Implementing Snort into SURFids

Sander Keemink and Michael van Kleij

February 6, 2008

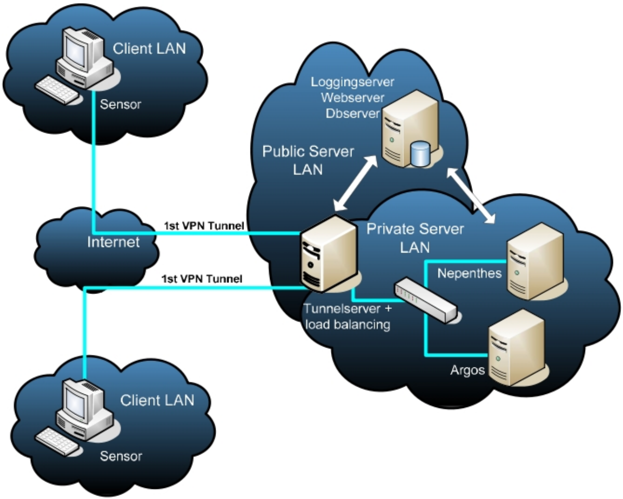
1. SURFids
2. Snort
3. Assignment
4. Experiments and results
5. Integrating Snort
6. Conclusion
7. Future work

IDS

Intrusion Detection System

- Detects unwanted activity
- Host based or Network based

SURFids


Client LAN
Sensor
Loggingserver
Webserver
Dbserver
Public Server
LAN
1st VPN Tunnel
Internet
Private Server
LAN
1st VPN Tunnel
Nepenthes
Tunnelserver +
load balancing
Argos
Client LAN
Sensor

Honeypots

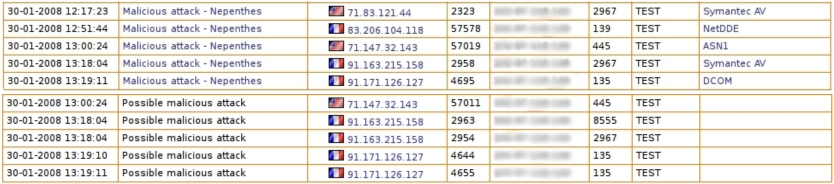
Nepenthes

- Low interaction honeypot
- Simulates known vulnerabilities

Argos

- High interaction honeypot
- Analyses the operating system

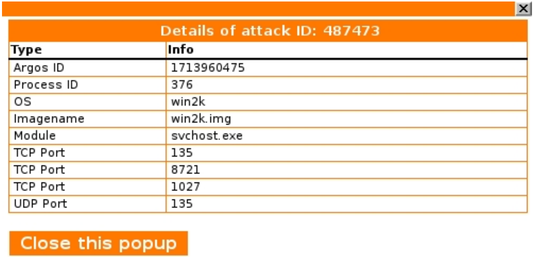
Nepenthes information



30-01-2008 12:17:23	Malicious attack - Nepenthes	🇺🇸 71.83.121.44	2323	[redacted]	2967	TEST	Symantec AV
30-01-2008 12:51:44	Malicious attack - Nepenthes	🇫🇷 83.206.104.118	57578	[redacted]	139	TEST	NetDDE
30-01-2008 13:00:24	Malicious attack - Nepenthes	🇺🇸 71.147.32.143	57019	[redacted]	445	TEST	ASN1
30-01-2008 13:18:04	Malicious attack - Nepenthes	🇫🇷 91.163.215.158	2958	[redacted]	2967	TEST	Symantec AV
30-01-2008 13:19:11	Malicious attack - Nepenthes	🇫🇷 91.171.126.127	4695	[redacted]	135	TEST	DCOM

30-01-2008 13:00:24	Possible malicious attack	🇺🇸 71.147.32.143	57011	[redacted]	445	TEST	
30-01-2008 13:18:04	Possible malicious attack	🇫🇷 91.163.215.158	2963	[redacted]	8555	TEST	
30-01-2008 13:18:04	Possible malicious attack	🇫🇷 91.163.215.158	2954	[redacted]	2967	TEST	
30-01-2008 13:19:10	Possible malicious attack	🇫🇷 91.171.126.127	4644	[redacted]	135	TEST	
30-01-2008 13:19:11	Possible malicious attack	🇫🇷 91.171.126.127	4655	[redacted]	135	TEST	

Argos information



Details of attack ID: 487473	
Type	**Info**
Argos ID	1713960475
Process ID	376
OS	win2k
Imagename	win2k.img
Module	svchost.exe
TCP Port	135
TCP Port	8721
TCP Port	1027
UDP Port	135

Snort

Network Intrusion Detection System

Rule and anomaly based

Assignment

Definition

"Which implementation of Snort into SURFids gives the most added value to the customer while not degrading performance in a noticable way."

