

Rilevazione dei Portscanning

Docente del Corso :
Prof. De Santis Alfredo

Relatori :

Capuano Giuseppe
Veropalumbo Edoardo
Vittore Emanuele

Introduzione

- Concetti Preliminari
- Obiettivi
- Portscanning
- Scan Detector

Concetti Preliminari

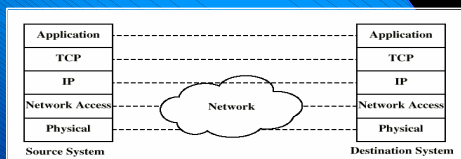
- Modello TCP/IP
- Three Way Handshake

Modello TCP/IP

- Strutturato in cinque livelli
- Sviluppato da Cerf e Kahn per DARPA (*Defense Advanced Research Projects*) nel '74
 - progetto operativo con tempi di definizione molto brevi
 - ha portato alla realizzazione di ARPANET
- Suite di protocolli per standardizzare la comunicazione tra computer
 - alla base della rete Internet

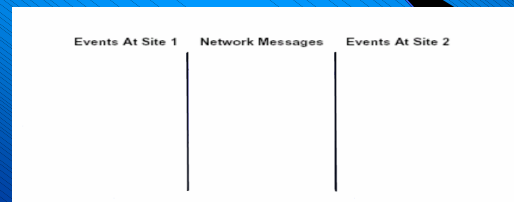
Livelli di TCP/IP

- livello delle applicazioni
- livello di trasporto (protocolli TCP o UDP)
- livello di internetworking (protocollo IP)
- livello di accesso alla rete
- livello fisico



Three Way Handshake

Scambio di messaggi tra client ed server per stabilire una connessione TCP.



Obiettivi

PROBLEMA

SOLUZIONE

Portscanning



Sicurezza su Reti: Rilevazione del Portscanning

7

Scan detector



Portscanning

è un processo di connessione a porte TCP e UDP di un sistema al fine di determinare quali servizi siano in **esecuzione** o stato di **listening**.

Sicurezza su Reti: Rilevazione del Portscanning

8

Scan Detector

è una tecnica per la rilevazione dei portscanning.

Sicurezza su Reti: Rilevazione del Portscanning

9

Scan Detector: Software

- Klaxon
- Portsenry

Sicurezza su Reti: Rilevazione del Portscanning

10

Klaxon

- software freeware per ambienti Unix e Linux
- ultima versione è la 1.0 e risale al 1998.
- è reperibile sul sito :
<http://www.ja.net/CERT/Software/klaxon>

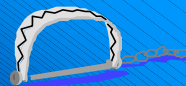
Sicurezza su Reti: Rilevazione del Portscanning

11

Klaxon: Idea di base

piazzare una "trappola" per ogni servizio che si intende salvaguardare (telnet, talk, ftp ...).

Una "Trappola" è un servizio fittizio che sostituisce quello reale.



Sicurezza su Reti: Rilevazione del Portscanning

12

Klaxon: Installazione

Compilazione dei sorgenti del programma Klaxon

```
bash-2.05# ls
Makefile README Klaxon.c wire.c rfc931.o
bash-2.05# make
make[1]: Entering directory '/root/Desktop/Klaxon/Klaxon'
cc -DDEBUG -DHOME -DLOG -DLOGDIR -c -o Klaxon.o Klaxon.c
cc -DDEBUG -DHOME -DLOG -DLOGDIR -c -o rfc931.o rfc931.c
cc -o Klaxon ./Klaxon.o Klaxon.o rfc931.o
make[1]: Leaving directory '/root/Desktop/Klaxon/Klaxon'
make[1]: Entering directory '/root/Desktop/Klaxon/Klaxon'
cc -DDEBUG -c -o Klaxon.o Klaxon.c
cc -o Klaxon ./Klaxon.o
make[1]: Leaving directory '/root/Desktop/Klaxon/Klaxon'
bash-2.05# ls
Klaxon.o Klaxon ./Klaxon.c Klaxon.c Klaxon.o
Makefile README Klaxon.c Klaxon.c wire.c rfc931.o rfc931.o
```

