Sicurezza In rete

Gregorio D'Agostino

28 Maggio 2021

Agenda

Riepilogo schema Comunicazioni in Rete

Shell locali, remote e sicure

Tecniche per la gestione del traffico di rete

Trasmissione sicura di documenti in rete

Esercitazione pratica

Comunicazioni

- Esame giovedì 1 Luglio.

Comunicazioni

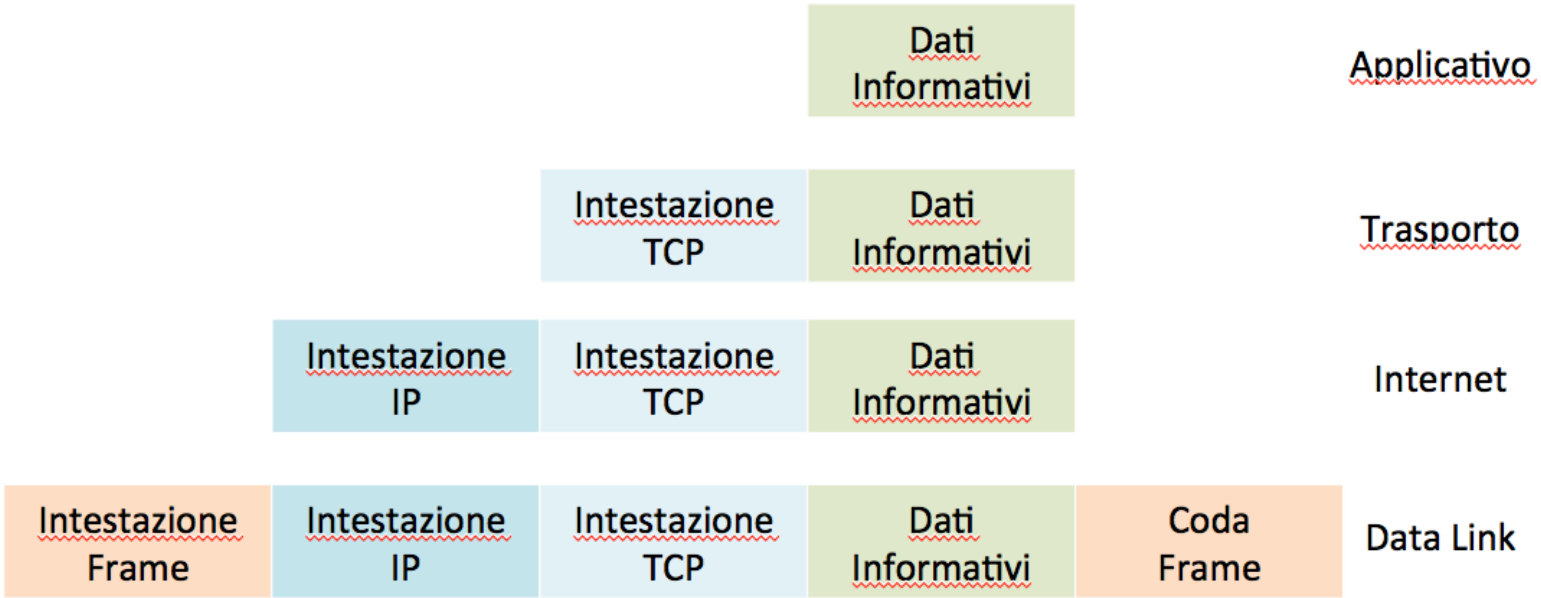
- Esame giovedì 1 Luglio.
- Modalità presenza.

Comunicazioni

- Esame giovedì 1 Luglio.
- Modalità presenza.
- Attendo conferma per la commissione.

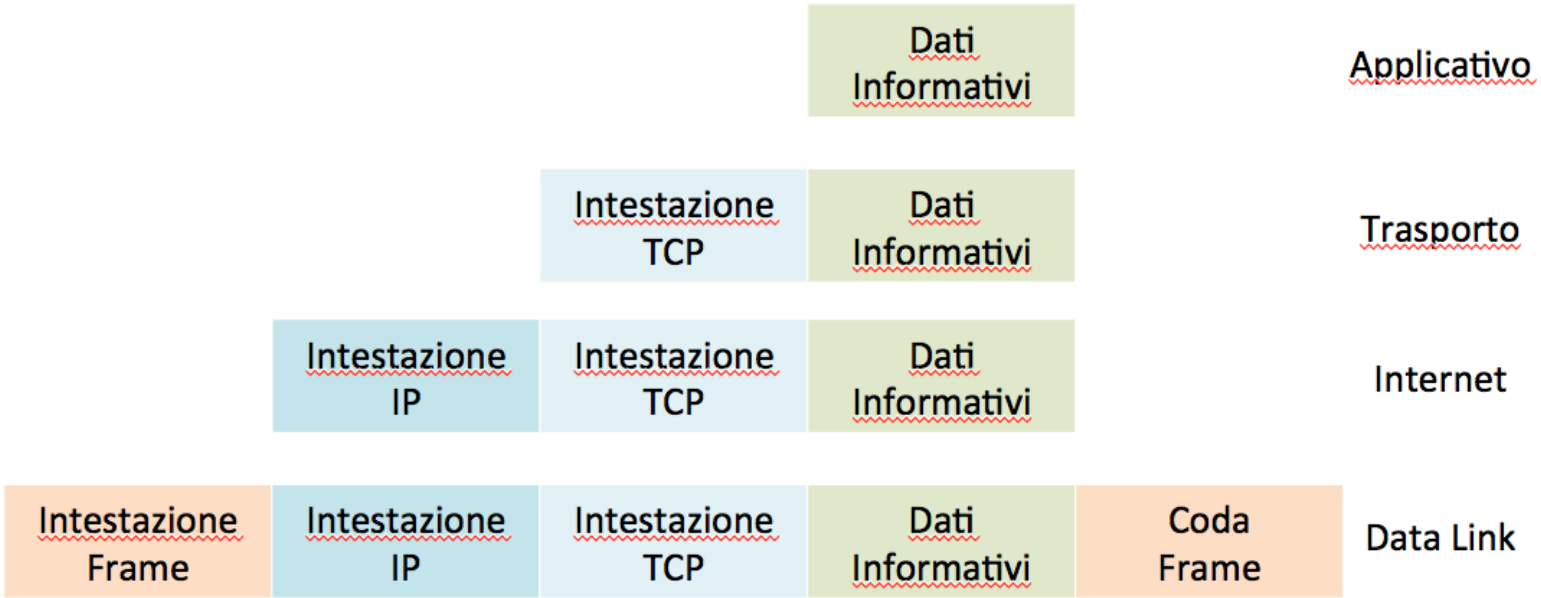
Schema generico TCP/IP

- Rivediamo la costruzione dei pacchetti TCP/IP:



