



# Sicurezza delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica e Comunicazione  
Università degli Studi di Milano, Italia

[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2010/11



Sicurezza delle  
reti

Monga

Aspetti  
architettonici

Posizionamento  
sensori

Risposta NIDS

Risposte  
automatiche

Tecniche di  
evasione

Conclusioni

## Lezione XIII: Architettura dei NIDS

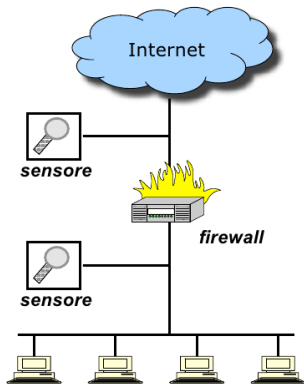


Data la natura di componente di monitoraggio, un NIDS è un componente che **complementa** altre soluzioni per la sicurezza aziendale contribuendo a formare un'architettura a diversi livelli di sicurezza (**defense in-depth**).

Sono quindi importanti aspetti architetturali quali:

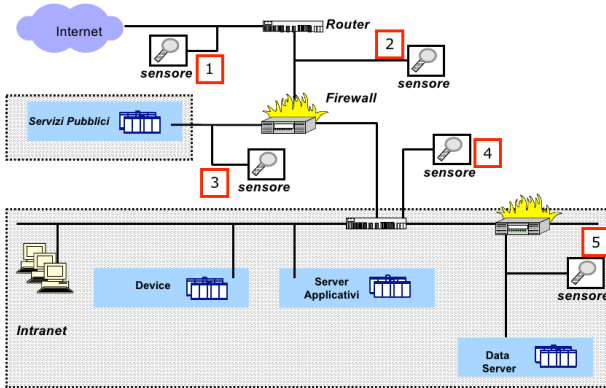
- Quanti sensori installare nella rete
  - costo e complessità di gestione vs. ricchezza di dati
- Dove installarli
  - visibilità del traffico vs. ridondanza di informazioni
- Come gestire i dati
  - analisi e logging centralizzato vs. analisi e/o logging distribuito

- Esterno
- Rileva l'intero traffico diretto alla rete
  - Maggiore quantità di dati
  - Maggiore incidenza di falsi allarmi
- Interno
- Rileva solo il traffico che entra effettivamente nella rete
  - Verifica l'efficacia del firewall
  - Non fornisce info sugli attacchi bloccati dal firewall





# Posizionamento nella rete aziendale



## 1. Esterno al border router

- Rileva l'intero traffico diretto alla rete aziendale.
- Informazione completa e non filtrata da nessun dispositivo.
- Maggiore mole di dati ed allarmi, alta incidenza di falsi allarmi.

Sicurezza delle reti

Monga

Aspetti architetturali

Posizionamento sensori

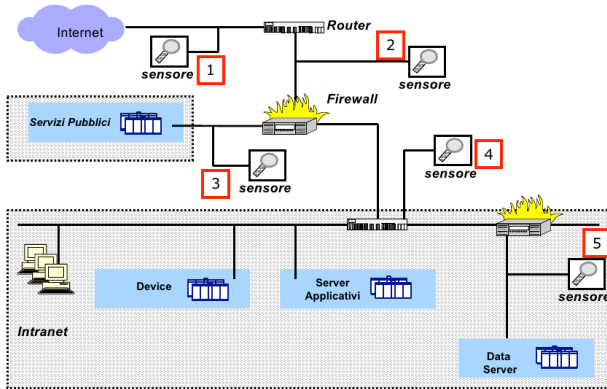
Risposta NIDS

Risposte automatiche

Tecniche di evasione

Conclusioni

# Posizionamento nella rete aziendale



## 2. Tra border router e firewall

- Tutto il traffico che entra nella rete tranne quello filtrato da ACL del router.
- Quantità elevata di dati da analizzare, molti falsi allarmi.

Sicurezza delle reti

Monga

Aspetti architetturali

Posizionamento sensori

Risposta NIDS

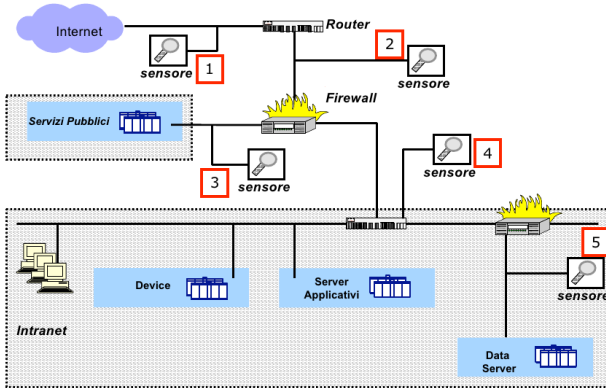
Risposte automatiche

Tecniche di evasione

Conclusioni



# Posizionamento nella rete aziendale



## 3. Sulla rete dei servizi pubblici, dietro il firewall

- Rileva tutto il traffico autorizzato dal firewall e diretto ai servizi pubblici.
- Possibilità filtraggio mirato con riduzione falsi positivi e maggiore efficienza.
- Rileva anche eventuale traffico non lecito originato dai server pubblici.

