che fornisce una connessione senza stato tra un mittente e un destinatario all'interno di una rete. Non offre garanzie di consegna affidabile, controllo del flusso o controllo della congestione. È progettato per applicazioni che richiedono una comunicazione veloce ed efficiente, ma che possono tollerare la perdita occasionale di dati o l'arrivo non sequenziale, ad esempio:

- Streaming multimediale: poiché la latenza è critica in tali applicazioni, UDP permette una consegna rapida dei dati senza il ritardo introdotto dai meccanismi di conferma e ritrasmissione di TCP. Se vengono persi alcuni pacchetti durante la trasmissione, potrebbe verificarsi una piccola interruzione o perdita di qualità nell'esperienza di visualizzazione o ascolto.
- VoIP: la velocità e la bassa latenza di UDP sono particolarmente adatte per la trasmissione in tempo reale della voce e del video durante una chiamata, mentre l'affidabilità di livello applicativo viene gestita da altri componenti del sistema VoIP.

- Protocolli di gioco online: la velocità e la bassa latenza di UDP sono importanti per garantire un'esperienza di gioco reattiva, consentendo una rapida trasmissione delle informazioni di gioco tra il server e i client. Generalmente si utilizza TCP per le comunicazioni critiche, come l'autenticazione e il matchmaking (il processo di accorpamento dei giocatori in una sessione di gioco multiplayer), mentre UDP è impiegato per la trasmissione dei dati di gioco strettamente necessari.
- Trasmissioni multicast: viene spesso utilizzato in applicazioni come lo streaming di contenuti in diretta, le conferenze web o le reti di distribuzione dei contenuti (**CDN**).
- DNS: le richieste DNS e le risposte sono tipicamente inviate tramite UDP, poichés ono di dimensioni ridotte e una comunicazione veloce è essenziale per le prestazioni del sistema.

3-Way Handshake: è il meccanismo alla base del protocollo TCP. Consiste appunto di 3 passaggi:

1. SYN: Il mittente desidera stabilire una connessione inviando un segmento SYN (Synchronize) al destinatario. Questo segmento contiene il numero di sequenza iniziale (ISN) del mittente, che rappresenta il primo byte di dati che verrà trasmesso durante la connessione. Il flag SYN viene impostato per indicare che il mittente desidera avviare la connessione.
2. SYN-ACK: Il destinatario riceve il segmento SYN e risponde inviando un segmento SYN-ACK in risposta. Questo

segmento ha due scopi: confermare la ricezione del segmento SYN da parte del mittente e stabilire i propri parametri di connessione. Il numero di sequenza iniziale del destinatario (DSN) viene incluso nel segmento SYN-ACK, insieme al flag SYN e ACK (Acknowledgment) impostato. L'ACK indica che il destinatario ha ricevuto il segmento SYN del mittente e che è pronto a ricevere dati.

3. ACK: Il mittente riceve il segmento SYN-ACK dal destinatario e risponde inviando un segmento ACK. Questo segmento conferma la ricezione del segmento SYN-ACK e completa il 3-Way Handshake. Il flag ACK viene impostato e il numero di sequenza viene incrementato di uno rispetto al valore ricevuto dal destinatario. A questo punto, la connessione è stabilita e il mittente e il destinatario possono iniziare a scambiare dati.

Socket IP: termine che viene utilizzato per riferirsi a una combinazione di un indirizzo IP e un numero di porta, che insieme identificano un **endpoint** di comunicazione. Ad esempio: 192.168.0.1:80

Endpoint: si riferisce a un dispositivo o un'entità finale che è in grado di inviare o ricevere dati attraverso una rete.

SYN scan: è una tecnica spesso utilizzata negli attacchi alle reti o nei penetration test, consiste in una scansione della rete che viene effettuato per rilevare le porte aperte su un host o la presenza di un firewall. Sfrutta il setting del flag RST durante il 3-way handshake, un flag che serve per terminare immediatamente una connessione TCP in modo anomalo o per rispondere a una richiesta di connessione

non valida. Funziona nel seguente modo: il mittente invia un pacchetto TCP con il flag SYN impostato al destinatario per avviare una connessione. Se la porta è chiusa, il destinatario risponderà con un pacchetto TCP contenente il flag RST (Reset) impostato, indicando che la porta è chiusa. Se la porta è aperta, il destinatario risponderà con un pacchetto TCP con il flag SYN-ACK impostato. Questa risposta indica che la porta è aperta e pronta ad accettare una connessione. Il mittente, dopo aver ricevuto la risposta SYN-ACK, invia un pacchetto TCP con il flag RST impostato per chiudere la connessione.

Multiplazione o multiplexing: è una tecnica che consente la trasmissione simultanea di più segnali o flussi di dati su un unico canale di comunicazione. Permette di sfruttare al massimo la larghezza di banda disponibile e di ottimizzare l'utilizzo della risorsa di trasmissione. Nelle reti permette al sistema di mantenere due flussi di dati distinti sullo stesso indirizzo IP di origine, differenziandoli in base alle porte.

Porte: servono a identificare specifici servizi di rete o applicazioni all'interno di un host. Le porte consentono ai protocolli di livello superiore, come TCP e UDP, di instradare correttamente i dati ai servizi corrispondenti. Sono costituite da 16 bit, e quindi variano tra i valori 0 e 65536. Lo IANA (Internet Assigned Numbers Authority) è l'ente che gestisce l'assegnazione standard delle porte ai vari servizi di rete e applicazioni:

- da 0 a 1023 sono dette System Ports o **Well Know Ports**, e sono assegnate ai servizi più comuni (ad esempio DNS porta 53, SMTP porta 25, FTP porta 21, HTTP porta 80);

- da 1024 a 49151 sono dette User Ports o **Registered Ports**, e sono in genere registrate dalle aziende presso lo IANA per le proprie applicazioni;
- le restanti fino a 65536 sono dette **Dynamic Ports**, e vengono scelte all'occorrenza dai protocolli quando è necessario stabilire le connessioni (ad es, nel FTP), in maniera generalmente causale.

Struttura di un pacchetto TCP: comprende vari campi

- Porta di origine (16bit): indica il numero di porta sorgente del mittente.
- Porta di destinazione (16bit): indica il numero di porta destinazione del destinatario.
- Numero di sequenza (32bit): contiene il numero di sequenza del primo byte dei dati contenuti nel pacchetto. È utilizzato per riordinare e ricostruire i dati correttamente nel destinatario.
- Numero di conferma (32bit): contiene il numero di sequenza successivo atteso dal mittente. Viene utilizzato per confermare la ricezione dei dati e per il controllo di flusso.
- Dimensione della finestra (4bit): indica la dimensione della finestra di ricezione del destinatario, ovvero la quantità di dati che il mittente può inviare senza attendere una conferma.
- Flag (6bit): sono diversi e vengono utilizzati per fornire informazioni di controllo, tra le quali ad esempio i flag del 3-

way handshake SYN e ACK, FIN (finish), RST (reset), URG (urgent).

- Offset dell'intestazione (16bit): indica la lunghezza dell'header in parole di 32 bit. È necessario per determinare l'inizio dei dati nel pacchetto.
- Checksum (16bit): contiene il controllo di integrità del pacchetto.
- Opzioni (16bit): contiene eventuali opzioni TCP aggiuntive.
- Dati (fino a 320 bit, ma comunque multiplo di 32 bit): contiene i dati effettivi contenuti nel pacchetto.

QUALCOSA SUL P2P

P2P: peer to peer, è un modello di rete informatica in cui i nodi sono "paritari" (peer) anziché essere gerarchizzati come client o server. Ogni nodo può svolgere entrambe le funzioni verso gli host della rete. Il P2P si classifica in tre categorie principali:

- **Puro**: è sprovvisto di server centrale di appoggio, ogni nodo si occupa di inviduare le risorse di rete disponibili e gli altri peer. Viene generalmente integrata con una rete virtuale sovrapposta, in cui i nodi formano una sottorete rispetto alla rete fisica principale, per poter indicizzare e mappare i nodi definendo la topologia della rete.
- **Discovery Server**: si appoggia a un server centrale cui ogni peer comunica la propria esistenza al momento dell'avvio, ricevendo una lista con gli altri nomi della rete. Il peer prima contatta il server individualmente e poi inoltra la richiesta.
- **Discovery con Lookup Server**: strutturato come nel P2P con Discovery Server, ma ogni peer invia una lista dei propri contenuti al server ad intervalli regolari. Ad ogni richiesta il server fornisce una lista dei partecipanti alla rete insieme ai relativi contenuti, riducendo richieste senza esito e ottimizzando i tempi.

P2P strutturata: ha una topologia specifica, che assicura che ogni nodo possa efficientemente cercare e trovare una risorsa o nodo. Integra una *Hash Table* distribuita, all'interno della quale a ogni risorsa corrisponde un codice identificativo univoco.

P2P non strutturata: i nodi creano collegamenti casuali con altri nodi della rete.

Sicurezza: i principali programmi per la connessione a reti P2P prevedono che l'utente metta a disposizione oltre alla banda di connessione anche dello spazio sul proprio disco per la condivisione dei file, aprendo inoltre alcune porte del proprio sistema per il file sharing.

Legalità: per la legislazione italiana chiunque effettua il download di un'opera protetta dal diritto d'autore e la mette in condivisione commette un illecito penale se lo fa "senza averne diritto, a qualsiasi scopo e in qualsiasi forma".

BitTorrent: è uno dei protocolli per reti di file sharing p2p più diffusi, utilizza un algoritmo distribuito sullo stile di quelli puri, ma che utilizza un server per l'aggancio alla rete, detto **tracker**, che si occupa di coordinare i rapporti fra chi offre e chi richiede il file. Si basa sulla distribuzione di file .torrent, che contengono la descrizione di tutti i pacchetti in cui è stato suddiviso il file originale, i relativi hash che garantiscono l'integrità degli stessi, gli URL e/o gli IP dei tracker. Funziona così:

- Un utente che desidera condividere un file utilizza un software client per creare un file .torrent. Questo file contiene le informazioni sul file da condividere, come il nome, la dimensione e una lista di pezzi in cui è suddiviso il file.
- Il file torrent contiene anche l'indirizzo del tracker, che è un server centrale che tiene traccia dei peer che partecipano alla condivisione del file.

- Il client si connette al tracker per ottenere informazioni sui peer che stanno attualmente condividendo il file. Il tracker risponde fornendo un elenco di peer attivi e le loro informazioni di connessione.
- Il client inizia a connettersi ai peer nella lista fornita dal tracker. Una volta stabilita la connessione, il client può scambiare parti del file con i peer. Il file è suddiviso generalmente in piccoli pezzi di dimensione fissa, che i peer possono scambiarsi in modo simultaneo. Ogni pezzo del file viene identificato da un hash univoco.
- Una volta che il client ha scaricato tutte le parti del file, assembla i pezzi per creare il file completo. A questo punto, può continuare a rimanere connesso alla rete per condividere il file con altri utenti in modalità "**seeding**".

Reti Mesh: è una topologia di WLAN in cui gli Access Point che la compongono, detti nodi, sono collegati tra loro direttamente, dinamicamente e non gerarchicamente. Questa tecnologia consente di creare reti Wi-Fi con ridotte perdite di segnale e prestazioni elevate. I nodi comunicano tra loro creando una rete p2p in cui ogni nodo svolge la funzione di router per gli altri elementi della rete. Possono funzionare in modalità routing (i pacchetti vengono instradati) o flooding (i pacchetti vengono inviati a tutti i nodi).

QUALCOSA SUL WIFI

WiFi: tecnologia per reti wireless basata su standard 802.11. Gli Access Point hanno in genere una portata di 20 metri all'interno e 100 metri circa all'esterno. La parte radio costituisce la rete di accesso, la rete cablata che interconnette gli AP costituisce la rete di trasporto. E' tipicamente opportuno non far gestire più di 30 client allo stesso AP (dipende comunque dall'hardware e dalla banda).

Canali: il wifi utilizza canali di frequenza diversi per la trasmissione. E' possibile utilizzare una banda a 2,4Ghz (standard 802.11a, 802.11b e 802.11g) o a 5Ghz (standard 802.11n e 802.11ac), suddivise in canali con diverse sottofrequenze.

La **banda a 2,4 GHz** dispone di 14 canali. I canali si sovrappongono tra loro (all'incirca con un range di 4 canali, quindi il canale 5 si sovrapporrà con i canali 1, 2, 3, 4 e 6, 7, 8, 9), tranne i canali 1, 6 e 11, che sono detti canali non sovrapponibili. L'ampiezza di banda è di 20Mhz, e la velocità massima è di 144,5 Mbps. E' possibile utilizzare una ampiezza di banda a 40Mhz raggiungendo 300Mbps di velocità, ma è sconsigliabile perché non conforme alle direttive IEEE e potenzialmente causa di disturbi e interferenze a reti limitrofe.