Schema generico TCP/IP

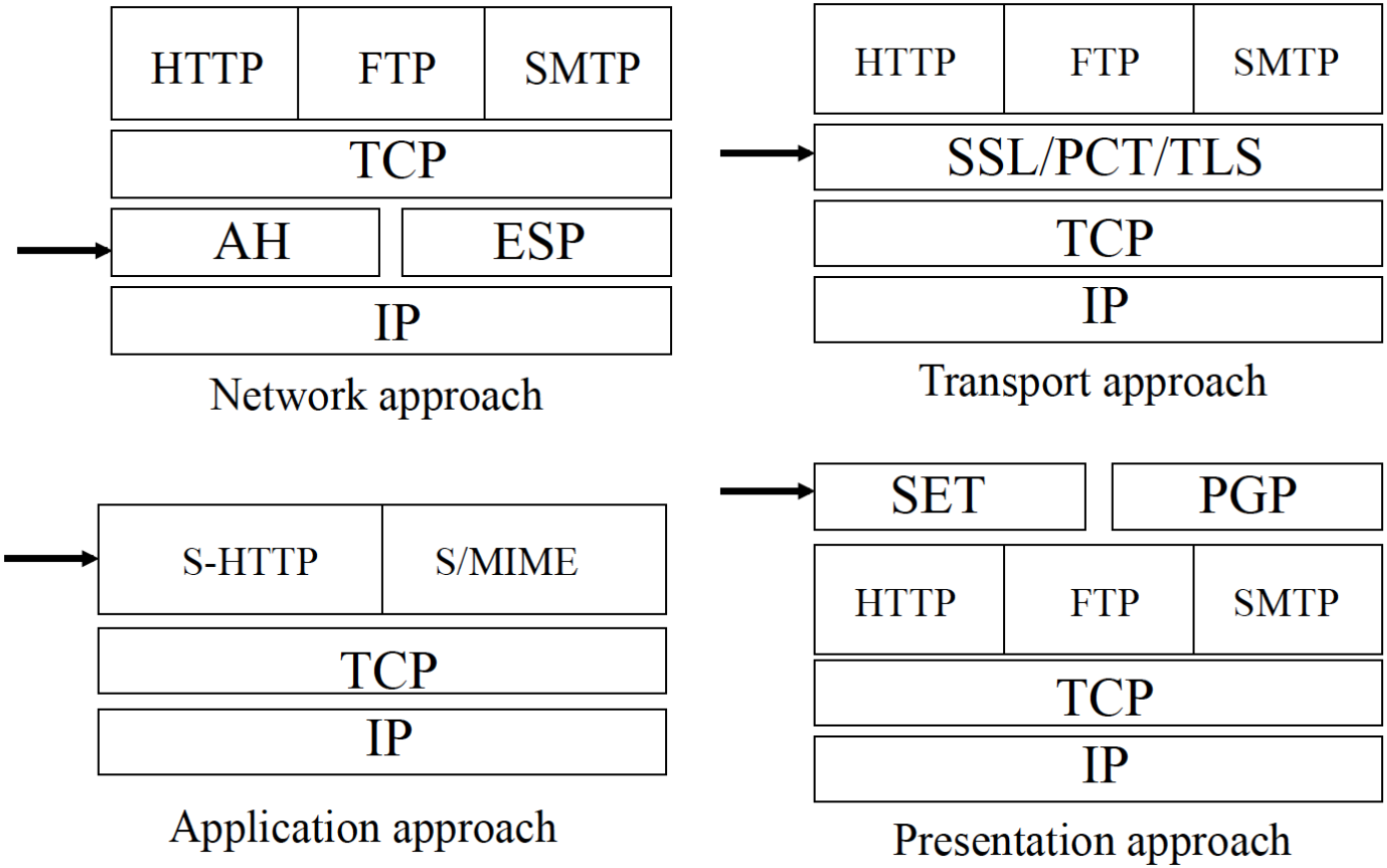
- Rivediamo la costruzione dei pacchetti TCP/IP:



- Il contenuto del campo Dati Informativi cambia in base all'applicativo utilizzato. Tranne IPsec che estende l'intestazione IP gli altri livelli di sicurezza ritagliano spazio nella parte dati. Con UDP lo schema è analogo.

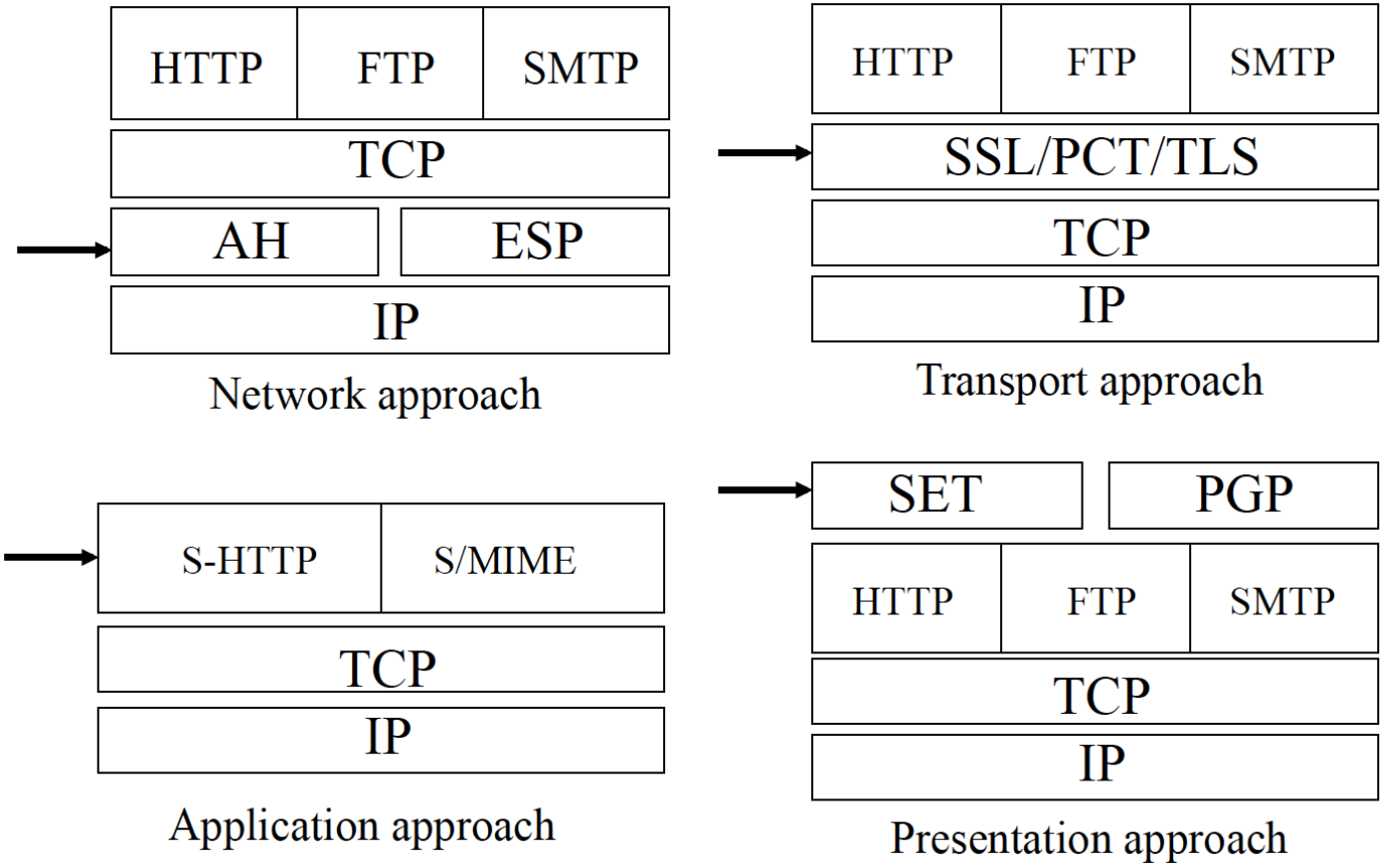
Schemi di locazione dei dispositivi di cifratura di rete

- Ripartiamo dallo schema delle collocazioni possibili dei dispositivi di sicurezza (cifratura) utilizzabili in rete. I diversi metodi coesistono e li utilizziamo per le diverse necessità:



Schemi di locazione dei dispositivi di cifratura di rete

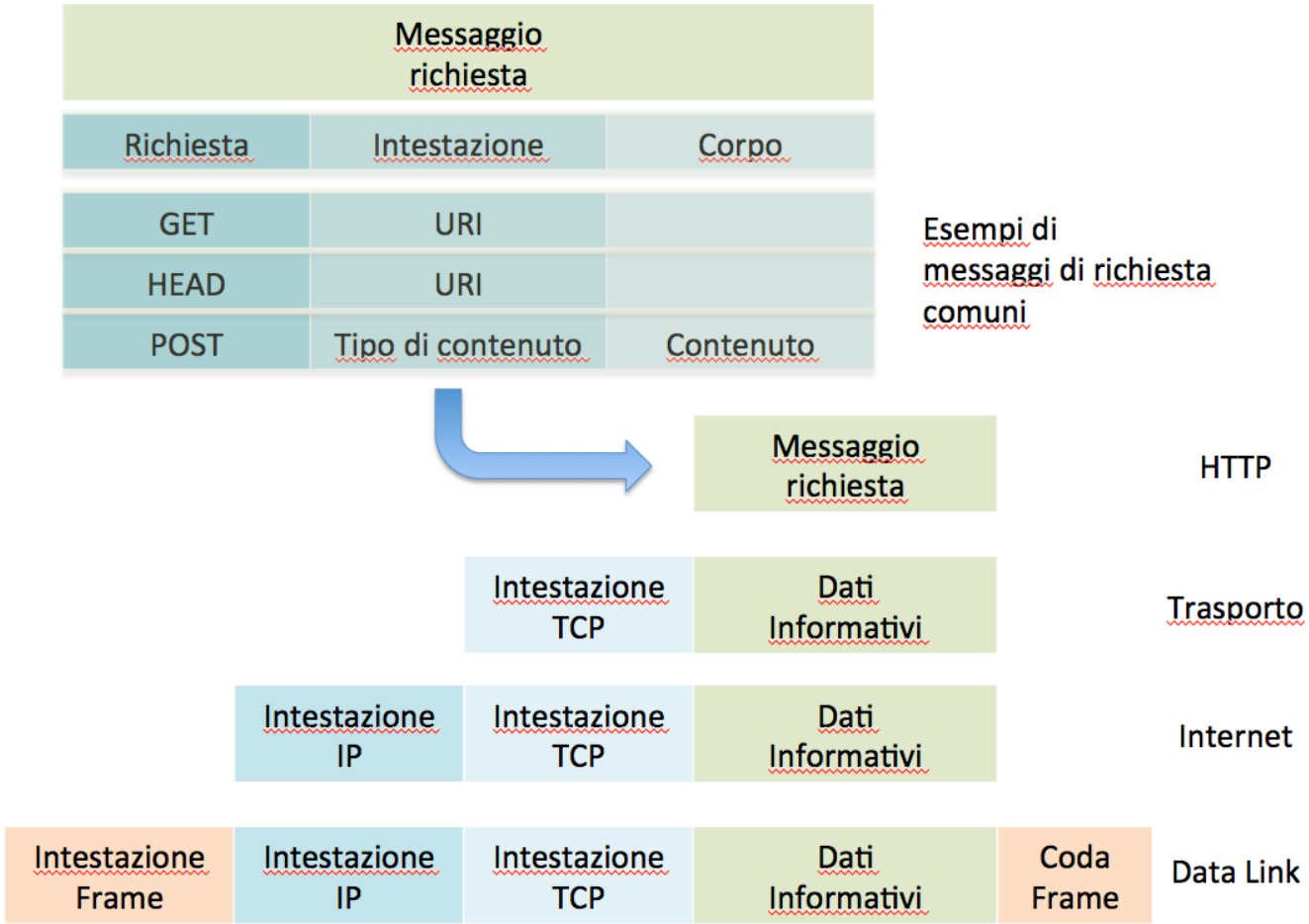
- Ripartiamo dallo schema delle collocazioni possibili dei dispositivi di sicurezza (cifratura) utilizzabili in rete. I diversi metodi coesistono e li utilizziamo per le diverse necessità:



