

Your business is Internet exposed?



<http://www.infosec.it>

info@infosec.it

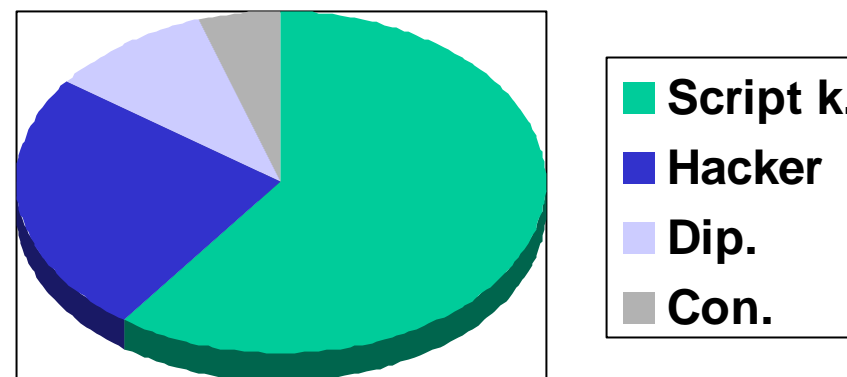
Sicurezza informatica, il problema e le soluzioni

Cos'è la sicurezza informatica?

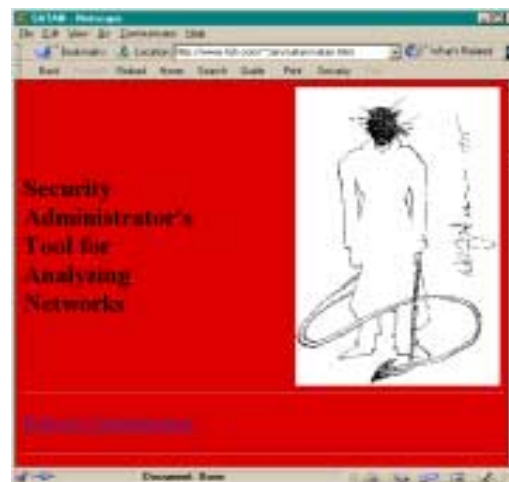
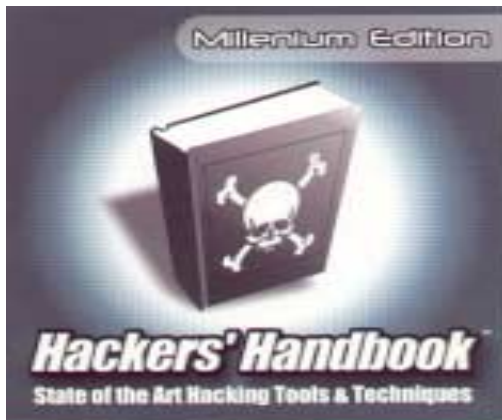
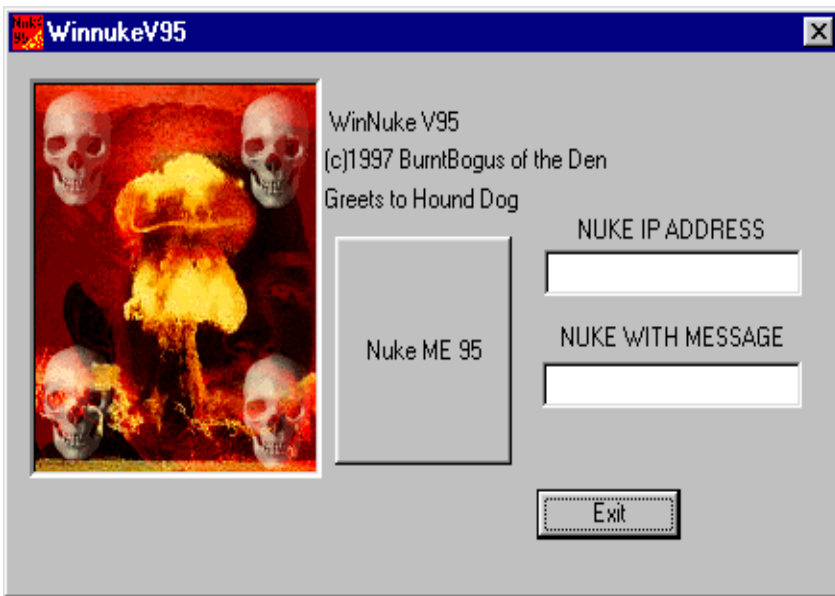
- Internet rappresenta un bacino d'utenza stimato sopra i 300milioni di utenti
- Lascereste la Vs. azienda con porte e finestre socchiuse? Senza vigilanza? Senza un sistema di allarme?

