Linee guida alla sicurezza nella configurazione del router

Introduzione

La topologia della rete GARR semplifica l'implementazione di una politica di sicurezza: la connessione a GARR da un sito utente avviene direttamente sul più vicino POP del backbone, gestito centralmente dal Network Operation Centre. Quindi, quasi tutti i siti utente in GARR sono delle semplici foglie della rete (anche se alcuni possono avere delle backdoor tra loro o con altri siti non GARR); inoltre il controllo centralizzato del backbone permette, in linea di principio, interventi di emergenza atti ad isolare situazioni "pericolose".
D'altra parte una politica di sicurezza preventiva può essere effettuata efficacemente solo a livello di sito utente tramite un'opportuna configurazione degli apparati.

Scopo di questo documento è esaminare politiche preventive di sicurezza, illustrando le forme di protezione implementabili sul router utente verso i più comuni attacchi via rete con particolare attenzione verso i problemi legati ai difetti intrinseci del protocollo IP.Gli esempi si riferiscono all'IOS dei router Cisco.

Configurazione di base

E` inutile dire che il server sul quale viene registrato il file di log deve essere adeguatamente protetto; è consigliabile inoltre adottare meccanismi automatici di allarme (ad es.: swatch)

!
!
!
service timestamps log datetime
logging trap debugging <LOG FILE>
logging facility logging <LOG SERVER>

- Il primo passo per la prevenzione è abilitare il sistema di log per tenere traccia di tutti gli eventi "interessanti".

- Per eliminare la possibilità che un router utente sia utilizzato come "ponte" per connessioni illecite, è consigliabile disabilitare la possibilità di fare telnet dal router, pur lasciando un account non privilegiato per diagnostica (analogamente all'account "garr-ip" in GARR-2): la connessione inoltre dovrà essere possibile solo da alcuni host prestabiliti (ad es.: dalla rete interna e dal router del PoP).

```
!
! account di servizio garr-ip
! non puo` fare telnet
!
username garr-ip access-class 1 nopassword
access-list 1 deny any log
....
access-list 2 permit <ROUTER POP> 0.0.0.0
access-list 2 permit <RETE INTERNA> 0.0.0.255
!
line vty 0 4
....
access-class 2 in
login local
```

```
!
! abilita la criptazione delle password
!
service password-encryption
!
! inserimento password di tipo secret
!
enable secret SECRET1
```

- I file di configurazione dei router vengono tipicamente salvati su un tftp server e sono quindi accessibili, in linea di principio, a tutti: è consigliabile permettere l'accesso al tftp server ai soli nodi interessati (ad es. mediante un sistema di tcp-wrapper sul server).
- La criptazione della password di accesso al router non è sufficiente: è infatti diffuso un "tool" che permette di decriptare la password di enable dei router CISCO, a partire dal file di configurazione (si veda il punto precedente), in quanto l'algoritmo di criptazione è reversibile. E`

fortemente consigliato quindi sostituire la password di enable con il "secret" che usa un algoritmo di criptazione non reversibile.

Attacchi di tipo Denial of Service (DOS)

Gli attacchi di tipo DoS hanno come scopo di rendere inutilizzabile un servizio o una risorsa, eventualmente per sostituirsi ad essa e trarne un illecito vantaggio. La tipologia di questi attacchi spazia dall'impedire la connessione ad un server (o a un router) al mandare in crash lo stesso. Vediamo i casi piu` diffusi.

Smurfing

Un grave disservizio può essere causato dall'invio dall'esterno di pacchetti ICMP all'indirizzo di broadcast di una delle reti del sito ("broadcast storm"): lo "smurfing".

Tale tipo di attacco coinvolge solitamente tre siti: il sito di origine dell'attacco (sito O) e altri due siti "vittime", uno intermedio che "amplifica" l'attacco (sito I) ed uno terminale (sito T).
Solitamente dal sito O vengono effettuati ping sull'indirizzo di broadcast di una (o più reti) del sito I, con il campo source ip address dell'header falsificato e posto uguale a quello di un host del sito T (per maggiori dettagli: CERT CA-98.01). In questo modo viene generato un flusso consistente di pacchetti ICMP dal sito I al sito T.

