PROF. ING. SIMONE ZANELLA

GUIDA DI SISTEMI E RETI

PER AUTOSTOPPISTI

DON’T PANIC

INTRODUZIONE

Lontano, nei dimenticati spazi non segnati nelle carte geografiche dell'estremo limite della Spirale Ovest della Galassia, c'è un piccolo e insignificante sole giallo. A orbitare intorno a esso, alla distanza di centoquarantanove milioni di chilometri, c'è un piccolo, trascurabilissimo pianeta azzurro-verde, le cui forme di vita, discendenti dalle scimmie, sono così incredibilmente primitive che credono ancora che gli orologi da polso digitali siano un'ottima invenzione.

Così inizia "*Guida galattica per gli autostoppisti*", un romanzo di fantascienza umoristica scritto da Douglas Adams nel 1979, anno importante, perché è quello di nascita dell'autore di questa "Guida di Sistemi e Reti per Autostoppisti".

Se avete bisogno di qualcosa mentre studiate Sistemi e Reti, in particolare in vista dell'Esame di Stato, questa Guida è il vostro riferimento. Dentro trovate:

- appunti sintetici sugli argomenti principali di Sistemi e Reti (e un po' di Telecomunicazioni);
- brevi definizioni e descrizioni degli argomenti e dei termini informatici da sapere;
- appunti (molto) veloci di esercitazioni di laboratorio;
- qualche appunto su argomenti approfonditi durante il corso e non presenti sul libro di testo;
- materiali di esempio per l'avvio del Colloquio Orale;
- appunti su argomenti di cultura informatica affrontati durante il triennio (documentari , film, ecc…) utili per il colloquio all'Esame

Non sostituisce il libro, gli appunti e tutto il resto del materiale fornito dai docenti, ovviamente, ma magari può essere un valido aiuto quando il tempo stringe e l'Esame si avvicina. Invece se siete ancora indecisi su cosa fare del vostro futuro dopo il Diploma, perchè siete in cerca della risposta alla "*Domanda Fondamentale sulla Vita, l'Universo e Tutto Quanto*", allora dovete consultare l'altra Guida, quella di Adams, per scoprire che la risposta è semplice: **42**.

BUON RIPASSO, NON DIMENTICATE L'ASCIUGAMANO E SOPRATTUTTO… NON FATEVI PRENDERE DAL PANICO!

QUALCOSA SULLE RETI

Topologie di rete: la topologia fisica descrive la struttura fisica delle rete (livelli 1 e 2) ovvero apparati utilizzati, collocazione, tipi di canali trasmissivi, interfacce; la topologia logica descrive le configurazioni degli apparati, l'indirizzamento IP, classi di indirizzi utilizzate, nomi degli host.

Le topologie fisiche classiche sono quelle a stella, a maglia ("mesh"), ad anello, a bus, ad albero.

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 tipicamente fino a 16Gbit/s.

Protocol Data Unit (PDU): unità d'informazione o pacchetto scambiata tra due strati in un protocollo di comunicazione di un'architettura di rete a strati. Nel TCP/IP si chiama datagramma.

Pacchetto: sequenza di dati trasmessi su una rete. 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 (Protocol Data Unit) che vengono trasferite per comunicare insieme ai messaggi di controllo, formate da un header (che contiene informazioni di controllo) e un payload (che contiene i dati).

Modello ISO/OSI: è un modello per le architetture di protocolli (Open System Interconnection), suddiviso in 7 strati funzionali che comunicano scambiandosi PDU (application, presentation, session, transport, network, data link, physical).

Il modello definisce una comunicazione per livelli: dati due nodi A e B, il livello n del nodo A può scambiare informazioni col livello n del nodo B, ma non con gli altri utilizzando un "**SAP**" (Service Access Point) del livello inferiore, incapsulando i messaggi di livello n in messaggi del livello n-1.

IEEE 802: è una famiglia di standard sviluppato dall'IEEE 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 (controllo dell'accesso al mezzo fisico) che identifica con un indirizzo univoco le stazioni di rete, formato da 6 ottetti (48 bit).

Ethernet: è lo standard 802.3 per la realizzazione delle LAN, noto anche come CSMA/CD.

PoE: Power over Ethernet, consente l'alimentazione di un apparato tramite cablaggio di rete. E' particolarmente utilizzata per i dispositivi impiegati nelle reti WiFi.[1923]

Fast Ethernet 100BASE-TX e **Gigabit Ethernet 1000BASE-TX:** tecnologie di rete utilizzate per i cablaggi più diffusi.

Dominio di broadcast: insieme di host in una rete che possono comunicare a livello.

Dominio di collisione: insieme di host che accedono allo stesso mezzo trasmissivo su cui vogliono trasmettere 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 WiFi.

Suite TCP/IP: definisce gli standard degli strati funzionali application, transport e internet (network).

Incapsulamento: è la procedura con cui un dato generato da un processo utente attraversa i vari strati del modello ISO/OSI.

Unicast: comunicazione uno a uno.

Multicast: comunicazione uno a molti.

Broadcast: comunicazione uno a tutti.

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 e una al HOST-ID.

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: inizia con 0, subnet: /8 blocchi: da 0 a 127
- 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 particolari e riservati: 0.0.0.0 (indirizzo IP non specificato, identifica "questo host"), indirizzo di host con tutti i bit a 0 (X.X.X.0) indica la rete corrente, da 127.0.0.1 a 127.255.255.255 (loopback, risponde il computer su cui si sta lavorando), 255.255.255.255 (broadcast a tutti gli indirizzi di rete corrente).

Indirizzi IPv4 non validi: sono quelli con NET-ID o HOST-ID costituiti da tutti bit a 0 o a 1, che non possono essere assegnati a un host, o riservati.

Reti private: non sono connesse direttamente a Internet, possono utilizzare i 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 formati da 128 bit, suddivisi in 8 campi da 16 bit separati da due-punti, espressi in esadecimale (es. hhhh:0000:0000:hhh0:0000:0000:0000:0000), 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. (es. basato sul precedente: hhhh::hhh0:0:0:0:0).

MAC Address: 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, separati 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) [1920]. L'indirizzo FF:FF:FF:FF:FF:FF viene utilizzato per il broadcast. Alcuni indirizzi sono riservati secondo le specifiche dettate dall'ente IANA.

IP vs MAC: il primo indica come un host è connesso a una rete, il secondo identifica l'host fisico.

Hub: 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: 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 (pertanto lo rende più efficiente e al tempo stesso più vulnerabile rispetto a un hub). Consente di ridurre drasticamente le collisioni, tuttavia richiede il collegamento di ogni singolo nodo allo switch, oppure i nodi ad hub connessi allo switch. 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).

Bridge: 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). Generalmente collega tra loro due o più segmenti di una rete dello stesso tipo oppure due o più reti di tipo diverso, regolando il passaggio delle trame da una all'altra sulla base dell'indirizzo di destinazione contenuto in queste ultime.

Differenza tra bridge e switch: 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.