Sicurezza su Reti: Rilevazione del
Portscanning

13

Klaxon: Configurazione

- Aprire il file `/etc/inetd.conf` con un editor
- Rimpiazzare l'eseguibile di ogni comando da salvaguardare con la "trappola" klaxon

Esempio per il comando telnet:

Sostituire la riga seguente:

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
```

con

```
telnet stream tcp nowait root /usr/local/klaxon in.telnetd
```

Sicurezza su Reti: Rilevazione del
Portscanning

14

Klaxon : Alcuni Test

- Test con Telnet
- Test con Ftp
- Test con Talk



Sicurezza su Reti: Rilevazione del
Portscanning

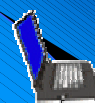
15

Klaxon : Test con Telnet

A attacco



B



1. A tenta l'attacco lanciando telnet
2. B rileva l'attacco leggendo in `/var/log/messages`
3. B chiude la connessione
4. A non si spiega perché la connessione è fallita

Sicurezza su Reti: Rilevazione del
Portscanning

16

Klaxon : Test con Ftp

A attacco



B



1. A tenta l'attacco lanciando ftp
2. B rileva l'attacco leggendo in `/var/log/messages`
3. B chiude la connessione
4. A non si spiega perché la connessione è fallita

Sicurezza su Reti: Rilevazione del
Portscanning

17

Klaxon : Test con Talk

A attacco



B



1. A tenta l'attacco lanciando talk
2. B rileva l'attacco leggendo in `/var/log/messages`
3. B chiude la connessione
4. A non si spiega perché la connessione è fallita

Sicurezza su Reti: Rilevazione del
Portscanning

18

Klaxon: Protocollo IDENT

fornisce l'username dell'utente che ha avviato la connessione e consente di monitorare gli accessi.

Klaxon : Test con IDENT



1. A tenta l'attacco lanciando telnet
2. B rileva l'attacco leggendo in /var/log/messages
3. B chiude la connessione
4. A non si spiega perché la connessione è fallita
5. B grazie al protocollo Ident scopre l'identità di A

Portsentry

- Software freeware per ambienti Unix e Linux
- Progettato da Craig H. Rowland
- Ultima versione v2.0b1 del 08 Aprile 2002
- Reperibile sul sito
<http://www.psonic.com/abacus/portsentry>
- Per maggiori informazioni è possibile consultare il sito ufficiale
<http://www.psonic.com>

Portsentry: Idea di base

- Permette di rilevare i tentativi di connessione alle porte messe sotto controllo
- Registrare in un file di log i tentativi di connessione
- Registrare l'indirizzo IP dal quale proviene il portscan
- Bloccare gli accessi provenienti dagli indirizzi "predefiniti".

Portsentry: Compilazione

Compilazione del Portsentry e specifica del sistema operativo

```
bash-2.03# ls
CHANGES  README.COMPAT  ignore.csh      portsentry.ignore
CREDITS   README.install portsentry.c    portsentry_config.h
KNOWNBUGS README.methods  portsentry.conf portsentry_io.c
LICENSE   README.stealth  portsentry.h    portsentry_io.h
Makefile  TODO            portsentru.h    portsentru_util.c

bash-2.03# make linux
SYSYTYPE=linux
Making
cc -O -Wall -D_BSD_SOURCE -o ./portsentru ./portsentru.c \
./portsentru_io.c ./portsentru_util.c -lpcap
bash-2.03#
```

Portsentry: Installazione

```
bash-2.03# make install
Creating psionic directory /usr/local/psionic
Setting directory permissions
Creating portsentry directory /usr/local/psionic/portsentry2
Setting directory permissions
chmod 700 /usr/local/psionic/portsentry2
Copying files
cp ./portsentru.conf /usr/local/psionic/portsentry2
cp ./portsentru.ignore /usr/local/psionic/portsentry2
cp ./portsentru /usr/local/psionic/portsentry2
Setting permissions
chmod 600 /usr/local/psionic/portsentry2/portsentru.ignore
chmod 600 /usr/local/psionic/portsentry2/portsentru.conf
chmod 700 /usr/local/psionic/portsentry2/portsentry2