- Il nome dell'approccio dipende dallo strato in cui si applicano i dispositivi di sicurezza.

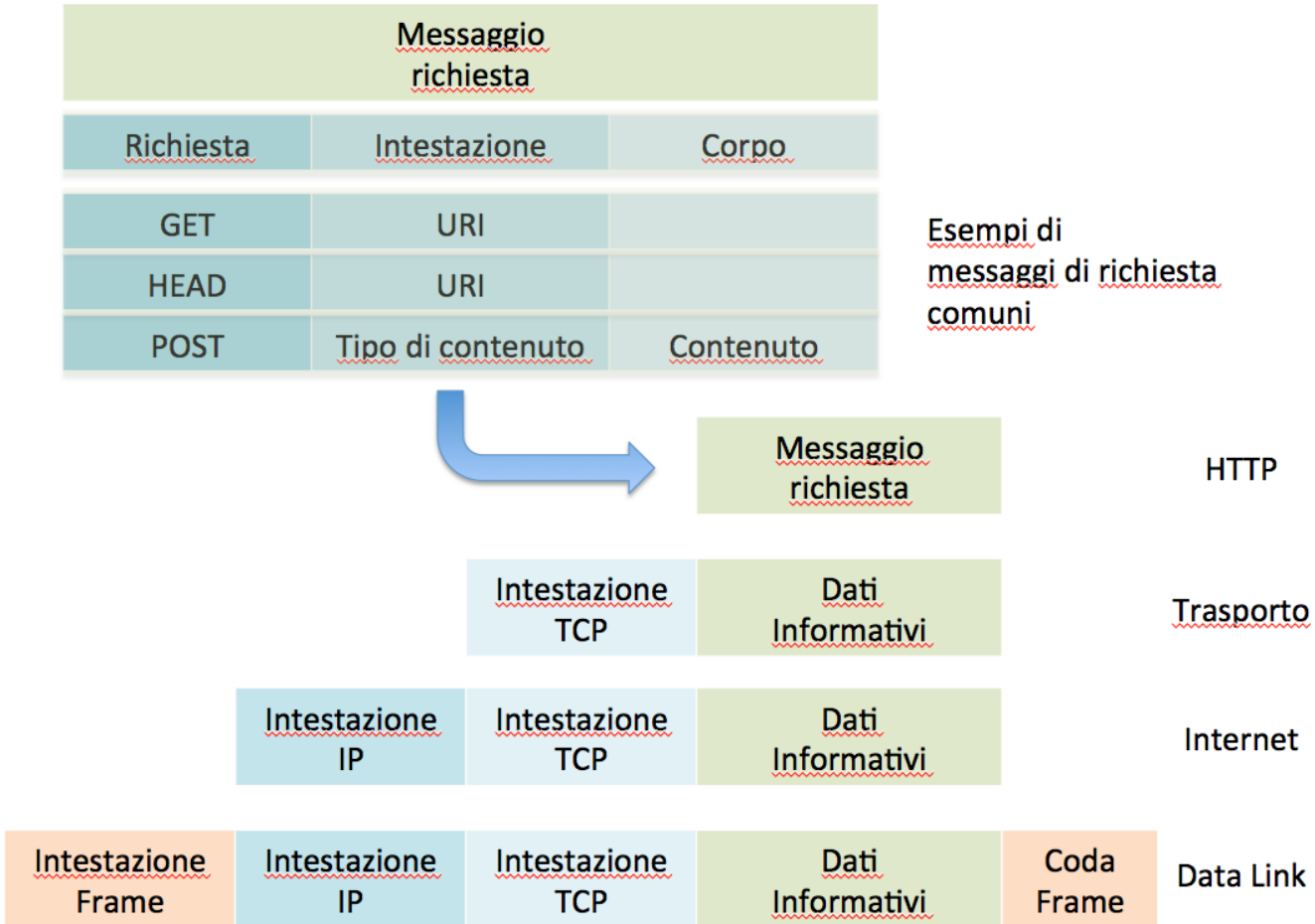
Schema esemplificativo HTTP

- Vediamo esempi di pacchetti HTTP. POST invia info (per ad esempio compilare un modulo), GET chiede una risorsa e HEAD solo i dati di creazione modifica etc.



Schema esemplificativo HTTP

- Vediamo esempi di pacchetti HTTP. POST invia info (per ad esempio compilare un modulo), GET chiede una risorsa e HEAD solo i dati di creazione modifica etc.



- Oltre a GET, HEAD e POST, si usano anche le richieste PUT, DELETE, TRACE, CONNECT, OPTIONS

Shell

- Una shell è una interfaccia utente piattaforma di elaborazione che di solito si realizza tramite un processo ricorrente. La shell può essere testuale se accetta una sequenza di caratteri da tastiera o grafica (full screen) se è possibile una interazione tramite altri dispositivi (mouse, tablet e tastiera).

Shell

- Una shell è una interfaccia utente piattaforma di elaborazione che di solito si realizza tramite un processo ricorrente. La shell può essere testuale se accetta una sequenza di caratteri da tastiera o grafica (full screen) se è possibile una interazione tramite altri dispositivi (mouse, tablet e tastiera).
- I programmi che realizzano le shell testuali si chiamano terminali (virtuali). Il comando cmd nei sistemi windows apre una shell testuale. In linux (debian/ubuntu) vi sono varie interfaccia (konsole, kterm, xterm etc). In OS X si usa "Terminal".

Shell

- Una shell è una interfaccia utente piattaforma di elaborazione che di solito si realizza tramite un processo ricorrente. La shell può essere testuale se accetta una sequenza di caratteri da tastiera o grafica (full screen) se è possibile una interazione tramite altri dispositivi (mouse, tablet e tastiera).
- I programmi che realizzano le shell testuali si chiamano terminali (virtuali). Il comando cmd nei sistemi windows apre una shell testuale. In linux (debian/ubuntu) vi sono varie interfaccia (konsole, kterm, xterm etc). In OS X si usa "Terminal".
- Ogni shell testuale ha un suo "linguaggio" ovvero un insieme di comandi interpretati dal sistema operativo.

Shell

- Una shell è una interfaccia utente piattaforma di elaborazione che di solito si realizza tramite un processo ricorrente. La shell può essere testuale se accetta una sequenza di caratteri da tastiera o grafica (full screen) se è possibile una interazione tramite altri dispositivi (mouse, tablet e tastiera).
- I programmi che realizzano le shell testuali si chiamano terminali (virtuali). Il comando cmd nei sistemi windows apre una shell testuale. In linux (debian/ubuntu) vi sono varie interfaccia (konsole, kterm, xterm etc). In OS X si usa "Terminal".
- Ogni shell testuale ha un suo "linguaggio" ovvero un insieme di comandi interpretati dal sistema operativo.
- La shell testuale più usata nei sistemi linux è zsh che sostituisce la bash (Bourne-Again Shell) detta semplicemente sh. Poi esistono ksh (Korn shell), csh (basata su sintassi c), Tenex shell (tcsh) ed altre. Ogni sistema windows ha la sua shell; la shell originale era l'MS-DOS che a sua volta derivava dal DOS.