Chi ha interesse a violare una rete?

- Script kiddie
- Hacker
- Dipendenti
- Concorrenti



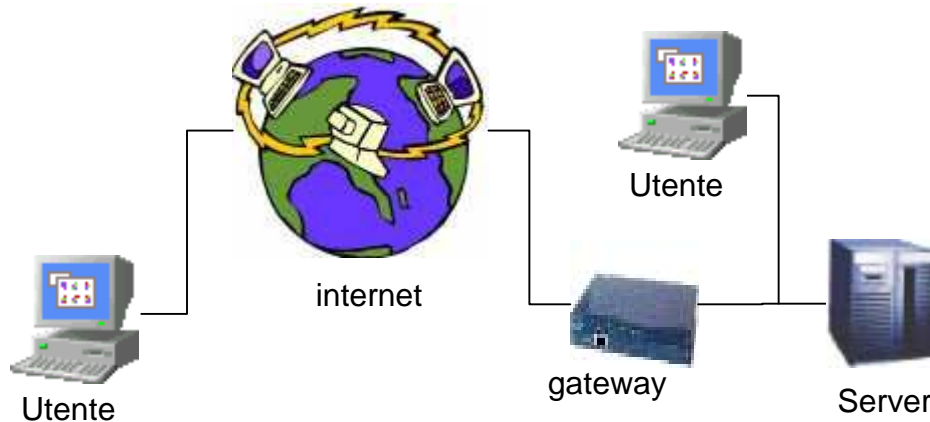
“hacker” su un motore di ricerca



SATAN



Reti

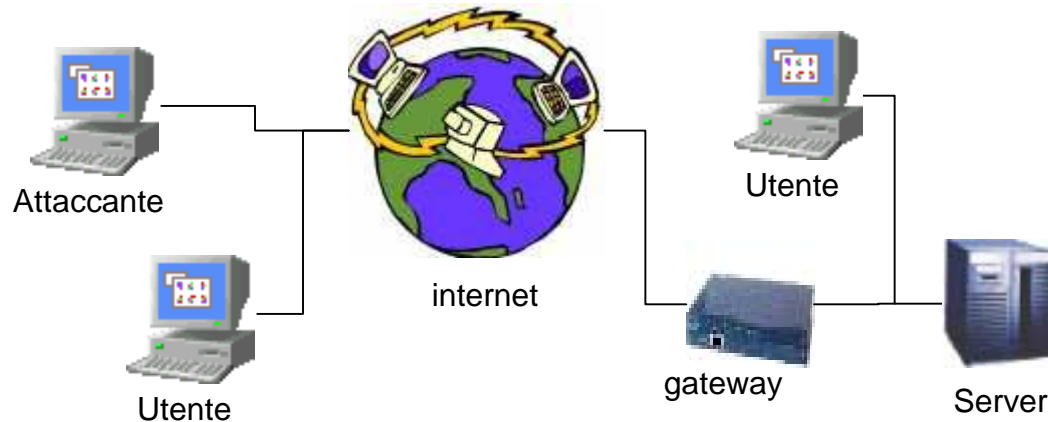


- ❑ Le reti sono uno strumento dinamico e competitivo che permette di condividere informazioni e dati in maniera molto rapida ed efficace.
- ❑ La scontata sicurezza delle reti derivante dalla complessità dello strato tecnologico è un falso clamoroso.
- ❑ I pericoli del “mondo reale” si ritrovano in forma tecnologica anche nella rete, il fatto che siano “tecnologicamente complessi” non implica che siano meno tangibili o meno pericolosi.
- ❑ L’apertura delle reti verso l’esterno e l’interconnessione sono potenziali pericoli, lavorare in sicurezza implica ridurre al minimo i rischi.

