Sicurezza dei router Cisco

Giuseppe Paternò

SOMMARIO

INTRODUZIONE

Scopo del documento

Lo scopo di questo documento è di riassumere in un unico punto le informazioni, procedure e spunti di riflessione per effettuare un hardening di un router basato su Cisco IOS. Con il termine *hardening* si intende la procedura utilizzata per rendere il sistema il più resistente possibile ai vari tentativi di attacco. La procedura di per se è abbastanza semplice, e si focalizza su tre scopi ben precisi:

- Controllare gli accessi
- Eliminare il traffico indesiderato
- Minimizzare la possibilità di attacco

Commenti e suggerimenti

Qualsiasi commento o suggerimento é benvenuto e può essere inviato al seguente indirizzo:

Giuseppe Paternò
Casella Postale 27
20090 Trezzano S/N (MI)
Italia

Oppure via e-mail a *info@gpaterno.com*. Successive edizioni ed eventuali correzioni di questa pubblicazione saranno disponibili sul sito Internet http://www.gpaterno.com/.

Nota di Copyright

L'autore

Giuseppe Paternò ha conseguito la certificazione CCNP ed è membro di IEEE e della Italian Linux Society. La sua passione ha spinto Giuseppe ad esplorare fin da giovanissimo tutti i settori dell'informatica, con particolare riguardo al settore della sicurezza e delle reti, senza tralasciare le nuove sfide tecnologiche. Attualmente lavora come consulente senior per Sun Microsystems occupandosi di architetture di rete e di sicurezza, ma nel suo passato spiccano esperienze di lavoro stimolanti tra cui IBM e Infostrada.

HARDENING DI BASE

Boot

La prima cosa da proteggere è proprio il boot del router. Di default il router esegue *boot flash* e *boot rom.* E' necessario definire quale immagine di software va caricata all'avvio, esempio:

```
boot system flash c3550-i5q3l2-mz.121-20.EA1a.bin
boot system room
```

Password di enable e di console

Il secondo passo e' quello di stabilire le password di enable e di console. E' meglio usare il nuovo comando *enable secret* che il vecchio *enable password*. Il comando *enable secret* usa un hash MD5 per conservare le password, mentre con il vecchio sistema la password era facilmente ricavabile. Cisco comunque raccomanda di usare AAA per l'autenticazione sulla console.

```
no enable password
enable secret PasswordSuperSegreta
service password-encryption
line console 0
      password PasswordConsole
      transport output none
line aux
      no exec
      transport input none
```

Autenticazione tramite RADIUS (AAA)

Cisco consiglia di appoggiarsi all'AAA (Authentication, Authorization and Accounting) per l'autenticazione degli utenti all'accesso interattivo ad un router Cisco. I comandi che seguono sono un esempio di autenticazione verso RADIUS.

```
aaa new-model
aaa authentication login RemoteAuth radius enable
radius-server host 172.16.1.12
radius-server key MiaChiave
line vty 0 4
      login authentication RemoteAuth
```

Banner

Inserire un banner per rendere evidente che si tratta di un'area ristretta. Per esempio:

```
banner motd ^C
---------------------------------------------------------------
This system is for the use of authorized users only.
Individuals using this computer system without authority, or in
excess of their authority, are subject to having all of their
activities on this system monitored and recorded by system
personnel.

In the course of monitoring individuals improperly using this
system, or in the course of system maintenance, the activities
of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring
and is advised that if such monitoring reveals possible
evidence of criminal activity, system personnel may provide the
evidence of such monitoring to law enforcement officials.
---------------------------------------------------------------
^C
```

Sincronizzazione del tempo

E' bene usare il protocollo NTP per sincronizzare i router con un NTP Server stratum 1 o stratum 2 (vedi http://www.ntp.org per informazioni)., avendo cura di autenticare –quando possibile- il protocollo NTP. Si consiglia di usare la timezone UTC qualora si gestiscano più router distribuiti su più fasce orarie: questo accorgimento facilita la lettura nel caso fosse necessario correlare i log. Esempio:

```
clock timezone UTC 0
no clock summer-time
ntp update-calendar
ntp authenticate
ntp authentication-key 10 md5 ntpkey
ntp trusted-key 10
ntp server 172.16.3.2 key 10
interface Serial 0/0
      ntp disable
interface Ethernet 0/0
      ntp broadcast
```

Collezione dei log

Innanzi tutto bisogna configurare il buffer della history. Si tratta di un buffer circolare, dove i log più vecchi vengono sovrascritti. Si faccia attenzione alla grandezza del buffer, in quanto occupa RAM, che potrebbe essere preziosa per altri processi. Ad esempio:

```
logging buffered 8192 debugging
```