La **banda a 5 GHz** dispone di 23 canali, in Europa si utilizza una ampiezza di banda a 20Mhz che consente di avere 8 canali non sovrapposti (26, 40, 44, 48, 52, 56, 60 e 64).

Il **segnale a 2,4 GHz** super meglio gli ostacoli ma è più soggetto a interferenze, il **segnale a 5Ghz** ha una copertura più ridotta ma ha migliori prestazioni di trasferimento dati.

Canali bloccati: a 2,4Ghz sono bloccati i canali 12,13 e 14 perché vietati per legge in diversi stati, in quanto possono essere ad esempio riservati alle forze militari. Gli unici sempre utilizzabili sono il 10 e l'11 (la Spagna blocca anche da 1 a 9). A 5 Ghz in Italia sono autorizzati 19 canali.

SSID: identificatore della rete WiFi. puòessere nascosto o visibile.

WEP: protocollo per la sicurezza del WiFi che utilizza due chiavi a 64 o 128 bit per la cifratura. Attualmente presenta seri problemi per la sicurezza essendo violabile in pochi minuti da molti software comuni.

WPA2: Wi-Fi Protected Access, protocollo per la sicurezza delle reti WiFi che utilizza chiavi a 256 bit. Utilizza l'algoritmo AES per la cifratura, include un controllo di integrità dei messaggi. puòessere utilizzato in modalità Personal per reti domestiche (con chiave a 128 bit derivata da una chiave a 256bit) o Enterprise per reti aziendali (che richiede un server RADIUS di appoggio).

WPS: è un sistema per la distribuzione delle chiavi per il WiFi per semplificare la connessione dei dispositivi in reti domestiche, che si basa su PIN e accesso fisico (tipicamente un pulsante posto sull'AP o sull'host da connettere). E' vulnerabile ad attacchi di forza bruta per il recupero del PIN e pertanto non va abilitato se possibile.

RADIUS: Remote Authentication Dial-In User Service, è un protocollo che serve a garantire i requisiti AAA per l'accesso a una rete protetta. Utilizza pacchetti UDP per il trasporto di informazioni di autenticazione e configurazione tra un server autenticatore (server di accesso alla rete, NAS - Network Access Server, in genere un router) che verifica le credenziali di accesso (username e

password) comunicando (in maniera crittografata) con un server di autenticazione (il server RADIUS) dotato di un database di utenti autorizzati. Il NAS in genere assegna al client, se autorizzato, la configurazione IP per l'accesso alla rete e ai suoi servizi (spesso integra un server DHCP).

Hotspot: punto di accesso pubblico a una rete WiFi.

WDS: Wireless Distribution System, tecnologia per la ripetizione del segnale WiFi ai vari AP facenti parte di una rete, in caso non sia possibile cablarli. Presenta un problema di perdita di prestazioni nella banda all'aumentare degli access point in WDS, poiché devono lavorare sullo stesso canale (e sulla stessa SSID), in cui ogni AP funge anche da bridge. La banda utile di trasmissione viene praticamente dimezzata per ogni AP attraversato.

QUALCOSA SULLA CRITTOGRAFIA

Crittologia: (*kryptos* "nascosto" - *logos* "parola") scienza che si occupa di scritture nascoste, che ha i suoi fondamenti nella matematica e nell'informatica.

Crittografia: branca della crittologia che sstudia sistemi per nascondere i messaggi e le informazioni attraverso l'operazione di cifratura (*encryption*). Un algoritmo di crittografia deve essere facilmente computabile ed invertibile se la chiave è nota, e difficilmente invertibile in assenza della chiave.

Crittanalisi: branca della crittologia che si occupa di trovare sistemi per decifrare (*decryption*) messaggi cifrati.

Codice: insieme di regole per cifrare un testo.

Crittogramma: testo che ha subito una cifratura.

Chiave: è una informazione utilizzata nel processo di cifratura da parte di un algoritmo.

Crittografia Simmetrica (o a chiave privata): tecnica di cifratura in cui la chiave viene usata per cifrare e decifrare un testo. Gli algoritmi a chiave simmetrica sono mediamente rapidi nell'esecuzione, tuttavia la loro sicurezza è legata alla segretezza della chiave. In una comunicazione la criticità è lo scambio della chiave tra mittente e destinatario.

Crittografia Asimmetrica (o a chiave pubblica): tecnica di cifratura in cui una chiave viene usata per cifrare un testo e una chiave diversa

viene usata per decifrarlo. Gli algoritmi a chiave pubblica sono lenti nell'esecuzione, ma superano il problema dello scambio delle chiavi. Generalmente la chiave pubblica è utilizzata per cifrare, la chiave privata per decifrare, in modo da garantire la segretezza della comunicazione. Se viceversa si utilizza la chiave privata per cifrare e quella pubblica per decifrare si ottiene un meccanismo di certificazione dell'identità del mittente di un documento.

Crittografia a tecnica mista: a causa della lentezza degli algoritmi a chiave asimmetrica, si utilizza tale tecnica per lo scambio della chiave privata che sarà utilizzata per poi avviare una comunicazione a crittografia simmetrica.

Firma Digitale: è un metodo matematico che consente di garantire diverse caratteristiche di un messaggio digitale:

- Autenticazione: garanzia dell'identità del mittente;
- Non ripudio: garanzia che il mittente non possa negare di aver inviato il messaggio;
- Integrità: garanzia che il messaggio non sia stato alterato.

Protocollo AAAA: è un insieme di regole e specifiche che realizzano in contesto informatico i principi di Autenticazione (Authentication), Autorizzazione (Authorization), Contabilizzazione (Accounting) e Revisione (Auditing)

- Autenticazione: dimostrazione della propria identità;
- Autorizzazione: verifica dei privilegi di accesso e consultazione di informazioni e risorse;

- Accounting: monitoraggio delle risorse utilizzate (ad esempio tramite file di LOG);
- Auditing: verifica della conformità dei monitoraggi svolti tramite l'accounting.

Principio "CIA": Confidenzialità (Confidentiality) intesa come protezione della lettura dell'informazione da soggetti non autorizzati, Integrità (Integrity) intesa come protezione dalla modifica non autorizzata dell'informazione, Disponibilità (Availability) intesa come garanzia di poter accedere ai propri dati quando se ne ha necessità sono i 3 cardini della sicurezza informatica.

Cifrario di Vigenère: tecnica di cifratura con cui si cifra ogni singolo carattere del messaggio spostando la lettera da cifrare di un numero di posti variabile determinato in base ad una parola chiave (detta verme), che viene ripetuta sotto il messaggio;

OTP - One Time Pad (detto anche Cifrario di Vernam): è una tecnica di cifratura (basata sulla tecnica del Cifrario di Vigenère) in cui viene usata una chiave casuale lunga quanto il testo da cifrare, utilizzabile una sola volta. Il testo cifrato non ha più alcuna relazione con quello originario. Senza conoscere la chiave è impossibile decifrare il messaggio.

Criterio di Shannon: un cifrario è sicuro se il testo cifrato non rivela alcuna informazione sul testo in chiaro. Ogni messaggio cifrato deve essere lungo almeno come il messaggio in chiaro.

Confusione: principio indicato da Shannon, non deve esserci relazione tra chiave e testo cifrato, affinchè non si possa risalire alla chiave partendo dall'analisi del testo.

Diffusione: principio indicato da Shannon, è la capacità di un algoritmo di crittografia di distribuire e cercare di eliminare le correlazioni statistiche proprie di un testo in chiaro in un testo cifrato, in modo da rendere vani attacchi basati sulla distribuzione statistica delle lettere.

Effetto valanga (*criterio di avalanche*): capacità di un algoritmo di crittografia di fare in modo che tramite la modifica di un solo carattere del testo in chiaro vi sia l'alterazione di tutto il testo cifrato (principio di diffusione), e che la modifica di un solo carattere della chiave comporti l'alterazione di tutto il testo cifrato (principio di confusione). E' importante, perché se due testi in chiaro simili producessero testi cifrati simili si potrebbe risalire alla chiave.

Principio di Kerchoffs: la sicurezza di un sistema di crittografia deve dipendere solo dalla segretezza della chiave, pertanto l'algoritmo può essere reso pubblico.

Attacchi attivi: minacce alla integrità e disponibilità dei dati, come virus e attacchi DOS.

Attacchi passivi: minacce alla confidenzialità dei dati. Sono i più difficili da individuare, perché sono difficili da individuare, perché vengono effettuati con tecniche come lo sniffing e il man-in-the-middle che non hanno un impatto diretto sui dati o sulle funzionalità di un sistema.

RSA: un algoritmo a chiave pubblica particolarmente robusto, basato sulla complessità computazionale della fattorizzazione in numeri primi, in cui nonostante le due chiavi siano generate con un procedimento matematico in cui una chiave è calcolata a partire dall'altra, risulta molto difficile computazionalmente risalire dall'una all'altra. Attualmente con una chiave a 2048 bit si garantisce la sicurezza del testo cifrato.

QUALCOSA SU PROGRAMMAZIONE CONCORRENTE E PROCESSI

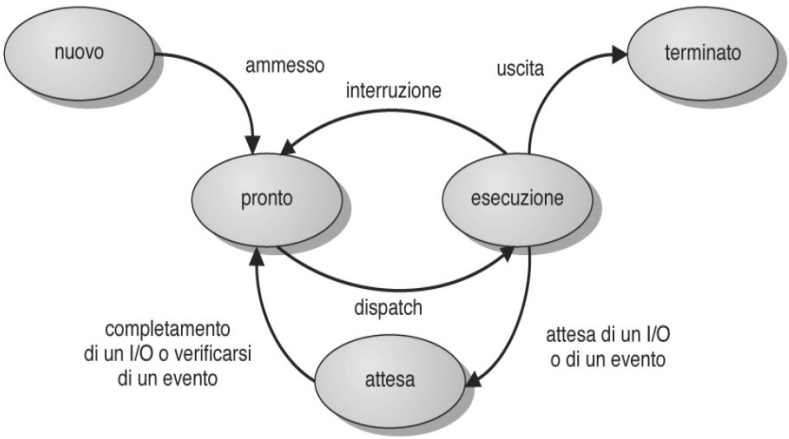
Programma: è un'entità statica che consiste nell'insieme di codice e istruzioni per completare un'attività.

Processo: è un'entità dinamica generata da un programma in esecuzione, è strutturato come una sequenza di **task** (attività).

Scheduler: è il componente di un sistema operativo che si occupa della gestione dei processi.

Processi leggeri e pesanti: un **thread** (o processo leggero) è un'unità di esecuzione che condivide codice e dati con altri thread ad esso associati. Un processo pesante equivale a un task con un solo thread.

Modello a 5 stati dei processi: rappresenta i vari stati in cui può trovarsi un processo durante la sua schedulazione nel sistema operativo.



Concorrenza: la programmazione concorrente è un modello di programmazione che si occupa dell'esecuzione simultanea di più attività o processi indipendenti all'interno di un'applicazione, consentendo di creare programmi che possono eseguire operazioni parallele, migliorando l'efficienza, l'interattività e la gestione delle risorse.

Mutex: è un meccanismo di blocco mutualmente esclusivo, che impedisce a più di un processo di accedere alla risorsa condivisa contemporaneamente. Un processo deve bloccare l'oggetto mutex per accedere alla risorsa e sbloccarlo quando la rilascia. Può avere valore 0 oppure 1.

Semaforo: è un meccanismo di segnalazione, che indica se un processo sta acquisendo o rilasciando una risorsa. Può avere valori diversi, ma più comunemente è un semaforo binario.

Problematiche: la complessità della programmazione concorrente comporta diverse problematiche, che vengono affrontate applicando varie tecniche di sincronizzazione, come i mutex, i semafori e le variabili di condizione, per garantire un corretto accesso alle risorse condivise. Queste le principali:

- **Race conditions**: si verificano quando l'esito di un programma dipende dall'ordine di esecuzione non deterministico delle operazioni concorrenti, ad esempio quando più thread modificano contemporaneamente una variabile condivisa senza una sincronizzazione appropriata.
- **Deadlock**: si verifica quando due o più thread sono bloccati indefinitamente perché ognuno sta aspettando che un'azione venga completata da un altro thread.

- **Starvation** (“morte per fame”): si verifica quando un thread viene privato delle risorse necessarie per completare la sua esecuzione a causa della priorità più elevata data ad altri thread, rimanendo bloccato indefinitamente.
- **Overhead**: l'utilizzo di thread aggiuntivi e la sincronizzazione tra di essi comportano un sovraccarico in termini di tempo di esecuzione e risorse di sistema, causando un calo delle prestazioni complessive dell'applicazione.

