Snort Tuning 101

Nick Moore

Sr. Sales Engineer

Sourcefire

Overview

- Why tune?
- Variables
- Rule Selection
- Brief demo

Why tune?

- You haven't got time for all those alerts
- Real threats hide like a needle in a haystack
- Your sensor will run more efficiently

Upfront Tasks

- Define your goals: inline, alerting, compliance
- Place sensors close to machines you want to protect
- Analyze what's in your network, what should be allowed and what shouldn't be

Wednesday, July 20, 2011

- NMAP or Nessus are good free tools to do this.
- If it's a server VLAN, put it close to the servers. If it's your home network and you want to go inline, put it just inside your firewall.
-

What's in your Network?

- Use nmap - www.insecure.org
- nmap -sF -O <network range>
- For more options, see the nmap man page

Sample nmap output

```
sf-ips-test ~ # nmap -O -sF 172.16.128.137
Starting Nmap 4.20 ( http://insecure.org ) at 2011-07-16 13:51 GMT
Interesting ports on 172.16.128.137:
Not shown: 1694 open|filtered ports
PORT     STATE  SERVICE
139/tcp  closed netbios-ssn
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
MAC Address: 00:0C:29:DD:2F:A1 (VMware)
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2000|2003|XP|Vista (91%)
Aggressive OS guesses: Microsoft Windows 2000  Server SP4 (91%), Microsoft Windows 2000 AS SP4 (91%),
Microsoft Windows 2000 Server SP4 (91%), Microsoft Windows 2000 SP3 (91%), Microsoft Windows 2000 SP4
(91%), Microsoft Windows 2000, SP0, SP1, or SP2 (91%), Microsoft Windows 2003 Server SP1 (91%), Microsoft
Windows Server 2003 Enterprise Edition 64-Bit SP1 (91%), Microsoft Windows XP SP2 (91%), Microsoft Windows
XP SP2 (firewall disabled) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 44.753 seconds
sf-ips-test ~ #
```

Variables

- Most rules use variables in them such as HOME_NET
- Don’t set EXTERNAL_NET to !$HOME_NET
- Define other groupings of hosts or services if you plan to write your own rules and want to customize, e.g. LDAP_SERVERS, PCI_HOSTS....