Il passo successivo e' di abilitare il timestamp sui log attraverso i seguenti comandi:

```
service timestamps debug datetime
service timestamps log datetime
```

Con il comando successivo, si disabilitano la traduzione dei nomi DNS nei log:

```
no ip domain lookup
```

E' poi consigliabile mandare i log verso un syslog server centralizzato attraverso i seguenti comandi:

```
logging 172.16.1.2
logging trap notification
```

Il livello syslog utilizzato dal router Cisco è il *local7*, che deve essere configurato sul log server.

Tuning dello stack IP

I comandi successivi servono ad effettuare un miglioramento dello stack IP del routerl. Il primo abilita l'algoritmo di Nangle per la gestione del controllo della congestione (RFC 896). Il secondo limita il tempo di timeout dei pacchetti Syn, il default è di 30 secondi. Il terzo e il quarto nel rispetto degli RFC 1323 e RFC2018.

```
service nagle
ip tcp synwait-time 10
ip tcp window-size 2144
ip tcp selective-ack
```

Tuning della CPU

Attraverso il seguente comando si garantisce il tempo minimo della CPU per i processi vitali (500 millisecondi)

```
scheduler-interval 500
```

Sui Cisco 7200 e 7500 si può anche inserire il seguente comando, che abilita 500 microsecondi per ciclo di clock sul fast-packet switching e 100 microsecondi per cliclo di clock per process-switching:

```
scheduler allocate 500 100
```

Abilitazione dei servizi necessari

Si consiglia di abilitare i servizi di password encryption e di tcp keepalive come segue:

```
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
```

Disabilitazione dei servizi non necessari

Si consiglia di disabilitare i seguenti servizi, non necessari al corretto funzionamento dell'apparato. Si consiglia particolare attenzione al CDP e all'SNMP che potrebbero essere utilizzati in azienda. Più avanti nel documento viene descritto come mettere in sicurezza il protocollo SNMP.

```
no cdp run
no boot network
no service config
no ip source-route
no service finger
no ip finger
no ip identd
no service pad
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no snmp-server
no tftp-server
no ip http-server
```

Disabilitazione degli UDP broadcast

Alcuni broadcast effettuati in UDP vengono ruotati di default. E' necessario capire se qualcuno di questi sia realmente utilizzato, ad esempio per il DHCP, ed abilitare solo quello corrispondente. Per disabilitare tutti i broadcast UDP:

```
no ip forward-protocol port 69
no ip forward-protocol port 53
no ip forward-protocol port 37
no ip forward-protocol port 137
no ip forward-protocol port 138
no ip forward-protocol port 67
no ip forward-protocol port 68
no ip forward-protocol port 49
no ip forward-protocol port 42
no ip helper-address
```

Hardening delle interfaccie

Sono parametri consigliabili da applicare alle singole interfaccie: bisogna capire se qualcuno di questi parametri è effetivamente utilizzato. Non utilizzare *shutdown* in quelle interfaccie già in uso, mentre mettere sempre in *shutdown* le porte non in uso. Si consiglia fortemente per quelle interfaccie direttamente collegate ad Internet.

```
no cdp enable
ip accounting access-violation
no ip directed-broadcast
no ip redirects
no ip unreachables
no ip mask-reply
no ip proxy-arp
no mop enabled
shutdown
```

Abilitazione del server SSH

Nelle nuove versioni del Cisco IOS sui router recenti e' possibile usare SSH come metodo di collegamento alternativo al telnet ed al tftp. Per abilitarlo, eseguire:

```
hostname miorouter
ip domain-name azienda.it
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 3
ip scp server enable
```

Restrizione dell'accesso via rete

E' bene restringere a determinati IP l'accesso via rete all'apparato attraverso le ACL, sia che si decida di usare SSH (attraverso *transport input ssh*) oppure telnet. Si vedranno in seguito cosa sono le ACL e come usarle in maniera più dettagliata.

```
access-list 80 permit 172.16.0.0 0.0.255.255 log
access-list 80 deny any log
line vty 0 4
      login
      password MiaPassword
      transport input ssh
      transport output none
      exec timeout 5 0
      access-class 80 in
```