Sicurezza delle reti

Monga

Aspetti architetture

Posizionamento sensori

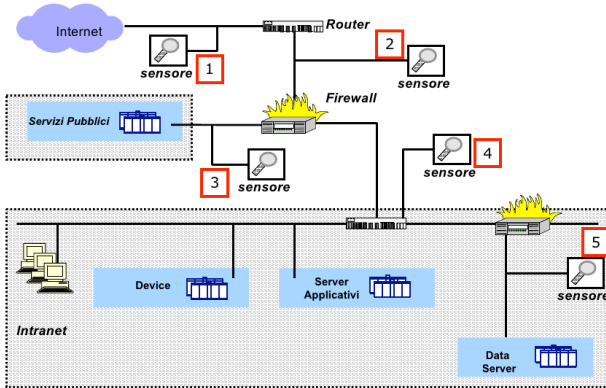
Risposta NIDS

Risposte automatiche

Tecniche di evasione

Conclusioni

# Posizionamento nella rete aziendale



## 4. Sulla Intranet

- Monitora sia il traffico proveniente da reti piú esposte a problemi di sicurezza (es. DMZ) che il traffico interno alla Intranet.
- Rileva eventuali usi non leciti interni alla rete aziendale.
- Difficile selezione delle firme, molti falsi allarmi.

Sicurezza delle reti

Monga

Aspetti architetturali

Posizionamento sensori

Risposta NIDS

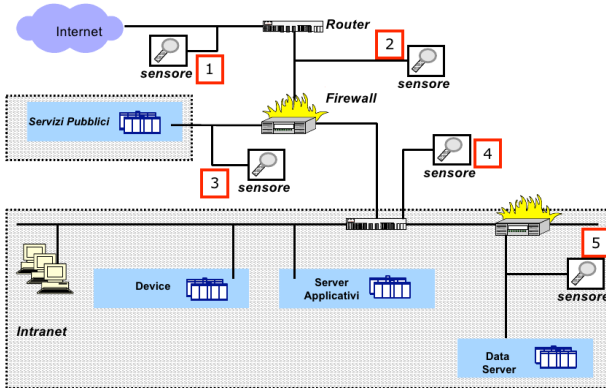
Risposte automatiche

Tecniche di evasione

Conclusioni



# Posizionamento nella rete aziendale



## 5. Su di un segmento critico della rete aziendale

- Monitora le connessioni dirette ad alcune risorse particolarmente critiche della rete aziendale per le quali si richiede un livello di sicurezza più elevato (es. i server contenenti dati aziendali sensibili).
- Servizi specifici, quindi possibilità di configurazione mirata delle firme.

Sicurezza delle reti

Monga

Aspetti architetturali

Posizionamento sensori

Risposta NIDS

Risposte automatiche

Tecniche di evasione

Conclusioni



- La tipica risposta di un NIDS al verificarsi di un evento che verifica una firma è la generazione di un **allarme**
- La forma piú standard di allarme è la scrittura in un corrispondente **file di log**

Esempio di log su syslog

```
[1:1122:2 ] WEBMISC /etc/passwd [Classification: Attempted  
Information Leak ] [Priority:2 ] 09/1610:04:15.826116  
192.168.1.1:3143 >192.168.1.2:80 TCP TTL:128 TOS:0x0  
ID:12832 IpLen:20 DgmLen:149 DF ***AP***Seq:0xDEFF5454  
Ack:0x1A51AF74 Win:0x4470
```

Esistono molte varianti implementate dai diversi NIDS, tra cui salvataggio in formato tcpdump, scrittura su database (es. MySQL), visualizzazione a video ecc.

Sicurezza delle  
reti

Monga

Aspetti  
architettruali

Posizionamento  
sensori

Risposta NIDS

Risposte  
automatiche

Tecniche di  
evasione

Conclusioni



Le scritture su log vanno successivamente analizzate: servono strumenti di supporto perché la mole di dati è spesso imponente.