Purtroppo non c'è modo per il sito T di difendersi direttamente, se non tramite una politica preventiva estesa a quanti più siti possibile tesa ad eliminare le cause (cioè ad impedire comportamenti "scorretti" dei propri utenti).
E` quindi importante impedire che la propria LAN sia origine dell'attacco o amplificatore ignaro (ed allo stesso tempo vittima) dello stesso.
Per evitare che la propria LAN agisca da sito intermedio, è necessario disabilitare la possibilità di inviare pacchetti dall'esterno sull'indirizzo di broadcast delle proprie reti nel seguente modo:

```
!
! impedisce di inviare pacchetti broadcast dall'esterno
!
interface ethernet 0
```

.....
no ip directed-broadcast

Questa operazione deve essere ripetuta su ogni router connesso alla propria LAN.

Inoltre, per evitare che la propria LAN sia origine dell'attacco o quanto meno per permettere di individuare l'origine dell'attacco, è necessario controllare che i pacchetti che escono dalla LAN abbiano nell'header, come source address un indirizzo appartenente ad essa. In questo modo è almeno possibile evitare di coinvolgere siti "terzi" e risalire all'origine dell'attacco disponendo di un sistema di monitoraggio sulla LAN (si veda ad es: "Building a Network Monitoring and Analysis Capability Step by Step")
L'access-list seguente effettua il controllo richiesto (si ricordi che le access-list estese sono identificate da un numero compreso nell'intervallo 100-199 e che l'IOS CISCO effettua il controllo sequenzialmente dalla prima istruzione, fermandosi al primo match di condizione esatto che trova).

!
! impedisce ai pacchetti con source address falsificato di uscire dalla LAN
!
interface serial 0
.....
ip access-group 101 out
.....
!
! definizione access-list (nell'esempio RETE e` una rete di "classe C")
!
!
access-list 101 permit ip <RETE> 0.0.0.255 any any
access-list 101 deny ip any any log

Attacchi UDP-TCP sulle porte di diagnostica del router

Un altro possibile attacco, di tipo DoS, cui sono soggetti router CISCO è l'invio di un grande numero di pacchetti spuri UDP o TCP sulle porte echo, chargen, discard e daytime (quest'ultimo solo TCP). In questi casi il router, per rispondere a queste richieste, può arrivare a consumare una grande percentuale della propria CPU fino, in casi estremi, ad andare in crash (per maggiori dettagli: "White Paper: Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks").

E` consigliabile disabilitare tale accesso, con le seguenti istruzioni in configurazione:

```
!
!
no service udp-small-servers
no service tcp-small-servers
!
```

L'uso di una access-list per filtrare i pacchetti in uscita dalla propria LAN (è sufficiente l'access-list applicata come misura preventiva per lo smurfing) permette di circoscrivere eventuali attacchi verso terzi provenienti dalla propria LAN.

Attacco "Land"

Come è noto, è diffuso un "tool" (noto come land) che permette l'invio ad un determinato host di pacchetti TCP SYN (inizio di connessione), con "ip source address" e "port" falsificati e posti uguali all'indirizzo ed alla porta dell'host di destinazione, causando in alcuni casi anche lo stallo del router. Il problema è stato risolto nelle più recenti versioni di IOS Cisco, ma negli altri casi è necessario applicare un filtro che blocchi per ogni interfaccia la ricezione di questi pacchetti (per maggiori dettagli: "TCP Loopback DoS Attack (land.c) and Cisco Devices").

```
!
! impedisce l'invio alle interfacce di pacchetti
! con ip source address uguale a quello dell'interfaccia
!
interface ethernet 0
.....
ip address <ETH ADDRESS> <SUBNET MASK>
ip access-group 102 in
.....
!
! il filtro e` inutile se l'interfaccia e` unnumbered o
! comunque se ha un indirizzo non annunciato
!
interface serial 0
......
ip address <SERIAL ADDRESS> <SUBNET MASK>
ip access-group 102 in
```