Shell

- Le shell grafiche in ambiente linux (open source) più comuni sono KDE (K Desktop Environment), GDE (Gnu Desktopo Enviroment),

Shell

- Le shell grafiche in ambiente linux (open source) più comuni sono KDE (K Desktop Environment), GDE (Gnu Desktopo Enviroment),
- Nei sistemi OS X (Apple) la shell grafica nativa è il Finder

Shell

- Le shell grafiche in ambiente linux (open source) più comuni sono KDE (K Desktop Environment), GDE (Gnu Desktopo Enviroment),
- Nei sistemi OS X (Apple) la shell grafica nativa è il Finder
- Nei sistemi Windows la shell grafica originale è File Explorer , ma ne esistono molte altre.

Shell

- Le shell grafiche in ambiente linux (open source) più comuni sono KDE (K Desktop Environment), GDE (Gnu Desktopo Enviroment),
- Nei sistemi OS X (Apple) la shell grafica nativa è il Finder
- Nei sistemi Windows la shell grafica originale è File Explorer , ma ne esistono molte altre.
- Ogni applicativo dotato di una GUI (Graphic User Interface) può eseguire in modalità grafica tutti i comandi consentiti all'utente che attiva il processo.

Secure Shell: Sessioni Sicure

- Quando l'interfaccia avviene tra piattaforme connesse tramite la rete si parla di shell remote.

Secure Shell: Sessioni Sicure

- Quando l'interfaccia avviene tra piattaforme connesse tramite la rete si parla di shell remote.
- Una sessione è una sequenza di comunicazioni continuativa tra due entità (nodi e processi) di una rete. Nella classificazione OSI (open System Interconnection) è al livello superiore al trasporto.

Secure Shell: Sessioni Sicure

- Quando l'interfaccia avviene tra piattaforme connesse tramite la rete si parla di shell remote.
- Una sessione è una sequenza di comunicazioni continuativa tra due entità (nodi e processi) di una rete. Nella classificazione OSI (open System Interconnection) è al livello superiore al trasporto.
- Le prime sessioni remote furono realizzate tramite il protocollo (in chiaro) telnet, in disuso da molti anni ed oggi praticamente proibito. Si tratta di un protocollo totalmente insicuro da evitare.

Secure Shell: Sessioni Sicure

- Quando l'interfaccia avviene tra piattaforme connesse tramite la rete si parla di shell remote.
- Una sessione è una sequenza di comunicazioni continuativa tra due entità (nodi e processi) di una rete. Nella classificazione OSI (open System Interconnection) è al livello superiore al trasporto.
- Le prime sessioni remote furono realizzate tramite il protocollo (in chiaro) telnet, in disuso da molti anni ed oggi praticamente proibito. Si tratta di un protocollo totalmente insicuro da evitare.
- Le shell sicure ssh (Secure Shell) sono delle sessioni remote sicure (cifrate).

Secure Shell: Client/Server

- Le connessioni ssh sono basate su un meccanismo client-server. L'utente deve installare il software client sulla sua macchina, mentre la piattaforma di servizio a cui si collega deve disporre del software server.

Secure Shell: Client/Server

- Le connessioni ssh sono basate su un meccanismo client-server. L'utente deve installare il software client sulla sua macchina, mentre la piattaforma di servizio a cui si collega deve disporre del software server.
- Lo standard ssh richiede che siano cifrate sia la fase di autenticazione remota che le successive comunicazioni nell'ambito di una sessione.

Secure Shell: Client/Server

- Le connessioni ssh sono basate su un meccanismo client-server. L'utente deve installare il software client sulla sua macchina, mentre la piattaforma di servizio a cui si collega deve disporre del software server.
- Lo standard ssh richiede che siano cifrate sia la fase di autenticazione remota che le successive comunicazioni nell'ambito di una sessione.
- Una sessione è quindi definita dalle chiavi scambiate e dai protocolli sicuri concordati (ad esempio EAS). Al termine di ogni sessione occorre una nuova autenticazione.

Secure Shell: Client/Server

- Le connessioni ssh sono basate su un meccanismo client-server. L'utente deve installare il software client sulla sua macchina, mentre la piattaforma di servizio a cui si collega deve disporre del software server.
- Lo standard ssh richiede che siano cifrate sia la fase di autenticazione remota che le successive comunicazioni nell'ambito di una sessione.
- Una sessione è quindi definita dalle chiavi scambiate e dai protocolli sicuri concordati (ad esempio EAS). Al termine di ogni sessione occorre una nuova autenticazione.
- Esiste una versione open source denominata open-ssh che consente l'istallazione dei servizi ssh e delle interfacce (client) degli utenti su tutte le architetture.

Secure Shell: Client/Server

- Le connessioni ssh sono basate su un meccanismo client-server. L'utente deve installare il software client sulla sua macchina, mentre la piattaforma di servizio a cui si collega deve disporre del software server.
- Lo standard ssh richiede che siano cifrate sia la fase di autenticazione remota che le successive comunicazioni nell'ambito di una sessione.
- Una sessione è quindi definita dalle chiavi scambiate e dai protocolli sicuri concordati (ad esempio EAS). Al termine di ogni sessione occorre una nuova autenticazione.
- Esiste una versione open source denominata open-ssh che consente l'istallazione dei servizi ssh e delle interfacce (client) degli utenti su tutte le architetture.
- Come detto la sicurezza si instaura sopra il livello trasporto (TCP).

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.
- Il Transport Layer Protocol di ssh (che è sempre sopra TCP) svolge le seguenti funzioni:

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.
- Il Transport Layer Protocol di ssh (che è sempre sopra TCP) svolge le seguenti funzioni:
  - Negoziazione algoritmi cifratura

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.
- Il Transport Layer Protocol di ssh (che è sempre sopra TCP) svolge le seguenti funzioni:
  - Negoziazione algoritmi cifratura
  - Scambio delle chiavi necessarie

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.
- Il Transport Layer Protocol di ssh (che è sempre sopra TCP) svolge le seguenti funzioni:
  - Negoziazione algoritmi cifratura
  - Scambio delle chiavi necessarie
  - Autenticazione del server (ricezione chiave pubblica da una autorità certificante) [può mancare l'autorità certificante].

Secure Shell: tre protocolli interni

- L'instaurazione della sessione sicura prevede tre fasi a cui corrispondono tre protocolli: Transport Layer Protocol, User Authentication Protocol e Connection Layer Protocol.
- Il Transport Layer Protocol di ssh (che è sempre sopra TCP) svolge le seguenti funzioni:
  - Negoziazione algoritmi cifratura
  - Scambio delle chiavi necessarie
  - Autenticazione del server (ricezione chiave pubblica da una autorità certificante) [può mancare l'autorità certificante].
  - Crittografia della connessione: eventuale compressione dei dati e algoritmi di integrità.

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)
  - Ricezione chiave dell'utente da parte del server (si autentica il nodo di provenienza)

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)
  - Ricezione chiave dell'utente da parte del server (si autentica il nodo di provenienza)
  - Autenticazione dell'utente (di solito tramite username e password)

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)
  - Ricezione chiave dell'utente da parte del server (si autentica il nodo di provenienza)
  - Autenticazione dell'utente (di solito tramite username e password)
- Il Connection Layer Protocol, consente (quando serve) di stabilire una comunicazione multicanale.

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)
  - Ricezione chiave dell'utente da parte del server (si autentica il nodo di provenienza)
  - Autenticazione dell'utente (di solito tramite username e password)
- Il Connection Layer Protocol, consente (quando serve) di stabilire una comunicazione multicanale.
- Un altro uso molto utile è il port forwarding in cui si trasmettono in modo sicuro i pacchetti che si vorrebbe utilizzare su una (o più) determinata porta. Una applicazione è il NAT (Network Address Translation) in cui si raggiunge un nodo con un IP privato tramite un router che gli attribuisce una porta fittizia.

