# Building Enterprise IDS Using Snort™, Splunk™, SSH and Rsync

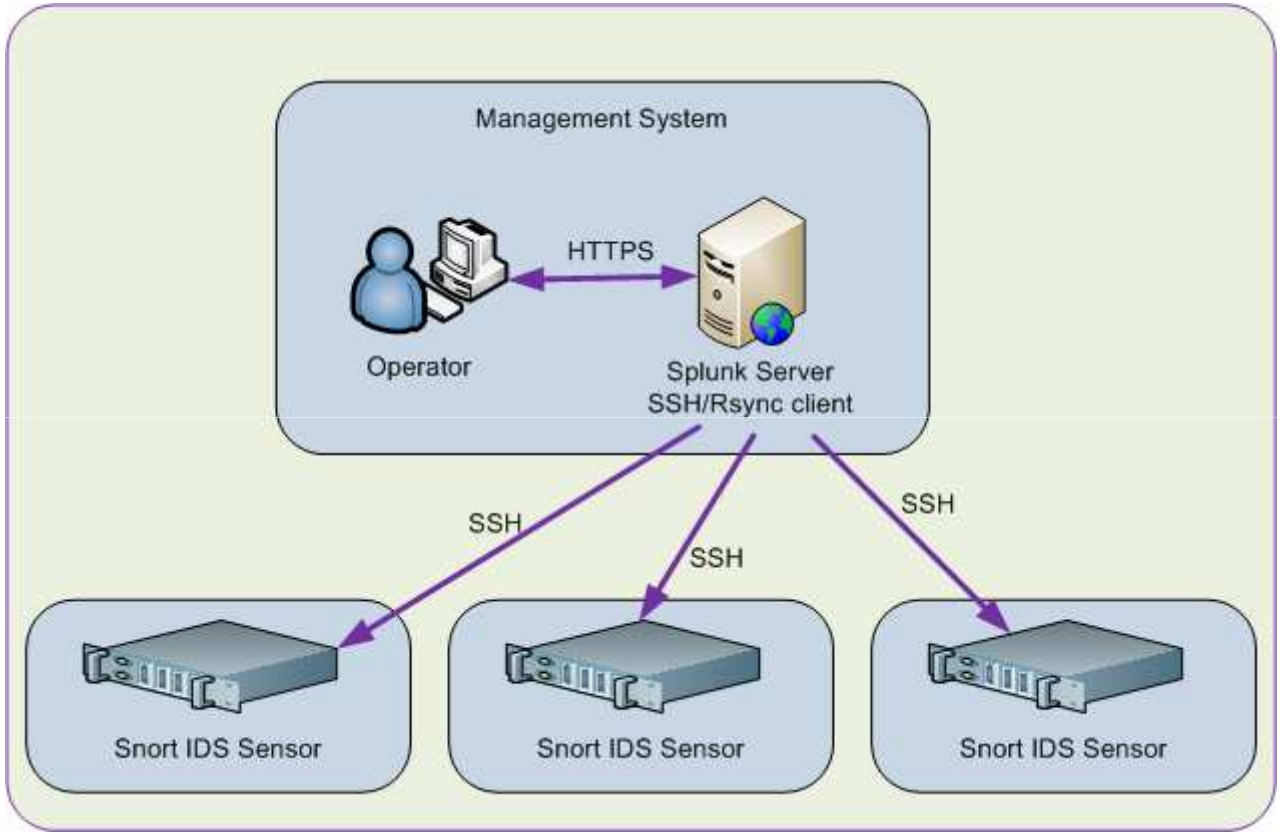
Rafeeq Rehman

www.rafeeqrehman.com

# Presentation Outline

- Introduction to Snort, Splunk, SSH, Rsync
- What is an enterprise IDS solution
- Architecture of an enterprise IDS solution
  - Multiple IDS sensors
  - Management system with options to check status of sensors, restart sensors, push new rule sets, get alert data
  - Graphical user interface to view and analyze data, generate reports and alerts, dashboards for management
- Building enterprise IDS solution
  - Compiling Snort
  - Implementation of rules
  - Building communication channel using SSH and Rsync
  - Installing Splunk and Snort application inside Splunk

