


 FACOLTÀ DI SCIENZE
 MATEMATICHE FISICHE E NATURALI
 Università degli Studi di Salerno

Syslog-NG

Corso di Sicurezza su Reti
 Prof. Alfredo De Santis
 Anno Accademico 2003/2004
 Francesco Di Rienzo
 Gianluca Esposito
 Feliciano Nigro

Syslog-NG

- Introduzione
- Installazione e Setup
- Configurazione ed utilizzo
- Scenario di utilizzo

2

Syslog-NG

Parte 1
 Introduzione

3

Syslog-NG

DIFFUSIONE INTERNET

+

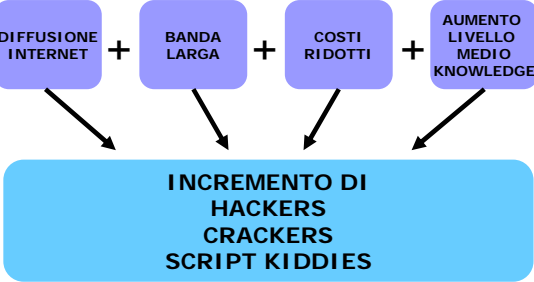
BANDA LARGA

+

COSTI RIDOTTI

+

AUMENTO LIVELLO MEDIO KNOWLEDGE



**INCREMENTO DI
 HACKERS
 CRACKERS
 SCRIPT KIDDIES**

4

Syslog-NG

Introduzione

- Chi si occupa della sicurezza di una rete o dell'amministrazione dei server **DEVE** poter tracciare
 - intrusioni andate a buon fine
 - tentate intrusioni
 - modifiche fatte dall'attacker al sistema violato

Analisi approfondita dei log di sistema

→

Log validi e non modificati in alcun modo

Copia sempre valida dei log di sistema

→

Log validi e non modificati in alcun modo

5

Syslog-NG

Cosa è un log server

- Raccoglie i log di altre macchine
- Consente di avere una copia sicuramente valida dei log delle macchine che lo utilizzano
- Vantaggi: Protezione
 - L'attacker può modificare i log sulla macchina locale
 - L'attacker NON può modificare i log sulla macchina remota
- Vantaggi: Semplicità
 - **analisi** real-time dei log
 - **report** periodico delle attività delle macchine
 - **archiviazione** e backup dei log

6

Syslog-NG

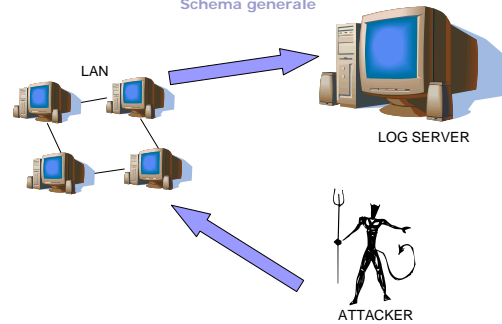
Installazione ideale

- Tutte le macchine da controllare devono inviare i log ad una macchina remota
- Inviare i log in maniera crittografata
- Il log server deve essere molto sicuro
- I log sul log server devono essere organizzati
- Non si deve rischiare di perdere messaggi (UDP vs TCP)
- Invisibile ad un attacker

7

Syslog-NG

Schema generale



8

Syslog-NG

Le nostre scelte

- **syslog-ng**
 - gestisce in maniera semplice i log provenienti da diversi host
 - consente di inviare i log via TCP e non solo in UDP come syslogd
- **stunnel**
 - Crea un tunnel SSL tra la macchina client e il log server
 - L'attacker non può catturare la comunicazione

Syslog-NG:
<http://www.balabit.hu/en/downloads/syslog-ng/downloads/>

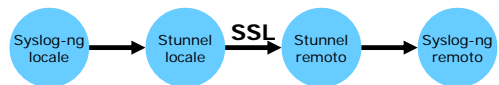
STunnel:
<http://www.stunnel.org>

9

Syslog-NG

stunnel

- cifra le connessioni TCP arbitrarie tramite SSL, che si appoggia ad OpenSSL o SSLeay