.....
!
access-list 102 deny ip <ETH ADDRESS> 0.0.0.0 <ETH ADDRESS> 0.0.0.0
access-list 102 deny ip <SERIAL ADDRESS> 0.0.0.0 <SERIAL ADDRESS> 0.0.0.0
access-list 102 permit ip any any

Attacchi "TCP SYN"

Un altro possibile attacco di tipo DoS è l'attacco "TCP SYN" caratterizzato dalla richiesta di un grande numero di connessioni, apparentemente da host diversi, ad un router il quale però non riceverà mai l'acknowledgment di chiusura del "TCP three-way handshake" per queste connessioni, causando quindi il riempimento della sua coda di connessione e quindi realizzando una situazione di Denial of Service (per maggiori dettagli si veda: "White Paper: Defending Strategies to Protect Against TCP SYN Port Denial of Service Attacks").
Non è possibile rintracciare l'origine dell'attacco in quanto il mittente viene falsificato, né esistono metodi semplici di difesa (non è fattibile ad esempio l'attivazione di una access-list che filtri le connessioni in ingresso, perchè tipicamente l'ip sorgente è falsificato in maniera casuale e quindi un attacco può coprire buona parte dello space-address di Internet).
Sono attuabili alcune contro-misure come aumentare la dimensione della coda di connessione (SYN ACK queue) e diminuire il tempo di time-out per il "three-way handshake".
Anche in questo caso l'implementazione dell'acces-list per filtrare i pacchetti in uscita diminuisce la probabilità che la LAN sia utilizzata come base per questo tipo di attacchi (è sufficiente l'access-list applicata come misura preventiva per lo smurfing).

Uso non autorizzato delle risorse

Protezione degli host sulla LAN

In situazioni normali è difficilmente attuabile il controllo centralizzato di tutti gli host sulla propria LAN. La misura alternativa è filtrare selettivamente sul router i servizi tendenzialmente pericolosi.
In linea di principio, la situazione ottimale è isolare su una LAN dedicata i server "esterni" ovvero quelli che devono essere visibili a tutti, permettendo l'accesso verso di essi però solo limitatamente ai servizi "ufficiali" offerti; per quanto

riguarda invece le macchine utente, dovrebbe essere bloccato tutto il traffico diretto verso le porte "pericolose" (dalle quali comunque di norma non dovrebbero essere offerti servizi).
Nella seguente tabella sono riportati i servizi da filtrare o bloccare.

Servizio	Porta	Protocollo	Azione	Note
echo	*7*	*TCP/UDP*	*Bloccare*	**DoS**
systat	*11*	*TCP/UDP*	*Bloccare*	**informativo**
daytime	*13*	*TCP/UDP*	*Bloccare*	
netstat	*15*	*TCP*	*Bloccare*	**informativo**
quotd	*17*	*TCP/UDP*	*Bloccare*	
chargen	*19*	*TCP/UDP*	*Bloccare*	**DoS**
smtp	***25***	***TCP***	***Filtrare***	
time	*37*	*TCP/UDP*	*Bloccare*	**inutile**
tacacs	*49*	*TCP/UDP*	*Bloccare*	
domain	***53***	***TCP***	***Filtrare***	**TCP usato solo per zone-transfert**
bootp	*67-68*	*UDP*	*Bloccare*	
tftp	*69*	*UDP*	*Bloccare*	
gopher	*70*	*TCP*	*Bloccare*	*obsoleto*
finger	*79*	*TCP*	*Bloccare*	**informativo**
http	***80***	***TCP***	***Filtrare***	
link	*87*	*TCP*	*Bloccare*	
supdup	*95*	*TCP*	*Bloccare*	
pop2	*109*	*TCP*	*Bloccare*	obsoleto
pop3	***110***	***TCP***	***Filtrare***	
sunrpc	***111***	***TCP/UDP***	***Filtrare***	
nntp	***119***	***TCP***	***Filtrare***	
nbios-ns	***137***	***TCP/UDP***	***Filtrare***	
nbios-dgm	***138***	***TCP/UDP***	***Filtrare***	
nbios-ssn	***139***	***TCP/UDP***	***Filtrare***	
imap	***143***	***TCP***	***Filtrare***	
NeWS	***144***	***TCP***	***Bloccare***	
snmp	***161***	***UDP***	***Filtrare***	
snmptrap	***162***	***UDP***	***Bloccare***	
xdmcp	***177***	***UDP***	***Filtrare***	
irc	***194***	***TCP/UDP***	***Bloccare***	

