Facoltà di Scienze Matematica Fisica e Naturali

I NETWORK SCANNER

A cura di:
Acunzo Gaetano
Mariano Andrea
Punzo Ivano
Vitale Valentino

NETWORK SCANNER

- Introduzione
- Cos'è un network scanner
- L'evoluzione
- Gli scanner sono legali?
- Alcuni scanner più famosi
- Uno scanner in particolare

Introduzione

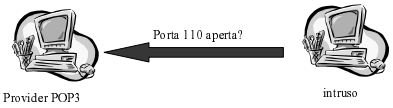
Qual è la prima cosa che un hacker si chiede quando prova ad attaccare un sistema remoto?

- Quali sono i servizi attivati sulla macchina da colpire
- Quale S.O. è in esecuzione sulla macchina

Cos'è un network scanner

- Il protocollo TCP/IP dispone di una serie di ***porte***
- Le porte vengono utilizzate per far comunicare le applicazioni

Un esempio di attacco:



Cos'è un network scanner

Altri attacchi si possono effettuare su:

- il servizio di invio posta, SMTP, porta 25
- il servizio telnet, porta 23
- HTTP, porta 80

Controllare manualmente una serie di macchine senza l'ausilio di un programma si rivela un'operazione lenta ed inefficace

Cos'è un network scanner

- per evitare perdite di tempo nel controllo delle porte "aperte", sono nati programmi di controllo di tali porte
- Tali programmi sono i cosiddetti ***Portscanner*** o ***Network scanner***
- ***Uno scanner scopre quindi la vulnerabilità dei sistemi***

Un esempio primitivo

```
#!usr/bin/perl
$count == 0;
open(MAIL, "|/usr/lib/sendmail mikal") || die "Cannot open mail\n";
print MAIL "To: Administration\n";
print MAIL "Subject: Password Report\n";
print MAIL "Reply-To: Password-scanner\n";
open(PASSWORD,"cat /etc/passwd|");
while (<PASSWORD>) {
        $linenumber = $.;
        @fields = split(/:/, $);
        if($fields[1] eq "") {
```

Un esempio primitivo

```
            $count++;
            print MAIL "Line $linenumber has a blank password. \n";
            print MAIL "Here's the record: @fields \n ";
          }
      }
close(PASSWORDS);
if ($count < 1) {
     print MAIL " I found no blank password fields \n";
}
print MAIL " \n";
close(MAIL);
```

Un esempio primitivo

- Questo programma scansiona /etc/passwd, guardando se ci sono campi vuoti.
- Per ogni campo vuoto trovato, avvisa via e-mail l'utente

Cos'è un network scanner

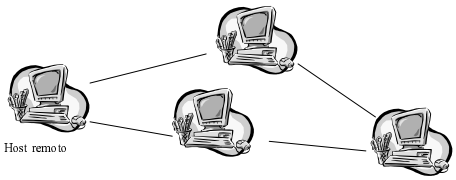
A seconda delle debolezze che sfruttano gli scanners, si collocano in due categorie:

- ***System scanners***

- i System scanners analizzano un host locale
- rilevano la vulnerabilità del sistema

Cos'è un network scanner

- ***Network scanners***



- i network scanner analizzano i servizi e le porte di host remoti

L'evoluzione

Per valutare uno scanner è importante tener conto di alcuni particolari:

- Deve permettere l'inserimento arbitrario di inizio e fine scansione
- Deve poter controllare un gruppo di porte o una porta in particolare
- Deve permettere il salvataggio della scansione
- Deve permettere di attivare più scansioni in parallelo

L'evoluzione

Sebbene i network scanner differiscono sotto alcuni punti di vista, essi condividono alcune caratteristiche tra cui la ***logica nei processi.*** La maggior parte segue questa sequenza:

- Carica un insieme di regole o attacchi
- Testa l'obbiettivo all'interno di questi parametri
- Riporta i risultati ottenuti

Gli scanner sono legali?