10

Syslog-NG

Parte 2 Installazione e set-up

11

Syslog-NG

I client - syslog-ng

Estrarre l'archivio ed editare il file src/syslog-ng.h modificando la linea

```
#define PATH_SYSLOG_CONF /etc/syslog-ng/syslog-ng.conf  
in qualcosa di un poco più nascosto tipo  
#define PATH_SYSLOG_CONF /etc/.conf/default.conf
```

Compilare e installare eseguendo

```
./configure && make && make install  
oppure nel caso non si siano installate le libol  
./configure --with-libol=/path/to/libol && make && make  
install
```

12

Syslog-NG

I client - configurazione di syslog-ng

Creare un file di configurazione di syslog-ng di base :

```
options {
  use_fqdn(yes); keep_hostname(yes); use_dns(yes);
  long_hostnames(off); sync(3); log_file_size(300); };
source client-01 { unix-stream ("/dev/log"); internal(); };
destination local { file ("/var/log/syslog"); };
destination remote { tcp("localhost" port(1666)); };
log { source(client-01); destination(local); };
log { source(client-01); destination(remote); };
```

In questa maniera TUTTI i messaggi verranno loggati in /var/log/syslog e inviati a stunnel

13

Syslog-NG

I client - configurazione di stunnel

Per poter installare stunnel occorrerà avere, sulle macchine client e sulla macchina server, [OpenSSL](#) o oppure in alternativa [SSLeay](#)

Effettuare il download di [stunnel](#) da [www.stunnel.org]

Estrarre e installare stunnel come di consueto :
./configure && make && make install

Editare un file di init (ad esempio rc.local) per eseguire al boot
stunnel -c -d 127.0.0.1:appsrv -r ip.log.server:appsrvs

14

Syslog-NG

Il server - libol e syslog-ng

Procediamo con il download e l'installazione delle libol e di syslog-ng come fatto con i client

Usare un file di configurazione di base :

```
options { use_fqdn(yes); sync(0); use_dns(yes);
  chain_hostnames(yes); keep_hostname(yes);
  log_fifo_size(1000); };
source locallog { unix-stream ("/dev/log"); internal(); };
source remotelog { tcp(ip(port(666) max-connections(10)); };
destination local { file ("/var/log/syslog"); };
destination remote { file ("/var/log/syslog-remote/$HOST/$FACILITY" create_dirs(yes)); };
log { source(locallog); destination(local); };
log { source(remotelog); destination(remote); };
```

In questa maniera TUTTI i messaggi locali verranno loggati in /var/log/syslog e quelli remoti nella dir /var/log/syslog-remote/nomehost/nomefacility

15

Syslog-NG

Il server - configurazione di stunnel

Anche per stunnel eseguiamo la configurazione come per i client

Sul log server, stunnel gira in server mode, quindi occorrerà generare un certificato per stunnel

Editare un file di init (ad esempio rc.local) per eseguire al boot
stunnel -p /path/del/certificato -d ip.log.server:667 -r ip.log.server:666

16

Syslog-NG

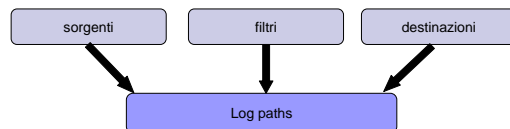
Parte 3 Configurazione ed utilizzo

17

Syslog-NG

In Syslog-NG un messaggio è composto da

- una o più sorgenti
- una o più regole di filtraggio
- una delle possibili destinazioni (pozzi)
- log paths



18

Syslog-NG

Syslog-NG: Sorgenti

- insieme di driver sorgenti
 - raccoglie messaggi usando un metodo predefinito
 - piattaforme diverse = metodi diversi
-
- Dichiarazione di sorgente (Source statement)

```
source <identificatore> { source-driver(parametri);
                          source-driver(parametri); ... };
```