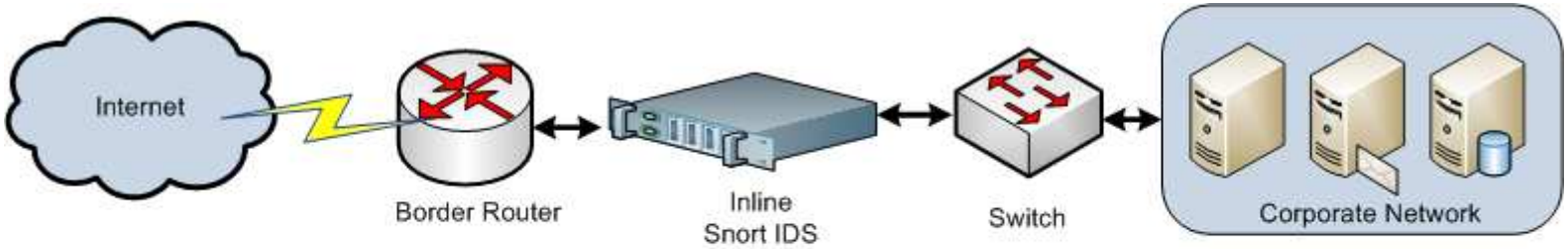
# Enterprise IDS with Multiple Sensors

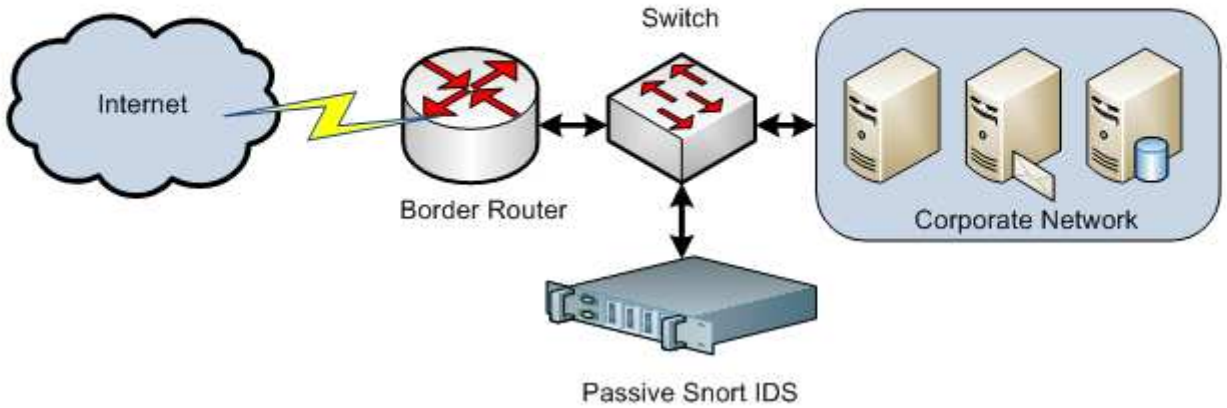


# Introduction to Snort

- Snort is an open source intrusion detection system (www.snort.org)
- It can be implemented on any UNIX/Linux and Windows operating systems
- Basic building blocks of Snort consist of a detection engine, preprocessors, output modules, rules and configuration files
- Snort can be used to monitor common vulnerabilities/exploits, malware, data extrusion, use of insecure protocols, anomalies and so on.
- Snort rules are quite flexible and easy to write
- Pre-compiled binaries are available for most of the platforms
  - Windows
  - Linux
  - HP-UX
  - Solaris

# Typical Snort Implementation - Single Sensor



# Snort Preprocessors

- Preprocessors handle data before it is handed over to detection engine and after packet decoding.
- Major preprocessors include:
  - Frag 3 - IP defragmentation
  - Streams 5 - TCP stream reassembly
  - sfPortscan - Detect reconnaissance
  - RPC Decode
  - Performance Monitor
  - HTTP Inspect - Find and normalize fields
  - SMTP - Find SMTP commands and responses
  - FTP and Telnet Preprocessors - FTP/Telnet commands and responses
  - SSH - Detects SSH protocol exploits
  - DNS - Detects DNS exploits by looking and DNS queries
  - ARP Spoof detection
- You can write your own preprocessors

# Output Modules

- Logging and Alerting
  - You can only log, alert, or both
- Logging and Alerting Mechanisms
  - Storing Snort data in files using Full and Fast alerting
  - Syslog
  - Unix Socket
  - Database
  - CSV
  - TCP dump logging
- You can create your own output modules

# Snort Rule Anatomy

- Snort rules consist of two major parts:
  - Rule Header
  - Rule Options

- A sample rule will be as follows:

  *action protocol src_addr src_port direction dst_addr dst_port Options*

- A real rule looks like this:

  alert tcp any any -> any 21 (msg: "FTP Traffic";)

- The red part is *header* and the green part is *options*

# Compiling From Source Code (Continued)

- You will need to install at least the following libraries and header files:
  - libpcap
  - pcre
  - libnet
  - libdnet
- You may also need to have following tools if you have not already installed. The configure command will show you what you need to install
  - bison
  - flex or lex
- Continue running configure command until you succeed. Each time you will install any missing software needed for compilation.

