



Sicurezza dei sistemi e delle reti¹

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Lezione XII: Risposta



- 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**

Risposta di un NIDS



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

```
[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.



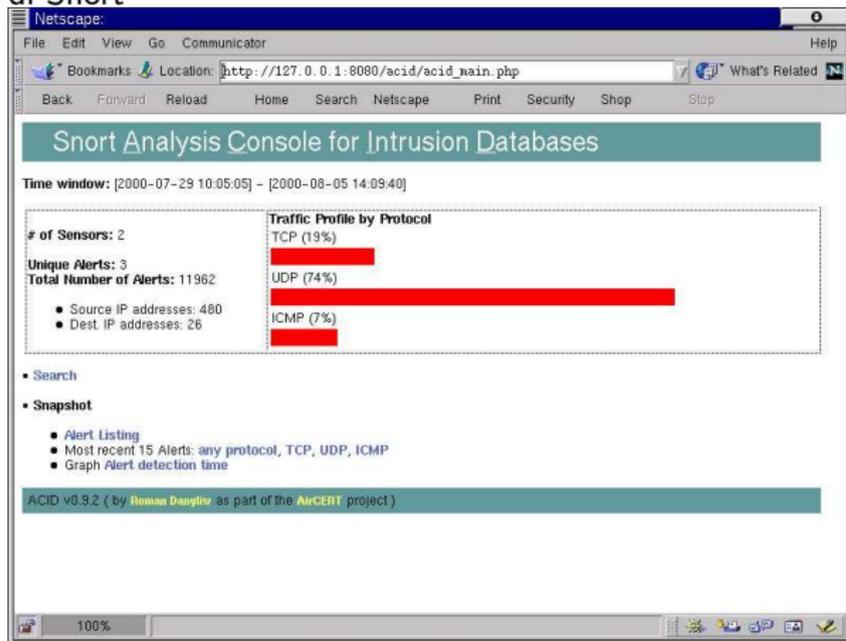
La mole di dati è imponente.

- 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).



ACID (Analysis Console for Intrusion Databases)

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



Sicurezza delle reti

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione



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

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione

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 search bar with a query: 'WHERE: sancp.start_time = 2004-11-29 AND (sancp.src_ip = INET_AION('10.200.211.32') OR sancp.dst_ip = INET_AI)'. A table of network events follows, with columns for Sensor, Sncp ID, Start Time, End Time, Src IP, SPort, Dst IP, DPort, Pr, S, Pkts, and S Bytes. One event is highlighted in blue. Below the table, a detailed view of the selected event is shown, including source and destination IP addresses, a reverse DNS lookup, and a summary of flags. The flags summary shows 'UAPRSF' and 'RRRCSSYI' for both source and destination. A note explains that the summary is data across a session and that a flag in the summary does not necessarily mean it was seen in a single packet. At the bottom, there are tabs for 'System Messages' and 'User Messages', with the latter showing connection status logs.

Sensor	Sncp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S	Pkts	S Bytes
orr	4734589612964100650	2004-12-06 18:25:47	2004-12-06 18:25:47	10.200.211.32	56091	10.200.211.99	111	17	1	64	
orr	4734589612964103123	2004-12-06 18:25:47	2004-12-06 18:25:48	10.200.211.32	86425	10.200.211.99	1023	6	5	94	
orr	473458961333098264	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	951	10.200.211.99	111	17	1	64	
orr	473458961333098882	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	767	10.200.211.99	2048	17	1	98	
orr	473458961333098813	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	781	10.200.211.99	111	17	1	64	
orr	473458961333098817	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	628	10.200.211.99	1022	17	1	108	
orr	47345896133301706176	2004-12-06 18:25:52	2004-12-06 18:25:52	10.200.211.32	786	10.200.211.99	2048	17	1	108	
orr	47345811648936652740	2004-12-06 18:34:01	2004-12-06 18:34:01	10.200.211.32	62578	66.93.110.10	80	2	1	0	
orr	47345811764642810456	2004-12-06 18:34:08	2004-12-06 18:34:08	10.200.211.32	43381	192.168.0.3	3128	6	5	417	
orr	473458117646431402186	2004-12-06 18:34:08	2004-12-06 18:34:08	10.200.211.32	56427	192.168.0.3	3128	6	8	435	
orr	47345811769931435985	2004-12-06 18:34:08	2004-12-06 18:34:10	10.200.211.32	62188	192.168.0.3	3128	6	17	1501	
orr	4734581176993154721	2004-12-06 18:34:08	2004-12-06 18:34:09	10.200.211.32	62857	192.168.0.3	3128	6	10	824	
orr	47345811769931670338	2004-12-06 18:34:08	2004-12-06 18:34:09	10.200.211.32	65042	192.168.0.3	3128	6	5	438	

Display Sncp Details

Src IP: 10.200.211.32
Src Name: Unknown
Dst IP: 66.93.110.10
Dst Name: www.taosecurity.com

Reverse DNS: hois Quer: None Src IP Dst IP

Speakeasy Network SPEAKEASY-S (NET-66-92-0-0-1)
66.92.0.0 - 66.83.255.255

Identity Vector Solutions SPEK-978294-0 (NET-66-93-11-0-0-1)
66.83.110.0 - 66.93.110.31

System Messages | User Messages

connected
[2004-12-06 18:33:00] sguild: ***** Sensor Agent
Status: *****
[2004-12-06 18:33:00] sguild: test
[2004-12-06 18:33:00] sguild: orr
connected



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 11:58:55 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	Summary
N/A	(snort_decoder): Truncated Top Options	3	1	1	Summary
N/A	(portscan) ICMP Sweep	3	1	2	Summary
N/A	(portscan) TCP Decoy Portscan	4	4	1	Summary
N/A	(portscan) UDP Distributed Portscan	9	8	1	Summary
N/A	(portscan) UDP Portscan	16	6	1	Summary
N/A	(portscan) TCP Distributed Portscan	17	17	1	Summary
N/A	(http_Inspect) IIS UNICODE CODEPOINT ENCODING	39	2	13	Summary

Sicurezza delle reti

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione

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/Norht 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 2:36:30 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

Risposta NIDS

Risposte automatiche

Tecniche di evasione



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



Le tecniche piú diffuse sono:

- Reset di sessioni (Session Sniping)
 - L'esempio precedente con Snort è di questo tipo
- Aggiornamento del firewall



Per lo sniping, il NIDS deve essere in grado di forzare la terminazione della connessione

- inviando un pacchetto contenente un RST a entrambi
- devono apparire ai riceventi come inviati dalle controparti



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)



Cosa fare delle segnalazioni dell'IDS

- usare tool di analisi
- interrompere connessioni
- riconfigurare, piú o meno automaticamente, le regole dei firewall



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 piú sofisticate utilizzano pacchetti frammentati per la loro difficoltà di gestione.

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

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).



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

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

- Le risposte automatiche hanno costi organizzativi e possono risultare strumenti di evasione o attacco
- Il processo di risposta agli incidenti è molto oneroso e richiede staff esperto