- alcuni considerano questa attività criminale

- Altri pensano che avendo un sito internet si è dato un permesso implicito, consentendo quindi di essere analizzati dagli scanner

Gli scanner sono legali?

- Fino ad oggi nessuna legge è stata scritta contro gli scanner.

Per ora quindi la risposta è: SI

Alcuni scanner più famosi

- SATAN
- CGI SCANNER
- COLDSCAN
- ISS (Internet Security Scanner)
- DNSWALK
- DOC

Uno scanner in particolare

Satan

- Introduzione al Satan
- Satan
- Metodologie di lavoro utilizzate dal Satan
- Fiducia (Trust)
- Requisiti Hardware
- File di configurazione del Satan
- Pericoli nell'uso
- Controllare il Satan
- Conclusioni sul Satan

Introduzione al Satan

- Ideato da Dan Farmer (Aprile 1995)
- Security Analisys Tool for Auditing Network
- Raccoglie informazioni di host remoti e reti
- Utilizza alcuni servizi di rete

Satan

- Trova falle nella sicurezza del sistema
- Utilizza servizi di rete come: Finger, Nfs, ftp, Tftp, Rexd ed altri
- Tali servizi devono essere configurati in modo adeguato
- Utilizza come interfaccia un qualunque Html Broswer

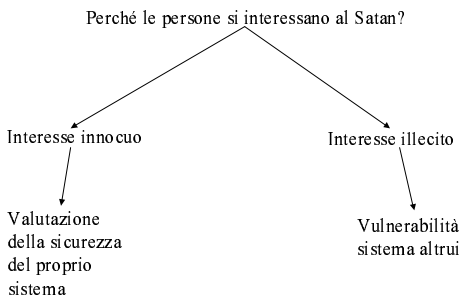
Satan

- Utilizzando il Satan è possibile ottenere varie informazioni :
  - Topologia della rete
  - Servizi di rete in esecuzione
  - Tipo di software usato sulla rete
  - Tipo di Hardware usato sulla rete

Satan

- Valuta le vie di fiducia(Trust)
- Valuta le dipendenze tra i vari host
- Controlla gli host secondari sulla base dei dati raccolti
- Le informazioni raccolte possono essere usate per raggiungere un buon grado di sicurezza

Satan



Satan

Il tool Satan è stato progettato per i seguenti obbiettivi:

1) Scoprire se i problemi di organizzazione della sicurezza di vaste reti erano risolvibili
2) Progettare un pacchetto software sulla sicurezza che risulti didattico e facile da usare
3) Creare un tool che fosse disponibile per qualsiasi persona che ne avesse bisogno

Satan

4) scoprire come divulgare la sicurezza e le informazioni sulle reti senza essere distruttivo

5) Creare il migliore 'investigatore' sulla sicurezza delle reti

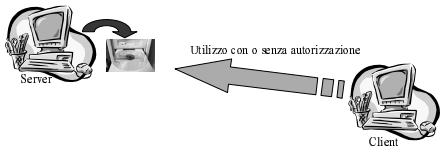
6) Mostrare come sia decisamente insicura Internet attualmente, e come molti siti dipendendo da molti altri siti siano potenzialmente insicuri

Metodologia di lavoro

- Il Satan richiede l'acquisizione dell'obiettivo (target), utilizza il comando 'fping' per tale operazione
- Una lista di obiettivi vivi viene passata ad un processo, che eseguirà operazioni per ogni obiettivo
- I risultati dell'analisi sono salvati in un file

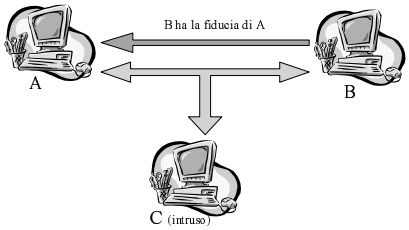
Fiducia (Trust)