Secure Shell -cont

- User Authentication Protocol (protocollo autenticazione utente)
  - Ricezione chiave dell'utente da parte del server (si autentica il nodo di provenienza)
  - Autenticazione dell'utente (di solito tramite username e password)
- Il Connection Layer Protocol, consente (quando serve) di stabilire una comunicazione multicanale.
- Un altro uso molto utile è il port forwarding in cui si trasmettono in modo sicuro i pacchetti che si vorrebbe utilizzare su una (o più) determinata porta. Una applicazione è il NAT (Network Address Translation) in cui si raggiunge un nodo con un IP privato tramite un router che gli attribuisce una porta fittizia.
- Il Connection Layer Protocol consente di stabilire X forwarding che consente l'interfaccia grafica.

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.
- Scegliere App.

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.
- Scegliere App.
- Scegliere “Gestisci funzionalità facoltative”

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.
- Scegliere App.
- Scegliere “Gestisci funzionalità facoltative”
- Scegliere “Aggiungi una funzionalità”

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.
- Scegliere App.
- Scegliere “Gestisci funzionalità facoltative”
- Scegliere “Aggiungi una funzionalità”
- Scegliere Installiare “Client OpenSSH” e “Server OpenSSH”

Abilitare SSH (Secure Shell) in windows 10

- Usando Start scegliere Impostazioni.
- Scegliere App.
- Scegliere “Gestisci funzionalità facoltative”
- Scegliere “Aggiungi una funzionalità”
- Scegliere Installiare “Client OpenSSH” e “Server OpenSSH”
- Aprendo il terminale si ottengono gli stessi comandi di linux o altre piattaforme.

NAT Network Address Translation

- Il Network Address Translation (traduzione dell'IP) consente di usare un'unico IP (ma diversi socket cioè diverse porte) pubblico per un gruppo di IP privati di una LAN

NAT Network Address Translation

- Il Network Address Translation (traduzione dell'IP) consente di usare un'unico IP (ma diversi socket cioè diverse porte) pubblico per un gruppo di IP privati di una LAN
- A volte il NAT è utilizzato anche per motivi di sicurezza per i nodi con IP pubblico ai quali si accede sempre tramite il router gate che effettua la traduzione.

Tunneling

- Il tunneling è il trasferimento di alcune informazioni (ad esempio pacchetti IP o TCP/IP) usando un altro protocollo (di solito sicuro).

Tunneling

- Il tunneling è il trasferimento di alcune informazioni (ad esempio pacchetti IP o TCP/IP) usando un altro protocollo (di solito sicuro).
- Gli esempi precedenti port forwarding e X forwarding sono forme di tunneling: in quel caso sockets.

Tunneling

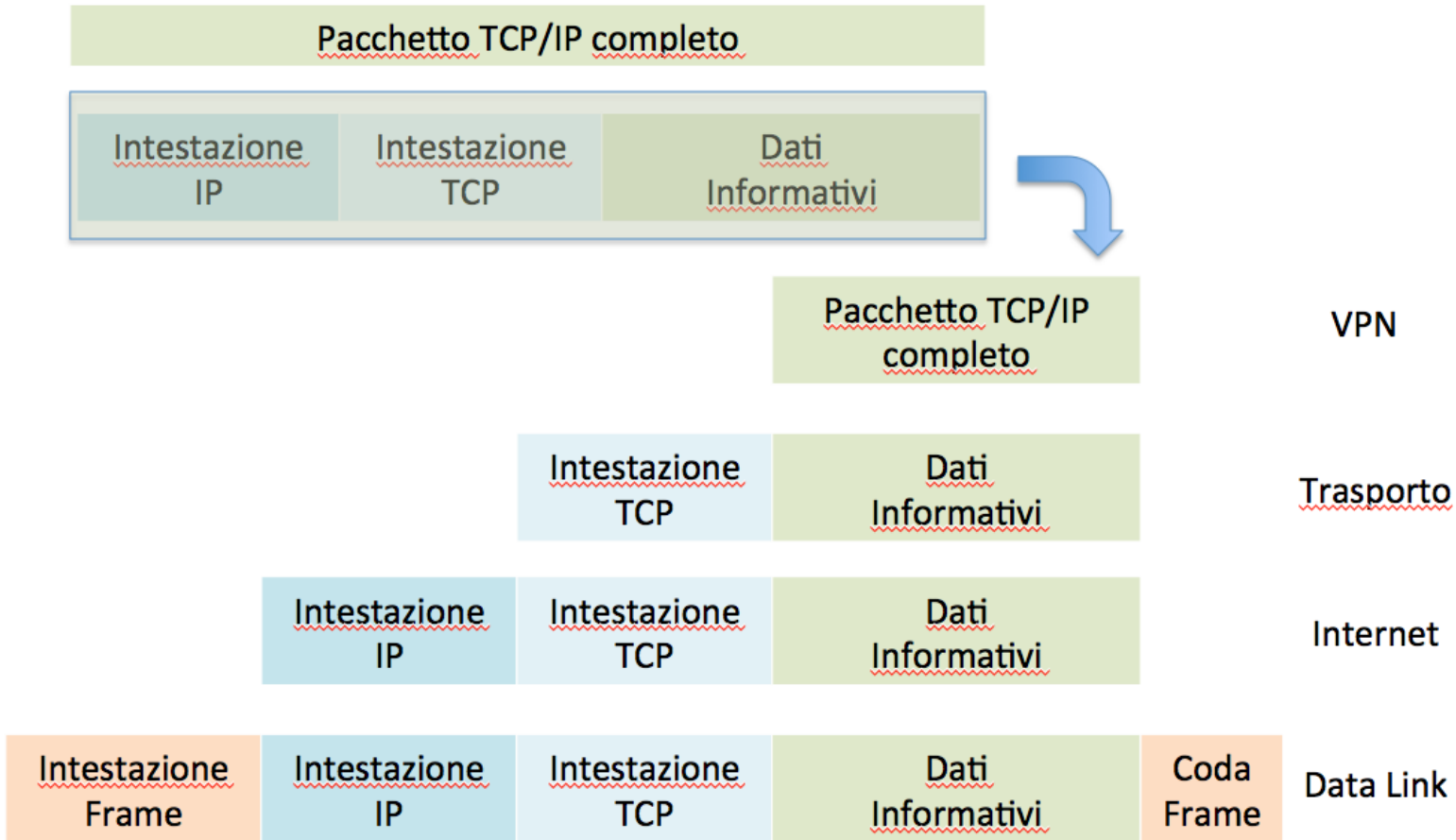
- Il tunneling è il trasferimento di alcune informazioni (ad esempio pacchetti IP o TCP/IP) usando un altro protocollo (di solito sicuro).
- Gli esempi precedenti port forwarding e X forwarding sono forme di tunneling: in quel caso sockets.
- In generale per il tunneling si usa la tecnica dell'incapsulazione, in cui nella parte informativa si include un "pacchetto", una unità di cumunicazione PDU (Protocol Data Unit) del protocollo di livello superiore (come in http dentro TCP/IP).

Tunneling

- Il tunneling è il trasferimento di alcune informazioni (ad esempio pacchetti IP o TCP/IP) usando un altro protocollo (di solito sicuro).
- Gli esempi precedenti port forwarding e X forwarding sono forme di tunneling: in quel caso sockets.
- In generale per il tunneling si usa la tecnica dell'incapsulazione, in cui nella parte informativa si include un "pacchetto", una unità di cumunicazione PDU (Protocol Data Unit) del protocollo di livello superiore (come in http dentro TCP/IP).
- L'esempio più utile di tunneling è la realizzazione delle Virtual Private Network (VPN). Che sono delle rete virtuali in quanto, un nodo esterno ad una LAN collegato da remoto ad un server interno, si comporta come se avesse i privilegi dati ai nodi interni. Dentro un pacchetto TCP/IP c'è un altro pacchetto IP completo di intestazione che viene istradato come se giungesse dall'interno della rete dove opera il server.