Problema del banchiere: un banchiere gestisce una certa quantità di risorse (ad esempio, soldi) e diversi clienti che richiedono un certo numero di risorse per eseguire le loro attività. Il banchiere deve garantire che le risorse vengano assegnate in modo sicuro ai clienti, senza causare deadlock o starvation. Il banchiere tiene traccia delle risorse disponibili e delle risorse richieste da ciascun cliente. Prima di assegnare le risorse a un cliente, il banchiere valuta se l'assegnazione rispetta i limiti di disponibilità delle risorse e se non provocherà situazioni di deadlock o starvation. In caso affermativo, il banchiere assegna le risorse al cliente; altrimenti, il cliente deve aspettare finché non ci sono abbastanza risorse disponibili.

Problema del filosofo a cena: un gruppo di filosofi condividono un tavolo per cenare e un set di bacchette per mangiare. Ogni filosofo si alterna tra due stati: "pensare" e "mangiare". Per mangiare, un filosofo deve raccogliere le due bacchette a lui adiacenti. Occorre garantire che i filosofi possano mangiare senza causare deadlock. Se ogni filosofo cerca di prendere prima la bacchetta a sinistra e poi quella a destra, potrebbe verificarsi una situazione in cui tutti i filosofi tengono la bacchetta a sinistra e attendono la bacchetta a destra, causando un deadlock. Per evitare ciò, è necessario utilizzare

una strategia di gestione delle bacchette che eviti le situazioni di deadlock, come ad esempio permettere ai filosofi di prendere le bacchette solo se entrambe sono disponibili contemporaneamente o limitare il numero di filosofi che possono prendere le bacchette contemporaneamente.

Problema del produttore-consumatore: in una fabbrica ci sono dei lavoratori (produttori) che producono oggetti e dei magazzinieri (consumatori) che prelevano gli oggetti prodotti. Il problema consiste nel garantire che i produttori non producano oggetti quando il magazzino è pieno e che i consumatori non prelevino oggetti quando il magazzino è vuoto.

Problema del lettore-scrittore: diverse persone (lettori) possono accedere a un libro per leggere, ma solo una persona alla volta (scrittore) può apportare modifiche. Il problema consiste nel garantire che più lettori possano leggere contemporaneamente senza interferire tra loro, ma che il processo di scrittura sia esclusivo e non venga interrotto dai lettori.

Problema dei barbieri addormentati: si basa su un salone con un barbiere e alcune sedie per i clienti in attesa di essere serviti. Il problema consiste nel garantire che i clienti possano entrare nel salone e aspettare il loro turno senza causare un deadlock. Se il salone è pieno e il barbiere è occupato, i clienti devono aspettare, ma se i clienti si accumulano troppo, potrebbero essere bloccati indefinitamente.

QUALCOSA SULLA DIFESA PERIMETRALE DELLE RETI

Difesa perimetrale: insieme delle tecniche per la protezione di una rete, da implementarsi tra rete esterna e rete interna, sul "perimetro" della rete da proteggere.

Firewall: elemento passivo di difesa perimetrale di una rete. La difesa tramite firewall in generale si occupa di impedire gli accessi non autorizzati, del controllo del traffico dati e del blocco di eventuali traffici dovuti a malware. I firewall lavorano tramite insiemi di regole di filtraggio. Esistono varie tipologie di firewall:

- **Personal firewall**: sono firewall software installati direttamente sulla macchina da proteggere. Per loro natura sono meno sicuri, possono servire per controllare su una macchina le applicazioni che accedono alla rete esterna ad esempio, o in contesti privati e non aziendali.
- **Packet Filter Firewall**: si occupano di filtrare i pacchetti singolarmente secondo i dati contenuti negli header. E' una tipologia di filtraggio semplice, rapida e non pesante a livello di risorse. Operano principalmente sui primi 3 livelli della pila OSI. Questa tecnica è soggetta ad attacchi di spoofing dell'IP.
- **Stateful Inspection Firewall**: i pacchetti vengono analizzati come nei Packet Filter Firewall, ma tenendo conto delle porte, dello stato della connessione e dei protocolli utilizzati, e quindi anche dei pacchetti precedenti di una trasmissione di informazioni. Analizzano fino al livello 4 della pila OSI,

funzionano tramite tabelle che possono subire attacchi di tipo DOS di saturazione del contenuto. Utilizza tabelle per memorizzare ad esempio i seq e gli ack number di una connessione TCP e i relativi messaggi di ACK e SYN scambiati. Non funzionano sui protocolli non orientati alla connessione come UDP.

- **Application firewall**: sono specifici per una determinata applicazione, analizzano pertanto fino al livello 7 della pila OSI. Sono molto sicuri, tuttavia comportano un eccessivo rallentamento nella rete.
- **Next-generation firewall**: implementano le varie tecnologie esistenti di firewall, con funzionalità aggiuntive utili quali ad esempio il servizio NAT e la gestione delle VPN.

Egress traffic: indica il traffico in uscita dalla rete.

Ingress traffic: indica il traffico in ingresso sulla rete.

DMZ (DeMilitarized Zone): è un'area della rete interposta tra la rete esterna e la rete interna, usata per consentire l'accesso dalla rete pubblica esterna a server o altri componenti, ad esempio server mail e server web, in modo da non compromettere la rete interna da proteggere. Si possono utilizzare più firewall per isolare le DMZ, che generalmente agiscono con sistemi di tipo packet filter, e consentono la comunicazione da parte delle macchine nella rete interna tramite il servizio NAT. Possono comunque essere soggette ad attacchi passivi come lo sniffing e attivi come lo spoofing.

Host bastione: è la macchina posta come primo punto di difesa perimetrale di una rete, configurata per essere specializzata nella protezione dagli attacchi esterni.

ACL (Access Control List): è una lista di regole che determina accessi autorizzati e vietati alle risorse di una rete. Le regole sono dette Access Control Entry (ACE). Le regole si consultano in ordine partendo da quella in cima alla lista fino all'ultima, fino a che si verifica una corrispondenza (match): in tal caso si applica la regola corrispondente. In caso non si verifichi nessun match, verrà applicata la policy di default.

Regole e comandi principali di una ACL:

- **Default-deny**: policy in cui il traffico è bloccato in via predefinita, le regole indicano quali tipi di traffico sono autorizzati. E' il criterio che consente maggiore sicurezza.
- **Default-allow**: policy in cui il traffico è consentito in via predefinita, le regole indicano quali tipi di traffico sono bloccati.
- **Permit**: indica l'azione di consentire il traffico in caso di match.
- **Deny**: indica l'azione di bloccare il traffico in caso di match.
- **Wildcard-mask**: indica quali bit di un indirizzo IP devono essere controllati dalla regola nell'ACL. I bit a 1 nella maschera corrispondono ai bit che non devono essere controllati. Per controllare una subnet intera il valore della wildcard-mask si ottiene sottraendo a 255.255.255.255 il valore della subnet mask interessata.

- **host**: corrisponde alla wildcard mask 0.0.0.0
- **any**: corrisponde alla wildcard mask 255.255.255.255
- **eq**: seleziona solo i pacchetti con la porta indicata.

Le **ACL standard** specificano solo la sorgente del traffico (vanno posizionate vicino alla sorgente di destinazione), le **ACL estese** specificano anche la destinazione, le porte e il protocollo (vanno posizionate vicino alla sorgente da filtrare).

Esempio di sintassi ACL standard:

Sintassi: *Router(config)# access-list numero_ACL deny|permit ip_sorgente wildcard_mask*

Esempi

Router(config)# access-list 1 permit host 192.168.0.1

//consente il traffico all'host 192.168.0.1

Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255

//consente il traffico alla rete 172.16.X.X con wildcard mask 0.0.255.255

Esempio di tabella:

ACL	Sorgente	Wildcard mask src	Azione
1	192.168.0.1	0.0.0.0	Permit
2	172.16.0.0	0.0.255.255	Permit
*			Deny

Esempio di sintassi ACL estesa:

Sintassi: Router(config)# access-list numero-ACL [deny|permit] protocollo ip_sorgente wildcard_mask ip-destinazione wildcard_mask condizione applicazione

Esempio:

Router(config)# access-list 101 permit tcp 172.16.2.0 0.0.0.255 any eq 25

//consente il traffico TCP della rete 172.16.2.x sulla porta 25

Esempio:

Router(config)# access-list 1 deny tcp any any eq 80

//blocca tutto il traffico con protocollo TCP sulla porta 80

Proxy: è un servizio fornito tramite un server che riceve e inoltra le richieste e le risposte che fanno parte della comunicazione tra client e server esterni alla rete, tra cui viene posto al fine di gestire e monitorare il traffico. Il client si collega al proxy, che si occuperà di inviarle al server (se consentito) da cui poi riceverà la risposta da consegnare al client. Il proxy può memorizzare (**caching**) per un certo tempo i risultati delle richieste degli host, in tal modo può fornire le risposte se le ha memorizzate senza doverle richiedere nuovamente al server, velocizzando la comunicazione. Il proxy può monitorare e regolare le richieste (in tal caso funziona concettualmente come un firewall) attraverso opportune regole, impedendo traffico verso servizi non autorizzati, ad esempio in una rete scolastica si possono vietare gli accessi ai social network oppure

a siti malevoli o vietati ai minori in base a opportune liste (whitelist - blacklist) che li raccolgono. L'utilizzo di un proxy consente inoltre di avere un unico punto di uscita dalla rete interna per le richieste effettuate verso servizi esterni alla rete stessa, migliorando la sicurezza, e mascherando all'esterno le macchine che hanno richiesto il servizio o la risorsa, garantendo l'anonimato (ad esempio come nel caso della rete TOR).

QUALCOSA SULLE VPN

VPN: è un servizio di comunicazione sicuro e affidabile che crea un canale virtuale fra due o più macchine che si implementa sopra una infrastruttura di rete pubblica (il che le rende particolarmente flessibili e scalabili), caratterizzata da tecnologie che garantiscono i principi di confidenzialità, integrità ed autenticazione. Le VPN sono tipicamente utilizzate per consentire l'accesso alle risorse di una rete privata ad utenti esterni fisicamente alla rete stessa, o per consentire di mantenere una connessione protetta tra sedi remote e sede centrale di una stessa azienda. Con appositi apparati perimetrali viene effettuato un “tunneling” su internet.

Tunneling: è il termine che rappresenta idealmente la realizzazione della connessione sicura in una VPN, come se venisse scavato un “tunnel” nella rete pubblica dentro cui avviene la comunicazione protetta.

Remote VPN: consente l'accesso da remoto ai dati presenti in una rete aziendale. Si realizza tramite un client di connessione installato sulle macchine utente che si collega a un server VPN per l’accesso alle risorse remote.

VPN site to site: consentono di collegare sedi geograficamente distanti tra loro, tramite dei tunnel logici permanenti. Possono essere Extranet (collegano sedi di aziende e organizzazioni esterne) o Intranet (collegano sedi esterne della stessa azienda). Esistono diversi tipi di implementazione:

- **Trusted**: sono realizzate al livello 2 della ISO/OSI, sono spesso fornite dagli ISP e non necessitano di tunneling e crittografia. Sono praticamente delle “parti” di reti pubbliche dedicate a connessioni private.
- **Secure**: si basano su protocolli di crittografia sicuri, come SSL/TLS o IPSec.
- **Hybryd**: utilizzano una tecnica mista, in pratica implementando la crittografia nelle VPN Trusted.

QUALCOSA SULL'AUTENTICAZIONE IN AMBIENTI DISTRIBUITI

Ambienti distribuiti: sono dei sistemi software eseguiti su più macchine distinte che appaiono come un'unica macchina. Sono caratterizzati da condivisione delle risorse e distribuzione del carico, una elevata scalabilità e tolleranza ai guasti. I sistemi e le reti che li costituiscono sono spesso eterogenei, la loro comunicazione avviene tramite messaggi; l'architettura è strutturata a livelli e gestita dal "**middleware**" (livello intermedio), che si interpone tra i vari OS (livello basso) e le applicazioni destinate agli utenti (livello alto).

Kerberos: è un sistema che supporta l'implementazione della sicurezza in sistemi distribuiti, stabilendo canali sicuri tra client e server. E' composto da un Authentication Server AS che autentica un utente e gli fornisce una chiave per il canale, e un Ticket Granting Service TGS che stabilisce canali sicuri con un server tramite dei "**ticket**" ovvero chiavi segrete crittografate. Il client ottiene prima un ticket di lunga durata dall'AS, valido per l'intera sessione di comunicazione, e in seguito ottiene un ticket di breve durata dal TGS per richiedere il singolo servizio.