19

Syslog-NG

Syslog-NG: Parametri per le sorgenti

Nome	Descrizione
internal	Messaggi generati internamente da Syslog-NG
unix-stream	Apri gli unix socket specificati in modalità SOCK_STREAM, e ascolta i messaggi.
unix-dgram	Apri lo unix socket specificato in modalità SOCK_DGRAM, e ascolta i messaggi.
file	Apri i file specificati e legge messaggi.
pipe, fifo	Apri i named pipe specificati e legge messaggi.
udp	Ascolta sulla porta UDP specificata.
tcp	Ascolta sulla porta TCP specificata.
sun-stream, sun-streams	Apri gli STREAMS device specificati su sistemi Solaris, e legge i messaggi.

20

Syslog-NG

Syslog-NG: Filtri

- instradamento dei messaggi all'interno di Syslog-NG
 - espressioni booleane
-
- Dichiarazione di filtro (filter statement)

```
filter <identificatore> { espressione; };
```

21

Syslog-NG

Syslog-NG: Destinazioni

- luogo dove vengono raccolti i messaggi
 - diversi driver
-
- Dichiarazione di destinazione (destination statement)

```
destination <identificatore> { destination-
driver(parametri); destination-driver(parametri);
... };
```

22

Syslog-NG

Syslog-NG: Destinazioni disponibili

Nome	Descrizione
file	Scrivi i messaggi nel file specificato
fifo, pipe	Scrivi i messaggi al pipe specificato
unix-stream	Invia i messaggi al socket specificato di tipo SOCK_STREAM (Linux)
unix-dgram	Invia i messaggi al socket specificato di tipo SOCK_DGRAM (BSD)
udp	Invia i messaggi all'host e alla porta UDP specificati
tcp	Invia i messaggi all'host e alla porta TCP specificati
usertty	Invia i messaggi all'utente specificato se registrato
program	Sblocca e lancia il programma specificato, e invia i messaggi al suo standard input.

23

Syslog-NG

Syslog-NG: Log paths

- unione logica tra
 - sorgenti
 - filtri
 - destinazioni

- Dichiarazione di log (log statement)

```
log { source s1; source s2; ...
      filter f1; filter f2; ...
      destination d1; destination d2; ... };
```

24

Syslog-NG

Syslog-NG: Flag dei log statement

Flag	Descrizione
final	il processo di log termina
fallback	solo i messaggi che non corrispondono ad alcun 'non-fallback' log statement saranno inviati
catchall	<ul style="list-style-type: none">la fonte del messaggio viene ignoratasoltanto i filtri sono presi in considerazione quando i messaggi vengono rilevati

25

Syslog-NG

Syslog-NG: Driver sorgenti

- internal()
- unix-stream()
- unix-dgram
- tcp()
- udp()
- file()
- pipe()
- sun-streams()

26

Syslog-NG

Syslog-NG: Le opzioni delle sorgenti
unix-stream() e unix-dgram()

- owner()
- group()
- perm()
- keep-alive()
- max-connections()

27

Syslog-NG

Syslog-NG: Le opzioni delle sorgenti
udp() e tcp()

- ip o localip
- port o localport
- keep-alive
- max-connections

28

Syslog-NG

Syslog-NG: Le opzioni della sorgente file()

- log_prefix

Syslog-NG: Le opzioni della sorgente pipe()

- pad_size

Syslog-NG: Le opzioni della sorgente sun-stream()

- door

29

Syslog-NG

Syslog-NG: Driver destinazioni

- file()
- pipe()
- unix-stream()
- unix-dgram
- tcp()
- udp()
- usertty()
- program()

30

Syslog-NG

Syslog-NG: Le macro della destinazione file()

- FACILITY
- PRIORITY o LEVEL
- TAG
- DATE
- FULLDATE
- ISODATE
- YEAR
- MONTH
- DAY
- WEEKDAY
- HOUR
- MIN
- SEC
- TZOFFSET
- TZ
- FULLHOST
- HOST
- PROGRAM
- MSG o MESSAGE