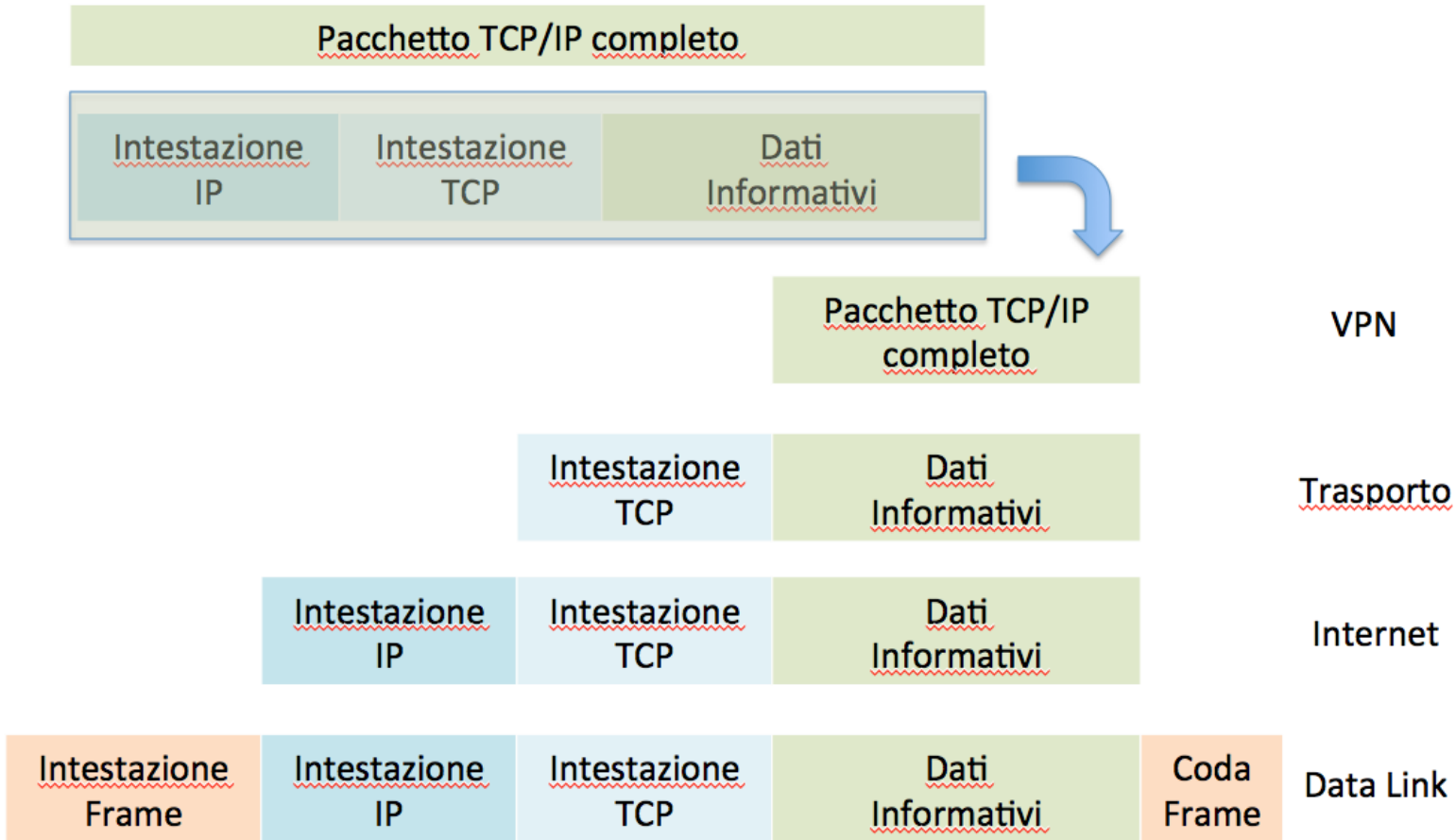
Schema esemplificativo VPN

- Vediamo esempi di pacchetti modificati per usare una VPN:



Schema esemplificativo VPN

- Vediamo esempi di pacchetti modificati per usare una VPN:



- Il server VPN crea un pacchetto con nuovo IP e porta e lo immette in rete dall'interno.

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono
  - controllo: il filtraggio di cui sopra.

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono
  - controllo: il filtraggio di cui sopra.
  - modifica: ad esempio il NAT; oppure il cambio della sola porta (port forward) o altro.

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono
  - controllo: il filtraggio di cui sopra.
  - modifica: ad esempio il NAT; oppure il cambio della sola porta (port forward) o altro.
  - monitoraggio: si memorizzano le singole operazioni (esempio instaurazione di sessioni) o le statistiche dei pacchetti.

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono
  - controllo: il filtraggio di cui sopra.
  - modifica: ad esempio il NAT; oppure il cambio della sola porta (port forward) o altro.
  - monitoraggio: si memorizzano le singole operazioni (esempio instaurazione di sessioni) o le statistiche dei pacchetti.
- Le IP tables sono liste (in chiaro o in nero) di IP (o sockets) autorizzati (in chiaro: white list) o bloccati (in nero: black list).

Firewall: parete tagliafuoco

- Un firewall è un software (di solito installato in router) che filtra i pacchetti di rete.
- Il filtraggio consiste nel bloccare, rispedire o verificare i pacchetti destinati o provenienti da un socket (coppia IP-Porta).
- Le operazioni principali svolte sono
  - controllo: il filtraggio di cui sopra.
  - modifica: ad esempio il NAT; oppure il cambio della sola porta (port forward) o altro.
  - monitoraggio: si memorizzano le singole operazioni (esempio instaurazione di sessioni) o le statistiche dei pacchetti.
- Le IP tables sono liste (in chiaro o in nero) di IP (o sockets) autorizzati (in chiaro: white list) o bloccati (in nero: black list).
- Per raggiungere una piattaforma può essere necessario attraversare molti firewall in cascata.

File Transfer Protocol

- Un file (dall'italiano filza o sfilza) è un insieme contiguo di bit a cui è associato un nome ed una locazione iniziale (un indirizzamento interno alla piattaforma computazionale per l'accesso sequenziale).

File Transfer Protocol

- Un file (dall'italiano filza o sfilza) è un insieme contiguo di bit a cui è associato un nome ed una locazione iniziale (un indirizzamento interno alla piattaforma computazionale per l'accesso sequenziale).
- I file vengono organizzati in cartelle (folders) che contengono la lista dei nomi con le locazioni. Le cartelle possono contenere altre cartelle formando le strutture gerarchiche in cui sono organizzati i dati. Nei sistemi unix (linux, OSX etc) e nei vecchi sistemi VMS le cartelle sono chiamate directory.

File Transfer Protocol

- Un file (dall'italiano filza o sfilza) è un insieme contiguo di bit a cui è associato un nome ed una locazione iniziale (un indirizzamento interno alla piattaforma computazionale per l'accesso sequenziale).
- I file vengono organizzati in cartelle (folders) che contengono la lista dei nomi con le locazioni. Le cartelle possono contenere altre cartelle formando le strutture gerarchiche in cui sono organizzati i dati. Nei sistemi unix (linux, OSX etc) e nei vecchi sistemi VMS le cartelle sono chiamate directory.
- Il primo protocollo di trasferimento file in rete fu denominato ftp (File Transfert Protocol). In questo sistema che opera sopra TCP/IP (sopra il trasporto) l'informazione non viene cifrata. Il sistema è ancora in uso in molti service provider per la gestione dei siti pubblici. Chiunque abbia accesso ai pacchetti in rete potrebbe leggerli ed eventualmente manipolarli (se la rete non è ipsec).

Secure File Transfer Protocol

- sftp è il discendente sicuro del File Transfer Protocol (ftp).

Secure File Transfer Protocol

- sftp è il discendente sicuro del File Transfer Protocol (ftp).
- Funziona in maniera del tutto analoga alla ssh: i primi tre passi negoziazione, scambio chiavi e autenticazione del server sono uguali; ma i comandi a disposizione dell'utente (client) sono mirati al trasferimento dei file.
- L' upload (caricamento) si effettua con il comando
  put filename [newfilename] ([ ] indicano campo opzionale)

Secure File Transfer Protocol

- sftp è il discendente sicuro del File Transfer Protocol (ftp).
- Funziona in maniera del tutto analoga alla ssh: i primi tre passi negoziazione, scambio chiavi e autenticazione del server sono uguali; ma i comandi a disposizione dell'utente (client) sono mirati al trasferimento dei file.
- L' upload (caricamento) si effettua con il comando
  put filename [newfilename] ([ ] indicano campo opzionale)
- Il download (scaricamento) si effettua con il comando
  get filename [newfilename]

Secure File Transfer Protocol

- sftp è il discendente sicuro del File Transfer Protocol (ftp).
- Funziona in maniera del tutto analoga alla ssh: i primi tre passi negoziazione, scambio chiavi e autenticazione del server sono uguali; ma i comandi a disposizione dell'utente (client) sono mirati al trasferimento dei file.
- L' upload (caricamento) si effettua con il comando
  put filename [newfilename] ([ ] indicano campo opzionale)
- Il download (scaricamento) si effettua con il comando
  get filename [newfilename]
- Si può usare l'asterisco per indicare un gruppo di file con una parte dei nomi condivisa.