Configurazione dell'SNMP

Si rende necessario l'uso del Simple Network Management Protocol (SNMP) nei grandi ambienti, dove è necessario il monitoring della rete. Sebbene non sia un protocollo sicuro, viene però considerato come un “male necessario”, in quanto è difficile gestire un numero elevato di apparati di rete senza di esso. Quello che si può fare è impostare l'SNMP in modo tale da limitare gli attacchi, ad esempio restringendo tramite ACL le macchine abilitate alla gestione e scegliendo communities non facilmente intuibili. Per esempio

```
access-list 80 permit 172.16.0.0 0.0.255.255
access-list 90 permit 172.16.1.2
snmp-server communityReadStringviewViewNameRO 80
snmp-server communityWriteStringRW 90
snmp-server viewViewName1.3.6.2.4 excluded
snmp-server enable traps
snmp-server host 172.16.1.2 version 2c TrapString
```

Step finale dell'hardening di base

Come ultimo passo e' necessario copiare la configurazione in flash, effettuare una copia di backup e riavviare il router per vedere che effettivamente la configurazione rimanga inalterata.

```
copy running-config startup-config
copy running-config scp://user@host
reload
```

LE ACCESS CONTROL LISTS (ACL)

Le Access Control Lists, o più semplicemente ACL, sono una lista ordinata di criteri a cui un determinato pacchetto deve essere conforme. Le ACL possono essere usate per filtrare l'attraversamento di determinati flussi di traffico, per i protocolli di routing o per limitare l'accesso interattivo al router.

Le ACL di base

Ripassiamo velocemente i tipi di ACL di base sui router, che ci serviranno in seguito. Possiamo distinguere quattro tipi fondamentali di ACL, le base:

```
access-list 1 permit 1.1.2.0 0.0.1.255
```

Le estese con commenti

```
access-list 100 remark telnet access list
access-list 100 permit tcp host 1.1.1.1 2.2.2.0 0.0.0.255 telnet
```

Quelle con un Type-Code

```
access-list 200 permit 0x0000 0x0d0d
```

Le ACL con nomi (named)

```
ip access-list standard allow-telnet
      remark machine from which telnet is accepted
      permit 1.1.1.1
      permit 2.2.2.2
```

Le ACL a tempo (Time-Based)

Sono ACL che vengono abilitate solo in un determinato spazio temporale, ad esempio limitando l'accesso al solo orario lavorativo. Per esempio:

```
access-list 100 remark Only allow IP traffic during open hours
access-list 100 permit ip any any time-range only-during-open-hours
!
time-range only-during-open-hours
absolute start 00:00 01 January 2002
periodic weekdays 7:30 to 18:30
periodic Saturday 8:30 to 13:30
periodic Sunday 8:30 to 18:30
```

Le ACL Lock & Key

Le ACL di tipo Lock & Key, talvolta riferite anche come Dynamic Extended access list, abilitano l'accesso ad un determinato IP sorgente in base all'utente. In pratica si tratta di un firewall dinamico in cui l'utente si autentica via telnet al router e abilita il proprio IP all'accesso. Ad esempio:

```
interface ethernet0
      ip address 172.18.23.9 255.255.255.0
      ip access-group 101 in
access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any
line vty 0
      login local
      autocommand access-enable timeout 5
```

Le ACL di tipo TCP Intercept

Queste ACL sono solitamente usate per proteggere i server da un attacco di tipo Syn Flood. Esistono due modalità: *watch*, che controlla e termina le connessioni incomplete, ed *intercept*, che tenta di completare la connessione con il client al posto del server. Se il 3-WAY handshake del TCP è andato a buon fine, crea una connessione al server, altrimenti chiude la connessione al client. Ad esempio:

```
access-list 120 remark Web Servers
access-list 120 permit tcp any 1.1.1.0 0.0.0.255
ip tcp intercept list 120
ip tcp intercept mode watch
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept one-minute low 1500
ip tcp intercept one-minute high 6000
```

Le ACL reflexive

Le ACL di tipo reflexive permettono di creare dinamicamente una access list relativa allo stato di una connessione. Si possono usare le reflexive access list per permettere il traffico IP originato dalla propria rete, ma negare qualsiasi traffico in ingresso tranne per le sessioni aperte dall'interno. Di seguito un esempio:

```
interface Serial 1
      description Access to the Internet via this interface
      ip access-group inboundfilters in
      ip access-group outboundfilters out
!
ip reflexive-list timeout 120
!
ip access-list extended outboundfilters
      permit tcp any any reflect tcptraffic
!
ip access-list extended inboundfilters
      permit bgp any any
      permit eigrp any any
      deny icmp any any
      evaluate tcptraffic
```