31

Syslog-NG

Syslog-NG: Le opzioni della destinazione file()

- log_fifo_size()
- fsync()
- sync_freq()
- encrypt()
- compress()
- owner()
- group()
- perm()
- dir_perm()
- create_dirs()
- template()
- template_escape()
- remove_if_older()

32

Syslog-NG

Syslog-NG: Le opzioni delle destinazioni udp() e tcp()

- localip
- localport
- port o destport

33

Syslog-NG

Syslog-NG: Funzioni filtro

- facility()
- level()
- priority()
- program()
- host()
- match()
- filter()

34

Syslog-NG

Syslog-NG: Opzioni globali

- time_reopen()
- time_reap()
- sync()
- mark()
- stats()
- log_fifo_size()
- chain_hostnames()
- keep_hostname()
- check_hostname()
- bad_hostname()
- create_dirs()
- owner()
- group()
- perm()
- dir_owner()
- dir_group()
- dir_perm()
- create_dirs()
- use_time_recvd()
- use_dns()
- dns_cache()
- dns_cache_size()
- dns_cache_expire()
- dns_cache_expire_failed()
- log_msg_size()
- use_fqdn()
- gc_idle_threshold()
- gc_busy_threshold()

35

Syslog-NG

Syslog-NG: Performance Tuning

- Gestione del cestino
 - gc_idle_threshold()
 - gc_busy_threshold()
- Dimensione della coda di output
 - log_fifo_size()
- Sincronizzazione dell'output
 - Sync()

36

Syslog-NG

Parte 4 Scenario di utilizzo

37

Syslog-NG

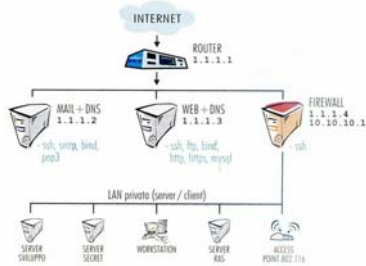
Parte 4 – Tavola dei contenuti

- Organizzazione base della rete d'esempio
- Fasi dell'attacco
- Rete di esempio
- Esempi pratici
- Introduzione di firewall
- Introduzione di IDS
- Schema di raccolta dei log

38

Syslog-NG

Organizzazione base della rete di esempio



39

Syslog-NG

Requisiti minimi e macchine di prova

■ Requisiti minimi di sistema

- Processore Intel o compatibile (400Mhz)
- Memoria RAM almeno 256 Mb
- Sistema Operativo: Linux con Kernel 2.3.2.

■ Macchina di prova

- Processore AMD Athlon XP 2800+ (2.08 GHz)
- RAM 256 Mb
- Sistema Operativo:
- SuSE Linux 8.1 – Kernel 2.4.19-4GB emulato mediante Connectix VirtualPC 5.4 (build 418) in ambiente Microsoft Windows XP Professional

40

Syslog-NG

Fasi dell'attacco

- **HIDING**
Mascheramento
- **INFORMATION GATHERING**
Raccolta di informazioni
- **SYSTEM PENETRATION**
Intrusione
- **CLEANING**
Pulizia

41

Syslog-NG

Hiding

- L'attacker cerca di "camuffarsi", nascondendo la propria reale ubicazione per scongiurare il pericolo di essere tracciato ed identificato
- **Launchpad**
 - Utilizzo di sistemi ponte
- **Dialout**
 - Mascheramento della propria utenza telefonica

42

Syslog-NG

Information Gathering - 1

- **Network Surveying**
 - Ricerca dati
 - Raccolta di informazioni importanti
 - Controllo delle politiche di sicurezza
 - Information disclosure
 - Es.: Nomi di dominio, indirizzi IP, indirizzi email validi, etc.
- **Port Scanning**
 - probing invasivo delle porte di sistema