(Microsoft) Active Directory: è un servizio che "archivia le informazioni relative agli oggetti sulla rete e semplifica la ricerca e l'uso di queste informazioni da parte degli amministratori e degli utenti. […] usa un archivio dati strutturato come base per un'organizzazione logica e gerarchica delle informazioni di directory" (*tratto dal sito di Microsoft*). Il servizio di "**directory**" è una sorta di database organizzato ottimizzato per la lettura e la ricerca su grandi moli di dati, reso disponibile a tutte le entità di una rete tramite un

Controller di Dominio (**Domain Controller**), che possiede un database contenente i dati di accesso e i permessi di tutti gli utenti, incluse anche le risorse di rete come computer e stampanti, tramite un meccanismo di policy di gruppo (**Group Policy Object - GPO**). I dati vengono poi condivisi con i client presenti nella rete. In poche parole, sarà possibile accedere con il proprio utente ed avere le proprie risorse sempre disponibili da qualsiasi PC in azienda (**Single Sign-On - SSO**).

LDAP: Lightweight Directory Access Protocol ovvero protocollo “leggero” per l’accesso a servizi di directory. Un server LDAP è un protocollo che consente di effettuare operazioni sui dati contenuti in un servizio di directory (ad esempio Active Directory), ottimizzato per effettuare operazioni di ricerca ed accesso alle informazioni.

QUALCOSA SULLA VIRTUALIZZAZIONE

Virtualizzazione: è una tecnica che consente di eseguire l'astrazione dall'hardware fisico e renderlo disponibile al software. Tramite un **hypervisor** (detto anche **VMM - Virtual Machine Manager**) il sistema operativo e le applicazioni vengono separate dall'hardware fisico. La macchina che esegue la virtualizzazione (il sistema hardware) è detta **host**, le macchine virtualizzate sono dette **guest**. Il VMM crea ed esegue le macchine virtuali.

Virtual Machine: è il software che crea l'ambiente virtuale.

Tecniche di virtualizzazione:

- **Virtualizzazione completa**: si realizzano sistemi virtuali dello stesso tipo del sistema fisico ospitante;
- **Emulazione**: si eseguono applicazioni su un sistema diverso da quello per cui sono scritte (diverso dalla simulazione, in cui viene riprodotto un sistema operativo, anche a livello logico;
- **Paravirtualizzazione**: gli OS guest accedono all'hardware fisico del OS host tramite delle API messe a disposizione dall'hypervisor, senza emularne la CPU;
- **Virtualizzazione a livello di OS**: detti anche **container**, la virtualizzazione è gestita dal kernel che isola le risorse hardware e software in uso dalle varie applicazioni. In questa tecnica i container sono isolati tra loro, e non vengono utilizzate VM e non ci sono sistemi guest (un esempio la tecnologia *Docker*).

- **Virtualizzazione a livello di applicazione**: detti anche run-time systems, consentono di eseguire un programma indipendentemente dall'architettura hardware fisica ospitante (ad esempio la Java Virtual Machine che consente di eseguire i programmi Java su qualsiasi OS su cui è disponibile).

Tipi di hypervisor:

- **Tipo 0**: l'hardware mette a disposizione le funzionalità tramite un firmware dedicato.
- **Tipo 1**: detti anche nativi o bare metal, eseguiti sull'hardware dell'host (ad esempio VMWare Server, Microsoft Hyper-v)
- **Tipo 2**: detti hosted, eseguiti su un sistema operativo come applicazione (ad esempio Oracle Virtual Box, VMWare Player).

Interpretazione: si basa sulla lettura di ogni istruzione del codice macchina da eseguire e sulla sua esecuzione sul sistema ospitante, sfruttando la possibilità di emulare elementi di altre architetture (diversi o non presenti, come ad esempio i registri delle CPU) sfruttando aree di memoria. Il metodo è potente, ma comporta molte istruzioni da eseguire e quindi un carico considerevole sulla CPU. Un esempio di **emulatore** basato sull'interpretazione è il popolare emulatore MAME, che consente di emulare il funzionamento delle ROM contenenti il codice macchina dei videogiochi arcade "da sala giochi".

Ricompilazione dinamica: vengono letti blocchi di codice, tradotti e ottimizzati per l'architettura ospitante, sfruttando dove possibile la bufferizzazione di porzioni di codice di utilizzo frequente.

Emulatore: è un software in grado di replicare le funzioni di un determinato sistema su un altro sistema differente dal primo.

Differenze tra simulatore, emulatore e virtualizzatore:

- **Simulazione**: l'ambiente necessario al funzionamento del sistema ospitato non è legato all'ambiente reale ed è ricreato in maniera indipendente dall'hardware e dal software ospitante.
- **Emulazione**: il sistema ospitante riproduce l'ambiente necessario al sistema ospitato in modo che possa funzionare su un software ed hardware differente.
- **Virtualizzazione**: il sistema ospitante è realizzato per mettere a disposizione uno o più ambienti virtuali, isolati tra loro, ai sistemi ospitati, ricreando gli ambienti di lavoro con un livello minimo di intermediazione tra tali ambienti e l'hardware sottostante .

QUALCOSA SULLA SICUREZZA INFORMATICA

Attacchi attivi: utilizzano modalità offensive che operano in maniera diretta (ed eventualmente distruttiva) su sistemi e informazioni, ad esempio accessi non autorizzati, modifica o cancellazione delle informazioni, blocco dei sistemi, impersonazione di altri utenti, ecc…

Attacchi passivi: si limitano alla lettura delle informazioni, analisi del traffico, "*sniffing*", senza effettuare modifiche alle informazioni e ai sistemi.

Penetration Test: processo di analisi e valutazione della sicurezza di un sistema informatico o di una rete, spesso effettuato utilizzando vari tipi di attacchi, compresa l'ingegneria sociale.

0-days: una vulnerabilità non ancora nota (oppure appena resa nota, per la quale ci sono "zero" giorni di tempo per fixarla) attaccabile da un exploit.

Zombie Zero: un attacco informatico famoso che sfruttava un malware inserito in lettori di codici a barre per avviare delle backdoor sfruttando connessioni wireless. E' particolarmente significativo perché mostra la potenziale pericolosità dei dispositivi IoT.

Hacker: termine che nasce nelle prime comunità virtuali appassionate di programmazione informatica, con il termine "**hack**" si intendeva "un progetto in fase di sviluppo o un prodotto realizzato con scopi costruttivi". E' alla base della filosofia del

software libero e dell'open source, in particolare per il piacere di modificare e migliorare lavori, prodotti, progetti. Hacker è inteso oggi (in modo un po' limitativo) come un esperto in un particolare settore, principalmente informatico. Spesso confuso con la figura del "cracker".

Cracker: è un esperto di informatica e materie affini che sfrutta le capacità per scopi distruttivi sui sistemi altrui.

White Hat: è un hacker esperto nei penetration test con scopi etici quali rendere consci il bersaglio di un problema o una vulnerabilità.

Black Hat: ha le caratteristiche del White Hat, ma le usa per scopi distruttivi e criminali.

Gray Hat: è un White Hat che talvolta sfrutta le proprie capacità in modo distruttivo o per tornaconto personale.

Ingegneria sociale: insieme delle tecniche per carpire informazioni da una persona per poterle sfruttare per realizzare attacchi attivi a un sistema informatico.

DoS: tipologia di attacco attivo in cui si cerca di rendere inutilizzabile un servizio (Denial of Service)

DDoS: attacco DoS di tipo Distribuito, ovvero attuato sfruttando più postazioni di attacco (soprattutto bot).

Bot: abbreviazione di robot. Generalmente sono software che effettuano operazioni automatizzate.

Spoofing: definisce una tecnica di attacco basata sulla falsificazione dell'informazione (ad esempio l'identità dell'utente, l'indirizzo IP, ecc…)

ARP spoofing: attacco che si basa sulla modifica delle tabelle ARP al fine di realizzare un MITM.

MITM: indica un attacco di tipo Man In The Middle, in cui un utente si frappone nella comunicazione tra due host per carpirne informazioni, in maniera invisibile agli host stessi.

Reverse Engineering: tecnica con la quale si cerca di ricostruire un codice sorgente da un codice compilato.

CSRF - Cross Site Request Forgery: attacco che si basa sul riutilizzo su internet di sessioni utente per eseguire azioni dannose. Un cracker fa visitare un proprio sito dalla vittima mentre è collegata a un sito bersaglio, quindi riutilizzerà un'azione HTTP eseguita dalla vittima sul proprio sito inoltrandola opportunamente al sito bersaglio sfruttando la sessione ancora attiva, che consentirà di eseguire azioni non autorizzate.

XSS - Cross-Site Scripting: sono attacchi che sfruttano vulnerabilità dei siti web (spesso non aggiornati) tramite cui si iniettano (**injection**) script malevoli in pagine web, che consentono di diffondere malware o rubare informazioni agli utenti.

Privilege Escalation: tecnica di attacco attivo con cui si sfruttano vulnerabilità di un sistema per acquisire diritti (privilege) utente non autorizzati, ad esempio quelli di amministratore.

DNS poisoning: tecnica con la quale si "avvelenano" i record DNS con fini di DoS o redirezione su siti malevoli e di phishing.

Jammer: dispositivo in grado di siturbare frequenze e interrompere comunicazioni.

Deauth WiFi: tecnica di tipo DoS che consente di sfruttare il protocollo 802.11 per scollegare dalla rete WiFi un utente se combinata con una tecnica di spoofing IP della vittima.

Data breach: è un incidente informatico che comporta violazione di informazioni riservate.

Sniffing: attacco passivo che prevede l'ascolto e intercettazione non autorizzata di dati e comunicazioni.

Meltdown e Spectre: vulnerabilità scoperte nel 2018 che interessano CPU Intel, AMD e ARM (i principali produttori mondiali) che consentono ai programmi che la sfruttano di accedere ad aree di memoria non autorizzate di altri programmi.

Rootkit: software malevoli utilizzati per accedere alle risorse di un sistema senza autorizzazione.

Ping of Death: attacco di tipo DoS che sfruttava una vulnerabilità del protocollo IP tramite invio di comandi ping opportunamente modificati per mandare in buffer overflow i sistemi causandone il crash.

Rogue AP: access point inserito senza autorizzazione in una rete o in un'area coperta da una rete wireless, allo scopo di effettuare attacchi MITM, phishing, ecc…

Defacing: attacco attivo in cui un sito viene sostituito da un sito malevolo.

Rogue Server: è un server DHCP che viene inserito senza autorizzazione in una rete al fine di far autenticare le vittime (sfruttando il funzionamento del DHCP, che prevede l'invio in broadcast di richieste di configurazione IP) al fine di fornire una

configurazione generalmente utilizzata per utilizzare gateway o DNS malevoli per attacchi MITM o per effettuare phishing ecc…

x.800: è un'architettura di sicurezza di riferimento per il modello OSI, che introduce delle linee guida e delle racccomandazioni per identificare le minacce e gli attacchi, analizzare e prevenire le minacce, gestire gli attacchi informatici e le compromissioni dei sistemi e dei servizi (Attacks, Mechanism, Services).

GDPR: è il regolamento generale sulla protezione dei dati in Europa, introdotto nel 2016. Indica come i dati personali e sensibili debbano essere gestiti, riguarda le modalità di raccolta, utilizzo, protezione e condivisione dei dati stessi a tutela dell'utente.

Dati personali: sono quelle informazioni che identificano, direttamente o indirettamente, una persona fisica. L'indirizzo IP della propria connessione Internet è considerato ad esempio un dato personale se consente di identificare la persona.

Dati sensibili: sono quelle informazioni che rivelano informazioni sulla persona fisica riguardanti ad esempio orientamento religioso, politico, sessuale, dati medici, ecc…

QUALCOSA SUI SOCKET

Socket: astrazione software che consente la comunicazione tra due processi in una rete, o sulla stessa macchina. Un socket è costituito da una coppia indirizzo IP – porta, possono essere basati sul protocollo UDP (socket datagram) o TCP (socket stream, con garanzia della consegna).

Funzioni fondamentali:

- Creazione del socket: il processo crea un socket per iniziare la comunicazione.
- Ascolto: il server ascolta su un numero di porta specifico per ricevere richieste da client.
- Connessione: il client si connette al server mediante l'indirizzo IP e il numero di porta.
- Invio dati: il client invia dati al server attraverso il socket.
- Ricezione dati: il server riceve i dati inviati dal client e li elabora.
- Chiusura del socket: il processo chiude il socket per terminare la comunicazione.

Esempio di implementazione in pseudocodice:

si prende come riferimento il Quesito 1 della prova di Esame sessione ordinaria del 2024, in cui si vuole realizzare un socket per la comunicazione client – server tra un sistema automatico a microcontrollore e delle colonnine di ricarica per auto elettriche.

