



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Sicurezza delle reti¹

Mattia Monga

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

a.a. 2012/13

¹ © 2011–13 M. Monga. Creative Commons Attribution-Condividi allo stesso modo 3.0 Italia License.
<http://creativecommons.org/licenses/by-sa/3.0/it/>. Derivato con permesso da © 2010 M. Cremonini.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Lezione XI: Risposta



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

- 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

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

```
[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

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

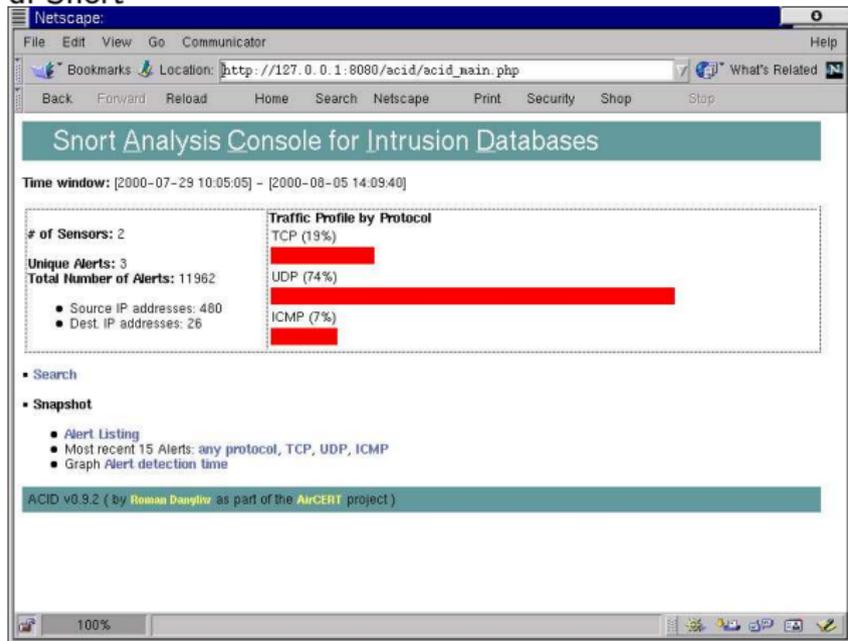
La mole di dati è imponente.

- 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

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa



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

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa

The screenshot shows the SGUIL web interface. At the top, it displays 'SGUIL-5.3 - Connected To localhost' and '2004-12-06 18:40:26 GMT'. Below this is a navigation bar with 'RealTime Events', 'Escalated Events', 'Event Query 1', and 'Snarp Query 1'. A table of events is shown with columns for Sensor, Snarp 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, there are sections for 'Display Snarp Details' with 'Src IP: 10.200.211.32', 'Src Name: Unknown', 'Dst IP: 66.93.116.10', and 'Dst Name: www.taosecurity.com'. There are also 'Reverse DNS' and 'Speakeasy Network' sections. At the bottom, there are 'System Messages' and 'User Messages' sections.

Sensor	Snarp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S	Pkts	S Bytes
orr	4734588612864100650	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	4734588612864103123	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	4734588613330508264	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	4734588613330508882	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	4734588613330508813	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	4734588613330508817	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	4734588613330510616	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	52745911648936652240	2004-12-06 18:33:41	2004-12-06 18:33:41	10.200.211.32	65278	66.93.116.10	80	2	0	0	
orr	47345911769642810456	2004-12-06 18:34:08	2004-12-06 18:34:08	10.200.211.32	43391	192.168.0.3	3128	6	5	417	
orr	47345911769643140186	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	47345911769931433885	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	4734591176993254721	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	4734591176993767038	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 Snarp Details

Src IP: 10.200.211.32
Src Name: Unknown
Dst IP: 66.93.116.10
Dst Name: www.taosecurity.com

Reverse DNS: hois Quer: None Src IP: Dst IP

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

Identify Vector Solutions SPEAK-3/RE294-0 (NET-66-93-11-0-0-1)
66.93.110.0 - 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



Tool di analisi

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 51	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

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa



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

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa



Sicurezza delle
reti

Monga

Risposta NIDS

**Risposte
automatiche**

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Le tecniche piú diffuse sono:

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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)



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Cosa fare delle segnalazioni dell'IDS

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

- 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).



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

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



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

- 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. . .



- 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

Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

I NIDS signature-based si basano sull'assunzione di **saper caratterizzare un attacco**.

- 1 Identificare una **vulnerabilità**: la firma cercherà di rappresentare tutti gli attacchi capaci di sollecitarla;
- 2 Riconoscere un **exploit**: la firma cercherà di rappresentare tutte le varianti.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Zero day

Un attacco può essere del tutto inatteso: in questo caso si parla di **zero-day**, ossia il giorno *prima* di quando i NIDS sono in grado di riconoscerlo.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Il tempo che intercorre fra il momento in cui un attaccante si rende conto di una vulnerabilità e capisce come sfruttarla e il momento in cui l'attacco è identificato dal difensore può essere molto lungo (*vulnerability window*).

Nel 2008 Microsoft ha reso nota una vulnerabilità di IE presente dal 2001, quindi con una finestra potenzialmente di 7 anni!



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

La ricerca delle vulnerabilità non note è una delle attività dei “laboratori di sicurezza” .

- Si cercano vulnerabilità generiche (non di una rete specifica): si analizzano applicazioni e protocolli
- Gli *zero-day* hanno un mercato (non solo underground!)



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

studio analitico si studiano le specifiche più o meno formali di applicazioni e protocolli

fuzzing si provano le applicazioni (o i protocolli) con input “strani” casuali

honeypot un sistema che viene realizzato e messo in opera solo come bersaglio



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

La medesima vulnerabilità può essere sfruttata da exploit con forme diverse: gli attacchi hanno quindi natura **polimorfica**.

In generale è impossibile prevedere tutte le possibili varianti e costruire le firme che permettano di rilevarli.

Una forma completamente nuova è analoga a uno zero-day, anche se la vulnerabilità è già nota.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Una delle tecniche piú diffuse è la **cifratura**.

- Viene generata per ogni attacco una chiave casuale
- il *payload* dell'attacco viene cifrato, appearing così sempre diverso
- l'unica parte di codice costante è una piccola routine di decifratura (possono bastare 3-4 istruzioni: p.es. cifratura XOR)
- anche la routine di decifratura può essere variata con ulteriori tecniche di polimorfismo

dead-code insertion o trash insertion:
aggiungere codice senza modificare il comportamento.

- La tecnica piú semplice è inserire `nop`
- Metodi piú sofisticati fanno uso di sequenze di codice che si annullano vicendevolmente

La ricerca di stringhe costanti fallisce.