La situazione di insicurezza odierna è dovuta ad alcuni fatti:

- i fornitori di software tagliano test e verifiche di sicurezza per limitare i costi;
- la comunità informatica trova i problemi di sicurezza lavorando sui prodotti;
- per garantire democraticamente la salvaguardia delle informazioni vengono pubblicati i problemi di sicurezza (da governi, gruppi di cittadini, associazioni di tutela);
- bisognerebbe difendere e mantenere i sistemi in funzione dei problemi di sicurezza che vengono scoperti e pubblicati;
- le aziende hanno il problema principale di far funzionare i sistemi e non si pongono il problema di operare in sicurezza

Attacchi alle reti



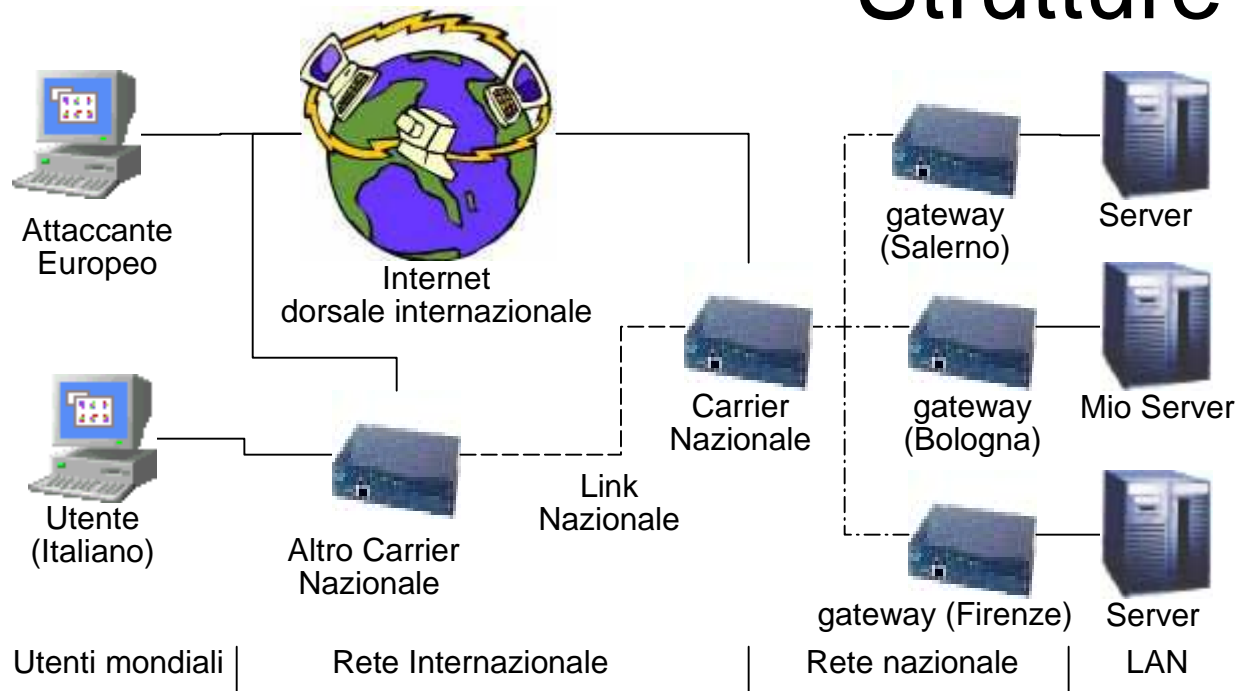
- ❑ Nel momento in cui una rete e' connessa chiunque sia collegato alla rete puo' portare degli attacchi con diversi fini:
 - ✓Ottenere informazioni;
 - ✓Ottenere risorse in rete;
 - ✓Nascondere la propria identita';
 - ✓Colpire la rete e bloccarne il funzionamento;
- ❑ Buona parte degli attacchi vengono condotti da ex-dipendenti che vogliono vendicarsi nei confronti dell'azienda.
- ❑ Altri attacchi vengono portati in maniera automatizzata da computer collegati alla rete che visto il grande numero di macchine cercano di penetrare indiscriminatamente in quelle non difese senza sapere a priori chi siano gli amministratori.