Secure File Transfer Protocol

- sftp è il discendente sicuro del File Transfer Protocol (ftp).
- Funziona in maniera del tutto analoga alla ssh: i primi tre passi negoziazione, scambio chiavi e autenticazione del server sono uguali; ma i comandi a disposizione dell'utente (client) sono mirati al trasferimento dei file.
- L' upload (caricamento) si effettua con il comando
  put filename [newfilename] ([ ] indicano campo opzionale)
- Il download (scaricamento) si effettua con il comando
  get filename [newfilename]
- Si può usare l'asterisco per indicare un gruppo di file con una parte dei nomi condivisa.
- In tutte le piattaforme esistono applicativi che realizzano il processo tramite delle GUI che rendono il processo trasparente per l'utente.

Socket

- Un socket è la coppia: IP, porta che caratterizza la provenienza o destinazione di un pacchetto internet.

Socket

- Un socket è la coppia: IP, porta che caratterizza la provenienza o destinazione di un pacchetto internet.
- Le porte con in numeri più bassi 0-1023 sono assegnate ai servizi di rete dalla autorità IANA (Internet Assigned Numbers Authority) che gestisce gli indirizzi pubblici al livello globale. IANA è sotto il controllo di ICANN (Internet Corporation for Assigned Names and Numbers). Questi valori sono universali.

Socket

- Un socket è la coppia: IP, porta che caratterizza la provenienza o destinazione di un pacchetto internet.
- Le porte con in numeri più bassi 0-1023 sono assegnate ai servizi di rete dalla autorità IANA (Internet Assigned Numbers Authority) che gestisce gli indirizzi pubblici al livello globale. IANA è sotto il controllo di ICANN (Internet Corporation for Assigned Names and Numbers). Questi valori sono universali.
- Le porte nell'intervallo 1024-49151 vengono invece registrate da soggetti privati per attività specifiche.

Socket

- Un socket è la coppia: IP, porta che caratterizza la provenienza o destinazione di un pacchetto internet.
- Le porte con in numeri più bassi 0-1023 sono assegnate ai servizi di rete dalla autorità IANA (Internet Assigned Numbers Authority) che gestisce gli indirizzi pubblici al livello globale. IANA è sotto il controllo di ICANN (Internet Corporation for Assigned Names and Numbers). Questi valori sono universali.
- Le porte nell'intervallo 1024-49151 vengono invece registrate da soggetti privati per attività specifiche.
- Le porte dell'intervallo 49152-65535 sono dette private o dinamiche e non sono utilizzati da una applicazione in particolare. Tipicamente si usano per distinguere utenti o processi che utilizzano lo stesso IP pubblico, ma diverso IP privato in una LAN.

Porte Standard

- Esempi di porte adibite a servizi comuni:

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP
  - 88 Kerberos

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP
  - 88 Kerberos
  - 110 POP3 (server posta)

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP
  - 88 Kerberos
  - 110 POP3 (server posta)
  - 443 HTTPS

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP
  - 88 Kerberos
  - 110 POP3 (server posta)
  - 443 HTTPS
  - 995 POP3 (su secure shell) (server posta sicura)

Porte Standard

- Esempi di porte adibite a servizi comuni:
  - 20,21 ftp (controllo e dati)
  - 22 ssh sftp
  - 23 telnet
  - 25 SMTP - Simple Mail Transfer Protocol (E-mail)
  - 53 DNS
  - 80 HTTP
  - 88 Kerberos
  - 110 POP3 (server posta)
  - 443 HTTPS
  - 995 POP3 (su secure shell) (server posta sicura)
  - etc

Porte Registrate

- Esempi di porte adibite a servizi comuni:

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).
  - 2049 Network File System (sistemi di gestione file in rete)

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).
  - 2049 Network File System (sistemi di gestione file in rete)
  - 3306 MySQL (banca dati gestita in rete)

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).
  - 2049 Network File System (sistemi di gestione file in rete)
  - 3306 MySQL (banca dati gestita in rete)
  - 6000 X11 (sistema grafico a finestre open source introdotto dall'IMT)

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).
  - 2049 Network File System (sistemi di gestione file in rete)
  - 3306 MySQL (banca dati gestita in rete)
  - 6000 X11 (sistema grafico a finestre open source introdotto dall'IMT)
  - 8080 HTTP (servizi alternativi) per separarlo da traffico normale su porta 80.

Porte Registrate

- Esempi di porte adibite a servizi comuni:
  - 1080 SOCKS Proxy (vedremo)
  - 1194 OpenVPN (reti virtuali gestite con server open source).
  - 2049 Network File System (sistemi di gestione file in rete)
  - 3306 MySQL (banca dati gestita in rete)
  - 6000 X11 (sistema grafico a finestre open source introdotto dall'IMT)
  - 8080 HTTP (servizi alternativi) per separarlo da traffico normale su porta 80.
  - etc

Esempi pratici

- Tentativo di stabilire una sessione ssh ed sftp, non va manca la rete.

Esempi pratici

- Tentativo di stabilire una sessione ssh ed sftp, non va manca la rete.
- Accesso alla rete tramite eduroam (primo dispositivo di sicurezza).

Esempi pratici

- Tentativo di stabilire una sessione ssh ed sftp, non va manca la rete.
- Accesso alla rete tramite eduroam (primo dispositivo di sicurezza).
- Tentativo di stabilire una sessione ssh a gordion.casaccia.enea.it: non va il firewall blocca il traffico sulla porta 25 (standard di ssh). Attivazione della VPN.

Esempi pratici

- Tentativo di stabilire una sessione ssh ed sftp, non va manca la rete.
- Accesso alla rete tramite eduroam (primo dispositivo di sicurezza).
- Tentativo di stabilire una sessione ssh a gordion.casaccia.enea.it: non va il firewall blocca il traffico sulla porta 25 (standard di ssh). Attivazione della VPN.
- Stabilire una sessione ssh. OK ma xclock non parte (applicazione grafica). Riprovare con ssh -X ma continua a non funzionare (abbiamo attivato il connection level protocol in modo trasparente per l'utente).

Esempi pratici

- Tentativo di stabilire una sessione ssh ed sftp, non va manca la rete.
- Accesso alla rete tramite eduroam (primo dispositivo di sicurezza).
- Tentativo di stabilire una sessione ssh a gordion.casaccia.enea.it: non va il firewall blocca il traffico sulla porta 25 (standard di ssh). Attivazione della VPN.
- Stabilire una sessione ssh. OK ma xclock non parte (applicazione grafica). Riprovare con ssh -X ma continua a non funzionare (abbiamo attivato il connection level protocol in modo trasparente per l'utente).
- Il motivo è che adesso (con la zsh) anche con l'opzione -X le estensioni grafiche sono soggette alle autorizzazioni della macchina client. Nella mia macchina sono disabilitate ricezioni delle estensioni grafiche. Per superare i controlli del client si può usare ssh -Y che elimina ogni controllo, ma espone il computer a potenziali attacchi.

Esempi pratici - cont

- Cancellare il file .know-nodes (analogo in windows) e ricevere nuovamente la chiave pubblica del server. Non c'è autorità certificante in questo caso.

Esempi pratici - cont

- Cancellare il file .know-nodes (analogo in windows) e ricevere nuovamente la chiave pubblica del server. Non c'è autorità certificante in questo caso.
- Upload file con sftp.

Esempi pratici traceroute

- Il comando traceroute consente di vedere il percorso dei pacchetti dal nostro sistema al destinatario al livello IP.

Esempi pratici traceroute

- Il comando traceroute consente di vedere il percorso dei pacchetti dal nostro sistema al destinatario al livello IP.
- traceroute gordion.casaccia.enea.it

```
traceroute to gordion.casaccia.enea.it (192.107.77.13), 64 hops max, 52 byte packets
1 modemtelecom (192.168.1.1) 2.011 ms 1.282 ms 1.293 ms
2 * * *
3 172.17.65.209 (172.17.65.209) 10.135 ms 8.981 ms 8.694 ms
4 172.17.66.100 (172.17.66.100) 12.507 ms
172.17.64.129 (172.17.64.129) 11.648 ms *
5 172.17.13.190 (172.17.13.190) 14.087 ms
172.17.13.182 (172.17.13.182) 12.279 ms
172.17.13.190 (172.17.13.190) 12.913 ms
6 r-rm197-vl3.opb.interbusiness.it (151.99.29.151) 8.504 ms
r-rm197-vl4.opb.interbusiness.it (151.99.29.215) 9.257 ms 9.280 ms
7 172.17.5.210 (172.17.5.210) 10.071 ms 9.345 ms 8.526 ms
8 garr-nap.namex.it (193.201.28.15) 9.347 ms 9.315 ms 9.925 ms
9 rx2-rm2-rx1-rm2.rm2.garr.net (90.147.81.49) 9.937 ms 9.129 ms 9.884 ms
10 * rx1-rm2-ru-eneacas-l2.rm2.garr.net (193.204.217.254) 10.788 ms *
11 * * *
12 * * *

13 gordion.casaccia.enea.it (192.107.77.13) 12.596 ms 11.492 ms 11.203 ms
```