Edit /usr/local/psionic/portsentry2/portsentru.conf and change
your settings if you haven't already. (route, etc)
```

Portsentry: Log degli eventi

I tentativi di portscan rilevati da Portsentry o gli eventi generati dallo stesso vengono trascritti in un file di log (/var/log/messages).

Portsentry: Livelli di sicurezza

- adminalert - messaggi che indicano lo stato di Portsentry;
- securityalert - messaggi che indicano un evento rilevante di sicurezza;
- attackalert - messaggi utilizzati nel caso di rilevazione di una scansione sull'host protetto

Portsentry: Modalità operative

- Stealth mode
- Advanced Stealth mode

Portsentry: Stealth Mode

- Il programma non apre alcuna porta.
- Crea un socket raw.
- Controlla i pacchetti che attraversano l'interfaccia in entrata.
- Se il pacchetto è diretto a una delle porte protette esegue le azioni definite dall'utente.

Portsentry: Advanced Stealth Mode

- Crea un socket raw.
- Vengono monitorate solo le porte entro un determinato range.
- L'ampiezza del range per default è di 1024
- Il numero delle porte è estendibile fino a 65535.

Portsentry: Scansioni rilevabili

full connect scan	Completa un three-handshake.
SYN/Half open scan	Verifica solo se la porta è in listening poi manda un RST.
FIN scan	Manda un FIN alla porta da attaccare, se riceve in risposta un RST allora la porta è chiusa.
NULL scan	Manda un pacchetto con tutti i flag disabilitati alla porta da attaccare: l'output è uguale a quello del FIN scan.
XMAS scan	Come il FIN scan, solo che manda un pacchetto con FIN, URG e PUSH impostati.
UDP scan	Manda un pacchetto UDP alla porta da attaccare. Se riceve in risposta un ICMP Port Unreachable allora la porta è aperta.

Portsentry: Configurazione e Test

Per ognuna delle modalità operative di Portsentry sono possibili due opzioni:

- Opzione non bloccante
- Opzione bloccante



Portsentry: Opzione non bloccante

- Un tentativo di connessione viene immediatamente bloccato e viene registrato nel file di log.
- L' IP dell'aggressore è registrato nel file `portsentry.blocked`.
- Il file `portsentry.history`, tiene memoria di tutti gli host che sono stati bloccati nel tempo.

Portsentry: Esempio Advanced Stealth mode non bloccante

Eseguiamo un telnet dall'host remoto "emavit" all'host "edover":

```
emavit:~ # telnet 193.205.161.191 11
Trying 193.205.161.191...
Connected to edover.diareti.diaedu.unisa.it(193.205.161.191).
Escape character is '^]'.*** ACCESSO NON AUTORIZZATO!!!
*** Connection closed by foreign host.
```

L' IP dell'aggressore è registrato nel file `portsentry.blocked` `portsentry.blocked` conterrà:

```
Connect from host: emavit.diareti.diaedu.unisa.it/193.205.161.192 to TCP port:
Sep 6 11:44:36 edoverportsentry[1330]: attackalert: 11
```

Portsentry: Opzione bloccante

- Rileva i tentativi di connessione alle porte messe sotto controllo
- Li registra in un file di log
- Registra l'indirizzo IP dal quale proviene il portscan nei file `portsentry.blocked` e `host.deny`
- Impedisce agli host "incriminati" di ricevere pacchetti in risposta alla loro scansione

Portsentry: Esempio Advanced Stealth mode bloccante

Eseguiamo un telnet dall'host remoto "emavit" all'host "edover":

```
emavit:~ # telnet 193.205.161.191 143
Trying 193.205.161.191...
telnet: Unable to connect to remote host: Connection refused
```

Il contenuto del file di log è:

```
Jul 4 12:54:00 edover portsentry[1826]: attackalert: SYN/Normal scan
from host: emavit.diareti.diaedu.unisa.it/193.205.161.192 to TCP port: 143
Jul 4 12:54:00 edover portsentry[1826]: attackalert: Host 193.205.161.192
has been blocked via wrappers with string: "ALL: 193.205.161.192"
```

I pacchetti provenienti da "emavit" non ottengono risposta da "edover"

Fine della Presentazione