La struttura delle reti e' in ordine gerarchico con una struttura piramidale:

- Internet mondiale;
- Governi e multinazionali;
- Carrier nazionali;
- Provider locali
- Aziende;
- Privati cittadini;

E' da notare il fatto che e' possibile portare attacchi a qualunque componente della scala, specialmente a coloro che hanno un collegamento fisso alla rete, in particolare esistono una serie di strumenti automatizzati per raccogliere informazioni e portare attacchi nella maniera piu' efficace al fine di ottenere altri strumenti.

Strutture

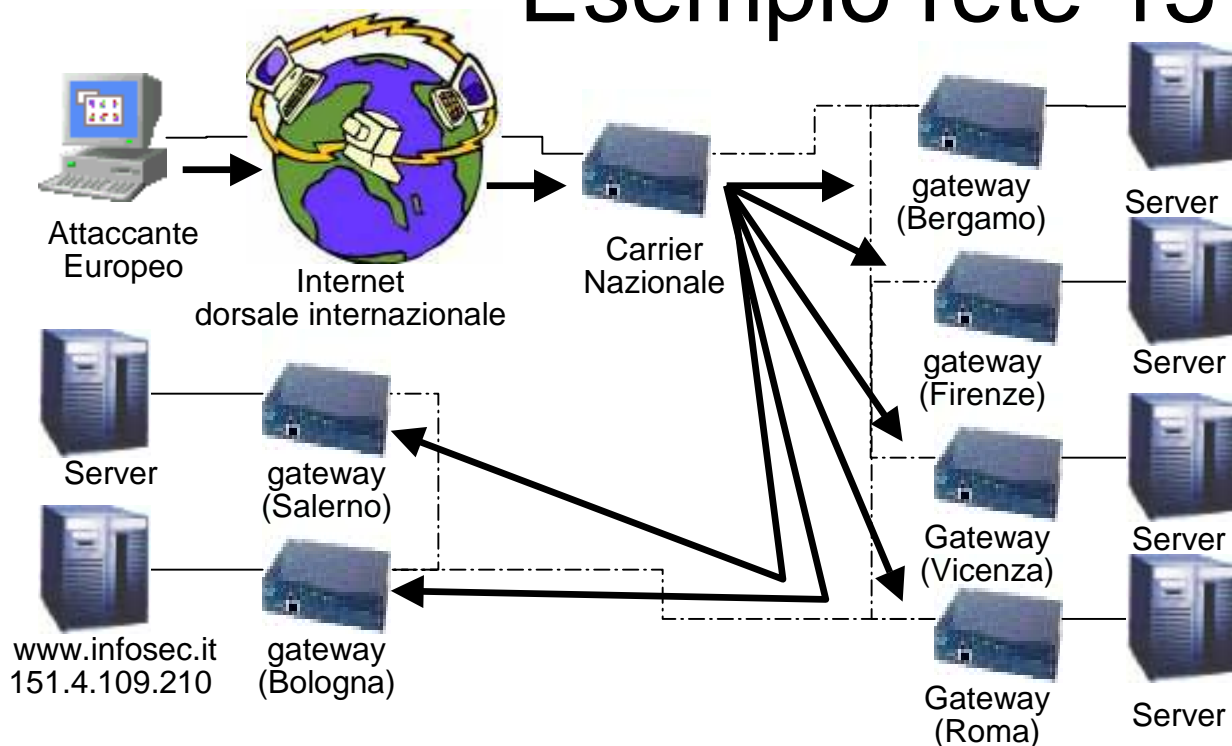


Punti di riflessione relativi alle strutture di rete:

- ❑ Nel momento in cui una rete e' connessa alla Rete viene connessa ad un sistema di internetwork mondiale.
- ❑ Un potenziale attaccante europeo mediamente fornito di strumenti tecnologici potrebbe completare degli attacchi mirati ad una vulnerabilita' specifica in pochi giorni.
- ❑ Un potenziale attaccante mondiale abbondantemente fornito di strumenti tecnologici potrebbe completare degli attacchi mirati ad intere nazioni in pochi giorni.