Le ACL di tipo Reverse Path Forward

Il Reverse Path Forward (RPF) serve per mitigare i problemi causati dallo spoofing degli indirizzi IP, in quanto scarta i pacchetti IP non provenienti da una sorgente verificabile. Nel caso successivo, la ACL 197 ha delle istruzioni tali per cui nega o permette il traffico di rete per un intervallo specifico di indirizzi IP. Il RPF è configurato nell'interfaccia Ethernet0 per verificare i pacchetti che arrivano da quella interfaccia.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log
```

Le ACL e l'ICMP

Non è detto che disabilitare tutto possa essere la soluzione, anzi! Bisogna tenere conto che alcuni pacchetti ICMP sono vitali al buon funzionamento del TCP in genere. Ad esempio, l'ICMP viene usato per negoziare la MTU di una connessione TCP, per cui sarà necessario usare:

```
access-list 110 permit icmp any any packet-too-big
```

Per abilitare l'ICMP solamente in uscita:

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any parameter-problem
access-list 102 permit icmp any any source-quench
access-list 102 deny icmp any any log
```

Per abilitare anche il traceroute:

```
access-list 102 permit udp any any range 33400 34400 log
access-list 102 permit icmp any any time-exceeded
```

Le Turbo ACL

Le turbo ACL sono state introdotte a partire dalla versione di IOS 12.1.5T per i router Cisco di fascia alta. Il tempo per confrontare i pacchetti si riduce drasticamente ed ha un tempo fisso. La latenza quindi e' minore, con una miglior stabilita' della rete e un minor tempo di attraversamento del router. I comandi per agire sulle turbo ACL sono:

```
access-list compiled
show access-list compiled
```

Le ACL ed il rate limiting

Oltre all'uso delle ACL di tipo TCP Intercept, è possibile usare una ACL per limitare un attacco Syn Flood. Oltre a questa tipologia di attacco, tramite variazioni all'esempio successivo e' possibile attacchi Fraggle (UDP) e attacchi Smurf (ICMP)

```
access-list 120 deny tcp any any established
access-list 120 permit tcp any any
interface Serial 0/0
      rate-limit input access-group 120 64000 8000 8000
      conform-action transmit
      exceed-action drop
```

Le ACL per proteggersi dallo spoofing

Le Access Control Lists possono essere usate anche come tecnica di anti-spoofing. Lo spoofing è l'invio di pacchetto con IP address legittimo proveniente da una rete totalmente diversa. In particolare, vogliamo che il router non faccia routare indirizzi IP che non hanno senso. Ad esempio, su un router di bordo su Internet non vogliamo che i nostri indirizzi privati (RFC 1918) vengano ruotati su Internet, ma soprattutto che qualcuno su Internet non si presenti con tali indirizzi IP (di cui ci fidiamo). Ammettiamo che i nostri indirizzi IP sulla rete ethernet interna siano 192.106.21.0/24, l'esempio sarebbe:

```
interface Serial0/0
 ip access-group serial-acl-incoming in
!
ip access-list extended serial-acl-incoming
 remark Deny RFC1918
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 remark Deny loopback
 deny   ip 127.0.0.0 0.255.255.255 any
 remark Anti-spoofing Rule
 deny   ip 192.106.21.0 0.0.0.255 any
 remark Deny Multicast traffic
 deny   ip 224.0.0.0 15.255.255.255.255 any
 remark Allow traffic to flow
 permit ip any any
```

Le CBAC (IOS Firewall)

Le Context-Based Access Control (CBAC) sono una funzionalità tipica dell'IOS Firewall, che è una versione speciale dell'IOS di Cisco. Questo firmare contiene opzioni di sicurezza aggiuntive: esso integra robuste funzionalità di firewall e di intrusion detection, ideali per una sicurezza perimetrale. Vediamo un esempio di CBAC:

```
interface Serial0/0
      ip access-group 116 in
      ip inspect myfw in
      ip auth-proxy mywebproxy
!
access-list 116 permit tcp any any eq www
access-list 116 permit tcp any any eq smtp
access-list 116 deny ip any any
!
ip inspect name myfw http timeout 3600
ip inspect name myfw smtp timeout 3600
!
ip auth-proxy name mywebproxy http
ip http authentication aaa
ip http server
```

Per maggiori informazioni sulle CBAC, si invita la consultazione del CCO Cisco.