- Esistono molti strumenti, sia open-source che integrati nei prodotti commerciali, di analisi dei log prodotti da un NIDS.
- Tipicamente vengono mostrati grafici, statistiche ecc. Sono utili per le analisi *post-mortem* e per il tuning dei sistemi, ma inefficaci per un'azione di contenimento real-time
- L'invio di email a un amministratore è un'altra modalità di risposta diffusa (e onerosa).

Sicurezza delle  
reti

Monga

Aspetti  
architettonici

Posizionamento  
sensori

Risposta NIDS

Risposte  
automatiche

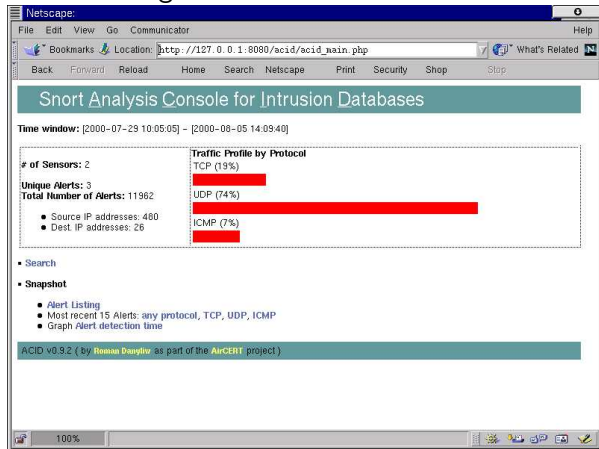
Tecniche di  
evasione

Conclusioni



## ACID (Analysis Console for Intrusion Databases)

<http://acidlab.sourceforge.net/> Interfaccia in PHP di analisi dei log di Snort



Sicurezza delle reti

Monga

Aspetti architeturali

Posizionamento sensori

Risposta NIDS

Risposte automatiche

Tecniche di evasione

Conclusioni



# Tool di analisi

SGUIL (The Analyst Console for Network Security Monitoring)

<http://sguil.sourceforge.net/index.php> Interfaccia per la visualizzazione real-time di alarm generati da Snort

Sicurezza delle reti

Mongia

Aspetti  
architeturali  
Posizionamento  
sensori  
Risposta NIDS  
Risposte automatiche  
Tecniche di  
evasione  
Conclusioni

The screenshot displays the SGUIL web interface. At the top, it shows the user is logged in as 'sguil' on 'localhost'. Below this is a table of 'RealTime Events' with columns for Sensor, Sncp ID, Start Time, End Time, Src IP, SPort, Dst IP, DPort, Pr, S, Pkts, and S Byte. The table contains several rows of data, with one row highlighted in blue. Below the table, there is a 'Display Sncp Details' section showing source and destination IP addresses, DNS information, and network details. A note explains that the Sncp summarizes data across a session. At the bottom, there are sections for 'System Messages' and 'User Messages'.

Sensor	Sncp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S	Pkts	S Byte
orr	4734588612964100650	2004-12-06 18:25:47	2004-12-06 18:25:47	10.200.211.32	56091	10.200.211.39	111	17	1	64	
orr	4734588612964103123	2004-12-06 18:25:47	2004-12-06 18:25:48	10.200.211.32	89425	10.200.211.39	1023	6	5	64	
orr	4734588634330598264	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	951	10.200.211.39	111	17	1	64	
orr	4734588634330598882	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	767	10.200.211.39	2040	17	1	64	
orr	4734588634330598513	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	781	10.200.211.39	111	17	1	64	
orr	4734588634330598817	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	628	10.200.211.39	1022	17	1	108	
orr	4734588634330598716	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	786	10.200.211.39	2040	17	1	108	
orr	4734581170462910450	2004-12-06 18:34:08	2004-12-06 18:34:08	10.200.211.32	63391	192.168.0.3	3128	6	5	417	
orr	47345811704629142186	2004-12-06 18:34:08	2004-12-06 18:34:08	10.200.211.32	30427	192.168.0.3	3128	6	5	435	
orr	47345811708937435985	2004-12-06 18:34:08	2004-12-06 18:34:10	10.200.211.32	62185	192.168.0.3	3128	6	17	1501	
orr	47345811708937547721	2004-12-06 18:34:08	2004-12-06 18:34:09	10.200.211.32	62657	192.168.0.3	3128	6	10	824	
orr	47345811708937670238	2004-12-06 18:34:08	2004-12-06 18:34:09	10.200.211.32	65042	192.168.0.3	3128	6	5	439	

Display Sncp Details

Source IP: 10.200.211.32  
Src Name: Unknown  
Dst IP: 66.93.110.10  
Dst Name: www.foosecurity.com

Reverse DNS: foosecurity.com

Speakeasy Network SPEAKEASY-5 (NET-66-92-0-0-1)  
66.92.0.0 - 66.93.255.255

Identify Vector Solutions SPEK-3/8294-0 (NET-66-93-0-0-1)  
66.93.110.0 - 66.93.110.31

NOTE: Sncp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.