- una rete efficiente per trasportare dati e informazioni legittime in maniera veloce funziona altrettanto bene per operazioni illegali;
- sottovalutare cosa succede sulla propria rete non impedisce che vengano portati attacchi;
- non mantenere, aggiornare e verificare periodicamente il sistema, genera dei meccanismi di invecchiamento e di vulnerabilita';
- non reagire quando si e' verificata una penetrazione implica il fatto di essere alla merce' degli intrusi;
- avere consapevolezza della propria rete non e' un optional ma una necessita' per poterla gestire correttamente.

Esempio rete 151.4.109.x

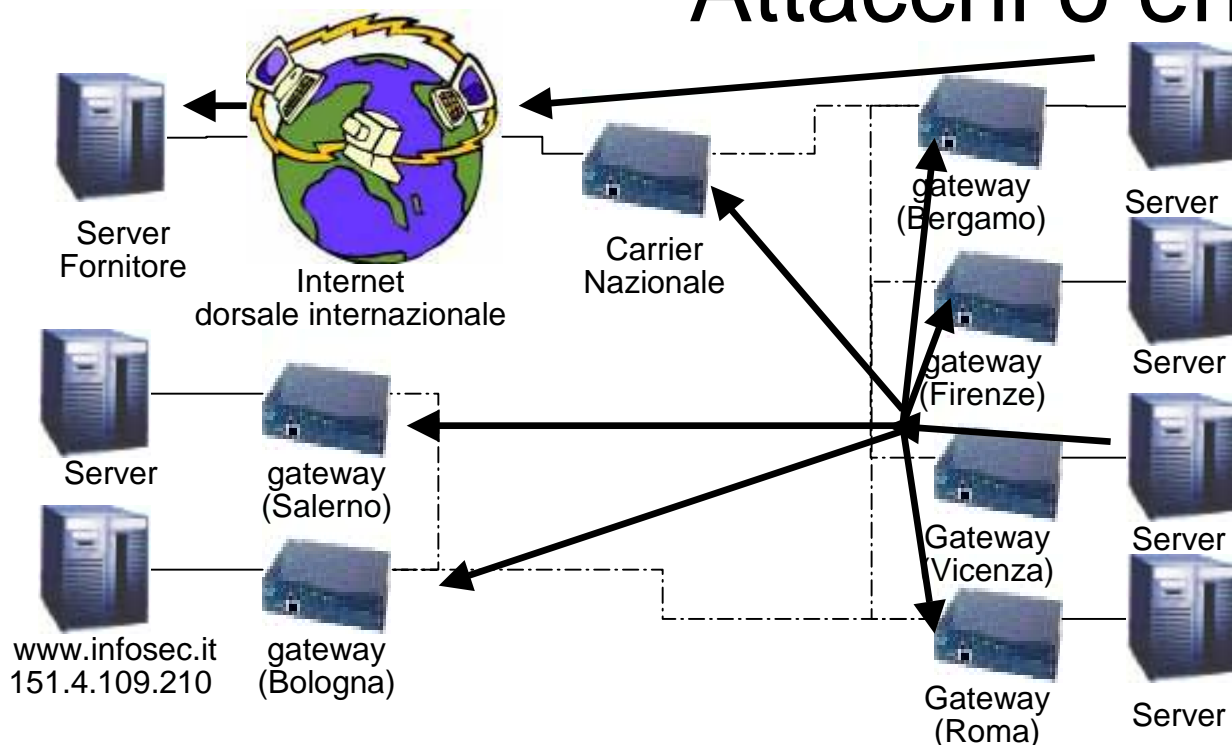


- ❑ Quindi per esempio portare un attacco ad una rete di duecento cinquantaquattro computer (al massimo) per colpire una ditta che si occupa di sicurezza informatica puo' portare a coinvolgere una serie di ditte/computer/citta'/persone che sono legate solo per "rapporti di vicinato" alla vittima che si intendeva colpire.
- ❑ Un intruso che cerchi di colpire una vittima puo' "erroneamente" colpire un bersaglio (in termini informatici) vicino alla vittima sia per scarsa attenzione che per volersi avvicinare all'obiettivo, entrano in causa anche i fini dell'attacco voluto. (A volte sono gli stessi strumenti informatici che "colpiscono" intere reti "di default").