- Significato di fiducia



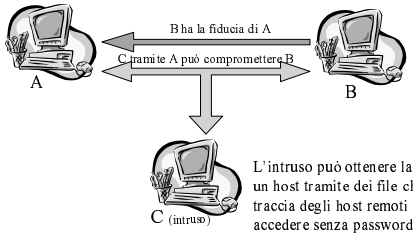
Fiducia (Trust)

- La fiducia gode della proprietà transitiva



Fiducia (Trust)

- La fiducia gode della proprietà transitiva



L'intruso può ottenere la fiducia da un host tramite dei file che tengono traccia degli host remoti e quindi accedere senza password

Requisiti Hardware

- Satan non lavora con tutti i Sistemi Operativi
- Satan richiede 20 MB di spazio per l'istallazione
- Necessita di almeno 14 MB di RAM
- Per eseguire Satan è necessario essere 'root'

File di configurazione

- SATAN crea e usa pochi file
- File che il SATAN utilizza durante la sua esecuzione:
  - bin/* (programmi da cui Satan dipende per l'acquisizione dei dati)
  - config/* (file di configurazione di Satan)
  - html/* (programmi che generano le pagine per l'interfaccia utente)
  - perl/* (codice utilizzato dal Satan o dai 'Tool' di acquisizione dati)

File di configurazione

- File che il SATAN utilizza durante la sua esecuzione:
  - result/database-name ogni database è composto di tre parti :
    - all-hosts (lista degli hosts che Satan ha trovato durante l'esplorazione compresi quelli non toccati)
    - facts (responso della scansione del Satan)
    - todo (elenca gli hosts e le incursioni che ha intrapreso contro di essi)
  - rules/* (regole utilizzate dal Satan)
  - src/* (codice sorgente di alcuni programmi di supporto al Satan)

File di configurazione

Il file *config/satan.cf* controlla le azioni del Satan

- livello di incursione
- esplorazione di hosts e reti
- test eseguiti

Questo file è scritto in linguaggio Perl

File di configurazione

Opzioni del file config/satan.cf :

- livello di attacco

```
#Default attack level (0=light, 1=normal, 2=heavy)
     $attack_level = 0;
```

- Contengono programmi per l'esplorazione del server remoto

File di configurazione

- Attacco *light* :

```
@light =(
        'dns.satan',
        'rpc.satan',
        'showmount.satan?',
       );
```

SI

SI

?

File di configurazione

- File di stato

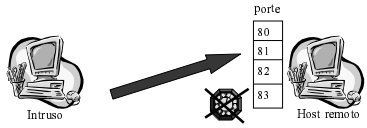
```
$status_file = "status_file";
```

- tiene traccia del risultato dell'ultimo attacco
- viene aggiornato ad ogni nuova incursione

File di configurazione

• Tempi di attesa

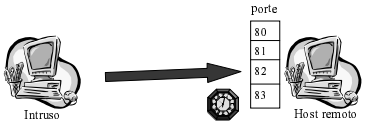
```
$slow_timeout = 60;
$med_timeout = 20;
$fast_timeout = 10;
```



File di configurazione

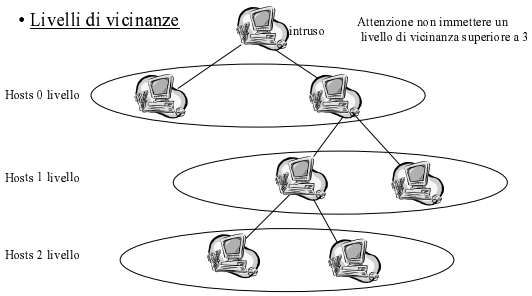
• Tempi di attesa

```
$slow_timeout = 60;
$med_timeout = 20;
$fast_timeout = 10;
```