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: dispositivo di livello 3, istrada 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 invia i dati al gateway predefinito. E' dotato di firmware. Tipicamente ha 4 porte.

Uplink: è una porta usata per trasmettere dati da un host ad uno switch, un router, un hub o una dorsale, oppure per collegare tra loro hub tramite cavi cross.

Segmento di rete: porzione di rete separata dalle altre da un dispositivo di rete (hub, switch, bridge).

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): permette di accedere a una rete in modalità wireless, generalmente tramite onde radio. 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: standard utilizzato negli edifici adibiti a uffici per la realizzazione degli impianti di rete, basati generalmente su cavi di categoria 5 o superiore e connettori RJ-45, con possibilità di uso della fibra ottica per le dorsali di collegamento. I cavi hanno una lunghezza massima di 100 metri. Per ogni postazione da servire, vengono posati uno o più cavi in apposite canalizzazioni nelle pareti, nei controsoffitti o nei pavimenti dell'edificio, fino a raggiungere un armadio di distribuzione di piano (**Floor Distributor, FD,** ovvero cablaggio orizzontale) noto anche come **rack**. Gli FD vengono collegati a un armadio di edificio (**Building Distributor, BD**), tramite cavi in rame o in fibra ottica (cablaggio verticale). Allo stesso modo, i diversi edifici di un cosiddetto "campus" sono collegati a un **Campus Distributor, CD**. I locali che ospitano gli armadi di distribuzione dovrebbero avere caratteristiche adeguate per alimentazione elettrica (meglio se protetta da un gruppo di continuità - UPS), condizionamento, controllo d'accesso del personale. Si distingue tra cablaggio verticale (cablaggio di edificio) e orizzontale (di piano).

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).

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) o un elemento terminale come un client o un server.

Host: nodo terminale della rete. Significa “ospite”, può essere un client o un server.

QUALCOSA SU PROTOCOLLI E SERVIZI DI RETE

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 tra sistema operativo e programmi applicativi.

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.

DNS: Domain Name System, serve a tradurre i nomi di dominio (www.google.it) in indirizzi IP. Il DNS è organizzato 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 (.it) o un'organizzazione (.com, 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 sito web, smtp.google.it per il server per la posta in uscita, ecc…)

URI: Uniform Resource Identifier, identifica una risorsa in maniera univoca su internet. La prima parte indica il protocollo da utilizzare. Esempio http://www.google.it/maps/

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

FTP: File Trasnfer Protocol, protocollo per il trasferimento di file. E' basato su TCP e ha una architettura client/server. Utilizza la porta 21 per creare una connessione di controllo, in seguito viene aperta una porta per lo scambio dei dati con il client (in modalità attiva viene scelta dal client, in modalità passiva viene scelta casualmente dal server). Non prevede cifratura.

POP3: Post Office Protocol è un protocollo per la consultazione di posta elettronica, utilizzato per ricevere email da un server remoto in un client locale per leggerli 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 il browser), senza richiedere lo scaricamento dei messaggi. La posta viene consultata direttamente sul server. Utilizza la porta 143 (993 in modalità sicura tramite SSL/TLS, di base non fornisce cifratura).

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, di base non fornisce cifratura).

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.

QUALCOSA SU SOTTORETI, ROUTING E VLAN

Subnetting: tecnica che consente di suddividere una rete in sottoreti attraverso l'uso di una subnet mask.

Subnet Mask: è formata da 4 ottetti di bit (come un indirizzo IP), la maschera di sottorete è composta da bit a 1 per il Net-ID e per la sottorete di appartenenza, e a 0 per la parte Host-ID, e viarp -ene messa in AND bit a bit con l'indirizzo IP del destinatario di un pacchetto, consentendo di "estrarre" la sottorete di appartenenza. Per la determinazione della subnet mask vengono utilizzati i bit più significativi dell'Host-ID dell'indirizzo IP.

- *Esempio: indirizzo di rete 192.168.1.0. Essendo di classe C sono utilizzabili 8 bit per l'Host-ID (256 host). Scegliendo il 1° bit dell'Host-ID per la subnet mask si ottiene (in binario):*
  11111111. 11111111. 11111111. 10000000 ovvero 255.255.255.128
  utilizzando 1 bit per la subnet si possono realizzare 2 ^ 1=2 sottoreti, ognuna di 2 ^ 7=128 host (-2 host ciascuna tolti gli indirizzi di rete e broadcast).

- *Esempio: indirizzo di rete 128.1.1.0. Essendo di classe B sono utilizzabili 16 bit per l'Host-ID (65.536 host). Scegliendo i primi 4 bit dell'Host-ID per la subnet mask si ottiene (in binario):*
  11111111. 11111111. 11110000. 00000000 ovvero 255.255.240.0
  utilizzando 4 bit per la subnet si possono realizzare 2 ^ 4=16 sottoreti, ognuna di 2 ^ 12=4096 host (-2 host ciascuna tolti gli indirizzi di rete e broadcast).

VLSM: tecnica che consente di utilizzare subnet di lunghezza diversa all'interno dello stesso indirizzo di rete.

- *Esempio: indirizzo di rete 192.168.1.0. Posso utilizzare una maschera a 1 bit per dividere la rete in 2 sottoreti da 128 host, e utilizzare 2 bit nel range di indirizzi per la seconda sottorete per dividere il segmento in 2 ulteriori sottoreti da 64 host:*
  192.168.1.0 / 255.255.255.128
  host sottorete n°1: da 192.168.1.1 a 192.168.1.127
  192.168.1.0 / 255.255.255.64
  host sottorete n°2: da 192.168.1.129 a 192.168.1.191
  host sottorete n°3: da 192.168.1.193 a 192.168.1.254

Classful: indica l'indirizzamento con Classi IP.

Classless: indica l'indirizzamento senza Classi IP di appartenenza (e quindi consente di scegliere liberamente le subnet mask e gli indirizzi).

CIDR: Classless Inter-Domain Routing, identifica l'aggregazione di sottoreti (operazione detta anche di **supernetting**). Utilizzando un indirizzamento classless è possibile utilizzare i bit per le subnet mask in maniera "libera". Utilizza la notazione indirizzo IP/numero di bit per indicare la lunghezza della subnet mask.

- Esempio: 192.168.1.0/22 indica che la subnet mask utilizza 22 bit, quindi **11111111. 11111111. 11111**00.00000000 ovvero 255.255.252.0

Piano di indirizzamento completo: prevede di specificare per il progetto di rete assegnato indirizzo di rete, indirizzo di broadcast, range di indirizzi disponibili, range di indirizzi assegnati/riservati, indirizzi IP di ogni host o dispositivo presente nella rete, e le subnet mask.

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;
- inoltro (**forwarding**) del pacchetto verso l'interfaccia di output del router scelta ("**match**"). Appena acquisito l'indirizzo IP del pacchetto il router controlla la propria netmask e determina se è relativo a un host della propria rete, in tal caso utilizzerà i servizi del livello 2 per inoltrare il pacchetto direttamente all'host destinatario (**routing diretto**); altrimenti se è destinato ad un'altra rete consulta la propria **Routing Table**, se è collegato alla rete inoltra direttamente il pacchetto, altrimenti lo spedisce al router indicato dalla tabella o a quello di default, che ripeterà il processo (**routing indiretto**).

