END

PORT SCANNING

- Definizione e Premesse
- Modalità
- Risposte
- Etica e Legalità

END

DEFINIZIONE

È una tecnica informatica progettata per sondare un server o un host stabilendo quali porte siano in ascolto sulla macchina inviando delle richieste, stabilendo quali servizi di rete siano attivi su quel computer analizzato.

PREMESSE

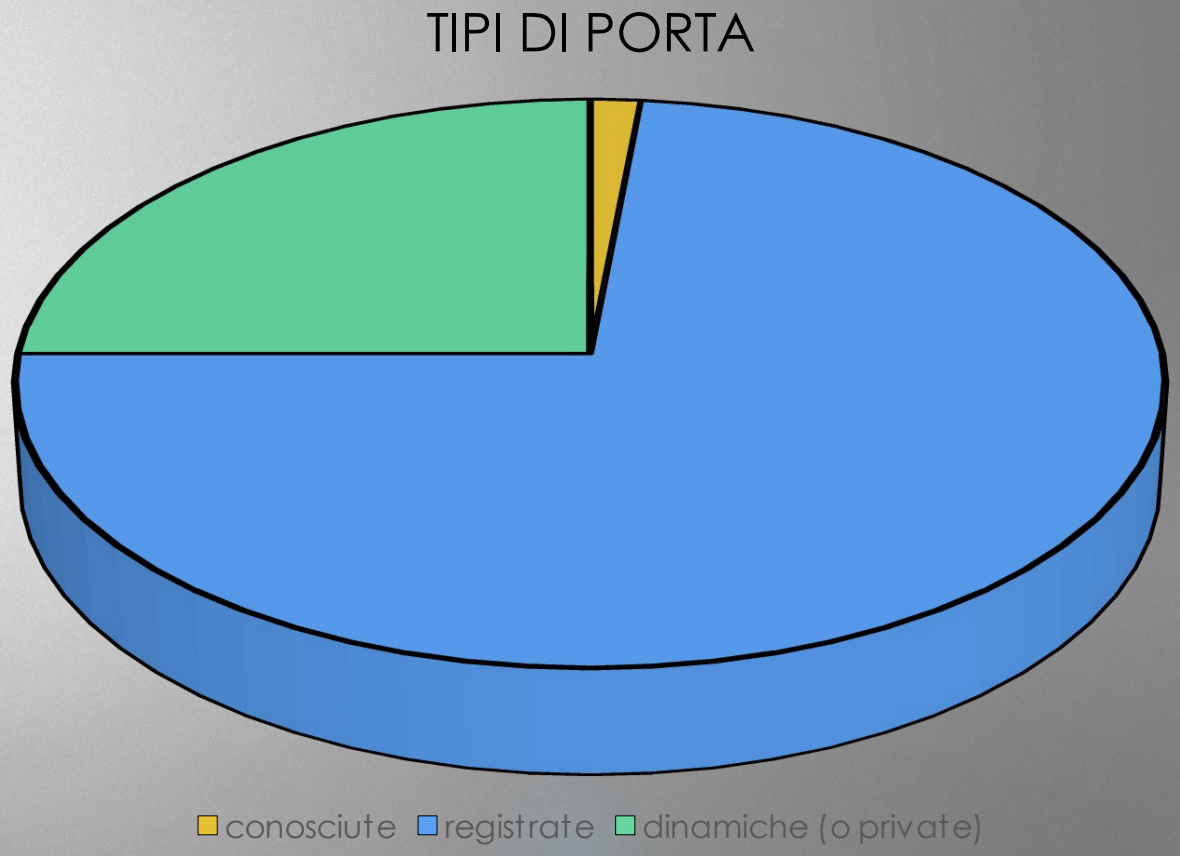
Tutte le forme di port scanning si basano sul presupposto che l'host mirato è conforme a RFC 793 Transmission Control Protocol.

PORTA

END

È una sequenza di 16 bit utilizzati al livello di trasporto da TCP e UDP per riconoscere un'applicazione che opera su rete.

- CONOSCIUTE ("*well known ports*"): dalla 0 alla 1023
- REGISTRATE ("*registered ports*"): dalla 1024 alla 49151
- DINAMICHE O PRIVATE ("*dynamic and/or private ports*"): dalla 49152 alla 65535