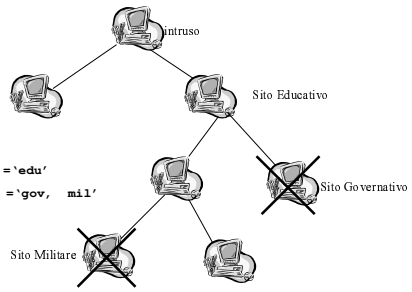


File di configurazione

• Livelli di vicinanze



File di configurazione



• variabili

```
$only_attack_these ='edu'
$dont_attack_these ='gov,  mil'
```

Pericoli nell'uso

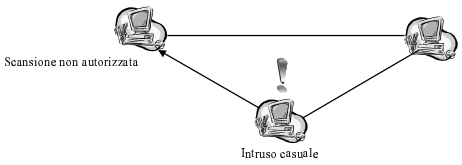
• Il Satan può essere pericoloso?

SI

Ragioni :
- System Crackers
- Superare i limiti di autorizzazione

Pericoli nell'uso

System Crackers



Controllare il Satan

- Il Satan non si avventurerà mai al di là del livello di vicinanza
- La variabile di selezione del target "$only_attack_these"
- La variabile "dont_attack_these"

Conclusioni sul Satan

Conclusioni sul Satan

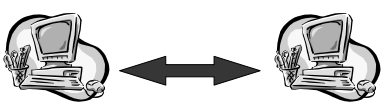
- Scopo principale
  - aiutare l'amministratore del sistema
  - testare un prodotto per il mondo telematico
- Prospettive per il futuro
  - aumentare l'efficienza del prodotto

Progetto Network Scanner

- Fondamenti del TCP/IP
- La nascita del WinSock
- Nomi di domini e indirizzi IP
- Che cosa sono le porte
- Implementazione del Network Scanner
- Funzioni principali
- Bibliografia

Fondamenti del TCP/IP

- Lo scambio di informazioni tra computer e computer richiede che questi siano in grado di parlare un linguaggio comune



Fondamenti del TCP/IP

- I protocolli in TCP/IP sono organizzati in una serie di livelli

Stack di protocolli

HTTP	Telnet	FTP	SMTP	Finger
Secure Socket Layer (SSL)				
Transmission Control Protocol (TCP)				
Internet Protocol (IP)				

La nascita del Winsock

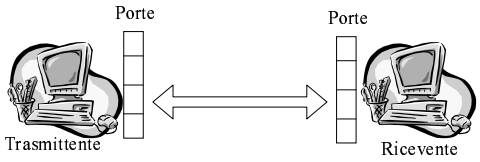
- Winsock è uno standard che è mantenuto da Microsoft
- Winsock è composto da un insieme di routine
- Le routine descrivono le comunicazioni da e per lo stack TCP/IP
- Winsock comunica con stack TCP/IP e lo stack TCP/IP comunica con Internet

Nomi di domini e indirizzi IP

- Riconoscimento di computer remoti
- Un indirizzo IP identifica univocamente un computer connesso alla rete
- L'indirizzo IP è un numero di quattro byte
- DNS (Domain Name Service)

Che cosa sono le porte

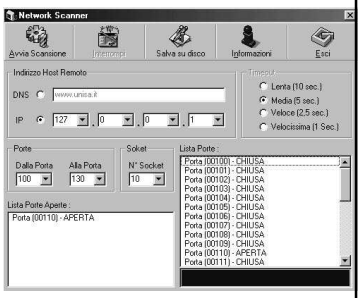
- Una porta è una speciale locazione di memoria



Implementazione del Network Scanner

L'interfaccia grafica del nostro Scanner

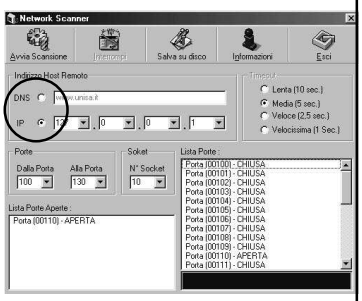
- Utilizzo semplice e veloce di tutte le sue parti
- Facile consultazione dell'output