# Installing and Configuring Snort

- Compile from source code
- Be patient and persistent with missing software components
- You may need to use yum or apt-get or something similar to get the missing libraries on Linux.
- Unpack source code *tar -zxvf snort-2.9.0.4.tar.gz* which will create directory *snort-2.9.0.4*
- Go to directory using command "*cd snort-2.9.0.4*"
- Run configure command: "*./configure --prefix=/opt/snort --enable-normalizer --enable-reload --enable-dynamicplugin --enable-ipv6 --enable-zlib --enable-gre --enable-mpls --enable-targetbased --enable-decoder-preprocessor-rules --enable-ppm --enable-perfprofiling --enable-profile*"
- Use *make* and then *make install* to install it under /opt/snort directory

# Configuring Snort and Installing Rules

- Create/Edit main configuration file snort.conf
- Get latest rules from either snort.org (needs registration) or Emerging threats web site
- Emerging Threats Snort Rules

  http://rules.emergingthreats.net/open-nogpl/snort-2.9.0/
- Create automated startup/shutdown scripts
- Start Snort and test creation of alerts (usually a simple ping will generate some alerts)

# Creating and Sharing SSH Keys

- Generate SSH keys on management server
  - $ ssh-keygen -f ~/.ssh/id_rsa -t rsa
  - Generating public/private rsa key pair.
- Copy public key to snort sensors
  - Public key is placed in ~/.ssh/authorized_keys file
- Test ssh from management server to sensor to ensure you can login without requiring a password (SSH key authentication is working)

# Management Scripts

- Management Scripts
  - eids_checkrulesversion.sh
  - eids_checkstatus.sh
  - eids_getalerts.sh
  - eids_pushrules.sh
  - eids_restart.sh
- Configuration Files
  - eids_rulesversion.conf
  - eids_sensorlist.conf

- Run eids_getalerts through cron to schedule receiving alerts data every 5 minutes (or an interval you like)

# Management System Directory Structure

- The administrative directory

```
/opt/snort/admin
    |-- etc
    |-- logs
    |    `-- 192.168.144.154
    |         `-- snort
    |-- preproc_rules
    |-- rules
    |-- scripts
    |-- so_rules
    `-- temp
```

- Each sensor has a directory under /opt/snort/admin/log directory

# Sensor Directory Structure

- All directories are under /opt/snort directory

```
.
|-- admin
|-- bin
|-- etc
|-- lib
|-- preproc_rules
|-- rules
|-- share
|-- so_rules
`-- src
```

# Splunk Installation

- Download from splunk.com and install using rpm

  rpm -i --prefix=/opt <splunk rpm file>

- Add splunk user and groups

  groupadd splunk

  useradd -g splunk splunk

- Create startup scripts (you will need to accept license)

  /opt/splunk/bin/splunk enable boot-start -user splunk

- Change owner and group permissions of /opt/splunk

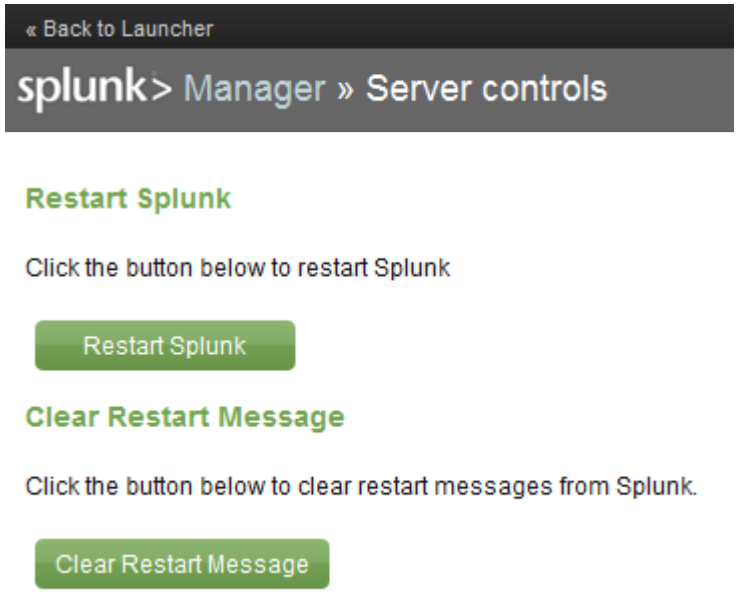
  chown -R splunk.splunk /opt/splunk

- Start splunk for the first time

  /etc/init.d/splunk start --accept-license

# Installing Snort Application

- Go to /opt/splunk/etc/apps folder
- Run tar zxvf <Snort App File Name>
- Restart Splunk by going to Manager->Server controls