↓

Mappa di rete sufficientemente dettagliata

43

Syslog-NG

Information Gathering - 2

- **Service Identification**
 - esame attivo delle applicazioni in ascolto sulle porte
 - l'attaccante individua i possibili punti deboli dell'infrastruttura bersaglio
- **System Identification**
 - probing attivo
 - l'attaccante individua la tipologia di sistema operativo, la sua versione ed altre ulteriori informazioni specifiche
 - TCP/IP fingerprinting

↓

Mappa di rete più dettagliata

44

Syslog-NG

System Penetration - 1

- **System security**
 - vulnerabilità a livello di sistema operativo e nel software di base
 - alcuni servizi e programmi applicativi datati oppure mal configurati
 - accesso non autorizzato al sistema che ne fa uso (vulnerabilità remote)
 - realizzare una scalata di privilegi (vulnerabilità locali)
- **Network security**
 - vulnerabilità che minano il livello di sicurezza globale della rete
 - la tipologia di rete e la presenza di punti di accesso alla rete privata
 - la tipologia e la configurazione dei sistemi per il routing ed il firewalling
 - il monitoraggio passivo del traffico (Network Sniffing)

45

Syslog-NG

System Penetration - 2

- **Application security**
 - insicurezze del software applicativo
 - attacchi mirati a reperire informazioni riservate o ad ottenere un accesso non autorizzato ai sistemi che erogano i servizi pubblici
 - SQL injection, cross-site scripting, session hijacking
- **Procedural security**
 - falle strutturali all'interno del proprio modello di gestione
 - social engineering, human deception

46

Syslog-NG

Cleaning

- Rimozione delle tracce lasciate
 - nei file di log
 - su altre regioni del file system
 - sugli eventuali dispositivi di monitoraggio delle attività di rete per il rilevamento delle intrusioni (Intrusion Detection Systems).

47

Syslog-NG

Information Gathering - Network Surveying – Esempio 1

```
# whois -h whois.ripe.net 1.1.1.3
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights reserved by copyright
% See http://www.ripe.net/whois
% - Sub-services@copyright.html
inetnum: 1.1.1.0 - 1.1.1.7
netname: ROSENDO-NET
descr: Profumaria RoseNoir Srl
country: IT
admin-c: [...]
tech-c: [...]
status: ASSIGNED PA
mnt-by: ISP-NCC
notify: noc@isp
changed: noc@isp 20020711
route: 1.1.0.0/9
source: RIPE
descr: ISP
origin: [...]
remarks: ALLOCATED PA Space do not break up
notify: noc@isp
mnt-by: ISP-NCC

changed: noc@isp 20020711
RIPE
person: Giuseppe Rossi
address: Profumaria RoseNoir Srl
address: via Roma 00
address: 00000 Milano (MI)
address: Italy
phone: +39 02 XXXXXXXX
fax-no: +39 02 XXXXXXXX
e-mail: Giorgio@profumi-online.biz
[...]
changed: noc@isp
source: RIPE
person: Giuseppe Rossi
address: Profumaria RoseNoir Srl
address: via Roma 00
address: 00000 Milano (MI)
address: Italy
phone: +39 02 XXXXXXXX
fax-no: +39 02 XXXXXXXX
e-mail: beppe@profumi-online.biz
[...]
changed: noc@isp
source: RIPE
```

48

Syslog-NG

Information Gathering - Network Surveying – Esempio 2

```
# whois -h whois.networksolutions.com profumi-online.biz
[...]
Domain Name: PROFUMI-ONLINE.BIZ
Domain ID: [...]
Sponsoring Registrar: [...]
Domain Status: OK
Registrar ID: [...]
Registrar Name: Giorgio Rossi
Registrar Organization: Profumeria RoseNoir Srl
Registrar Address1: via Roma 00
Registrar City: Milano
Registrar State/Province:
Registrar Postal Code: 00000
Registrar Country: Italy
Registrar Country Code: IT
Registrar Phone Number: +39.02XXXXXXX
Registrar Facsimile Number: +39.02XXXXXXX
Registrar Email: g.rossi@libero.it
Name Server: DNS.PROFUMI-ONLINE.BIZ
Name Server: DNS2.PROFUMI-ONLINE.BIZ
Created by registrar: [...]
```