Tabella di Routing: è la tabella utilizzata dai router per effettuare l'instradamento. Contiene:

- un record per ciascuna rete collegata direttamente al router, con l'indicazione della relativa interfaccia di rete;
- un record per (alcune) reti non collegate direttamente al router, insieme con l'indicazione del router a cui inoltrare i pacchetti (Next Hop oppure Gateway);
- un record per un router (vicino, cui è collegato) di default, a cui inoltrare i pacchetti destinati a reti sconosciute.

- nel caso l'instradamento sia diretto viene inserito un asterisco come Next Hop, mentre nel caso di reti sconosciute si indica con default la rete destinazione e con /0 la subnet mask.

- le tabelle vengono verificate tramite la tecnica del **longest prefix matching**: dato che nella tabella sono presenti generalmente varie sottoreti l'indirizzo IP di destinazione di un pacchetto può generare un match per più record, verrà quindi scelta come destinazione quella con la maschera di sottorete più specifica, ovvero con più bit a 1 nella subnet:

Esempio: con la tabella di routing seguente un pacchetto con destinazione 192.168.1.42 che realizza un match su entrambe le reti 192.168.1.0/25 e 192.168.1.32/28 verrebbe indirizzato all'interfaccia N, in quanto più specifica.

Router	Rete destinazione	Mask	Gateway/Next Hop	Interfaccia
R1	192.168.1.0	/25	*	S
R1	192.168.1.32	/28	*	N
R2	default	/0	130.192.192.128	E

- generalmente le interfacce di rete di un router (se a 4 porte, versione più diffusa) si indicano con i punti cardinali N,S,O,E (in Inglese N,S,W,E).

Esempio di tabella di una rete con due router, R1 ed R2:

Router	Rete destinazione	Mask	Gateway/Next Hop	Interfaccia
R1	130.192.192.128	/26	*	S
R1	130.192.192.0	/25	*	N
R1	default / 0.0.0.0	/0	130.192.192.131	S
R2	130.192.5.0	/24	*	O
R2	10.9.0.0	/16	*	S
R2	10.0.0.0	/15	10.9.0.2	S
R2	10.0.0.0	/13	10.8.0.4	N
R2	default	/0	130.192.192.128	E

Hop: salto, indica l'attraversamento di un dispositivo di instradamento lungo il percorso di un pacchetto.

Costo: rappresenta la somma dei costi delle linee attraversate, è inversamente proporzionale alla sua velocità, che è legata a banda trasmissiva, tipo e affidabilità del mezzo trasmissivo, lunghezza del percorso, traffico di rete.

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 caso di modifiche della topologia o del traffico. 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 e prevede appunto 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.

Link State Routing; protocollo utilizzato nel routing statico che si basa sullo stato dei collegamenti tra i nodi. A ciascun router vengono inviati in flooding dei pacchetti LSP (Link State Packet) contenenti lo stato di ogni link, l'identità di ogni vicino e i costi dei link connessi al nodo che lo invia. Utilizza l'**Algoritmo di Dijkstra** (**Shortest Path First**) per il calcolo del percorso più breve. Tutti i nodi mantengono una copia intera della mappa della rete ed eseguono un calcolo completo con l'algoritmo di Dijkstra dei migliori percorsi, pertanto il calcolo non è distribuito.

Distance Vector Routing: protocollo utilizzato nel routing dinamico in cui viene inviata la tabella di routing da un router a tutti i router vicini sotto forma di vettore, con indicati i costi di collegamento.

Esempio: vettore del router A [A-0, B-2, C-4, D-2] indica che il router A è routing diretto (local, costo zero), inviare al router B ha un costo di 2, e così via.

E' un algoritmo iterativo, distribuito e asincrono (non richiede che i nodi operino in contemporanea). Utilizza l'**Algoritmo di Bellman-Ford** per il calcolo del percorso più breve. Bellman-Ford ha il problema di non rilevare i loop (cicli) infiniti, per i quali si utilizzano il **route poisoning** (cerca di bloccare ponendo il costo a infinito le rotte verso cui il costo cresce progressivamente) e/o lo **split horizon** (non comunico a un nodo vicino percorsi che si apprendono da quel nodo).

RIP: protocollo di routing che utilizza la porta 520, di tipo Distance Vector, che utilizza indirizzi IP nelle tabelle. Utilizza una metrica "hop count" per la quale la distanza è il numero di link che vengono attraversati per raggiungere la destinazione, con numero variabile tra 1 e 15 (il 16 rappresenta costo infinito). I pacchetti RIP vengono inviati in broadcast ogni 30 secondi, e se entro 3 minuti la rotta non viene aggiornata viene posta a distanza 16 e successivamente rimossa.

IGRP: protocollo di routing di tipo Distance Vector proprietario di CISCO. Ha un hop count di 255 e consente di avere più entry nelle tabelle per la stessa destinazione.

Black hole: è un punto della rete in cui i pacchetti vengono scartati perché non viene trovata una destinazione.

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

VLAN: è una tecnica con la quale è possibile allestire più reti locali divise a livello logico ma che condividono la stessa infrastruttura fisica. Vengono gestite tramite appositi switch amministrabili, consentendo di predisporre diversi segmenti di rete all'interno dei quali i singoli sistemi e dispositivi possono comunicare tra di loro senza la necessità di un router, garantendo una elevata scalabilità della rete. Con le VLAN si realizzano domini di broadcast separati, garantendo le performance della rete. Con l'uso del protocollo 802.1Q è possibile estendere le VLAN su altre reti fisiche collegando gli switch attraverso delle apposite porte dette di "**trunk**". Ne esistono di 2 tipologie:

- **port VLAN**: le porte dello switch vengono assegnate alle VLAN, l'associazione è fatta direttamente per connessione tra dispositivo e switch (assegnazione statica);

- **tagged VLAN**: viene aggiunto un tag nel frame ethernet (32 bit di lunghezza) dopo l'indirizzo MAC, che identifica la VLAN di appartenenza tramite un **VID** (VLAN ID), che consente di gestire fino a 4096 VLAN diverse. Frame appartenti a VLAN diverse vengono instradati attraverso porte trunk. La porta trunk può inoltre servire per collegare lo switch

a server che forniscono servizi a più VLAN, in questi casi per realizzare l'inter-VLAN routing si utilizzano **switch L3**, che sono una sorta di router che opera sulla rete locale.

Inter-VLAN routing: per poter far comunicare VLAN diverse tra loro è necessario un dispositivo di routing. Ogni VLAN deve avere un gateway che consenta il routing, ovvero il router deve possedere un'interfaccia per ogni VLAN da mettere in comunicazione. E' possibile utilizzare il sistema del **Router-on-a-stick** per realizzare l'inter-VLAN routing utilizzando una sola porta: vengono configurate delle sub-interfacce virtuali (ognuna appartenente a ogni VLAN da connettere) dell'interfaccia fisica del router, che viene collegato a una porta truck dello switch cui sono collegate le VLAN.