# Tool di analisi

SNORTSNARF [http://www.snort.org/dl/contrib/data\\_analysis/snortsnarf/](http://www.snort.org/dl/contrib/data_analysis/snortsnarf/) Interfaccia WEB per l'analisi dei log generati da Snort

SILICON DEFENSE SnortSnarf start page  
All Snort signatures  
SnortSnarf v021111.1

[Signature section \(3393\)](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

3393 alerts found using input module SnortFileInput, with sources:  
• /var/log/messages

Earliest alert at 03:32:27 on 9/17/2005  
Latest alert at 11:58:58 on 9/21/2005

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	(snort_decoder) WARNING: TCP Data Offset is less than 5!	1	1	1	<a href="#">Summary</a>
N/A	(snort_decoder): Truncated Top Options	3	1	1	<a href="#">Summary</a>
N/A	(portscan) ICMP Sweep	3	1	2	<a href="#">Summary</a>
N/A	(portscan) TCP Decoy Portscan	4	4	1	<a href="#">Summary</a>
N/A	(portscan) UDP Distributed Portscan	9	8	1	<a href="#">Summary</a>
N/A	(portscan) UDP Portscan	16	6	1	<a href="#">Summary</a>
N/A	(portscan) TCP Distributed Portscan	17	17	1	<a href="#">Summary</a>
N/A	(http_inspect) IIS UNICODE CODEPOINT ENCODING	39	2	13	<a href="#">Summary</a>

Sicurezza delle reti

Monga

Aspetti architetturali

Posizionamento sensori

Risposta NIDS

Risposte automatiche

Tecniche di evasione

Conclusioni



# Tool di analisi

## Symantec Network Security 7120 Interfaccia per l'analisi dei log generati dall'appliance

Symantec Network Security Console - Connected to 10.0.0.254

File Configuration Topology Flows Reports Admin Help

Devices Incidents Policies

Customize Incident List:  
Columns... Filters... Showing: [All Nodes (except standby)]

Incidents - Last 8 Hours/1000 Incidents

Last Mod. Time	Name	Severity	Source	Destination	Event Count	State	Marked
11/11/04 2:24:42 PM	A Sensor Link Is Now Down	Critical			1	Closed	
11/11/04 2:24:42 PM	A Sensor Link Is Now Down	Critical			1	Closed	
11/11/04 2:09:30 PM	A Sensor Link Is Now Down	Critical			1	Closed	
11/11/04 1:57:05 PM	A Sensor Link Is Now Down	Critical			1	Closed	
11/11/04 2:25:39 PM	A Sensor Link Went Up	Critical			1	Closed	
11/11/04 2:25:51 PM	A Sensor Link Went Up	Critical			1	Closed	
11/11/04 2:11:05 PM	A Sensor Link Went Up	Critical			1	Closed	
11/11/04 2:43:19 PM	Bay/Nortel Networks Nautica Marlin DoS	Medium	10.0.0.4:40888	10.0.0.17:1032	49	Active	
11/11/04 2:18:36 PM	Malformed HTTP 'Content-Range' Value	High	(multiple IPs)	10.0.0.10:1271	6	Closed	
11/11/04 2:41:39 PM	Malformed POP3 Base-64 Encoding	High	159.149.10.4:110	10.0.0.12:1741	24	Active	
11/11/04 2:38:43 PM	POP3 Failed Login	Medium	10.0.0.17:51319	213.92.100.226:110	15	Active	
11/11/04 2:33:45 PM	SMB Guest Login Attempt	Information...	10.0.0.6:445	10.0.0.17:51298	5	Active	
11/11/04 2:27:45 PM	Super User Login	Information...	10.0.0.17		1	Closed	
11/11/04 1:50:28 PM	Super User Login	Information...	10.0.0.17		1	Closed	
11/11/04 2:36:39 PM	TCP Unusual-flags Portscan	Low	(multiple IPs)	10.0.0.17:50931	1	Active	
11/11/04 2:34:47 PM	Targeted UDP Flood	Medium	(multiple IPs)	10.0.0.1:192	2	Active	
11/11/04 2:24:17 PM	Targeted UDP Flood	Medium	10.0.0.1:53	10.0.0.17:50667	1	Closed	