PROTEZIONE DEI PROTOCOLLI DI ROUTING

I rischi di sicurezza

Il protocollo di routing serve ad aggiornare le tabelle di routing dinamicamente ed è utile soprattutto in caso di guasti all'interno della propria rete. I protocolli di routing però non sono stati progettati per resistere a possibili attacchi. Quali sono i tipi di rischi che esistono ? Possiamo dividerli in tre aree: attacchi alle tabelle di routing, attacchi di tipo Denial of Service sui router (es. saturazione della CPU) o attacchi di tipo buffer overflow. L'accento si pone in particolar modo sul protocollo di routing BGP, che il cuore di Internet e che si basa su di un rapporto di fiducia tra peers. Solitamente ci fidiamo delle rotte che gli altri router ci mandano, ma cosa succede se ci inviano delle false rotte attraverso per dirottare il traffico attraverso uno specifico percorso?

Mitigare i rischi

Per mitigare i rischi prospettati, è possibile prendere delle precauzioni, ovvero:

- Usare le distribute-lists per controllare gli aggiornamenti delle rotte
- Usare per quanto possibile le rotte statiche, soprattutto sui collegamenti verso l'esterno della nostra azienda (Internet, fornitori, extranet)
- Disabilitare i protocolli di routing sulle interfaccie in cui non servono (passive interface)
- Usare l'interfaccia console per amministrare i router in caso di attachi DoS.
- Usare l'autenticazione dei protocolli di routing e nel HSRP.

I prossimi paragrafi vogliono fornire degli spunti per abilitare l'autenticazione e per configurare in maniera più sicura i protocolli RIP, OSPF, EIGRP, BGP ed HSRP. Per maggiori informazioni sui comandi ed i protocolli, si suggerisce di approfondire on-line sul CCO.

Il protocollo RIP

Il protocollo RIP è ancora diffuso nelle piccole realtà. Vediamo un esempio di autenticazione del protocollo RIP tramite MD5.

```
key chain rabbitsfoot
 key 1
  key-string RIPpasswd

interface Loopback0
 ip address 70.70.70.70 255.255.255.255

interface Serial0
 ip address 142.106.0.10 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain rabbitsfoot

router rip
 version 2
 network 142.106.0.0
 network 70.0.0.0
```

Il protocollo OSPF

OSPF è un protocollo diffuso oggi nelle reti medio-grandi. Il comando successivo serve per usare la Digest Authentication nel protocollo OSPF:

```
ip ospf message-digest-key keyid md5 key
area area-id authentication message-digest
```

Vediamo un esempio completo:

```
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip ospf message-digest-key 1 md5 5 mypassword
!
router ospf 10
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication message-digest
```

Il protocollo EIGRP

EIGRP e' un protocollo proprietario di Cisco. Vediamo quali sono i parametri di configurazione per abilitare MD5:

```
Interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 holly
!
key chain holly
 key 1
 key-string 123456
 accept-lifetime infinite
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 passive-interface default
 no passive-interface FastEthernet0/0
```

Il protocollo BGP

Come accennato precedentemente, BGP è al cuore di Internet ed andrebbe configurato sempre in modo da richiedere l'autenticazione dai peer. L'esempio successivo abilita MD5 per il peer 145.2.2.2:

```
router bgp 109
 neighbor 145.2.2.2 password mypasswd
```

Un altra buona norma di protezione e' abilitare il route dampening, per evitare problemi dovuti all'instabilità del peer (RFC 2439). Un potenziale attaccante potrebbe usare l'instabilità per effettuare un attacco di tipo DoS.

```
router bgp 109
 bgp dampening
show ip bgp flap-statistics
```

Come ulteriore protezione e' possibile usare i filtri BGP, ad esempio attraverso le communities e i Bogon Filters.

Il protocollo HSRP

Le vulnerabilità di HSRP sono ben conosciute: la stringa autenticazione passa in chiaro ed esistono codici per fare spoofing dei pacchetti HSRP. Un eventuale attaccante può mandare dei falsi advertisement e assumere il ruolo di attivo: solitamente questa tecnica viene usata per attacchi DoS o Man-in-the-middle. Esistono due tecniche per evitare questo problema:

- Impostare a 255 la standy priority sui routers;
- Usare sui router gli indirizzi IP che finiscono per .254 o .253 (in una classe C), visto che il più alto IP address viene usato per determinare la precedenza del router.

BIBLIOGRAFIA

Coloradio Springs Cisco User Group
Cisco Router/Switch Hardening
Presentazione, Aprile 2003

NSA
Router Security Configuration Guide
WhitePaper, Dicembre 2003

Biggerstaff
Cisco Router Hardening
Presentazione

Dana Graesser
SANS Cisco Router Hardening Step-by-Step
WhitePaper, Luglio 2001