QUALCOSA SU TCP E UDP

TCP: è un protocollo del livello di trasporto della suite TCP/IP orientato alla connessione, la trasmissione dei dati avviene in maniera bidirezionale solo dopo che è stata stabilita la connessione tra i dispositivi. Include un sistema di controllo della consegna dei pacchetti. Ha una architettura di tipo client/server.

3-Way Handshake: è la procedura con la quale avviene la connessione TCP tra due host. Vengono scambiati 3 messaggi, in cui vengono impostati su certi in i campi e i flag:

- l'host A invia un segmento SYN all'host B (viene impostato a 1 il flag SYN e il campo Sequence number (seq) contiene il valore x che specifica l'Initial Sequence Number (ISN) di A);
  A -> B SYN, seq=x

- B invia in risposta un segmento SYN/ACK ad A (i flag SYN e ACK sono impostati a 1, il campo seq contiene il valore y che specifica l'ISN di B e il campo Acknowledgment number (ack) contiene il valore x+1 confermando la ricezione del ISN di A;
  B -> A SYN/ACK, ack=x+1, seq=y

- A invia in risposta un segmento ACK a B (il flag ACK è impostato a 1 e il campo ack contiene il valore y+1 confermando la ricezione dell'ISN di B).
  A -> B ACK, ack=y+1, seq=x+1

Il terzo segmento serve all'host B per stimare il timeout iniziale come tempo trascorso tra l'invio di un segmento e la ricezione del corrispondente ACK. Il flag SYN trova particolare utilizzo nei firewall poiché i segmenti con il flag non attivo appartengono a connessioni già stabilite.

SYN scan: è uno scan della rete che viene effettuato per rilevare le porte aperte su un host o la presenza di un firewall, non viene inviato l'ACK (ultimo step del 3-way handshake) per rendere più difficile la rilevazione della scansione in atto.

Multiplazione: il TCP consente di far transitare su una stessa linea dati provenienti da applicazioni diverse serializzando le informazioni arrivate in parallelo, attraverso l'assegnazione di una porta, con cui viene distinta l'applicazione di destinazione. La coppia porta + indirizzo IP è detta **socket**.

Porte: utilizzate nelle socket, sono composte 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 **Well Know Ports**, e sono assegnate ai servizi più comuni (DNS porta 53, SMTP porta 25, FTP porta 21, HTTP porta 80, ecc…);
- da 1024 a 49151 sono dette R**egistered 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 utilizzate all'occorrenza per le connessioni.

UDP: è un protocollo di trasporto senza connessione, basato sul trasferimento di datagrammi, per sua natura non garantisce che arrivino a destinazione, la ritrasmissione in caso di perdita d'informazione, e la corretta sequenza in ricezione, per questi motivi è definito non affidabile. Tuttavia trova impiego per comunicazioni in cui l'obiettivo è ridurre la durata della trasmissione, poiché non occorre creare una connessione con il destinatario e attendere una risposta: trasmissione audio e video, comunicazione multicast e real time, DNS, SNMP.

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 avere entrambe le funzioni verso gli host della rete. Si classificano 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 Virtual Overlay Network (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 (Discovery) cui ogni peer comunica la propria esistenza al momento dell'avvio e riceve una lista con gli altri nomi della rete. Il peer prima contatta il server individualmente e poi inoltra la richiesta.

- **Discovery + Lookup Server**: scome per il 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 (indice), i relativi hash che garantiscono l’integrità degli stessi, gli URL o IP dei tracker.

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. Può essere 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. Può essere 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 alal chiave partendo dall'analisi del testo;

Diffusione: principio indicato da Shannon, è la capcaità 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, perchè 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.

Attacchi passivi: minacce alla confidenzialità dei dati. Sono i più difficili da invididuare.

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 FIREWALL E PROXY

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 e non pesante a livello di risorse (e quindi rapida). 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.

- **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 esepio server mai 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.

Alcuni riferimenti e comandi:

- **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**:

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

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

ACL 1	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**:

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

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

Router(config)# access-list 1 deny tcp any any eq 80
//blocca tutto il traffico con protocollo TCP sulla porta 80

ACL 1	Sorgente	Wildcard mask src	Protocollo	Destinazione	Wildcard mask dst	Azione
1	172.16.2.0	0.0.0.255	tcp	0.0.0.0	255.255.255.255	Permit
2	0.0.0.0	255.255.255.255	tcp	0.0.0.0	255.255.255.255	Deny
*						Deny

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 occuperò 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 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 di **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 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:

- V**irtualizzazione 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 MAME, che consente di emulare il funzionamento delle ROM contenenti il codice macchina dei videogiochi "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.

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 0 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 scoperta recentemente (2018) che interessa CPU Intel, AMD e ARM (i principali produttori mondiali) che consente 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 gatewy 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…

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 il presunto prezzo 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 (collegandosi con quanto si apprende nella materia GPOI), in quanto un investimento in materiale e soluzioni più performanti 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'eleaborato che produciamo deve essere una sorta di "guida" per chi vuole 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 presente 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…), dispotitivi 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 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 gli 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, 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 può contenere al suo interno metadati con informazioni sull'autore, una foto può contenere metadati sul luogo dove è stata scattata e la data di scatto, un messaggio inviato con un sistema di i*nstant messaging* può contentere 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 ciò 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 statuto 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 può diffondersi 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, ciò 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 a base Windows XP o Windows 7 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: 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 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 fondò 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, per pagare da solo con la giustizia un conto così grande a 29 anni per tutti i reati commessi tramite la sua piattaforma.

"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. Sono state almeno 6 le morti accertate per overdose riconducibili ad acquisti su Silk Road, per i quali è stato accusato di responsabilità Ulbricht)

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, open source, che ha come obiettivo la navigazione realmente anonima e non tracciabile su internet, attraverso un sistema di onion routing.

Onion Routing: è 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 di volta in volta la destinazione successiva. Ogni step conosce solamente la posizione del nodo precedente e successivo, garantendo l'anonimato del mittente.

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 ciò 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.