Per prima cosa si definisce il **formato di trasmissione**:

struttura **messaggio** {
  "data_ora": "YYYY-MM-DD HH:MM:SS",
  "id_cliente": "stringa",
  "percentuale_carica": "numero decimale",
  "energia_erogata": "numero decimale"
}

Il formato definisce in che modo sono strutturati i dati da trasmettere. In caso di pacchetti IP può trasmettere pacchetti al massimo di 65.535 byte, corrispondenti al payload del pacchetto IP.

Per quanto riguarda lo pseudo-codice relativo a client e server:

SERVER

```
import socket
//inserimento ipotetiche librerie per supportare i socket

// Creazione del socket server
server_socket = new socket(AF_INET, SOCK_STREAM)

//AF_INET indica che verranno usati socket basati su IP
//SOCK_STREAM invece riguarda il tipo di socket basato su TCP

//associare coppia IP - porta
server_socket = bind(server_ip, porta)
//porre in "ascolto" il server
server_socket.listen()

//accettare connessioni
client_socket = server_socket.accept()

//ricezione messaggio
messaggio = client_socket.receive()

// chiusura
client_socket.close()
server_socket.close()
```

CLIENT

```
import socket

// Creazione del socket client
client_socket = new socket(client_ip, porta)

// Connessione al server
client_socket.connect(server_ip, porta)

//lettura dei dati da trasmettere, i valori sono di esempio
  data_ora = datetime.now()
  id_cliente = "COL_01"
  percentuale_carica = 0.5
  energia_erogata = 10.0

  //creazione del messaggio, usando i dati raccolti
  messaggio my_messaggio = {
    "data/ora": data_ora,
    "id_cliente": id_cliente,
    "percentuale_carica": percentuale_carica,
    "energia_erogata": energia_erogata
   }

// Invio del messaggio al server
client_socket.send(messaggio)

// chiusura
client_socket.close()
```

PROGETTARE UNA RETE

La progettazione di una rete è generalmente una delle richieste presenti nella II Prova dell'Esame di Stato. Sebbene alcune caratteristiche e configurazioni non siano esplicitate direttamente nel testo della prova, è bene indicarle al fine di rendere la progettazione completa e tecnicamente corretta. Inoltre bisogna sempre descrivere e motivare opportunamente le scelte effettuate, anche se possono sembrare ovvie. Ad esempio chiarificare perchè in un rack utilizzo 2 switch a 24 porte invece di 1 a 48 porte (paura dei guasti, più funzionale, ecc…): trattandosi di un progetto non esiste una soluzione unica, ma tante soluzioni che, se opportunamente motivate a livello teorico e tecnico, si possono considerare corrette e ugualmente funzionali.

Trattando materiale hardware e software le soluzioni sono molteplici, anche in termini di costi, pertanto proprio l'ipotetica spesa può essere una motivazione importante alla base di alcune scelte progettuali legate al contesto in cui la rete viene realizzata (una scuola con fondi limitati, una mega azienda internazionale, ecc…). Anche i benefici in ambito lavorativo possono essere tenuti in considerazione, in quanto un investimento in materiale e soluzioni più preformanti e costose hanno una ricaduta positiva sulla produttività lavorativa, o i benefici in termini di disaster recovery per evitare il blocco della attività e dei servizi di rete.

Insomma, occorre progettare la rete cercando di tenere conto di tutti questi aspetti, tenendo presente che l'elaborato che

produciamo deve essere una sorta di “guida” per chi volesse davvero realizzare la rete.

Ecco di seguito i principali aspetti da considerare in una progettazione di rete, con alcune indicazioni generali (da approfondire nella prova):

- **struttura della rete**: dare una descrizione di massima su come pensiamo di strutturare la rete, chiaramente analizzando bene il contesto fisico in cui viene realizzata e il contesto logico legato agli utilizzatori. Sono presenti più edifici? I servizi richiesti devono essere accessibili anche da postazioni remote? E’ un’azienda con più sedi internazionali? Ponendosi le giuste domande si può arrivare a una descrizione del tipo: “Prevedo una struttura fisica a stella nella sede principale, con connessioni protette per consentire l’accesso esterno ai servizi di rete dei dipendenti remoti, la connessione degli edifici aziendali limitrofi sarà effettuata con dorsali in fibra ottica cablate direttamente nelle aree esterne, ecc..”. Eventualmente si può arricchire indicando ipotesi (plausibili!) ed elementi aggiuntivi non specificati dal testo della prova che possano motivare meglio le scelte effettuate (ad esempio su come si pensa sarà il carico della rete da parte degli utenti, quali servizi hanno più necessità di essere protetti, ecc…).
- **topologia fisica**: indicare, disegnando una piantina stilizzata, dotata di opportuna legenda grafica, quella che è la disposizione degli elementi della rete nelle aree in cui sarà realizzata la rete, suddividendo ad esempio per gli edifici in topologia verticale (le connessioni tra i piani di un palazzo) e

orizzontale (le connessioni sul piano), seguendo le indicazioni date dalle normative per il cablaggio strutturato degli edifici. Non occorre disegnare tutti i cavi e tutte le postazioni, è sufficiente essere ordinati e utilizzare delle convenzioni grafiche (ad esempio dovendo indicare la posizione di 30 postazioni PC di un laboratorio si possono indicare le due postazioni estreme e indicare con tre puntini le postazioni da 2 a 29). In questa parte vanno descritte le scelte di materiale hardware effettuate, dalla tipologia dei cavi (CAT6, CAT 7, fibra, ecc…) ai dispositivi (Switch L2 a N porte, Switch amministrabile L3 a N porte, ecc…), armadi (tipologia ad esempio "rack", dove sono previsti, ecc…), postazioni PC, tipologia di prese di rete, quante e dove (2 per postazione PC, ecc…), dispositivi per la rete WiFi, ecc…

- **topologia logica**: nella topologia logica va rappresentata la struttura logica della rete, quindi le interconnesioni tra le varie reti, sottoreti, dispositivi di rete (come sono collegati gli switch, i router, ecc…), non serve che sia realizzata sulla piantina fisica, la topologia logica ignora dove sono fisicamente i dispositivi.

- **piano di indirizzamento**: indicare tutte le scelte effettuate per indirizzare la rete, le sottoreti, specificando ad esempio i gateway, gli indirizzi di rete, le subnet mask, gli indirizzi IP (eventualmente raggruppati in range) assegnati ai vari host (ricordando anche le porte dei router), i range di indirizzi IP liberi per ogni rete, le tabelle di routing dei router. Inoltre se vi è necessità di separare il traffico di rete indicare se si utilizzano le VLAN, specificando tipologia (tagged o

untagged), e assegnando in maniera chiara i VLAN ID alle varie reti interessate. Se si prevede di far comunicare le VLAN tra loro anche in questo caso indicare bene le connessioni con le porte trunk e con eventuali Switch L3 per l'inter-vlan routing.

- **sicurezza della rete e delle informazioni**: specificare i servizi e gli accorgimenti per proteggere la rete, analizzando preventivamente quelli che possono essere i rischi principali cui può essere esposta tra minacce attive e passive. Considerare l'utilizzo di firewall, proxy, autenticazione degli utenti e degli host, VPN, VLAN, sistemi di sicurezza sul WiFi, ecc…, indicando precisamente le configurazioni e specifiche richiesti (ad esempio WPA2 per il WiFi, DMZ per i servizi di rete esposti all'esterno, ecc…). Indicare l'utilizzo di crittografia e certificati per i servizi di rete (specificare quali e dove), eventuali sistemi di backup, specificare le principali politiche di sicurezza da seguire e considerare (aggiornamento costante dei dipendenti, aggiornamento periodico delle password, utilizzo di password sicure, verifiche/audit di sicurezza periodici, protezione dagli accessi fisici e remoti ai non amministratori/tecnici di rete, ecc…).

- **servizi di rete**: scegliere i servizi di rete opportuni, che possono essere utili sia per la produttività lavorativa che per la sicurezza (server FTP, DHCP, DNS, server mail interno, ecc…), motivando le scelte e descrivendo quale utilità hanno nella rete, dando indicazioni sui protocolli o configurazioni opportune.

- **autenticazione**: specificare i sistemi di autenticazione presenti, e in caso si prevedano più tipologie di utenti (ad esempio in una scuola possono essere Docenti, Amministrativi, Studenti, Ospiti, Amministratori/Tecnici) indicare quali permessi e operatività si vuole concedere o limitare.
- **ridondanza e disaster recovery**: prevedere servizi e procedure per gestire eventuali guasti o interruzioni di rete o di dati (ridondanza di router, utilizzo di più switch per ridurre la possibilità che un guasto hardware blocchi tutte le reti ma si limiti a interromperne alcune, ecc…), specificando gli accorgimenti individuati (utilizzo di più server, politiche di backup, sistemi RAID, virtualizzazione, ecc…).
- **rispetto delle normative**: verificare che il proprio progetto e le scelte effettuate rispettino le normative vigenti, in particolare per la realizzazione della rete occorre seguire la normativa del cablaggio strutturato degli edifici, per la sicurezza dei dati è da considerare sicuramente il GDPR, eventualmente analizzando quali tipologie di dati tratterà la nostra rete e quali criticità quindi comporta (oltre ai dati personali vengono trattati dati sensibili?).

APPROFONDIMENTI: SICUREZZA NAZIONALE VS PRIVACY

LA STORIA

L'aspetto della sicurezza nazionale ha storicamente avuto un ruolo dominante nella discussione sulla privacy e l'intrusione di terzi nelle comunicazioni altrui. Fin dagli anni Sessanta sono note operazioni su scala mondiale di "Signal Intelligence" (SIGINT), ovvero la raccolta di dati e informazioni attraverso l'intercettazione e analisi di segnali, sia di natura umana, sia inviati da macchine ed elaboratori. Una delle prime operazioni ad essere portata all'attenzione pubblica fu il progetto "Echelon", attraverso il quale diverse Nazioni eseguono un monitoraggio in maniera automatizzata di miliardi di comunicazioni, principalmente via e-mail, transitanti su internet, con largo uso delle intercettazione diretta delle grandi dorsali sottomarine di connessione intercontinentale. Non solo singole keywords vengono intercettate, ma sfruttando innovativi algoritmi vengono analizzate caratteristiche più profonde, quali contesto semantico ed impronte vocali. Spostandoci in tempi più recenti, nel 2013 grande clamore suscitarono le rivelazioni di Edward Snowden, all'epoca ex tecnico della CIA (Central Intelligence Agency, l'agenzia di spionaggio civile degli Stati Uniti d'America) e consulente della NSA (National Security Agency, organismo governativo degli Stati Uniti d'America che, insieme alla CIA e all'FBI, si occupa della sicurezza nazionale), rilasciate all'interno di una serie di inchieste giornalistiche pubblicate sul "The Washington Post" negli USA (testata resa celebre dalle inchieste negli anni Settanta sul caso "Watergate") e nel Regno Unito sul "The Guardian", corredate dalla pubblicazione di decine di documenti riservati di sicurezza nazionale che aveva

raccolto durante il suo operato per l'NSA, svelando dettagli di diversi programmi top-secret di sorveglianza di massa operati dai governo statunitense e britannico, anche in questo caso attraverso l'intercettazione delle comunicazioni su larga scala, basate soprattutto sull'analisi dei "metadati", ovvero informazioni che vengono aggiunte ai dati scambiati su una rete per descriverli. Ad esempio, un file o un documento puòcontenere al suo interno metadati con informazioni sull'autore, una foto puòcontenere metadati sul luogo dove è stata scattata e la data di scatto, un messaggio inviato con un sistema di instant messaging puòcontentere metadati sulla località di invio, l'ora, il destinatario e il mittente. Sebbene si sia diffuso il concetto di "comunicazione sicura", esso viene in realtà semplificato mostrando agli utenti delle rassicurazioni nell'uso di un servizio. Ad esempio nei browser web Chrome e Mozilla Firefox viene mostrata l'icona di un lucchetto per identificare la navigazione protetta da crittografia, mentre in app di instant messaging come Whatsapp e Telegram viene segnalato l'uso della crittografia end-to-end, una tecnica di cifratura della comunicazione che consente solo a mittente e destinatario di leggere i messaggi scambiati. Tutto ci conforta l'utente, ma non è realmente sufficiente a garantire che la privacy dell'individuo sia rispettata, in quanto si tratta soltanto una illusione di sicurezza e anonimato. Se la comunicazione è protetta da accessi esterni e mantiene la confidenzialità, lo stesso non è per i metadati associati, che sono spesso trasmessi in chiaro, senza crittografia), e di fatto sono a disposizione sia delle società che forniscono il servizio, sia di chi è in grado di intercettare le comunicazioni, e sono in grado di rivelare molte più informazioni di quanto l'utente possa pensare, o solamente esserne consapevole.