Esempio di rete (151.4.109.x):

- inetnum: 151.4.109.0 - 151.4.109.15
descr: Bergamo Jolly S.r.l.
address: I-24124 Bergamo (BG)
- inetnum: 151.4.109.16 - 151.4.109.31
descr: Internet Provider
address: I-50122 Firenze
- inetnum: 151.4.109.32 - 151.4.109.63
descr: VEM spa
address: I - 36078 - Valdagno (VI)
- inetnum: 151.4.109.80 - 151.4.109.95
descr: Fed. Naz. delle Imprese di Pesca
address: I-00198 Roma (RM)
- inetnum: 151.4.109.192 - 151.4.109.207
descr: Web Service
address: I-84012 Angri (SA)
- inetnum: 151.4.109.208 - 151.4.109.223
descr: Infosec s.r.l.
address: I-40133 Bologna

Attacchi o errori ?



- ❑ Spesso errori di configurazione nelle reti (in configurazioni particolari per ignoranza degli amministratori) causano la trasmissione involontaria di informazioni sensibili “ai propri vicini”;
- ❑ La controparte del fatto di ricevere informazioni da altre reti e’ quella di mandare proprie informazioni ad altre reti per errori di configurazione;
- ❑ Inoltre ci sono una serie di software che in maniera indebita inviano informazioni “riservate” ai fornitori dei programmi (che sono sostanzialmente degli sconosciuti che abusano di software per ottenere informazioni);

La gestione e l’amministrazione sicura di una rete implicano diversi tipi di operazioni:

- Pianificazione e progettazione in ottica di sicurezza;
- Installazione e utilizzo di sistemi di sicurezza;
- Verifiche di sicurezza e monitoraggio dei sistemi;
- Studio di procedure per affrontare al meglio i possibili problemi e/o rischi;
- Formazione del personale relativamente a problemi di sicurezza sia di server che di reti, nonché ad una corretta manutenzione.

Il rischio nel non seguire queste procedure e’ quello di lasciare in balia di qualcuno le proprie infrastrutture, i propri dati ed il lavoro dei propri dipendenti.

Le soluzioni?

- Esistono soluzioni Hardware e Software ma, per la natura intrinseca di questi prodotti, non saranno mai sufficienti al problema
- Non esiste e non esisterà mai una soluzione definitiva

La soluzione!

Dobbiamo ridurre gli attacchi

- Esistono i mezzi per ridurre drasticamente i rischi
- Esistono esperienze consolidate nel tempo
- Esistono metodologie, know-how specifici, soluzioni dedicate

Consapevolezza = Fattore rischio

- L'amministratore di sistema mi ha garantito che i nostri sistemi informatici sono sicuri. Perché dovrei fare una verifica?
- Perché un test di sicurezza?
- Perché in outsourcing?

Responsabilita':

Il responsabile della sicurezza ed il responsabile del trattamento dei dati personali sono i principali soggetti ad essere direttamente coinvolti; a loro vengono delegate queste funzioni, a loro ci si rivolge quando sorgono i problemi.

- Il Test di Sicurezza permette a tutti i soggetti di accertare e documentare la corrispondenza tra lo stato di fatto e lo stato dell'arte richiesto dalla Legge (L.675/96 e DPR318/99).
- Permette di assumere le proprie responsabilita' in modo chiaro, senza essere soggetti a rischi di cui non si è a conoscenza e individuare le aree di scarsa protezione.
- Fornisce informazioni preziose per la predisposizione di un solido piano di sicurezza.

Investimenti

- Quanto vale il patrimonio aziendale?
- Che valore ha il nostro database?
- Possiamo permetterci una perdita o una compromissione dei nostri dati aziendali?
- La ns. vetrina sul Web rispecchia l'immagine aziendale, e se domani contenesse pubblicita' negativa verso i nostri servizi e prodotti?

I costi

- Le percentuali di spesa per la messa in sicurezza della propria rete sono proporzionali al costo di un'antifurto per una automobile

Your business is Internet exposed?

<http://www.infosec.it>

Are you ready?