# Add Snort Log Files to Splunk

- Add a new data input file

« Back to Launcher

splunk> Manager » Data inputs

## Data Inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

| Type | Inputs | Actions |
|---|---|---|
| **Files & Directories**<br>*Upload a file, index a local file, or monitor an entire directory.* | 5 | Add new |
| **TCP**<br>*Listen on a TCP port for incoming data, e.g. syslog.* | 0 | Add new |
| **UDP**<br>*Listen on a UDP port for incoming data, e.g. syslog.* | 0 | Add new |
| **Scripts**<br>*Run custom scripts to collect or generate more data.* | 0 | Add new |

# Add Snort Logs

« Back to Launcher

splunk> Manager » Data inputs » Files & Directories » /opt/snort/logs

**Host**

Set host field for all events from this source.

Set host

constant value

*Specify method for getting host field for events coming from this source.*

Host field value

localhost.localdomain

**Source type**

Set sourcetype field for all events from this source.

Set sourcetype

Manual

*When this is set to automatic, Splunk classifies and assigns the sourcetype automatically, and gives unknown sourcetypes placeholder names.*

Source type (optional)

snort

**Index**

Set the destination index for this source.

Index

default

**Advanced options**

Whitelist (optional)

*Specify a regex that files from this source must match to be monitored by Splunk.*

Blacklist (optional)

*Specify a regex that files from this source must NOT match to be monitored by Splunk.*

Cancel Save

# Splunk Dashboard

splunk> Launcher

Logged in as admin | App | Manager | Jobs | Logout

Welcome | Your apps (4) | Browse more apps

## Your installed apps

Below you'll find Splunk apps to get the most out of your Splunk experience.

*nix

*NIX

Enable

*This is a useful app for helping monitor, manage, and troubleshoot *nix platforms. This app comes with set of scripted inputs for collecting CPU, disk, I/O, memory, log, configuration, and user info. It also provides convenient dashboards, form searches, and alerts to make getting started with Splunk a breeze.*

### Getting started

Get started with Splunk. This app introduces you to many of Splunk's features. You'll learn how to use Splunk to index data, search and investigate, add knowledge, monitor and alert, report and analyze.