APPROFONDIMENTI: 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 ciò 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 (ciò 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 pubblicò 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 ciò 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

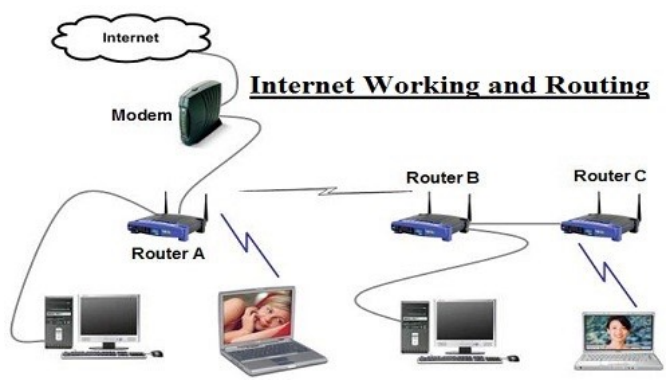
Metadati: informazioni che descrivono altre informazioni. Servono ad esempio a migliorare e ottimizzare l'accesso a tali informazioni all'interno di un sistema informatico. Nei sistemi di messaggistica ad esempio i metadati possono contenere informazioni sull'ora di invio del messaggio, sul luogo, se 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…

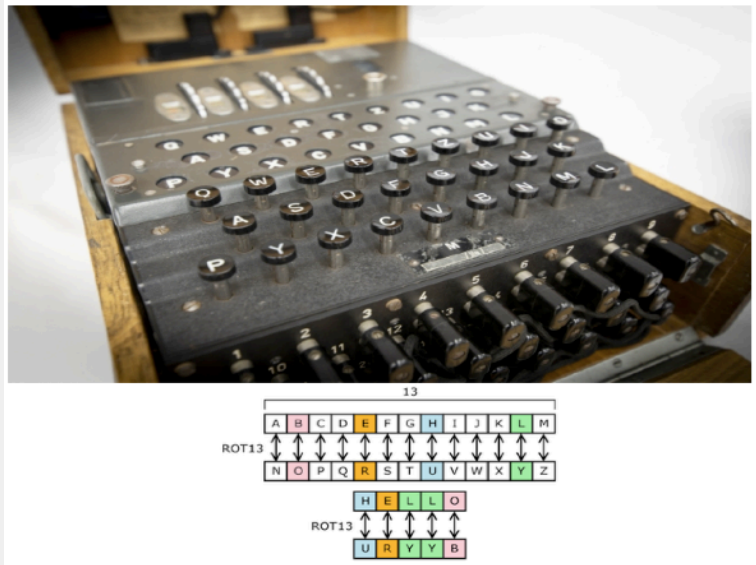
Fake News: informazioni inventate o distorte, appositamente rielaborate per renderle virali e nel frattempo generare opportune reazioni.

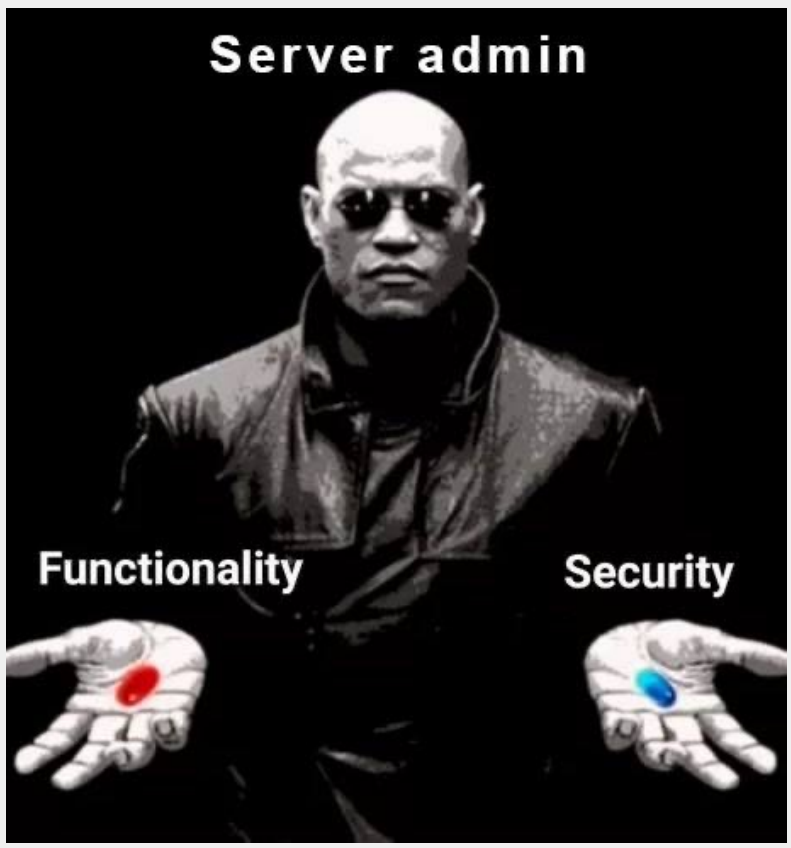
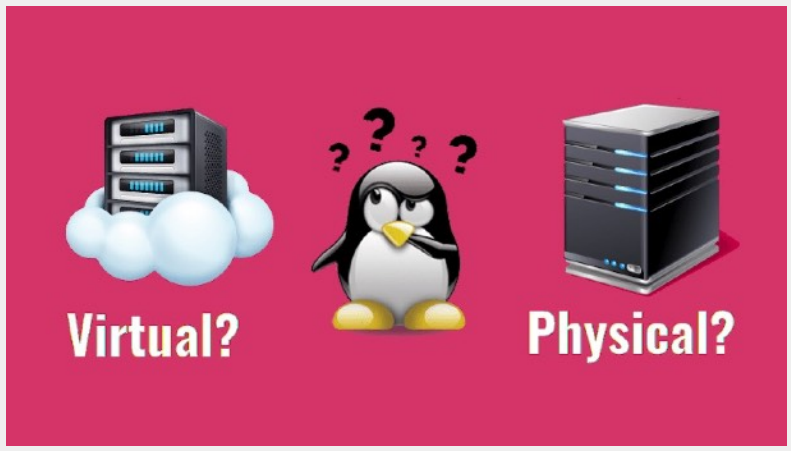
ESEMPI DI MATERIALI PER I COLLOQUI ORALI

La prova orale dell'Esame di Stato consiste in un **colloquio** che prende avvio da un **materiale** (in origine chiamato "busta"), che contiene un'immagine ed eventualmente del testo, costituito da estratti di brani di letteratura, poesie, fotografie, articoli di giornale, grafici, formule, spunti di progetti, problemi: dipende dalla Commissione. Non bisogna cercare di forzare collegamenti o perdere tempo a cercare tutti i possibili dettagli nelle foto (non ci sono "*easter egg*"!): il contenuto della busta è solo una suggestione per dare avvio al colloquio, molto probabilmente sarà impossibile collegare tutte le materie, e soprattutto non è un quiz.

Ecco alcuni esempi di buste utilizzate negli scorsi esami, con indicati alcuni spunti di argomenti di cui parlare nel colloquio.

	La sicurezza informatica è un tema centrale in Sistemi e Reti, ma la necessità di tenere celate le proprie comunicazioni è propria ad esempio delle operazioni militari e politiche (Storia), e si può parlare dell'importanza della matematica nelle funzioni legate alla crittografia.
	Con questo disegno si può guidare un profano a capire come funziona il web. Sulla legalità è facile un collegamento ai temi di educazione civica.
	Busta di impostazione classica: qui si collegano tutte le materie di indirizzo e si può approfondire gli aspetti delle reti che si sanno meglio.