exec	***512***	***TCP***	***Bloccare***	
biff	***512***	***UDP***	***Bloccare***	
login	***513***	***TCP***	***Bloccare***	
who	***513***	***UDP***	***Bloccare***	**informativo**
shell	***514***	***TCP***	***Bloccare***	
syslog	***514***	***UDP***	***Bloccare***	
printer	***515***	***TCP***	***Bloccare***	
route	***520***	***UDP***	***Bloccare***	
uucp	***540-541***	***TCP***	***Bloccare***	
mountd	***635***	***TCP/UDP***	***Filtrare***	
openwin	***2000***	***TCP***	***Bloccare***	
NFS	***2049***	***TCP/UDP***	***Filtrare***	
X11	***6000-6063***	***TCP***	***Filtrare***	

Mail spamming

Come esempio significativo di uso illecito delle risorse (soprattutto della rete) esaminiamo il "mail spamming", ovvero l'uso di mailer SMTP da parte di utenti non autorizzati per ottenere l'invio di decine di migliaia di messaggi di e-mail, di solito contenenti messaggi pubblicitari non richiesti dai destinatari (detti UCE: Unsolicited Commercial E-mails).
Per prevenire questo fenomeno, in linea di principio, è sufficiente configurare correttamente gli host di una LAN eliminando (selettivamente) la possibilità di utilizzarli come mail relay dall'esterno (per maggiori dettagli: sendmail organization)
In realtà però, come abbiamo notato precedentemente, è necessario filtrare il servizio smtp dall'esterno verso tutti gli host ritenuti non "affidabili" (cioé non controllati direttamente dai reponsabili del sito), lasciando pieno accesso smtp solo verso i mail server "ufficiali".
Viene riportato di seguito un esempio di access-list che implementa questo filtro.

```
!
! impedisce le connessioni smtp dall'esterno verso host non autorizzati
! (nell'esempio si suppone che la connessione verso l'esterno avvenga
! tramite l'interfaccia serial 0)
!
```

interface serial 0
.....
ip access-group 103 in
.....
!
! definizione access-list (nell'esempio RETE e` una rete di "classe C")
!
access-list 103 permit tcp any host <MAIL SERVER 1>
access-list 103 permit tcp any host <MAIL SERVER 2>
access-list 103 deny tcp any <RETE> 0.0.0.255 eq smtp log
access-list 103 permit ip any any

Si noti che una simile configurazione NON impedisce alle macchine interne di parlare SMTP tra di loro nè di trasmettere direttamente posta elettronica a tutto il mondo esterno: impedisce solamente al mondo esterno di accedere direttamente alla porta SMTP delle macchine non autorizzate.

Un problema che rimane comunque aperto è lo spamming con il metodo del "doppio non delivery". In questo caso lo "spammer", per aggirare le protezioni sul mail-relay, invia il mail ad un utente inesistente in un dato dominio con il campo From falsificato e posto uguale al "bersaglio": il sistema di mail del dominio ricevente accetta l'e-mail (è diretto ad utente del proprio dominio) ma poi constata che l'utente è inesistente e quindi lo rispedisce al mittente (a quello che crede essere il mittente...).
Purtoppo non c'e' modo di difendersi se non segnalando il fatto ai gestori dell'ISP dal quale avvengono queste connessioni ed eventualmente filtrare la connessione smtp dalle reti in questione (eliminando quindi anche i mail "legittimi"); d'altra parte questo tipo di "mail-spamming" è assolutamente inefficiente dal punto di vista dello spammer (deve mandare un mail per ogni "vittima").