Customize Event List:  
Columns... Filters... Showing: [All]

Events at Selected Incident - Top 100 Events

Time	Name	Severity	Source	Destination	Event Num
11/11/04 2:11:12 PM	TCP Unusual-Flags Portscan	Low	212.78.204.110:80	10.0.0.10:1268	2
11/11/04 2:12:41 PM	Malformed HTTP 'Content-Range' Val...	High	213.92.80.5:80	10.0.0.10:1285	4
11/11/04 2:11:14 PM	Malformed HTTP 'Content-Range' Val...	High	213.92.80.5:80	10.0.0.10:1271	1
11/11/04 2:12:38 PM	Malformed HTTP 'Content-Range' Val...	High	213.92.80.5:80	10.0.0.10:1283	3
11/11/04 2:18:34 PM	Malformed HTTP 'Content-Range' Val...	High	213.92.80.4:80	10.0.0.10:1307	5
11/11/04 2:18:36 PM	Malformed HTTP 'Content-Range' Val...	High	213.92.80.4:80	10.0.0.10:1310	6

Sicurezza delle reti

Monga

Aspetti  
architeturali

Posizionamento  
sensori

Risposta NIDS

Risposte  
automatiche

Tecniche di  
evasione

Conclusioni



## Risposta automatica

Una modalità di allarme che implica la generazione automatica di azioni allo scopo di rispondere attivamente ad una presunta intrusione senza richiedere l'intervento diretto di un operatore.

Esempio Snort:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS  
(msg:"WEB-IIS cmd.exe access"; content:"cmd.exe";  
react: block; ...)
```

L'opzione `react: block` fa sí che la connessione TCP nella quale si è verificato il tentativo di accesso a `cmd.exe` venga automaticamente terminata







Per realizzare lo sniping, il NIDS deve essere in grado di forzare la terminazione della connessione in corso tra client e server

- inviando un pacchetto contenente un RST ad entrambe le parti coinvolte nella connessione
- tali pacchetti devono apparire ai riceventi come inviati dalle corrispondenti controparti, non dal NIDS, altrimenti verrebbero ignorati
- devono quindi contenere valori corretti per i numeri di sequenza, numero di ack, ...



La rilevazione di un allarme può essere sfruttata per riconfigurare automaticamente le regole di un firewall

- Esempio: la rilevazione di attività di scan viene utilizzata per impedire automaticamente ogni connessione da parte degli indirizzi IP sorgenti coinvolti.

Meno efficace di quel che potrebbe sembrare:

- Un intrusore può provocare riconfigurazioni che risultano dannose, ad esempio inviando pacchetti con IP spoofed
- Gli effetti possono essere di bloccare le connessioni provenienti da sorgenti legittime (denial-of-service)



Qualunque meccanismo di risposta automatica ha il potenziale difetto di poter essere bypassato e/o sfruttato contro il sistema stesso che viene protetto

- Le risposte automatiche non sostituiscono l'intervento e l'analisi dell'operatore umano: un apparente risparmio di risorse può risultare in un aggravio di costi
- L'intrusion detection è per sua natura un'attività che necessariamente richiede una forte componente di analisi e di gestione manuale da parte di operatori specializzati (per questo è spesso esternalizzato).



Spesso l'elusione del rilevamento è possibile sfruttando l'uso di alias o altri trucchi che aggirano l'identificazione di una risorsa o di un attacco

Esempio: Una regola che cerchi di verificare la condizione `content:/etc/passwd`; potrebbe essere bypassata da formati equivalenti quali `/etc//\//passwd` oppure `/etc/rc.d/././.\passwd`.

Occorre cercare di riportare la regola all'esame di nomi canonici.



Tecniche di evasione più sofisticate utilizzano pacchetti frammentati per la loro difficoltà di gestione.

Per esempio, si supponga che il NIDS abbia un time-out per riassemblare i pacchetti frammentati inferiore rispetto al sistema vittima. Il NIDS considererebbe due frammenti come pacchetti indipendenti, il sistema destinatario come pacchetto unico.



Un famoso (e controverso) rapporto di Gartner Group del 2003 afferma che gli IDS non valgono gli investimenti richiesti, perché:

- Troppi falsi positivi e negativi
- Richiedono staff dedicato al monitoraggio che dev'essere compiuto 24×7
- Il processo di risposta agli incidenti è molto oneroso
- Non si riescono a monitorare reti con traffico superiore ai 600MB/s senza inaccettabili decadimenti prestazionali

Per questo motivo commercialmente si è passati al termine IPS (intrusion protection s.), suggerendo così di avere a che fare con strumenti più sofisticati. . .