	Enigma è un facile collegamento tra Storia e Sistemi e Reti con la crittografia, parlando di quest'ultima ci si può agganciare agli elementi informatici in cui viene usata e approfondirli.
 *"Non voglio vivere in un mondo in cui tutto ciò che faccio o dico viene registrato. Questo è qualcosa che io non sono disposto ad accettare o sostenere."* Tratto da "Citizenfour", di Laura Poitras. Oscar Miglior Documentario 2015.	Un caso di attualità pone spunti per un bel discorso sulla percezione (spesso errata) che si ha della privacy quando utilizziamo un dispositivo elettronico connesso a una rete.
 "Non basatevi sui firewall e le protezioni di Rete per tutelare le vostre informazioni. Cercate sempre i punti deboli, che di solito sono le persone." *Kevin D. Mitnick, "L'arte dell'Inganno", 2002*	Questa citazione racchiude il tema centrale della sicurezza delle reti, ovvero il problema di gestire chi le utilizza. Da qui si può proseguire ad analizzare esempi di reti e tecnologie più diffuse per individuarne le criticità.
	Questo materiale è una metafora visiva per spiegare i due principali protocolli di comunicazione su Internet, e passando dai servizi che li utilizzano si può proseguire nelle altre materie di indirizzo.

	La scena di un film famosissimo (Matrix) come punto di partenza per una riflessione sui compiti dell'amministratore di server. Il problema della scelta si può ad esempio collegare con Matematica e la Ricerca Operativa.
	Immagine tratta dai uno dei tanti forum di smanettoni che prendono in gira gli "utonti", consente ad esempio di spaziare dal funzionamento fisico del wi-fi (onde radio, interferenze) passando alla sicurezza delle reti wireless.
	Un altro spunto di discussione per un tecnico informatico, cui poi collegarsi con le altre materie di indirizzo, ad esempio GPOI in termini dell'impatto delle scelte di progettazione di una architettura informatica non solo sulle prestazioni ma anche sui costi.
	Attacchi informatici e sicurezza della rete, passando per il cablaggio strutturato le procedure di disaster recovery, magari collegando la cyberwarfare e gli scenari di guerra in Storia.

	Il tema delle guerre in Storia è preponderante, in questo materiale viene rappresentato l'attuale scenario di cyberwarfare sempre più diffuso nei conflitti attuali.
	Materiale molto semplice che indirizza subito sul tema della sicurezza delle reti e delle informazioni.
	Phishing e quindi sicurezza delle informazioni, ma volendo anche spunto per parlare di educazione civica e uso consapevole della rete, oppure cyberbullismo per quanto riguarda i social.

APPUNTI DI LABORATORIO

Qui trovi dei **brevi e stringati appunti** su programmi, comandi, termini, siti utilizzati per le esercitazioni, con alcuni richiami sul loro uso. Dato che molti esempi riguardano vulnerabilità ed 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) 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 **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.
- i sistemi operativi e i software vengono aggiornati spesso, alcuni comandi e appunti potrebbero non funzionare più o nello stesso modo in cui sono descritti nella Guida, pertanto prendete il tutto come **punto di partenza**.

MACCHINE VIRTUALI

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).
Per **condividere file** facilmente tra host e guest si può **attivare la condivisione file**: dal menu della VM avviata selezionare Dispositivi > Cartelle Condivise > Impostazioni Cartelle Condivise, dopodiché aggiungere una nuova cartella (icona sulla destra con il +), assegnare il percorso, selezionare Montaggio Automatico e Rendi Permanente. Su alcune VM (ad esempio quelle con Windows XP) sarà necessario da Virtual Box far installare le Guest Addition, selezionando dal menu Dispositivi della VM "Inserisci l'immagine CD delle Guest Additions".

Kali Linux: una delle più note tra le distribuzioni Linux dedicata alla sicurezza, basata su Debian, con preinstallati numerosi tool utili per l'hacking, il cracking, e più in generale i penetration test e l'analisi forense. Sono scaricabili alcune versioni in formato **.ova** già configurate, direttamente importabili in Virtual Box.
I dati di accesso di default potrebbero variare a seconda della versione o se avete scaricato una versione già configurata, ad esempio un *.ova*. Tipicamente sono root - toor oppure kali - kali.

metasploitable: una distribuzione Linux vulnerabile creata per sperimentare penetration test.

Dati di accesso di default:

login: msfadmin
password: msfadmin

Alcuni exploit utilizzabili con Metasploit per ottenere una shell da una macchina Metasploitable (utilizzando l'opzione "reverse connection"):

ftp > vsftpd_234_backdoor
irc > unreal_ircd_3281_backdoor

Target Machine: così si indica una macchina "bersaglio" per effettuare dei Penetration Test.

TOOL UTILI DA SHELL/TERMINALE

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.

Uso:

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

ipconfig: su Windows fornisce informazioni sulla propria connessione IP.

Uso dei parametri:

ipconfig /all :informazioni complete su tutte le interfacce di rete
ipconfig/displaydns :informazioni sulla cache DNS corrente
ipconfig/flushdns :svuota la cache DNS
ipconfig/release id_interfaccia :rilascia l'IP dell'interfaccia specificata (l'identificatore va individuato con /all)
ipconfig/renew id_interfaccia :rinnova l'IP dell'interfaccia specificata (l'identificatore va individuato con /all)

tracert (su Windows) e **traceroute** (su Linux): mostra tutti i salti che un pacchetto effettua per arrivare a destinazione. Utilizzando il parametro -d non risolve i nomi degli host. Per salvare il risultato su file si può utilizzare su Windows: (esempio)

tracert 192.168.1.42 > c:/output.txt

I valori in ms mostrati riguardano il tempo intercorso tra la spedizione e la ricezione di un pacchetto (se il tempo è maggiore di 3s 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 modificato 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.

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

nmap: su Linux è un potente tool di scansione della rete.

Uso:

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: su Kali esegue una scansione ARP della rete.

Uso:
arp-scan —interface=eth0 192.168.1.0/24 :specificando interfaccia e indirizzo di rete con subnet

arp: mostra la tabella arp corrente. Si utilizza con il parametro -a.

whois: fornisce informazioni dal servizio WhoIS su un dominio internet.
Esempio:
whois www.google.it

nslookup: fornisce informazioni sui record NS di un dominio internet.

Uso:

nslookup www.google.it :mostra informazioni sul dominio www.google.it

nslookup : attiva la console, i comandi seguenti si danno direttamente in essa:
set type=mx :etta come tipo solo i record di posta MX
www.google.it :dare invio per mostrare i risultati
set type=ns :setta solo i record NS
set type=any :setta tutti i record

TOOL DI LINUX

Wordlist: è un file contenente username, password e altro da utilizzare per provare degli attacchi a dizionario. Su Kali Linux la directory dove sono presenti quelle di default è **/usr/share/wordlists/**

smtp-user-enum: tool di Kali che serve a elencare l'esistenza di utenti su un server di posta, tramite l'analisi con dizionario.