```
call 0h
pop ebx
lea ecx, [ebx + 45h]
nop
nop
push ecx
push eax
inc eax
push eax
dec [esp - 0h]
dec eax
sidt [esp - 02h]
pop ebx
add ebx, 1Ch
cli
mov ebp, [ebx]
```



Code transposition

Sicurezza delle
reti

Monga

Sposta le istruzioni in modo che l'ordine del codice binario sia differente dall'ordine di esecuzione

- riordinando casualmente blocchi di istruzioni e inserendo salti incondizionati (facile da fare automaticamente)
- mischiando istruzioni indipendenti (richiede analisi sofisticate del codice)

```
call 0h
pop ebx
jmp Step2
Step3: push eax
push eax
sidt [esp - 02h]
jmp Step4
add ebx, 1Ch
jmp Step6
Step2: lea ecx, [ebx + 45h]
push ecx
jmp Step3
Step4: pop ebx
cli
jmp Step5
Step5: mov ebp, [ebx]
```

osta NIDS

oste

matiche

iche di

ione

Day

morfismo

i attacchi

iche di

morfismo

eratori di

ature

sa

Instruction substitution e register reassignment



Sicurezza delle
reti

Monga

Risposta NIDS

- **instruction substitution**: dizionari di sequenze di istruzioni equivalenti, che possono essere sostituite tra loro.
- **register reassignment** sostituisce l'uso di un registro con un altro equivalente.