Implementazione del Network Scanner

Opzioni di immissione del Target Host

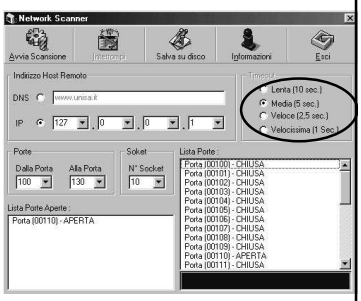
- Tramite DNS
- Tramite IP



Implementazione del Network Scanner

Time Out variabile

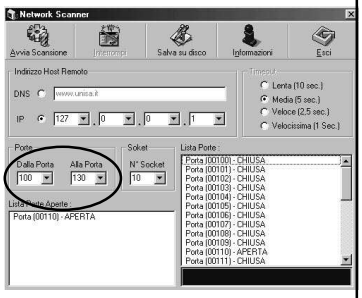
- 10 sec.
- 5 sec.
- 2,5 sec.
- 1 sec.



Implementazione del Network Scanner

Porte da controllare

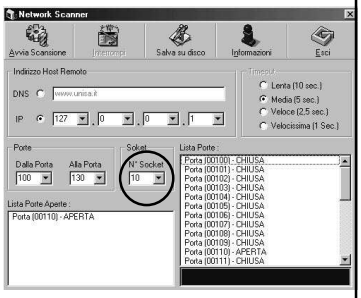
- Il numero di porte può essere variabile
- Può essere controllata anche una singola porta



Implementazione del Network Scanner

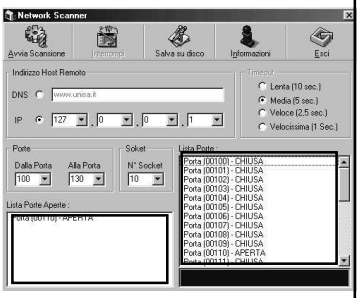
Numero di socket da utilizzare nella scansione

- Aumentando il numero di socket diminuisce il tempo di scansione
- Troppi socket potrebbero richiedere un numero eccessivo di risorse



Implementazione del Network Scanner

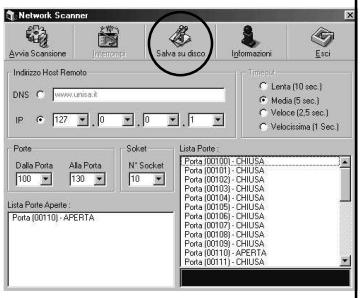
- Lista di porte visitate con il relativo stato
- Lista delle sole porte aperte



Implementazione del Network Scanner

- Si può effettuare un salvataggio della scansione per un eventuale consultazione futura

```
Network Scanner
Scansione del : 02/06/00
ore : 20.24.26
Host : 127.0.0.1
Porta (00001) - CHIUSA
Porta (00002) - CHIUSA
Porta (00003) - CHIUSA
Porta (00004) - TIME OUT
Porta (00005) - CHIUSA
Porta (00006) - TIME OUT
Porta (00007) - CHIUSA
Porta (00008) - CHIUSA
Porta (00009) - CHIUSA
Porta (00010) - APERTA
Porta (00011) - CHIUSA
```



Funzioni principali

- Procedura Connect
  - Creazione dinamica di socket
  - Connessione parallela dei socket
- Procedura Disconnect
  - Deallocazione della memoria associata ai socket
  - Chiusura dei socket

Funzioni principali

- Nella creazione del Network Scanner un fattore importante è la sincronizzazione dei socket

Problemi di sincronizzazione :

- Connessione all'host
- Errore di connessione
- Tempo scaduto (Time Out)

Bibliografia

[1] http://packetstorm.securify.com

[2] http://telemat.die.unifi.it/book/Unix/Hacker

[3] Nux Network Security

[4] ftp://ftp.switch.ch/mirror/security

Avvertenze

Maneggiare con cautela !!!