Esempio:
smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t 192.168.1.42

nikto: tool di Kali Linux per l'analisi delle vulnerabilità di web application, col quale si possono ottenere molte informazioni su un bersaglio.

Uso:

nikto -host www.google.it

Metasploit: tool di Kali Linux per l'utilizzo di exploit noti. Viene avviato in automatico lanciando **Armitage**, una GUI particolarmente utile per fare delle prove di penetration testing.

N.B. Se non si avvia automaticamente lanciare i seguenti comandi (ignorare eventuali errori):

#service postgresql start
#service metasploit start
msfconsole

e dalla console lanciare:
/msfdbinit
/armitage

N.B. se non fosse installato Armitage:

sudo apt-get update
sudo apt-get install armitage

Uso:

Per prima cosa dal menu HOST selezionare NMAP INTENSE SCAN 192.168.1.0/24 (oppure direttamente l'IP della macchina da attaccare).
Una volta apparsa la macchina (o le macchine) bersaglio, cliccare con il tasto destro sulla macchina e selezionare SCAN per avere informazioni.

Nel menu ARMITAGE selezionare SET EXPLOIT RANK dopodiché impostare a POOR.

Dal menu ATTACKS selezionare FIND ATTACKS e attendere. Al termine comparirà nel menu (tasto destro sulla macchina da attaccare) il comando ATTACK e si potranno selezionare possibili attacchi individuati da Metasploit, che invieranno il payload alla macchina bersaglio. Se l'exploit va a buon fine l'icona della macchina cambierà e verrà "avvolta" da fulmini, a indicare che è ora possibile interagire.

Nel menu è possibile anche selezionare la voce Hail Mary: è un comando dimostrativo che tenta degli exploit a caso sulle varie macchine.

John the Ripper: è un tool per il crack delle password.
/etc/passwd è il file di sistema di Linux dove sono memorizzate le password (crittate, è presente l'hash).
Per mostrare il contenuto del file: # cat /etc/passwd
Nel file non sono visibili gli hash delle password, per rivelarli e ottenere un file da utilizzare per provare a decrittare le password si usa il comando unshadow:

unshadow /etc/passwd /etc/shadow > hashfile (dove hashfile è il nome che vogliamo dare al file contenente gli hash visibili).

Uso:

john hashfile *:prova a crackare le password*
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 wordlist*

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 ranbow tables, ad esempio OPHCrack.

MITM con arpspoof: arpspoof è un tool di Kali per effettuare un attacco di Arp Poisoning, utilizzando 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 MITM.

Installare arpspoof:

sudo apt-get update
sudo apt-get install dsniff

Uso:
avviare una macchina Kali e una macchina bersaglio, ad esempio una VM Windows XP. Lanciare da cmd il comando

arp -a

e verificare il MAC address per l'IP corrente.
Sulla macchina Kali utilizzare il comando # ip route show per conoscere il proprio gateway, e poi abilitare la modalità promiscua sull'interfaccia in uso (ad esempio eth0) per intercettare tutto il traffico di rete:

ifconfig eth0 promisc
sysctl -w net.ipv4.ip_forward=1

Ora su Kali lanciare, in 2 finestre separate del terminale, i comandi:

arpspoof -i eth0 -t IP_gateway IP_bersaglio :dove eth0 è l'interfaccia di rete da usare su Kali)
arpspoof -i eth0 -t IP_bersaglio IP_gateway :dove eth0 è l'interfaccia di rete da usare su Kali)

L'attacco **MITM** tramite **Arp poisoning** (detto anche Arp spoofing) è avviato, si può ora verificare sulla macchina bersaglio come è cambiata la Arp Table. Per verificare gli effetti di un MITM si può avviare una macchina OWasp di appoggio, che fornisce ad esempio un web server navigabile in chiaro e senza crittografia, cui si accede da browser con http://192.168.1.42/owaspbricks/
Sulla macchina Kali si possono avviare diversi tool per intercettare il traffico svolto tra la VM bersaglio e Owasp semplicemente navigando il sito:

driftnet -i eth0 :intercetta ogni immagine visualizzata nella navigazione dell'utente. Funziona anche se l'utente naviga su internet, ma solo su siti in chiaro e senza https.

urlsnarf -i eth0 :intercetta tutti gli URL navigati dall'utente.

Si possono verificare ulteriori vulnerabilità dei protocolli senza crittografia utilizzando Wireshark su Kali, filtrando ad esempio con la stringa:

ip.addr==192.168.1.42 and http.request.method=="POST"

e provando a utilizzare la pagina di login di OWasp, vedendo nel pacchetto intercettato in chiaro la username e la password dell'utente.
Terminato l'attacco, chiudere i vari terminali e disabilitare la modalità promiscua:
sysctl -w net.ipv4.ip_forward=0

WIRESHARK

Wireshark: è un packet sniffer open source utilizzato per analizzare il traffico di rete. Presenta vari tool 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**
Qui si può cambiare la visualizzazione di default che indica i secondi da inizio cattura con data e ora dell'evento.

Ricerche e filtraggio

Cercare ed esportare un contenuto da HTTP o altro: collegarsi a un qualsiasi sito e scaricare un file (ad esempio un file di testo o PDF). Nel file di cattura filtrare con

http.request

per individuare i siti da cui si sono richiesti contenuti, eventualmente si può filtrare ulteriormente con

http contains "nomedelsito"

selezionando i pacchetti individuati da una GET nel campo info si può cliccare sul menu **File->Esporta Oggetti->HTTP** e salvare il contenuto del file dal file di cattura.

La stessa cosa si può fare determinando il tipo di contenuto di un pacchetto esaminando il flusso TCP, ad esempio se si individua del codice HTML si può esportare l'oggetto come file HTML.

Cercare ed esportare un contenuto da SMTP: tipico di malware che trasforma la macchina infettata in uno spambot, filtrare con:

stmp.data.fragment

File->Esporta Oggetti->IMF (Internet Message Format) e salvare il contenuto del file EML (email) dal file di cattura.

Cercare ed esportare un contenuto da FTP: collegarsi a un qualsiasi server FTP e scaricare un file (ad esempio un file di testo o PDF). Nel file di cattura filtrare con

ftp.request.command

e vedremo tutti i comandi scambiati, tra cui figureranno nome utente e password utilizzati.