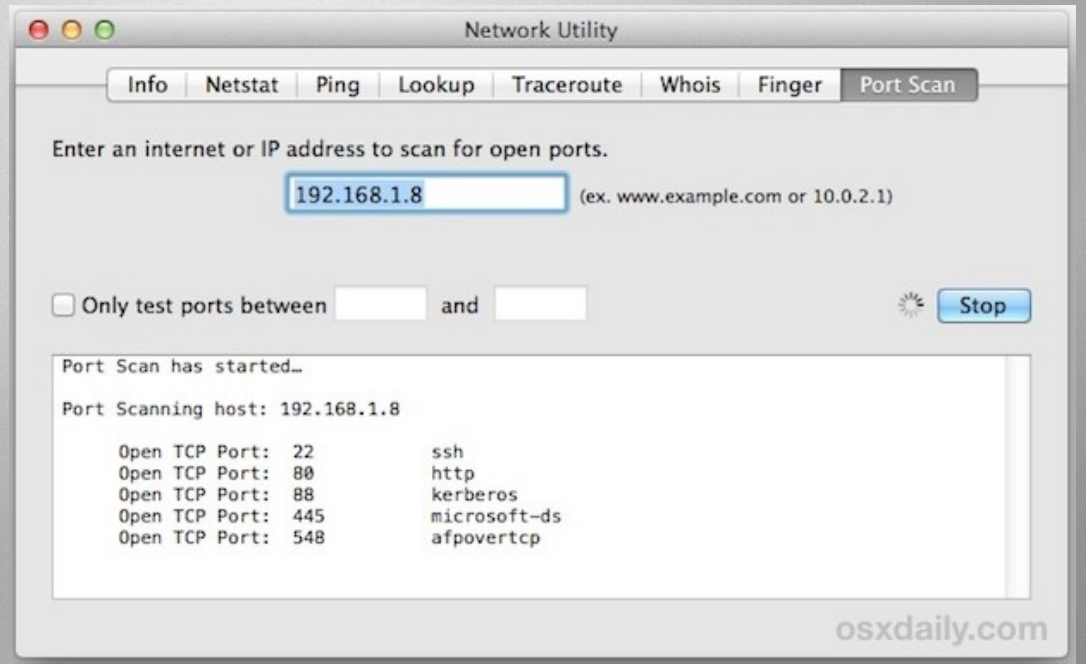


MODALITÀ

END

LENTA: della durata di diversi giorni; può nascondere le richieste di accesso effettuate con pacchetti-*civetta* in mezzo alle altre richieste "lecite", così da *dissimulare* il comportamento fraudolento e non far scattare alcun allarme.

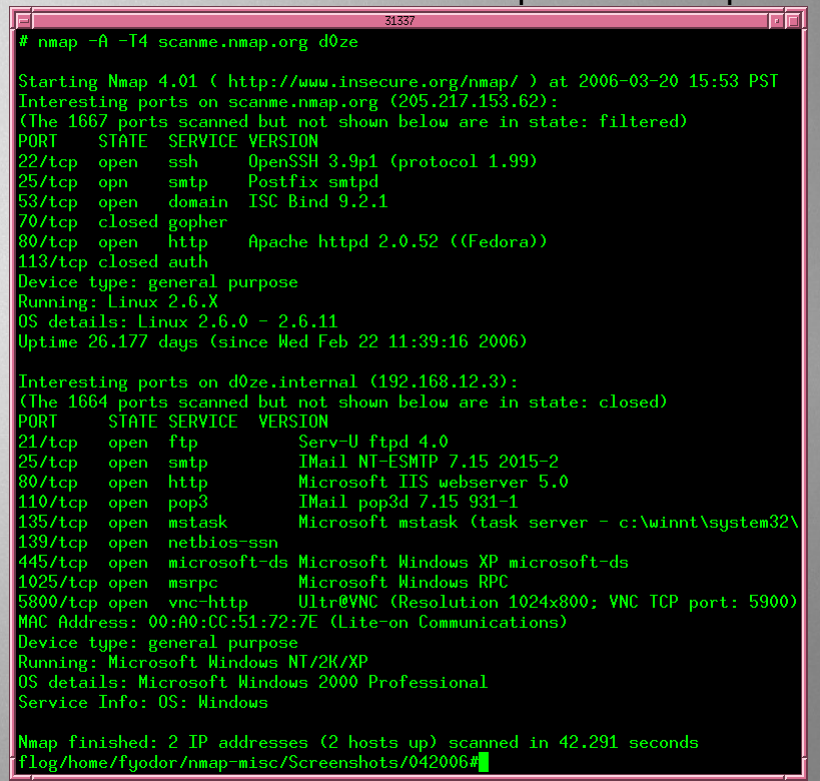
VELOCE: dura poche decine di secondi; inondazione di richieste; alta probabilità che l'amministratore del sistema obiettivo si accorga di una tale ondata di richieste di accesso anomale e quindi prenda le adeguate contromisure.



RISPOSTE

END

- APERTA (accepted): indica una porta in ascolto.
- CHIUSA (denied): le connessioni alla porta saranno rifiutate.
- BLOCCATA/FILTRATA (dropped/filtred): nessuna risposta causata da una possibile presenza di un firewall che ne impedisce il collegamento.



END

ETICA

Utilizzato dagli amministratori per verificare le politiche di sicurezza delle loro reti, e dagli hacker per identificare i servizi in esecuzione su un host e sfruttarne le vulnerabilità.
Le informazioni raccolte da un port scan possiedono molti usi legittimi; tuttavia può anche essere utilizzato per compromettere la sicurezza. Il livello di minaccia causato da un port scan può variare a seconda del metodo utilizzato, il tipo di porta scansionata, il suo numero e l'amministratore che controlla l'host. La probabilità di un attacco è più elevata quando il port scan è associato ad una scansione con un vulnerability scanner.

LEGALITÀ

I casi che coinvolgono le attività di port scanning sono un esempio delle difficoltà incontrate nel giudicare tali violazioni. Anche se questi casi sono rari, la maggior parte delle volte il processo legale richiede che venga dimostrato l'intento di commettere un brake-in o l'esistenza di accessi non autorizzati, piuttosto che l'esecuzione di un port scan.

END

RFC 793 - TRANSMISSION CONTROL PROTOCOL

È un documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet. Attraverso l'Internet Society gli ingegneri o gli esperti informatici possono pubblicare dei memorandum, sotto forma di RFC, per esporre nuove idee o semplicemente delle informazioni che una volta vagliati dall'IETF possono diventare degli standard Internet.

VULNERABILITY SCANNER

È un programma per controllare la vulnerabilità di un computer.