```
call 0h
pop ebx
lea ecx, [ebx + 42h]
sub esp, 03h
sidt [esp - 02h]
add [esp], 1Ch
mov ebx, [esp]
inc esp
cli
mov ebp, [ebx]
```



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Gli IDS misuse-based necessitano di *firme* degli attacchi:

- A volte non sono ancora note
- È difficile prevedere le varianti introdotte con tecniche di polimorfismo



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

L'idea di base è che grazie alla conoscenza di vulnerabilità e di un certo numero di exploit, si vogliono **generare automaticamente** signature utili a bloccare exploit non ancora rilevati "in the wild".



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

semantic-based modellano il **comportamento** di un attacco: se la rilevazione richiede l'interpretazione del modello, può essere molto dispendiosa.

content-based si basano sulla ricerca di **invarianti**: in realtà è piuttosto raro che la parte invariante di un exploit sia sufficientemente ricca per limitare i falsi positivi.



- Zhichun Li, Manan Sanghi, Yan Chen, Ming-Yang Kao and Brian Chavez. Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience. IEEE Symposium on Security and Privacy, Oakland, CA, maggio 2006.
- Utilizzabile a livello di rete (gateway e router)
- *content-based*:
 - invarianti byte il cui valore è fissato a priori e la cui variazione implica il fallimento dell'attacco
 - code byte parte potenzialmente polimorfica, ma con una semantica fissa
 - wildcard byte possono assumere qualsiasi valore

Esempio: Lion worm



Sicurezza delle reti

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione

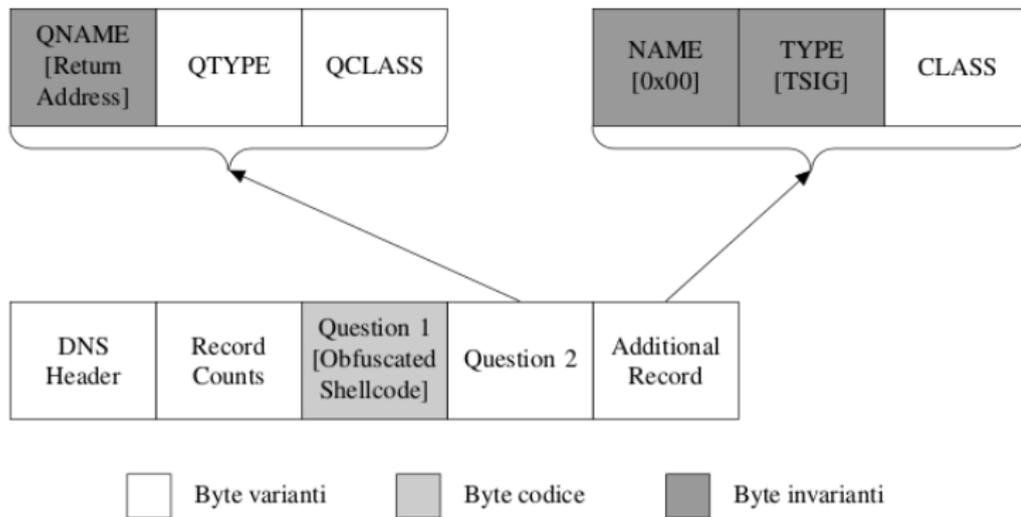
Zero Day

Polimorfismo degli attacchi

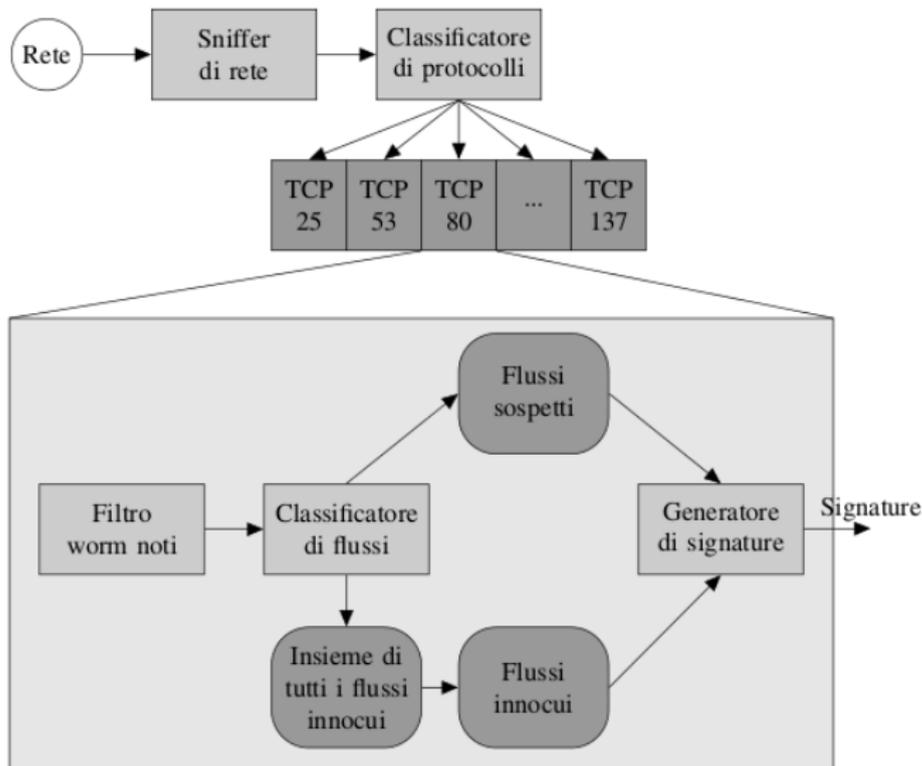
Tecniche di polimorfismo

Generatori di signature

Hamsa



Architettura di Hamsa



Sicurezza delle reti

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

classificatore di protocolli considera i flusso TCP (o i pacchetti UDP) e li classifica secondo la porta destinazione

politica di selezione indica quali flussi prelevare e inviare al generatore di signature

generatore di signature genera le signature, considerando i flussi innocui e sospetti



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

- Sono dette **conjunction signature**: consiste in un insieme di stringhe e un flusso viene considerato malevolo se contiene tutte le stringhe, indipendentemente dall'ordine.
- Si tratta in realtà di *multi-insiemi* di token, cioè insiemi in cui un elemento può apparire più volte.



Code-Red II	{'.ida?':1, '%u780':1, ' HTTP/1.0\r\n':1,'GET /':1, '%u':2}
ATPhttpd	{'\x9e\xf8':1, ' HTTP/1.1\r\n':1, 'GET /': 1}

I token indicati devono comparire in un unico flusso e con un numero di occorrenze maggiore o uguale a quello indicato.

Algoritmo di generazione delle firme



Input: Insieme degli invarianti I, insieme dei flussi malevoli M e dei flussi innocui N, vettore u dei falsi positivi massimi

Output: Signature S per un worm presente in M