Utilizzando un altro filtro:

ftp-data

si può vedere cosa è stato trasferito, per salvare un file bisogna cercare tra i pacchetti quelli con comando RETR (ovvero quelli richiesti per essere trasferiti dal server FTP), dentro il pacchetto cercare il nome del file (si trova in FTP DATA [Command: RETR nomefile.ext]), quindi selezionare il pacchetto, cliccare col destro e selezionare SEGUI->FLUSSO TCP, dopodiché nella schermata impostare MOSTRA E SALVA DATI COME - ASCII, e salvare con il nome del file individuato prima. Per cercare file specifici si può applicare un filtro:

ftp-data.command contains “estensione”

ad esempio

ftp-data.command contains “pdf”

Cercare ed esportare oggetti da un file di cattura (pcap):

L’operazione di esportazione si può fare **direttamente sul file pcap** senza filtrare, in tal modo vengono esportati tutti gli oggetti corrispondenti alla richiesta:

File->Esporta Oggetti->HTTP esporta contenuti HTTP

File->Esporta Oggetti->IMF esporta mail

Filtrare e cercare in navigazione web:

per cercare tra i siti visitati sia in HTTP che in HTTPS applicare il filtro:

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

per cercare all’interno di pacchetti HTTP siti specifici:

http.host contains “stringa”

oppure per i siti HTTPS:

ssl contains “nomedelsito”

Il filtro più complesso seguente invece può servire per cercare anche segmenti TCP che rivelano connessioni fallite (ad esempio a siti infetti a causa di un malware), escludendo il traffico utilizzato dalla porta 1900 usata dal protocollo SSDP (Simple Service Discovery Protocol, che serve per riconoscere periferiche di rete su una LAN), che ove presente rende troppo densi i file di cattura, e inserendo eventuali chiamate DNS che possono rivelare connessioni a server sospetti:

(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002 or dns) and !(udp.port eq 1900)

Cercare traffico torrent:

Vari filtri per cercare del traffico torrent:

bittorrent

http.request.uri contains .torrent

http.request.uri contains announce or http.request.uri contains scrape

info_hash= //cerca l'hash SHA del file richiesto tramite torrent, che hanno la forma /announce.php?info_hash=XXX

Cercare informazioni sugli host: si può filtrare il traffico DHCP per trovare informazioni sugli host della rete, attraverso il filtro:

bootp (oppure dhcp su precedenti versioni di Wireshark)

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.

Per cercare tramite filtro nei vari contenuti delle option vengono mostrati in un menu a tendina scrivendo:

bootp.option

ad esempio per cercare un hostname:

bootp.option.hostname contains "nome-host-da-cercare"

Dato che il traffico DHCP non è frequente, si possono cercare le tracce NBNS (dovute al protocollo **NetBIOS**, utilizzato, seppur obsoleto, da host Windows e MacOS):

nbns

e cercando informazioni in particolare nel campo Additional Records.

Cercare per IP:

ip.addr==192.168.1.42 //filtra pacchetti che contengono l'IP indicato

ip.addr==192.168.1.42 and ssl //filtra solo i pacchetti SSL

ip.addr==192.168.1.42 and tcp.port==443 //filtra solo pacchetti che utilizzano la porta TCP indicata

Filtraggi utili:

http.request || tls.handshake.extensions_server_name //filtra connessioni a siti web e consente di individuare le URL, anche per connessioni frittate

http.request.uri contains "/90" //filtra gli URI che contengono /90, in questo caso viene fatto perché si è alla ricerca di una parte di URI nota utilizzata da un malware

http.request.uri contains .exe //filtra gli URI che contengono un file di estensione .exe

ip contains mail //filtra pacchetti relativi a mail

ip contains "This program" //filtra pacchetti che contengono al loro interno la dicitura "This program cannot be run in DOS mode." che appartiene ai file eseguibili di Windows, se si pensa che sia stato scaricato qualche malware.

kerberos.CNameString and !(kerberos.CNameString contains $) //ricerca tra i pacchetti informazioni sugli utenti che si autenticano tramite il protocollo di autenticazione di rete Kerberos, il campo cname contiene il nome utente.

Http contains post //filtra pacchetti che contengono dei POST verso form web

RISORSE IN RETE

Url Shortner: è un servizio di rete che abbrevia gli URL sul web (ad esempio bit.ly). Nasce per semplificare la diffusione dei link, tuttavia è particolarmente utilizzato per attacchi informatici (dal phishing al XSS), poiché mascherando l'URL non è immediatamente chiaro all'utente su quale sia la destinazione del link. Viene inoltre utilizzato negli attacchi XSS proprio per nascondere l'aggiunta in coda a una URL di uno script malevolo.

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.
- sourceforge.net/projects/ophcrack : pagina ufficiale del progetto OPHCrack, un cracker di password per Windows basato su **Rainbow Table**.

- objectif-securite.ch/en/ophcrack : sito del produttore di **OPHCrack**, utilizzabile online per verificare il cracking tramite rainbow table.

- sourceforge.net/projects/owaspbwa/ : pagina ufficiale di **OWASP**, una versione di Linux farcita di servizi web vulnerabili. User: root, Password: owaspbwa

- sourceforge.net/projects/metasploitable/ : pagina ufficiale di **Metaspoitable**.

- www.exploit-db.com : **database** che raccoglie vulnerabilità e exploit noti.

- www.oldversion.com : sito da cui è possibile ricavare delle **vecchie versioni di software**, per testare exploit e vulnerabilità. Da utilizzare solo in ambienti di test (meglio una VM).

- www.archive.org : sito che raccoglie degli "**snapshot**" della maggioranza dei siti web, è possibile navigarlo e andare a recuperare vecchie pagine e versioni dei siti.

- www.macvendors.com : sito per trovare il produttore di una interfaccia di rete fornendo il **Mac Address**.

- https://www.osboxes.org : sito che raccoglie delle VM Linux già pronte per l'uso per Virtual Box e VMWare. Generalmente i dati di accesso sono Login: root Password: osboxes.org

- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml : pagina del sito ufficiale dello **IANA** (Internet Assigned Numbers Authority) dove trovare l'elenco delle "**well known ports**".

- https://www.virustotal.com e https://www.hybrid-analysis.com : repository per l'analisi di file potenzialmente infetti.

- https://www.packettotal.com : repository per l'analisi di file pcap alla ricerca di malware e infezioni.

- https://clusit.it/ : Associazione Italiana per la Sicurezza Informatica, ogni anno redige un dettagliato rapporto.

- https://csirt.gov.it/ : CSIRT - Computer Security Incident Response Team della Repubblica Italiana.

- https://www.malware-traffic-analysis.net/index.html : una miniera di informazioni, tutorial ed esercizi per effettuare analisi di attività di malware sulle reti con Wireshark. (thank you Brad! https://twitter.com/malware_traffic)

PER CONCLUDERE

"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."* (da "Guida Galattica per autostoppisti" di Douglas Adams)

La scrittura di questa Guida è iniziata nel 2019, per poter fornire ai miei studenti un riferimento durante lo studio e il ripasso della disciplina "Sistemi e Reti" in vista dell'Esame di Stato. E' in continuo aggiornamento e frutto di un continuo lavoro di ricerca e sintesi degli argomenti più importanti (purtroppo fatto nei ritagli di tempo) e non è sicuramente completa, nè esente da errori, come un software non sarà mai esente da bug.

Sarò grato per qualsiasi feedback, segnalazione e correzione che vorrete inviarmi tramite il mio sito *www.simonezanella.it* oppure via mail a simone.zanella@istruzione.it.

Grazie per tutto il pesce!

Simone Zanella

LICENZA

VERSIONE aggiornata al 31/08/2022