49

Syslog-NG

Information Gathering - Network Surveying – Esempio 3

```
# host -t ns profumi-online.biz #name server
profumi-online.biz NS dns.profumi-online.biz
profumi-online.biz NS dns2.profumi-online.biz
# host -t mx profumi-online.biz # mail exchange
profumi-online.biz MX 20 mail.profumi-online.biz
# host -t profumi-online.biz # zone transfer
profumi-online.biz NS dns.profumi-online.biz
profumi-online.biz NS dns2.profumi-online.biz
profumi-online.biz MX 20 mail.profumi-online.biz
gw.profumi-online.biz A 1.1.1.1
mail.profumi-online.biz A 1.1.1.2
www.profumi-online.biz A 1.1.1.3
dns.profumi-online.biz A 1.1.1.2
dns2.profumi-online.biz A 1.1.1.3
fw.profumi-online.biz A 1.1.1.4
```

50

Syslog-NG

Information Gathering - Port Scanning – Esempio

```
# nmap 1.1.1.1 # gateway
Starting nmap V.2.54BETA30 www.insecure.org/nmap
Interesting ports on gw.profumi-online.biz (1.1.1.1):
Port State Service
79/tcp open finger
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
3306/tcp open mysql

# nmap -sU 1.1.1.1 # gateway
Starting nmap V.2.54BETA30 www.insecure.org/nmap
Interesting ports on gw.profumi-online.biz (1.1.1.1):
Port State Service
161/tcp open snmp

# nmap 1.1.1.2 # mail + DNS
Starting nmap V.2.54BETA30 www.insecure.org/nmap
Interesting ports on dns.profumi-online.biz (1.1.1.2):
Port State Service
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
110/tcp open pop3

# nmap 1.1.1.3 # web + DNS
Starting nmap V.2.54BETA30 www.insecure.org/nmap
Interesting ports on dns2.profumi-online.biz (1.1.1.3):
Port State Service
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
3306/tcp open mysql

# nmap 1.1.1.4 # firewall
Starting nmap V.2.54BETA30 www.insecure.org/nmap
Interesting ports on fw.profumi-online.biz (1.1.1.4):
are: filtered
```

51

Syslog-NG

System Penetration – Attacco alla rete pubblica

- **System insecurity**
 - Information Leak
 - Exploit
 - Brute Force
- **Application insecurity**
 - Web Application
- **Network insecurity**
 - SNMP Spoofing
 - Sniffing
 - Punti di accesso
- **Procedural insecurity**
 - Trust Relationship
 - Riciclo di password

52

Syslog-NG

System Penetration – Attacco alla rete privata

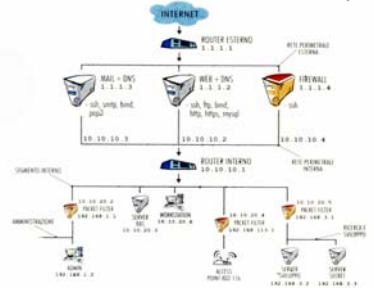
Stessi principi esposti nel caso dell'attacco alla rete pubblica, con alcune differenze:

- Information Gathering molto più veloce
- più servizi attivi
- aggiornamenti del software in genere meno frequenti
- dispositivi di rete spesso scarsamente protetti
- analisi passiva del traffico (Network Sniffing) molto più redditizia
- sono più frequenti le relazioni di fiducia tra sistemi
- controlli di sicurezza (IDS, etc.) molto più rilassati