Research questions

- Added value of Snort?
- Where to place Snort?
- How can Snort output be integrated?

Performance

SURFids

- 3 Mbits constant
- 30 Mbits max peaks

Snort

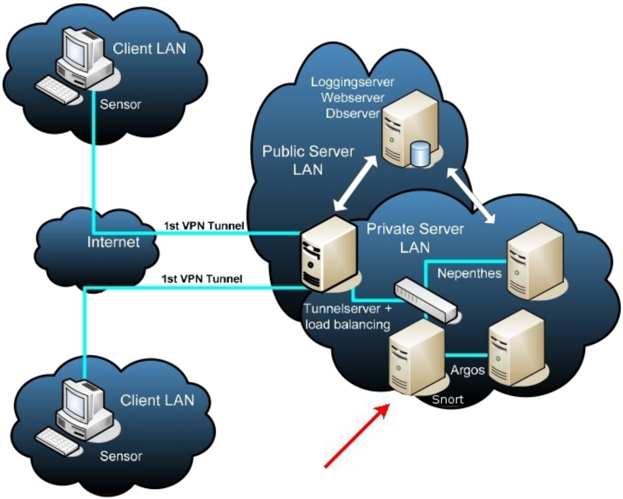
- 125 Mbits without packet loss

Experiments

Experiments

1. Snort before Argos
2. Snort besides Argos and Nepenthes
3. Snort on the tunnel server

Experiment 1

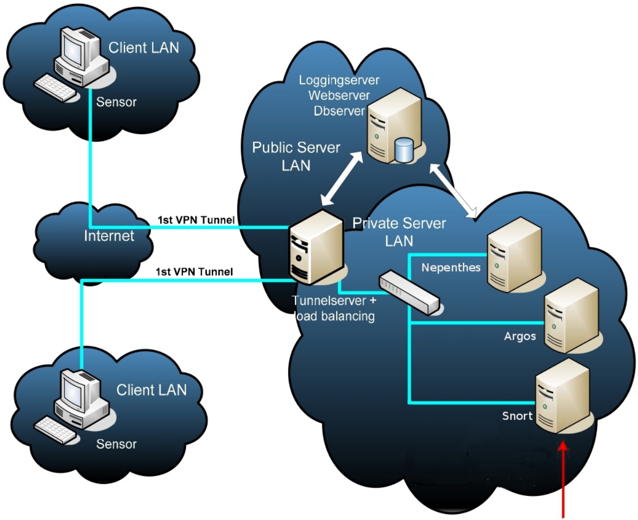


Results experiment 1

Results

- Over 90% of the attacks registered by Argos were detected by Snort
- Other attacks also recognized
- Timeskew, Multiple entries per attack

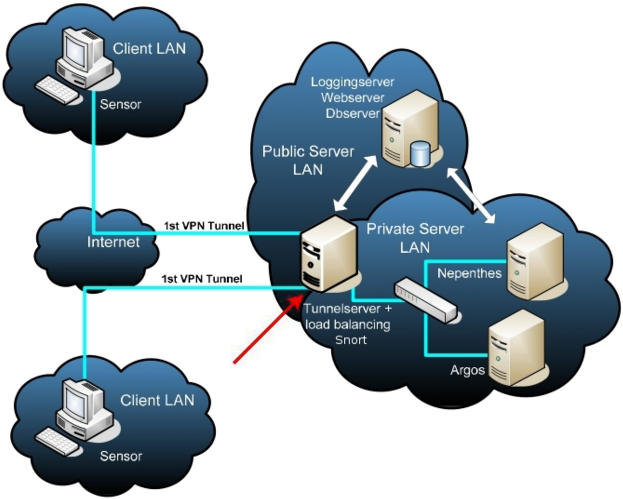
Experiment 2



Results experiment 2

Not conducted due to time and hardware limitations

Experiment 3



Results experiment 3

Over 90% of the attacks registered by Nepenthes were detected by Snort

Identification of 10% of the possible malicious attacks

Integrating Snort

Barnyard, a Snort output processor

- Offloads Snort
- Supports multiple output formats
- Database aware

Integrating Snort

Develop a database output plugin

- Shortest path
- IP packet payload information

Parse Comma Seperated Value output

- Relative easy to develop
- No IP packet payload informatioin

Conclusion

Snort provides added value to SURFids

Nepenthes possible malicious attacks can be discarded

Future work

Develop a program that deals with Snort output