Wednesday, July 20, 2011

- Changing EXTERNAL_NET to !$HOME_NET can result in missed peer to peer events

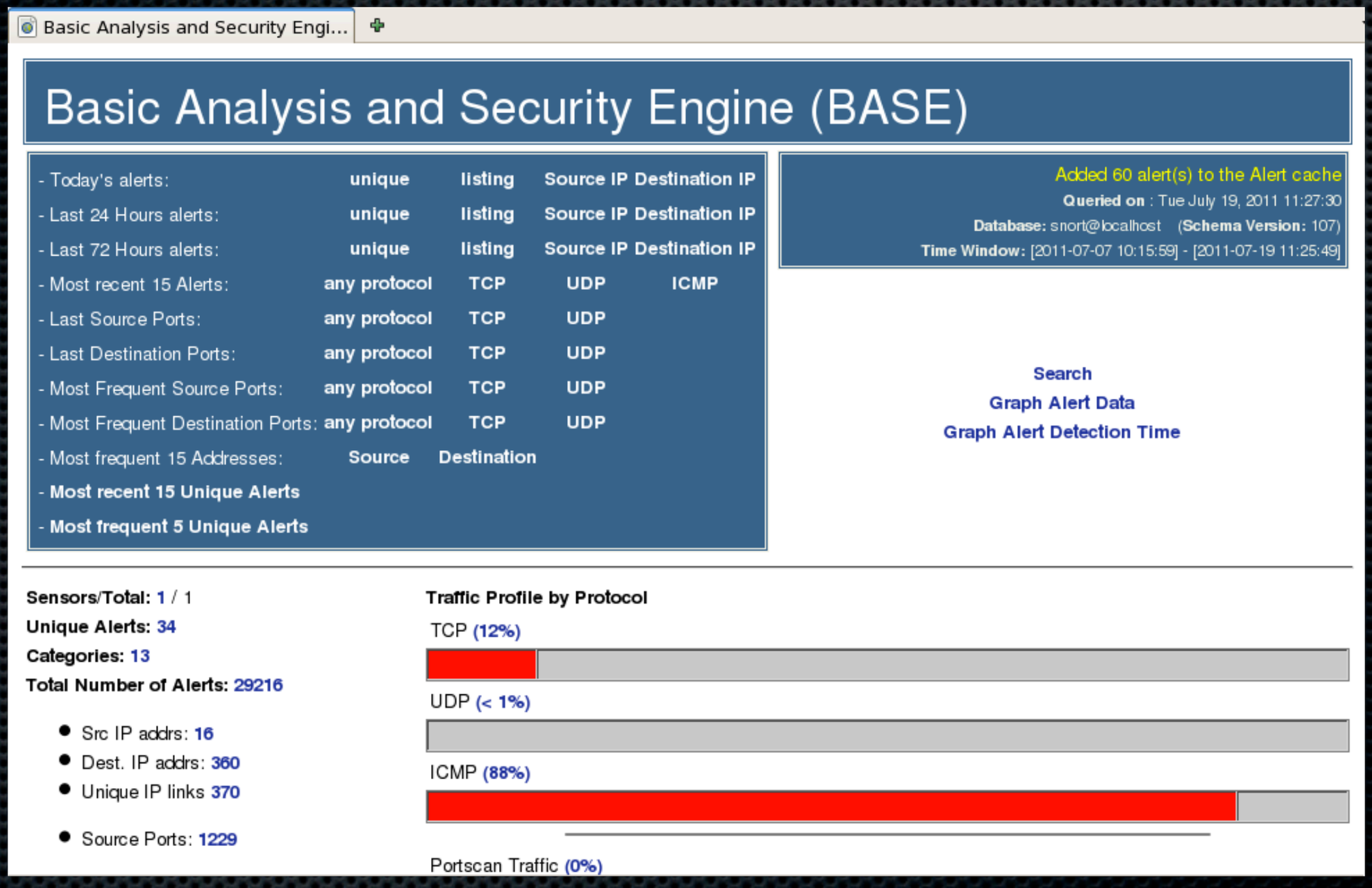
Rule Selection

- Lots of rules available, 19000+, not counting community rules
- Which ones make sense for your environment - by grouping
- What do you do once you have alerts

Wednesday, July 20, 2011

- If you have no Oracle servers, don't turn on the Oracle rules
- Demo the search for dst port 3389 on home_net

Brief Demo


Basic Analysis and Security Engi...
Basic Analysis and Security Engine (BASE)
- Today's alerts: unique listing Source IP Destination IP
- Last 24 Hours alerts: unique listing Source IP Destination IP
- Last 72 Hours alerts: unique listing Source IP Destination IP
- Most recent 15 Alerts: any protocol TCP UDP ICMP
- Last Source Ports: any protocol TCP UDP
- Last Destination Ports: any protocol TCP UDP
- Most Frequent Source Ports: any protocol TCP UDP
- Most Frequent Destination Ports: any protocol TCP UDP
- Most frequent 15 Addresses: Source Destination
- Most recent 15 Unique Alerts
- Most frequent 5 Unique Alerts
Added 60 alert(s) to the Alert cache
Queried on : Tue July 19, 2011 11:27:30
Database: snort@localhost (Schema Version: 107)
Time Window: [2011-07-07 10:15:59] - [2011-07-19 11:25:49]
Search
Graph Alert Data
Graph Alert Detection Time
Sensors/Total: 1 / 1
Unique Alerts: 34
Categories: 13
Total Number of Alerts: 29216
Src IP addrs: 16
Dest. IP addrs: 360
Unique IP links 370
Source Ports: 1229
Traffic Profile by Protocol
TCP (12%)
UDP (< 1%)
ICMP (88%)
Portscan Traffic (0%)

OK, this looks bad, what do I do?

- Don’t Panic
- Start by IP addresses - in my network range?
- Check Ports - are these expected?
- Go to Unique Alerts, look for big hits
- Threshold or suppress

Demo: By IP

- Are these expected?
- On the BASE home page, click Src IP addrs link
- Look for hosts with lots of alerts
- How do these compare to my HOME_NET values?
- Repeat with Dst IP addrs, pairs

Wednesday, July 20, 2011

Starting with 1755 alerts before any modifications to
Example - is the 10 net supposed to be reaching the 192.168.58 network?

Demo: Checking Ports

- Start with Dst port and sort by Occurences
- Look at large numbers first, then small ones
- Triage: are these potentially something bad (needs investigation), probable FP (threshold) or something I can ignore for now?

Wednesday, July 20, 2011

What is going on with 10.29.112.226? Lots of AAs - he may be sick - call desktop support
Is port 9000 a service I need in my network?
The port 80 ones are examples of FPs

Demo: Unique Alerts

- Click on Unique alerts and sort for Occurrences
- The larger numbers usually indicate areas where you can suppress, threshold or disable a rule
- The smaller numbers often need more careful investigation
- Also, do you really care about some of these?

ICMP Ping and Echo Reply are usually great candidates for thresholding

Suppression and Thresholds

- Suppression prevents a host from triggering particular alerts, e.g. a server that responds like an attack:
  supress gen_id 1, sig_id 402, track by_src, ip 172.16.128.1
- Thresholding prevents a rule from generating an alert based on number of times in a given period, e.g. 5 times in one minute:
  event_filter gen_id 1, sig_id 384, type limit, track by_src, count 25, seconds 60

Questions?