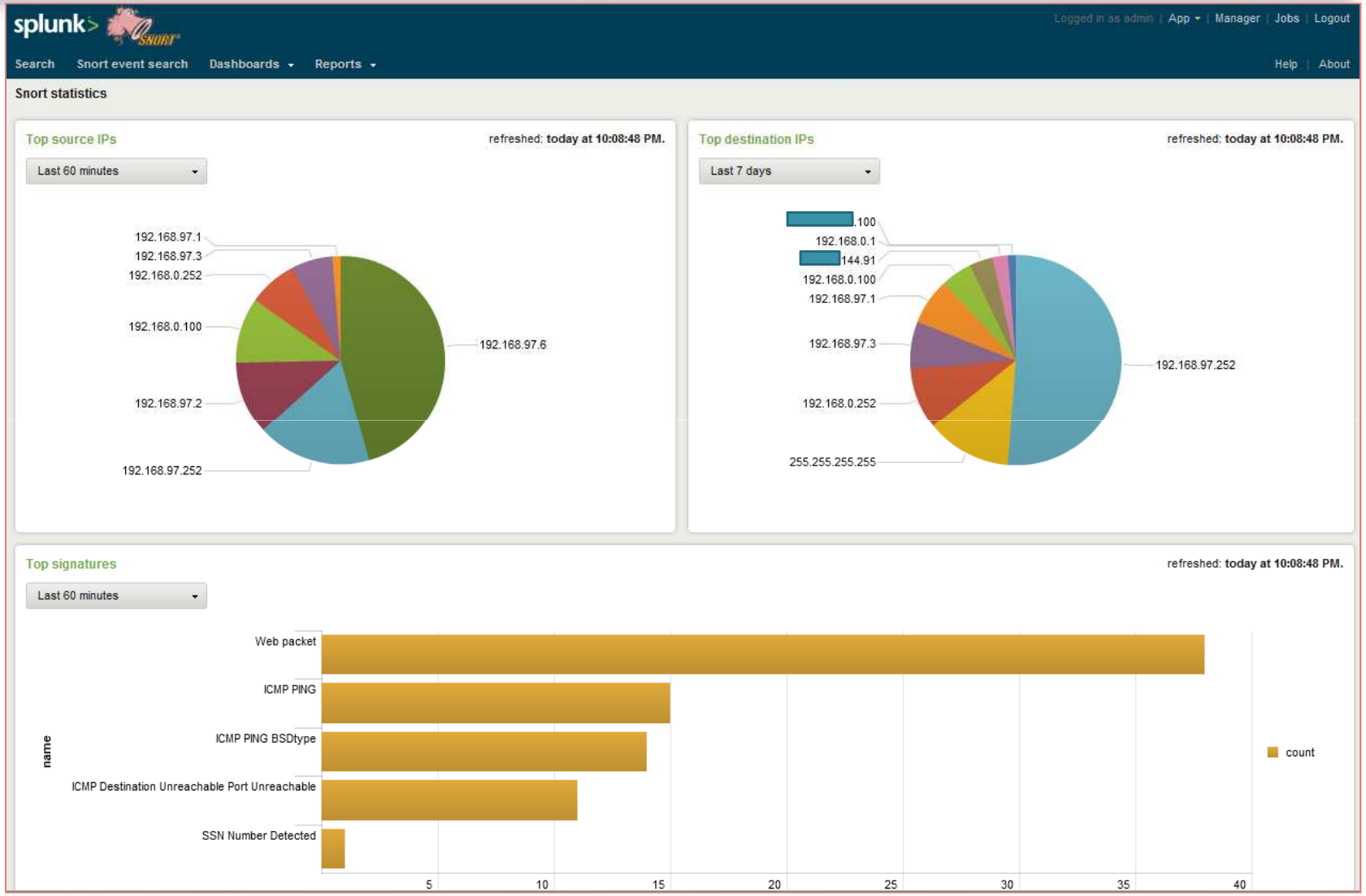
### Search

The Search app is Splunk's default interface for searching and analyzing IT data. It allows you to index data into Splunk, add knowledge, build reports, and create alerts. The Search app can be used across many areas of IT including application management, operations management, security, and compliance.

### Splunk for Snort

Splunk for Snort provides field extractions for Snort alert logs (fast and full) as well as dashboards, saved searches, event types, tags and event search interfaces.

# Snort Dashboard in Splunk



# Splunk Reports

splunk> Snort

Logged in as admin | App | Manager | Jobs | Logout

Search | Snort event search | Dashboards | Reports | Help | About

Search: Top 10 destination IPs | Actions

```
sourcetype="snort" | top dest_ip
```

All time

84 matching events | Save search | Show report

Timeline: zoom in | zoom out | Scale: linear | log

100 / 50

10:00 PM Thu Mar 3 2011 | 10:10 PM | 10:20 PM | 10:30 PM | 10:40 PM | 10:50 PM

52 fields | Pick fields

Selected fields (3)
- host (1)
- source (1)
- sourcetype (1)

Other interesting fields (34)
- Ack (n) (30)
- bytes_in (n) (16)
- dest_ip (9)
- dest_port (n) (13)
- DgmLen (n) (16)
- dgmlen (n) (16)
- eventtype (1)
- generator_id (n) (2)
- id (n) (71)
- ID (n) (71)

9 results over all time

Options... | Results per page 10

Overlay: None

| | dest_ip | count | percent |
|---|---|---|---|
| 1 | 192.168.97.252 | 43 | 51.190476 |
| 2 | 255.255.255.255 | 11 | 13.095238 |
| 3 | 192.168.0.252 | 8 | 9.523810 |
| 4 | 192.168.97.3 | 6 | 7.142857 |
| 5 | 192.168.97.1 | 6 | 7.142857 |
| 6 | 192.168.0.100 | 4 | 4.761905 |
| 7 | [redacted]4.91 | 3 | 3.571429 |
| 8 | 192.168.0.1 | 2 | 2.380952 |
| 9 | [redacted].100 | 1 | 1.190476 |

# Summary

- The whole system consists of the following software components:
  - Linux
  - Snort
  - Splunk
  - Scripts that use SSH and Rsync
- You can monitor and manage as many sensors as you need and as much the system can handle
- Splunk is not totally free and needs licensing. Please see licensing information from Splunk web site (usually up to 50 MB per day can be used - check with Splunk for licensing)
- You need to open only SSH port through firewall.

# Contact Information and Questions

My Blog

www.rafeeqrehman.com

Email

rafeeq.rehman@gmail.com

Configuration Files and Management Scripts Download

http://rafeeqrehman.com/downloads/eids.tgz