CINEFORUM: "CITIZENFOUR"

Regia di Laura Portrais, Genere Documentario - USA, 2014. Premio Oscar 2015 Miglior Documentario.

Il documentario racconta lo scandalo della sorveglianza di massa da parte della NSA, la National Security Agency statunitense. La regista, particolarmente attiva nei documentari sul monitoraggio degli USA sui cittadini a seguito degli eventi dell'11 Settembre 2001, era stata contattata tramite una e-mail crittografata da uno sconosciuto che usava il nickname CitizenFour , che dichiarava di poter mettere a disposizione documenti top secret riguardanti le attività dell'NSA a discapito della privacy degli individui. Lo sconosciuto è Edward Snowden, un ex tecnico informatico della CIA e collaboratore dell'NSA, che fu sconvolto sul piano etico personale dalle attività segrete di sorveglianza di massa con cui si era imbattuto nel suo lavoro. Snowden è in gergo un "whistleblowler", ovvero chi segnala pubblicamente attività illecite di un governo o un'azienda. Attualmente ha ottenuto l'asilo politico in Russia; il Governo americano in seguito a queste divulgazioni ha dichiarato Snowden colpevole di spionaggio, mentre il parlamento europeo ha riconosciuto il suo stato di informatore e di difensore internazionale dei diritti umani e ha chiesto agli stati membri di vietarne l'estradizione.

APPROFONDIMENTI: VIRUS ALL'ULTIMO GRIDO

LA STORIA

Molto spesso gli autori di virus e attacchi informatici scelgono nomi particolarmente "divertenti" e appropriati. Nel 1998 un taiwanese sviluppo' un virus per Windows 95 chiamato Chernobyl, che si diffuse sui computer di mezzo mondo infettando addirittura CD allegati a riviste e computer nuovi pre-installati, che si attivava automaticamente il 26 Aprile (anniversario di Chernobyl, appunto) con effetto devastante poiché sovrascriveva il BIOS rendendo i PC inservibili (e le schede madri da buttare…).

Nel 2017 si è verificata una delle più gravi infezioni da ransomware della storia tramite l'exploit EternalBlue. L'exploit sfrutta una falla di Windows, e fu reso noto da un gruppo hacker il 14 Aprile. Esattamente un mese prima Microsoft aveva già rilasciato una patch di sicurezza che correggeva proprio la falla sfruttata da EternalBlue, ma che non copriva ad esempio Windows XP, Windows 8 e Windows Server 2003. Tuttavia tali versioni erano (e probabilmente sono) ancora largamente utilizzate, e non tutti avevano provveduto ad aggiornare i propri sistemi con Windows Update. Il 12 Maggio il worm WannaCry venne lanciato in tutto il modo da un gruppo hacker, colpendo in pochi giorni oltre 200 mila computer nel mondo, facendo vittime anche in importanti aziende di telecomunicazioni e ministeri.

Nonostante WannaCry abbia iniziato a sensibilizzare l'opinione pubblica sulla facilità con cui attualmente un'infezione informatica puòdiffondersi causando seri danni (oltre ai riscatti non è da

trascurare i danni indotti dal blocco di sistemi e di servizi), il fenomeno del ransomware è dilagato proporzionalmente (e forse esponenzialmente) con la costante diffusione di internet nella quotidianità delle persone (si pensi anche solo al crescente interesse per l'IoT). Facendo leva sugli "utonti" (ma anche sugli utenti un po' più esperti) sfruttando tecniche di ingegneria sociale, gli effetti sono spesso devastanti, soprattutto perché sono in grado di paralizzare e mettere in crisi aziende ed enti governativi. Nel 2019 sono state rese note diverse città degli USA colpite da attacchi ransomware: la piccola città di Lake City in Florida ha scelto di pagare circa 400 mila dollari in bitcoin (valuta particolarmente apprezzata dai criminali in quanto difficilmente tracciabile) per sbloccare i propri servizi (ma senza riuscirci completamente, d'altronde non è garantito che trattare con un criminale abbia delle garanzie); Baltimora invece si è rifiutata di pagare il riscatto e si stima che abbia dovuto spendere circa 5 milioni di dollari per il ripristino dei sistemi.

A parte la spettacolarità dei casi, ci porta l'attenzione sul principale fattore utilizzato dai criminali per attaccare: l'utente. E' spesso un dipendente distratto, inesperto, o anche credulone a compromettere un intero sistema con un semplice click su un allegato di una mail. Oppure un tecnico responsabile della manutenzione della rete informatica, o un amministratore di rete, che tratta con leggerezza aggiornamenti del sistema operativo e dei software in uso rinviandoli, o sottovaluta possibili problematiche di sicurezza, quali la necessità di un firewall o la custodia delle password. E' sufficiente verificare quanto in aziende e uffici pubblici siano ancora impiegati sistemi basati su vecchie versioni di Windows che non hanno nemmeno più il supporto di Microsoft. Spesso

mancano inoltre delle serie procedure di backup e di Disaster Recovery.

GLOSSARIO

“Utonto”: in gergo informatico (detto luser in Inglese, contrazione di loser e user) è il tipico utente inesperto che utilizza un sistema, e che non si pone grosse preoccupazioni dei rischi che possono derivarne.

Ransomware: è un malware che punta a limitare l'accesso al dispositivo che infetta (ad esempio crittorgrafandone i dati tramite una chiave segreta per renderli illeggibili), richiedendo un riscatto da pagare all’utente finale. Proprio gli attacchi tramite crittografia sono particolarmente efficaci in quanto sono difficili da risolvere. Sono spesso veicolati tramite ingegneria sociale, sfruttando l’inesperienza degli utenti dei computer. Oppure, ed è il caso peggiore, sfruttano degli 0-days.

Disaster Recovery: è l'insieme delle procedure e delle tecnologie individuate e pianificate per ripristinare sistemi, dati e infrastrutture necessarie per il funzionamento di sistemi informatici e informativi, in caso di “disastri” dovuti a danni accidentali (incendi, rotture, guasti) e/o mirati (hackeraggi, intrusioni informatiche, furti, danneggiamenti dolosi).

APPROFONDIMENTI: OPEN SOURCE VS SOFTWARE LIBERO

Open Source: definisce un software il cui codice sorgente è pubblico. Si fonda sui seguenti principi:

- Libertà di redistribuzione del software (anche a pagamento);
- Libertà di consultare il codice sorgente;
- Necessità di approvazione per i prodotti derivati;
- Integrità del codice sorgente dell'autore;
- Nessuna discriminazione verso singoli o gruppi di persone;
- Nessuna discriminazione verso settori di applicazione (ad esempio limiti di uso in ambito accademico o non commerciale);
- La licenza deve essere distribuibile;
- La licenza non può essere specifica per un prodotto;
- La licenza non può estendersi ad altri software distribuiti contestualmente;
- La licenza deve essere tecnologicamente neutrale (ovvero indipendente dalle tecnologie che ne possano limitare la distribuzione).

Vantaggi dell'Open Source: un software può disporre di community che operano in maniera continuativa e produttiva sul codice. Le community offrono supporto, risorse e nuove funzionalità, anche solo a livello di idee. Aggiornamenti per bug e vulnerabilità possono

ricevere interventi tempestivi. Si può modificare il codice per risolvere problematiche specifiche per il proprio ambito lavorativo o di ricerca. Inoltre essendo il codice liberamente consultabile si è al sicuro sull'integrità dello stesso e sull'assenza ad esempio di malware, spyware o backdoor.

Vantaggi economici dell'Open Source: le aziende possono distribuire i costi di sviluppo tra di loro, anche tra competitor. Si riducono i costi per il supporto, nel software proprietario solo il produttore che ha accesso al codice sorgente lo può offrire. Aziende che investono in prodotti open source (ad esempio aziende che sviluppano distribuzioni Linux come Red Hat, con ricavi di 3 miliardi di dollari nel 2018) possono vendere servizi aggiuntivi come il supporto, la configurazione, la progettazione di infrastrutture, e l'implementazione di nuove funzionalità, che vengono poi rese di fatto pubbliche per tutti (e di conseguenza beneficiano successivamente del supporto della community). Oppure aziende investono nello sviluppo di un prodotto open source per detenere una posizione predominante nel mercato, ottenendo ricavi da royalties e altri prodotti veicolati tramite il software: ne è un esempio Mozilla Firefox, che nel 2017 ha guadagnato oltre 500 milioni di dollari grazie alla royalties pagate dagli investitori (spesso legate all'utilizzo del proprio motore di ricerca impostato come pagina iniziale).

Free Software (Software Libero): è un tipo di licenza che definisce un software che garantisce diverse libertà all'utilizzatore:

- Libertà di usare il programma senza impedimenti;

- Libertà di aiutare sé stesso studiando il codice disponibile e modificandolo in base alle proprie esigenze;
- Libertà di aiutare altri utenti, cioè la possibilità di distribuire copie del software;
- Libertà di pubblicare una versione modificata del software.

Da non confondersi con il software gratuito.

Unix: sistema operativo proprietario utilizzato principalmente in sistemi mainframe, sviluppato dai laboratori AT&T e Bell.

Linux: è il primo sistema operativo esempio di free software, realizzato in origine dalla Free Software Foundation, organizzazione senza scopo di lucro fondata da Richard Stallman negli anni Ottanta per eliminare le restrizioni sulla copia, redistribuzione, comprensione e modifica del software, con l'obiettivo iniziale di creare un'alternativa libera a Unix. Il kernel venne scritto dall'allora studente finlandese Linus Torvalds.

Kernel: è il software che gestisce l'accesso all'hardware ai processi in esecuzione su un computer.

Legge di Brooks: "aggiungere programmatori alla lavorazione di un software in ritardo, lo farà ritardare ancora di più". Spesso l'open source viene utilizzato per confutare tale legge, in un saggio famoso l'informatico Gerald Weinberg fece notare come laddove gli sviluppatori non si dimostrano territoriali rispetto al proprio codice, incoraggiando altre persone a collaborare per cercare bug e migliorarlo, i progetti software progrediscano molto più velocemente ed efficientemente.

APPROFONDIMENTI: CYBERWARFARE

“Strano gioco. L'unica mossa vincente è non giocare.”

CINEFORUM: “WARGAMES”

Regia di John Badham. Genere Fantascienza - USA, 1983.

Il film campione d’incassi nel lontano 1983 anticipa per la prima volta all’opinione pubblica il tema della cyberwarfare, o guerra cibernetica, ovvero gli effetti di una potenziale offensiva militare o criminale verso sistemi informatici, o semplicemente (ed è la trama del film) da parte di un ignaro hacker smanettone.

Il film mostra tecniche di hacking dell’epoca (che poi sono le prime della storia) quali il phreaking (ben nota a Kevin Mitnick), gli attacchi di forza bruta (per individuare sistemi cui connettersi telefonando col modem a numeri in sequenza), l’accesso a sistemi non protetti da autenticazione sicura (il protagonista che accede al registro elettronico della scuola e si cambia il voto), l’ingegneria sociale (con la quale risale alla password dell’account del creatore del sistema di sicurezza, con un accesso identificabile quasi come una backdoor) e la cyber deception (con la quale viene ingannato il sistema impedendo la “guerra termonucleare globale” semplicemente mandandolo in stallo giocando a tris con sé stesso).

Il Presidente degli Stati Uniti Ronald Reagan rimase colpito dal film e chiese ai suoi esperti se i sistemi informatici del governo fossero attaccabili in maniera così semplice (o fortuita). Fino dal 1967 esistevano rapporti tecnici sulle possibili vulnerabilità di tali sistemi, ma erano stati ignorati. Data la risposta affermativa da parte degli

esperti, Reagan fece emanare le prime leggi relative ai reati informatici (il Computer Fraud and Abuse Act) ed intensificare le misure di sicurezza attraverso una direttiva secretata (la NSDD-145) contro le minacce informatiche.

Nonostante atti e direttive, sempre a dimostrazione che l'uomo è sempre il punto debole di ogni sistema, si è recentemente scoperto che i codici di lancio dei missili Minuteman americani per il trasporto di testate nucleari (codici destinati all'utilizzo da parte del solo Presidente degli USA, praticamente la trama di Wargames) sono stati per circa 20 anni impostati con una sequenza di otto zeri 00000000, con la motivazione di renderli banali per ridurre il ritardo nel lancio di un missile durante una crisi militare, nel caso in cui il Presidente non ricordi la password.

GLOSSARIO

Cyber Deception: è l'insieme delle tecniche e delle strategie fondate sull'inganno di potenziali attaccanti a un sistema. Si fonda tendenzialmente sul depistaggio, drenaggio di risorse (ad esempio con false informazioni e sistemi esca, detti honeypot), sull'effetto Farewall (si fa dubitare all'avversario dell'integrità dei dati trafugati, il nome è legato a un'operazione della CIA contro il KGB negli anni '80), sull'analisi delle modalità di operazione e di reazione dell'avversario (una volta identificato si prova ad attaccarlo direttamente, per apprendere nuove informazioni), e sulla identificazione attraverso mine e "trappole".