```
S = creaSignatureVuota()
SignatureCandidata = S
VettoreSignature = []
i = 1
while i < k do
  foreach t ∈ I do
    S = S.aggiungi(t)
    FP = calcolaFalsiPositivi(S, N)
    if FP < u[i] then
      TP = calcolaVeriPositivi(S, M)
      if SignatureCandidata.TP < TP then
        SignatureCandidata = S
      end
    end
    S = S.rimuovi(t)
  end
end
if SignatureCandidata == creaSignatureVuota() then
  break
end
VettoreSignature.appendi(SignatureCandidata)
S = SignatureCandidata
SignatureCandidata = creaSignatureVuota()
i = i + 1
end
foreach S ∈ VettoreSignature do
  calcolaPunteggio(S)
end
return S con punteggio massimo
```

- k è il numero di token in \mathcal{I}
- $\text{calcolaPunteggio}(S) = -\log_{10}(\delta + FP_S) + a \cdot TP_S + b \cdot \text{lunghezza}(S)$
- tutti i parametri sono scelti in modo empirico (anche per la classificazione innocuo/sospetto)
- $u(i) = u(1) \cdot u_r^{(i-1)}$ con $u(1) = 0,15$ e $u_r = 0,5$

Sicurezza delle reti

Monga

Risposta NIDS

Risposte automatiche

Tecniche di evasione

Zero Day

Polimorfismo degli attacchi

Tecniche di polimorfismo

Generatori di signature

Hamsa



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Target feature manipulation Si cerca di variare le parti considerate invarianti

Innocuous pool poisoning prima di iniziare la diffusione vera e propria e quindi prima di lanciare un attacco verso una nuova macchina, ci si preoccupa di inviare una serie di pacchetti leciti contenenti ciascuno un invariante inserito nelle parti di traffico che possono essere modificate a piacere.

Suspicious pool poisoning l'attaccante incorpora finti invarianti all'interno dei flussi malevoli per portare alla generazione di signature che dipendono da tali finti invarianti al posto o in aggiunta agli invarianti veramente necessari.



Sicurezza delle
reti

Monga

Risposta NIDS

Risposte
automatiche

Tecniche di
evasione

Zero Day

Polimorfismo
degli attacchi

Tecniche di
polimorfismo

Generatori di
signature

Hamsa

Generare automaticamente le varianti di un attacco:

- È un'operazione con fortissime connotazioni empiriche (in generale è un obiettivo irrealizzabile)
- Come sempre, un meccanismo automatico può essere sfruttato anche dall'attaccante (*poisoning*)