Esempi pratici traceroute

- Il comando traceroute consente di vedere il percorso dei pacchetti dal nostro sistema al destinatario al livello IP.
- traceroute gordion.casaccia.enea.it

```
traceroute to gordion.casaccia.enea.it (192.107.77.13), 64 hops max, 52 byte packets
1 modemtelecom (192.168.1.1) 2.011 ms 1.282 ms 1.293 ms
2 * * *
3 172.17.65.209 (172.17.65.209) 10.135 ms 8.981 ms 8.694 ms
4 172.17.66.100 (172.17.66.100) 12.507 ms
172.17.64.129 (172.17.64.129) 11.648 ms *
5 172.17.13.190 (172.17.13.190) 14.087 ms
172.17.13.182 (172.17.13.182) 12.279 ms
172.17.13.190 (172.17.13.190) 12.913 ms
6 r-rm197-vl3.opb.interbusiness.it (151.99.29.151) 8.504 ms
r-rm197-vl4.opb.interbusiness.it (151.99.29.215) 9.257 ms 9.280 ms
7 172.17.5.210 (172.17.5.210) 10.071 ms 9.345 ms 8.526 ms
8 garr-nap.namex.it (193.201.28.15) 9.347 ms 9.315 ms 9.925 ms
9 rx2-rm2-rx1-rm2.rm2.garr.net (90.147.81.49) 9.937 ms 9.129 ms 9.884 ms
10 * rx1-rm2-ru-eneacas-l2.rm2.garr.net (193.204.217.254) 10.788 ms *
11 * * *
12 * * *

13 gordion.casaccia.enea.it (192.107.77.13) 12.596 ms 11.492 ms 11.203 ms
```

- Verificare i diversi risultati usando la VPN e non usandola.

Esempi pratici ispezionare porte aperte

- Il comando netstat -nltu (sulla macchina babylon.casaccia.enea.it), fornisce le porte aperte per udp e tcp:

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN [22 ssh]
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN [631 stampa file in rete CUPS o IPP]
tcp 0 0 0.0.0.0:5432 0.0.0.0:* LISTEN [5432 PostgreSQL ]
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN [25 SMPT posta INTERNA ]
tcp 0 0 127.0.0.1:6010 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:27017 0.0.0.0:* LISTEN
tcp 0 0 192.107.77.12:3306 0.0.0.0:* LISTEN
tcp6 0 0 :::80 :::* LISTEN [80 HTTP ]
tcp6 0 0 :::22 :::* LISTEN [22 ssh]
tcp6 0 0 ::1:631 :::* LISTEN
tcp6 0 0 :::5432 :::* LISTEN
tcp6 0 0 ::1:25 :::* LISTEN
tcp6 0 0 ::1:6010 :::* LISTEN
udp 0 0 0.0.0.0:53932 0.0.0.0:*
udp 6912 0 0.0.0.0:5353 0.0.0.0:* [5353 Multicast DNS ricerca stampanti]
udp 0 0 0.0.0.0:631 0.0.0.0:*
udp 0 0 0.0.0.0:1900 0.0.0.0:* [5353 ssdp ricerca dispositivi di rete]
udp6 16128 0 :::5353 :::*
udp6 0 0 :::56137 :::*

udp6 52992 0 :::1900 :::*
```

Esempi pratici ispezionare porte aperte

- Nelle macchine windows il comando netstat -an -p tcp oppure udp) fornisce le porte aperte per udp e tcp.

Esempi pratici ispezionare porte aperte

- Nelle macchine windows il comando netstat -an -p tcp oppure udp) fornisce le porte aperte per udp e tcp.
- Per vedere il file con l'associazione tra protocollo/porta e servizio (applicativo) che lo richiede si deve guardare il file C:/WINDOWS/system32/drivers/etc/services

Esempi pratici ispezionare porte aperte da remoto

- dando il comando (linux) sudo nmap -sT -O babylon.casaccia.enea.it – Password:

Esempi pratici ispezionare porte aperte da remoto

- dando il comando (linux) sudo nmap -sT -O babylon.casaccia.enea.it – Password:
- Si ottiene

Starting Nmap 7.40 (https://nmap.org) at 2018-05-31 18:59 CEST
Nmap scan report for babylon.casaccia.enea.it (192.107.77.12)
Host is up (0.00063s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
3306/tcp open mysql
5432/tcp open postgresql
Device type: general purpose
Running: Linux 3.X—4.X
OS CPE: $cpe : /o : linux : linux_kernel : 3 cpe : /o : linux : linux_kernel : 4$
OS details: Linux 3.2 - 4.6
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds

- Al sito https://nmap.org/man/it/ ci sono tutte le informazioni su nmap (con nmap -A -T4 scanme.nmap.org lo vediamo) e le istruzioni per istallarlo.

Violare (hackerare) un sito o un host

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.

Violare (hackerare) un sito o un host

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Esistono i malware "hacker tools" che forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.

Violare (hackerare) un sito o un host

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Esistono i malware "hacker tools" che forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.

Violare (hackerare) un sito o un host

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Esistono i malware "hacker tools" che forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.
- Per avere una lista di comuni "hacker tools" (strumenti grafici per violare i siti) basta cercare queste parole su un motore di ricerca.

Violare (hackerare) un sito o un host

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Esistono i malware "hacker tools" che forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.
- Per avere una lista di comuni "hacker tools" (strumenti grafici per violare i siti) basta cercare queste parole su un motore di ricerca.
- L'esistenza degli "hacker tools", che sono in aumento, ha ampliato il numero di potenziali attaccanti.

Messaggio

- Abbiamo visto alcuni esempi di applicativi (sftp ed ssh) per il trasferimento di file in rete e la realizzazione di connessioni tramite shell testuali e grafiche.

Messaggio

- Abbiamo visto alcuni esempi di applicativi (sftp ed ssh) per il trasferimento di file in rete e la realizzazione di connessioni tramite shell testuali e grafiche.
- In attesa che IPv6 e conseguentemente IPsec divengano uno standard per le comunicazioni gli internet service provider utilizzano ancora ftp che è un protocollo non protetto sopra il livello trasporto.

Messaggio

- Abbiamo visto alcuni esempi di applicativi (sftp ed ssh) per il trasferimento di file in rete e la realizzazione di connessioni tramite shell testuali e grafiche.
- In attesa che IPv6 e conseguentemente IPsec divengano uno standard per le comunicazioni gli internet service provider utilizzano ancora ftp che è un protocollo non protetto sopra il livello trasporto.
- Si possono istallare dei filtri al livello IP. I server che li realizzano sono detti Firewall. I firewall possono chiudere porte a tutti o selettivamente a gruppi di IP.

Messaggio

- Abbiamo visto alcuni esempi di applicativi (sftp ed ssh) per il trasferimento di file in rete e la realizzazione di connessioni tramite shell testuali e grafiche.
- In attesa che IPv6 e conseguentemente IPsec divengano uno standard per le comunicazioni gli internet service provider utilizzano ancora ftp che è un protocollo non protetto sopra il livello trasporto.
- Si possono istallare dei filtri al livello IP. I server che li realizzano sono detti Firewall. I firewall possono chiudere porte a tutti o selettivamente a gruppi di IP.
- Per garantire il corretto dispacciamento dei pacchetti si usa sempre la coppia IP-Porta detta Socket che però può cambiare accedendo ad un diverso (AS) sistema autonomo o rete locale.

Messaggio

- Abbiamo visto alcuni esempi di applicativi (sftp ed ssh) per il trasferimento di file in rete e la realizzazione di connessioni tramite shell testuali e grafiche.
- In attesa che IPv6 e conseguentemente IPsec divengano uno standard per le comunicazioni gli internet service provider utilizzano ancora ftp che è un protocollo non protetto sopra il livello trasporto.
- Si possono istallare dei filtri al livello IP. I server che li realizzano sono detti Firewall. I firewall possono chiudere porte a tutti o selettivamente a gruppi di IP.
- Per garantire il corretto dispacciamento dei pacchetti si usa sempre la coppia IP-Porta detta Socket che però può cambiare accedendo ad un diverso (AS) sistema autonomo o rete locale.
- le reti virtuali VPN consentono di aggirare i firewall e navigare come se si fosse all'interno di un sistema autonomo.