APPROFONDIMENTI: LEGALITA' E DEEP WEB

CINEFORUM - "DEEP WEB"

Regia di Alex Winter. Genere Documentario - USA, 2016.

Deep Web racconta l'arresto nel 2013 di Ross Ulbricht, all'epoca 29 anni, giovane insospettabile, laureato in Fisica e accusato di essere conosciuto in rete come "Dread Pirate Roberts". Si basa su interviste esclusive ai genitori di Ulbricht, divenuti dei pubblici sostenitori dei diritti digitali e del giusto processo. Ulbricht fond Silk Road, famigerato black market online meglio conosciuto per il traffico di droghe, farmaci, armi, dati di account bancari, materiale pedopornografico, servizi criminali su commissione. Nel portale gli utenti si registravano (anonimamente ovviamente) utilizzando la piattaforma per vendere e acquistare, come avviene su eBay o Amazon. Silk Road guadagnava una percentuale sulle transazioni, ma teoricamente non vendeva nulla direttamente, erano gli utenti. Proprio come eBay. Il documentario descrive e approfondisce le indagini che hanno portato all'arresto del giovane, (successivamente condannato all'ergastolo nel 2017, sentenza ritenuta da molti esagerata, ma a sua volta necessaria ed esemplare da parte del governo degli USA per dare un forte segnale a chi pensa di sfruttare l'anonimato del Dark Web per scopi criminali), ed esplora con interviste esclusive a esperti e addetti del Deep Web e del sistema dei Bitcoin aspetti etici e legali del futuro della rete, e della libertà e responsabilità degli individui sul web.

Un discorso fondamentale e delicato è legato alla facilità con cui chiunque potesse in completo anonimato avvicinarsi alle droghe tramite il Dark Web (di fatto dando possibilità anche ai più

insospettabili o timorosi di spingersi oltre i propri limiti), ma di fatto in un ambiente più sicuro per i consumatori rispetto alla strada (rendendo il degrado e lo spaccio per strada meno diffuso). In tutto questo, ci si domanda quale sia effettivamente la responsabilità di Ulbricht, costretto a pagare da solo con la giustizia per tutti i reati commessi tramite la sua piattaforma, lasciando di fatto impuniti gli utilizzatori.

"Ho avuto la mia giovinezza, dovete prendervi i miei anni di mezzo, ma per favore lasciatemi la vecchiaia." (Da una lettera di Ross Ulbricht al giudice)

"Visto quello che è successo, avrei dovuto avere più paura di internet. Internet rende tutto troppo facile. Silk Road ha reso sicuro comprare e vendere droga, perché fornisce una piattaforma che sfrutta i deboli e i vulnerabili." (Da una lettera di una madre che ha perso il figlio per overdose dopo aver comprato droga sul portale.)

GLOSSARIO

Surface Web: la parte del web indicizzata dai motori di ricerca. Spesso si rappresenta con la metafora dell'"iceberg", in quanto noi vediamo solo la parte emersa dello stesso (il surface web) e non quello che c'è sotto (che è molto più grande dell'emerso).

Deep Web: la parte del web non indicizzata dai motori di ricerca. Comprende siti non ancora indicizzati, siti privati o "oscurati" dai motori di ricerca.

Dark Web: è una parte del Deep Web sviluppata su reti particolari, accessibili con sistemi dedicati (ad esempio con il brower TOR). Con

essa in genere si identifica quella parte del Deep Web destinata a fini criminali.

TOR: un browser derivato da Mozilla che ha come obiettivo la navigazione realmente anonima e non tracciabile su internet attraverso un sistema di **onion routing**, una tecnica per anonimizzare la comunicazione attraverso l'incapsulamento crittografico a strati dei messaggi scambiati. I dati transitano attraverso dei cosiddetti **onion router**, che si occupano di invidiare la destinazione successiva. Ogni nodo conosce solamente la posizione del nodo precedente e successivo.

BitCoin: è una criptovaluta il cui valore è determinato da un meccanismo di domanda e offerta. Si basa su un database distribuito tra i nodi della rete in cui viene tenuta traccia delle transazioni e della loro integrità (detto **blockchain**), con impiego di tecniche crittografiche complesse per la generazione di nuove monete e la definizione della proprietà delle monete stesse (tramite chiave privata utilizzata come firma digitale per il proprio portafoglio). Le transazioni in attesa vengono incluse nella blockchain attraverso un processo detto di **mining**, che mantiene un ordine cronologico nella blockchain, protegge la neutralità della rete e consente a diversi computer di concordare sullo stato del sistema. Le regole crittografiche impediscono che qualunque blocco precedente venga modificato, perché ci invaliderebbe tutti i blocchi successivi. In questo modo nessuno può controllare cosa è incluso nella blockchain o sostituire parti della blockchain in modo da riottenere quanto speso. Consentendo il trasferimento anonimo, è particolarmente impiegata per fini criminali nel dark web. La rete ha una struttura P2P.

APPROFONDIMENTO: PROFILAZIONE E BIG DATA

LA STORIA

Cambridge Analytica è una società nata nel 2013 specializzata nell'analisi di moli di dati raccolti dai social network, per la realizzazione di campagne social di condizionamento psicologico degli utenti. Lo scandalo suscitato dalle rivelazioni di ex dipendenti sullo sfruttamento inconsapevole dei dati (meglio, dei metadati) di milioni di utenti dei social (in particolare di Facebook) e sugli effetti delle campagne profilate attuate ha portato alla chiusura della società nel 2018 e una multa di 5 miliardi di Dollari a Facebook (che molti hanno valutato come pochi, dato che sono circa 1 decimo del fatturato annuo della società, rispetto alla gravità di quanto successo).

La società sfruttava i big data e tecniche psicometriche per profilare individui, attraverso l'utilizzo di algoritmi di analisi dei dati raccolti combinati con tecniche di "data mining" (estrazione di informazioni da grandi quantità di dati). I dati vengono ottenuti da tutto ci che un utente fa sulle piattaforme, e questi dati sono tantissimi e talmente variegati da consentire di definire in maniera molto accurata il comportamento psicologico e le attitudini delle persone. Ad esempio venivano raccolte (da loro, ma vengono tuttora raccolti probabilmente da altre società) informazioni sui like, sulle reazioni a determinati articoli e immagini, a "storie", non solo sui contenuti, ma anche sugli orari, sulla localizzazione geografica, sulle etnie delle persone rappresentate nei contenuti commentati, sul tipo di commenti (positivi o negativi). Inoltre si possono raccogliere

informazioni tramite contenuti mirati da mostrare agli individui, con campagne social sviluppate ad hoc per vedere come il pubblico reagisce. Capita spesso di trovare inserzioni sponsorizzate di articoli, foto, pagine e simili sui social che non sempre “capiamo”, nel senso che non si tratta di classica pubblicità di un prodotto, ma magari di pagine o notizie “che potrebbero interessarci”, e non ne capiamo appunto il motivo. E anche fake news appositamente costruite. La reazione a cliccare , commentare, mettere un mi piace, e l’incrocio di questi dati con milioni di altri dati consente di far capire a una macchina tramite opportuni algoritmi cosa pensiamo.

Riguardo a Facebook, lo scandalo principale è stato che sfruttando una “falla” nel sistema la società ha avuto accesso ai dati non solo degli utenti che lo consentivano (ci che succede quando ci registriamo su qualche sito, app o gioco utilizzando “Connettiti tramite Facebook” e cliccando sul tipico “Autorizzi questo sito/app/ecc.. ad accedere ai tuoi dati bla bla… tranquillo non scriveremo nulla sulla tua bacheca non invieremo mai spam a te o ai tuoi amici (ma avremo accesso a tutto quello che fai sul social)”) ma anche a quello delle loro cerchie di amici (funzionalità ora non più presente su Facebook). Falla che non era un bug, ma una “leggerezza” di autorizzazioni, che consentiva a Cambridge Analytica di accedere a questi dati senza violare le condizioni di servizio di Facebook. In questo modo ha potuto raccogliere i dati relativi a oltre 80 milioni di utenti. Sebbene le persone siano più preoccupate che qualcuno conosca la propria mail o indirizzo di residenza, non è sufficientemente sensibilizzata a preoccuparsi che qualcuno raccolga dati su cosa le piace o meno, o su come commenta un certo contenuto.

Oltre a questi dati, la società comprava ulteriori dati da società apposite, dette broker, specializzate nel raccoglierli e venderli. Con tutta questa mole di dati ha sviluppato un sistema di microtargeting comportamentale, ovvero inviare contenuti con elevata personalizzazione individuale. Si lavora sulle reazioni e il comportamento dell'utente, e non sulle preferenze e i gusti personali. Con queste informazioni la società era in grado di fornire servizi di comunicazione strategica particolarmente apprezzati (ed efficaci) per campagne elettorali.

Travolta dalla fuga di informazioni, emersero dettagli del proprio coinvolgimento (e quindi utilizzo del microtargeting) nelle campagne che portarono al successo della Brexit nel Regno Unito e della vittoria di Trump alle presidenziali degli USA (come casi più eclatanti).

Nel 1964 il sociologo Marshall McLuhan pubblic il saggio "Understanding Media: The Extensions of Man", spesso sintetizzato nella sentenza cardine "the medium is the message" ("il mezzo è il messaggio"), anticipando di fatto ci che sarebbe diventato oggi Internet. MacLuhan focalizzava l'attenzione sulla necessità di studiare non solo i contenuti, ma anche le modalità con le quali essi vengono trasmessi, ritenendo i media di comunicazione come tecnologie non neutrali, ma strutture complesse in grado di influenzare i destinatari. Questa capacità dei media moderni di influenzare l'opinione pubblica attraverso la profilazione degli utenti, derivante dall'analisi di grandi quantità di dati e metadati, spesso, come visto, raccolti violando la privacy degli utenti, mostra quanto importante sia una maggiore conoscenza delle nuove tecnologie da parte di chi utilizza la Rete, e da parte di chi ne

propone, favorisce e, talvolta, impone un utilizzo sempre maggiore e integrato nelle nostre attività quotidiane.

CINEFORUM: " THE GREAT HACK"

Regia di Karim Amer e Jehane Noujaim - Genere: Documentario - USA 2019 - Esclusiva Netflix.

Il documentario ricostruisce accuratamente la storia di Cambridge Analytica e approfondisce le tecniche utilizzate; si focalizza in particolare sullo scandalo con Facebook, attraverso interviste e ricostruzioni seguendo da vicino il "dietro le quinte" del processo a Facebook attraverso la whistleblowler Brittany Keiser (ex Business Director di Cambridge Analytica), e intervistando Julian Wheatland (ex amministratore delegato di Cambridge Analytica), con il contributo del professore universitario della Parsons School of Design David Carroll (il primo a portare la società in tribunale chiedendole accesso ai propri dati) e della giornalista del Guardian Carole Cadwal (autrice dello scoop). Riguardo al primo whistleblowler a rendere pubblico lo scandalo, Christopher Wylie, sono forniti solo video di repertorio e non interviste dirette.

GLOSSARIO

Metadati: informazioni che descrivono altre informazioni. Servono ad esempio a migliorare e ottimizzare l'accesso a tali informazioni all'interno di un sistema informatico. Nei sistemi di messaggistica ad esempio i metadati possono contenere informazioni sull'ora di invio del messaggio, sul luogo, se è stato consegnato o visto dal destinatario, ecc… In un documento di testo possono riguardare

l’autore, il programma con cui è stato scritto (Word, Open Office), l’ora a cui è stato salvato, revisionato, ecc…

Fake News: informazioni inventate o distorte, appositamente rielaborate per renderle virali e nel frattempo generare opportune reazioni.

Big Data: grande quantità di dati digitali raccolti da dispositivi informatici, che richiedono metodi analitici e di elaborazione avanzati per poter estrarre informazioni utili a causa dell'eterogeneità degli stessi.

APPUNTI DI LABORATORIO

"Photo of a hacker working on a computer at a desk with many hi-tech and advance pcs and equiptment, trying to hack network" di 紅色死神 è concesso con licenza CC BY-NC-SA 2.0.

Qui sono raccolti dei brevi appunti su alcuni programmi utilizzati per le esperienze di laboratorio. Dato che molti riguardano attacchi informatici, è bene effettuare tutto tramite delle macchine virtuali, e ricordarsi che il **Codice Penale** punisce i reati informatici (a partire dalla legge 547 del 1993) tra i quali:

- frode informatica;
- accesso, detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici;

- diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare sistemi informatici e telematici.