53

Syslog-NG

Introduzione di firewall nella rete di esempio



54

Syslog-NG

I Firewall: terminologia - 1

- **Bastion host**
 - sistema più esposto ad attacchi esterni ed interni
 - tipicamente ospita servizi raggiungibili da Internet
- **Packet Filter**
 - controlla selettivamente la comunicazione tra due peer o tra Internet e la rete interna e viceversa
- **NAT (Network Address Translation)**
 - procedura che permette di modificare gli indirizzi contenuti nei datagrammi di rete
 - associa sistemi interni sprovvisti di indirizzi IP pubblici ad un unico indirizzo pubblico o ad un set limitato di indirizzi
 - nasconde i reali indirizzi IP

55

Syslog-NG

I Firewall: terminologia - 2

- **Proxy**
 - dialoga con server esterni per conto di client interni della propria rete
- **DMZ (De-Militarized Zone)**
 - rete inserita tra un ulteriore segmento protetto, interno, ed un'altra rete esterna
- **VPN (Virtual Private Network)**
 - rete in cui i datagrammi di competenza di sistemi interni, passano attraverso reti esterne, pubbliche, senza che questo sia ovvio o visibile ai sistemi interni

56

Syslog-NG

Introduzione dei firewall – Differenze dallo scenario base

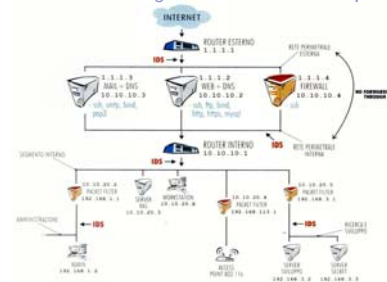
Stessi principi esposti nel caso dell'attacco alla rete pubblica, con alcune differenze:

- separazione del traffico pubblico e privato mediante due reti perimetrali senza forwarding di traffico
- unico punto di NAT tra le due reti perimetrali per le macchine dei dipendenti
- separazione mediante filtri di pacchetti tra il segmento interno e la seconda rete perimetrale
- ACL per controllare il traffico dei dipendenti verso la rete perimetrale
- separazione mediante firewall interni con router di controllo tra i segmenti di management, ricerca e sviluppo e dei dipendenti

57

Syslog-NG

Introduzione degli IDS nella rete di esempio



58

Syslog-NG

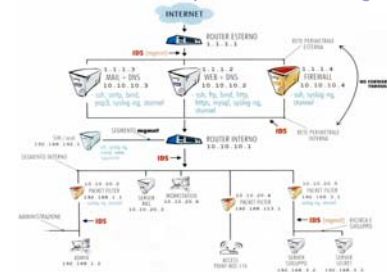
IDS – Elementi funzionali comuni

- l'interfaccia di rete del sistema è posta in modalità promiscua
- cattura tutto il traffico lungo il segmento analizzato
- filtri specifici per modificare la tipologia e la quantità di traffico da sottoporre all'attenzione del motore di ricerca degli attacchi
 - a ricerca di modelli
 - a frequenza
 - ad anomalie

59

Syslog-NG

Schema della rete di esempio – La rete di management



60

Syslog-NG

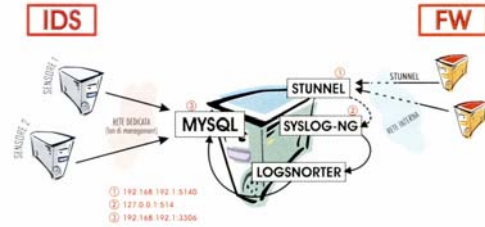
Firewall e IDS: linee guida per le policy di sicurezza

- regole icmp-info, icmp, experimental nei segmenti di accesso ai router
- regole attack-responses, DNS, exploit, MySQL, POP3, smtp, snmp, TFTP, virus nelle reti perimetrali
- regole bad-traffic, DoS, DDoS, mise, info, scan, shellcode in ogni segmento
- regole backdoor, exploit, netbios, FTP, virus, xll nel segmento interno
- regole chat, multimedia, p2p, porn se contemplati dalla policy per i dipendenti
- regole web-* per il segmento che contiene web server

61

Syslog-NG

Schema di raccolta dei log - 1



62

Syslog-NG

Schema di raccolta dei log - 2

Consideriamo solo i seguenti device:

- IDS esterno;
 - 1.1.1.4 firewall/NAT;
 - IDS interno;
 - 10.10.20.5 packet filter a difesa di secret/devel
-
- database centralizzato
 - canali "sicuri" o tunnel "cifrati"

63

Syslog-NG

Schema di raccolta dei log - 3

Strumenti OpenSource:

- ACID (Analysis Console for Intrusion Database)
- snort – logsnorter
- stunnel
- Syslog-NG

64

Syslog-NG

Configurazione di Snort

- File di configurazione snort.conf
 - output database: log, mysql, user=snort password=snort dbname=snort host=192.168.192.1
- Creazione delle tabelle MySQL per la memorizzazione
 - # mysql -u root -p mysql
 - Enter password: [password di root di MySQL]
 - mysql> CREATE DATABASE SNORT
 - mysql> GRANT INSERT, SELECT ON SNORT.* TO SNORT@localhost: (per logsnorter)
 - mysql> GRANT INSERT, SELECT ON SNORT.* TO SNORT@192.168.192.2: (interfaccia mgmnt IDS esterno)
 - mysql> GRANT INSERT, SELECT ON SNORT.* TO SNORT@192.168.192.3: (interfaccia mgmnt IDS interno)
 - mysql> FLUSH PRIVILEGES;
 - mysql> QUIT
 - # mysql -u root -p snort < CREATE _MYSQL
 - # Enter password: [password di root di MySQL]

65

Syslog-NG

Configurazione di Syslog-NG - 1

- File di configurazione syslog-ng.conf remoti
 - source src { unix-stream("/dev/log"); internal(); pipe("/proc/kmsg");};
 - filter f_firewall{match("IN=") and match("OUT=")};
 - destination firewall {tcp("127.0.0.1" port(5140))};
 - log{source(src); filter(f_firewall); destination(firewall)};

66

Syslog-NG

Configurazione di Syslog-NG - 2

- File di configurazione syslog-ng.conf locale
 - source src {
 unix-stream("/dev/log");
 pipe("/proc/kmsg");
 tcp(ip("127.0.0.1") port(514));
 tcp();
 internal();
};
 filter f_firewall{match("IN=") and match("OUT=")};
 destination firewall {file("/var/log/firewall.log" OWNER("root")
 GROUP("adm") PERM(0640))};
 log{source(src);
 filter(f_firewall);
 destination(firewall)};

67

Syslog-NG

Esecuzione di Stunnel

- Sulle macchine che inviano i log
 - # stunnel -c -d 5140 -r 192.168.192.1:5140
- Sull'host remoto
 - # stunnel -p stunnel.pem -d 5140 -r 192.168.192.1:514

68

Syslog-NG

Configurazione di logsnorter

- Dalla linea di comando
 - # logsnorter -u snort -p snort -s 127.0.0.1 -d snort -
 T/var/log/firewall.log -L 8 -t

69

Syslog-NG

Configurazione di ACID

- Modifica delle ACL
 - # mysql -u root -p
 # Enter password: [password di root di MySQL]
 mysql> GRANT SELECT INSERT, UPDATE, UPDATE ON SNORT.* TO
 SNORT@localhost IDENTIFIED BY 'SNORT';
 mysql> QUIT
- Modifica del file acid_conf.php
 - <?php
 \$ACID_VERSION = "0.9.6b22";
 \$DbType = "MySQL";
 \$alert_dbname = "SNORT";
 \$alert_host = "localhost";
 \$alert_port = "";
 \$alert_user = "SNORT";
 \$password = "SNORT";
 [snip]

70

Syslog-NG

Esempio di log prodotto

- 192.168.1.55 - - [15/jan/2003:19:09:18 + 0100] "GET
 /index.html http/1.0" 200 14025 "http://1.1.1.2/index.html"\n
 "lynx /2.8.5dev.7 libwww-FM/2.1.4 ssl -
 mm/1.4.1openssl/0.9.6b"

71