Pertanto ricorda che quanto indicato nella Guida segue un preciso scopo:

IMPARIAMO A DIFENDERE

STUDIANDO COME SI ATTACCA

N.B.:

- come indirizzo IP di esempio sarà spesso indicato un IP privato generico 192.168.1.42, andrà ovviamente sostituito con l'indirizzo IP effettivo della macchina in uso o bersaglio;
- il simbolo # indica un comando da inserire nel terminale o nel software cui si fa riferimento, se non indicato diversamente si intendono da eseguire su macchina Linux;

VirtualBox: è un software open source di proprietà di Oracle per l'esecuzione di VM. Per gli esperimenti di laboratorio è particolarmente importante impostare la configurazione della scheda di rete virtuale, a seconda della modalità di utilizzo: NAT (il traffico viene mascherato come se provenisse dalla macchina host, creando una subnet separata) oppure Bridged (la VM ottiene un proprio IP).

netstat:

fornisce statistiche sulle attività di rete, e informazioni su porte e indirizzi su cui sono attive connessioni TCP e UDP. Funziona su Windows e Linux.

Comandi utili:

 # netstat : elenca tutte le connessioni attive

 # netstat -a :elenca le porte aperte

 # netstat -e :statistica interfacce

 # netstat -r :elenca le tabelle di routing

 # netstat -p proto

dove *proto* può essere ad esempio IP, IPv6, TCP, ICMP, UDP (e altri), indica le connessioni attive relative al protocollo specificato.

ifconfig:

su Linux fornisce informazioni sulla propria connessione IP. Con il parametro -a fornisce informazioni complete su tutte le interfacce di rete.

 # ifconfig

ipconfig:

su Windows fornisce informazioni sulla propria connessione IP.

Uso dei parametri:

mostrare informazioni complete su tutte le interfacce di rete, incluso l'**identificatore di interfaccia** (*id_interfaccia)* che serve per altri comandi**:**

 # ipconfig /all

mostrare informazioni sulla cache DNS corrente:

 # ipconfig/displaydns

svuotare la cache DNS:

 # ipconfig/flushdns

rilasciare l'IP dell'interfaccia specificata (l'identificatore di interfaccia va individuato con il precedente parametro /all)

 # ipconfig/release id_interfaccia

rinnovare l'IP dell'interfaccia specificata (l'identificatore di interfaccia va individuato con /all)

 # ipconfig/renew id_interfaccia

tracert (su Windows) e **traceroute** (su Linux):

mostrano tutti i salti che un pacchetto effettua per arrivare a destinazione. Utilizzando il parametro -d non vengono risolti i nomi degli host.

 # tracert 192.168.1.42 > c:/output.txt

Nell'output i valori in ms riguardano il tempo intercorso tra la spedizione e la ricezione di un pacchetto (se il tempo è maggiore di 3 secondi viene mostrato un asterisco). Di default vengono effettuati

al massimo 30 salti, il calcolo viene effettuato inviando dei pacchetti ICMP e attendendo la risposta dai gateway attraversati (ICMP TIME_EXCEEDED), ogni pacchetto ha un MAX_TTL (**time to live**) di 1 hop inizialmente, e successivamente fino a raggiungere 30 (a meno che non sia diversamente impostato dall'utente).

route:

su Linux mostra le tabelle di routing correnti, su Windows va utilizzato con il parametro PRINT. Serve anche a modificare le tabelle di routing manualmente.

 # route

ping:

viene utilizzato per misurare il tempo in ms impiegato da un pacchetto ICMP a raggiungere una destinazione di rete.

ping 192.168.1.42

nmap:

su Linux è un potente tool di scansione della rete.

Comandi utili:

scansione di un host, senza completare il 3-way handshake TCP:

 # nmap -sS 192.168.1.42

scansione completa:

 # nmap -sV 192.168.1.42

output su file:

 # nmap -sV -oN file.txt 192.168.1.42

scansione su porta:

 # nmap -sS -p 8080 192.168.1.42

scansione tutte le porte:

 # nmap -sS -p 192.168.1.42

scansione UDP:

 # nmap -sU -r -v 192.168.1.42

scansione sistema operativo:

 # nmap -O 192.168.1.42

scansione versione servizi:

 # nmap -sV 192.168.1.42

scansione “common ports” :

 # nmap -F 192.168.1.42

scansione tramite ARP:

 # nmap -PR 192.168.1.42

scansione tramite PING:

 # nmap -sP 192.168.1.42

scansione senza PING:

 # nmap -PN 192.168.1.42

arp-scan:

esegue una scansione ARP della rete.

 # arp-scan -interface=eth0 192.168.1.0/24

specificando interfaccia e indirizzo di rete con subnet su cui eseguire l scansione

arp: mostra la tabella arp corrente.

 # arp -a

whois: fornisce informazioni dal servizio WhoIS su un dominio internet.

 # whois www.simonezanella.it

nslookup:

fornisce informazioni sui record NS di un dominio internet.

 # nslookup

attiva la modalità di uso a "console"

 # www.simonezanella.it

mostra le informazioni sul dominio www.simonezanella.it

 # set type=mx

imposta come tipo di ricerca solo i record di posta MX

 # set type=ns

imposta come tipo di ricerca solo i record NS

 # set type=any

imposta come tipo di ricerca tutti i record

Wordlist: è un file contenente username, password e/o altro da utilizzare per provare attacchi a dizionario.

John the Ripper:

è un tool per il crack delle password. Su Linux si può provare ad esempio ad accedere al file di sistema in cui sono memorizzate le associazioni tra username e hashing della password, che si trovano tipicamente in */etc/passwd* che possono essere rivelate utilizzando il comando:

 # unshadow /etc/passwd /etc/shadow > hashfile

dove *hashfile* è il nome che vogliamo dare al file da generare contenente gli hash visibili.

Per quanto riguarda John The Ripper ecco alcuni comandi utili:

 # john hashfile

prova a crackare le password contenute nel file "hashfile"

 # john --show hashfile

prova a crackare le password e mostra il risultato a terminale

 # john --wordlist=/usr/share/password.lst --rules hashfile

usa un attacco a dizionario tramite la wordlist indicata (nell'esempio il file password.lst)

Rainbow Table: è un file contenente gli hashing di migliaia di parole, stringhe, numeri e loro combinazioni, vengono utilizzati risalire alle password in chiaro. Esistono diversi servizi online per testare la sicurezza delle proprie password tramite rainbow tables.

Arpspoof:

è un software per effettuare un attacco di tipo **arp poisoning**, utilizzando delle *Arp Reply* falsificate, sfruttando il fatto che non vengono verificate dal protocollo. Il computer che attacca fa credere al server di essere il client, e al client di essere il server di una comunicazione, tramite un attacco di tipo MITM *"Main In The Middle"*. Come strumento fa parte del software **dsniff** e si installa tramite il comando:

 # sudo apt install dsniff

Procedura per avviare un MITM:

1. individuare una macchina bersaglio in rete, individuando il suo indirizzo IP. Individuare anche il gateway di rete utilizzato con il comando:

   # ip route show

2. sulla macchina attaccante occorre abilitare la modalità promiscua sull'interfaccia di rete in uso (ad esempio *eth0*):

   # ifconfig eth0 promisc

   # sysctl -w net.ipv4.ip_forward=1

3. sulla macchina attaccante lanciare in 2 shell separate i comandi:

 # arpspoof -i eth0 -t IP_gateway IP_bersaglio

sulla prima shell

 # arpspoof -i eth0 -t IP_bersaglio IP_gateway

sull'altra shell.

Si può ora verificare sulla macchina bersaglio ad esempio come è cambiata la Arp Table. oppure usare dei tool di **sniffing** (analisi di rete) come Wireshark effettuando una connessione in chiaro via browser a un sito web (si possono cercare dal motore di ricerca utilizzando il filtro *inurl: http://*) andando a ricercare il traffico, oppure un software come driftnet che intercetta ogni immagine visualizzata nella navigazione dell'utente:

 # driftnet -i eth0

Terminato l'attacco, chiudere i vari terminali e disabilitare la modalità promiscua con il comando:

 # sysctl -w net.ipv4.ip_forward=0

Wireshark

è un packet sniffer open source utilizzato per analizzare il traffico di rete. Presenta vari tools per l'ispezione dei pacchetti e dei protocolli.

Configurazioni utili

Andare nella voce di menu: Preferences -> Appearance -> Columns

Cliccare su + per aggiungere filtri, poi cliccare su "Titolo" e cambiare il nome, poi su "Tipo" e selezionare il filtro desiderato. Per le analisi sono utili SRC PORT e DST PORT per vedere le porte sorgente e

destinazione dei pacchetti. Aggiungere inoltre come tipo CUSTOM il filtro:

http.host || http.request || tls.handshake.extensions_server_name

per filtrare sugli host consultati tramite una connessione http o https.

Andare nella voce di menu:

Visualizza -> Formato di visualizzazione del tempo

per cambiare con il formato "data e ora" del pacchetto la visualizzazione di default, che indica i secondi trascorsi da inizio cattura.

Esempi di ricerca e filtraggio

Collegarsi via browser, con Wiresharl avviato, a un qualsiasi sito web con una connessione in chiaro http, scaricare un file (ad esempio un file di testo o PDF), terminare la cattura e su Wireshark filtrare con

 # http.request

eventualmente specificando il sito:

 # http contains "nomedelsito"

selezionare quindi i pacchetti in cui compare un comando GET di http nel campo "info", poi andare nel menu *File->Esporta Oggetti->HTTP* e salvare il contenuto del file, che corrisponderà a quello scaricato dal browser.

Si può inoltre usare la funzionalità **SEGUI FLUSSO TCP** o SEGUI FLUSSO HTTP (a seconda ovviamente dei pacchetti in esame) per

ricostruire tutti i pacchetti catturati legati a una determinata connessione.

Filtrare contenuti **SMTP** (mail inviate):

 # stmp.data.fragment

con il menu *File->Esporta Oggetti->IMF* (Internet Message Format) è possibile esportare eventuali mail catturate.

Per ricercare quali **siti** sono stati visitati sia in HTTP che in HTTPS applicare il filtro:

 # http.request or ssl.handshake.type == 1

oppure per ricercare una specifica *"stringa"*:

 # http.host contains "stringa"

o anche:

 # ssl contains "nomedelsito"

Per cercare **informazioni sugli host** si può filtrare ad esempio il traffico DHCP per trovare informazioni sugli host della rete, attraverso il filtro:

 # bootp

oppure su precedenti versioni di Wireshark

#dhcp

selezionare un pacchetto DHCP REQUEST, espandere la scheda "Bootstrap Protocol," e nelle "Option" si possono trovare il Client Identifier (che contiene il Mac Address) e l'Host Name.

Volendo applicare un filtro nei vari contenuti delle “option” si può usare:

 # bootp.option.hostname contains “nome-host-da-cercare“

Filtraggio di **indirizzi IP**:

ip.addr==192.168.1.42

per combinare filtri si utilizzano gli operatori logici, ad esempio l’operatore “and”:

 # ip.addr==192.168.1.42 and ssl

 # ip.addr==192.168.1.42 and tcp.port==443

filtrare connessioni a siti web per individuare le URL, anche per connessioni criptate;

 # http.request || tls.handshake.extensions_server_name

filtra gli URI che contengono una “**stringa**” definita, ad esempio una estensione di file o parte del dominio internet:

 # http.request.uri contains “stringa"

filtrare pacchetti relativi a **mail**:

 # ip contains mail

filtrare pacchetti che contengono al loro interno la dicitura *“This program cannot be run in DOS mode.”* presente in file eseguibili, se si pensa che sia stato scaricato qualche **malware**:

 # ip contains "This program”

trovare il **nome utente** su una rete con autenticazione Kerberos, all’interno del campo *“cname”* del pacchetto:

 # kerberos.CNameString and !(kerberos.CNameString contains $) //

filtrare pacchetti che contengono dei **POST** in http:

 # http contains post

Alcuni siti utili:

- any.run: sito tramite il quale si possono eseguire su vari sistemi operativi in modalità sandbox file sospetti e malware per verificarne l'azione.
- exploit-db.com: database che raccoglie vulnerabilità e exploit noti.
- oldversion.com: sito da cui è possibile ricavare delle vecchie versioni di software, per testare exploit e vulnerabilità.
- osboxes.org: sito che raccoglie delle VM Linux (e non solo) già pronte per l'uso con Virtual Box o VMWare.
- virustotal.com: repository per l'analisi di file potenzialmente infetti.
- packettotal.com: repository per l'analisi di file *pcap* di Wireshark alla ricerca di malware e infezioni.
- malware-traffic-analysis.net: una miniera di informazioni, tutorial ed esercizi per effettuare analisi di attività di malware sulle reti con Wireshark.
- shodan.io: motore di ricerca dedicato ai dispositivi collegati a Internet.