Intrusion Detection & SNORT

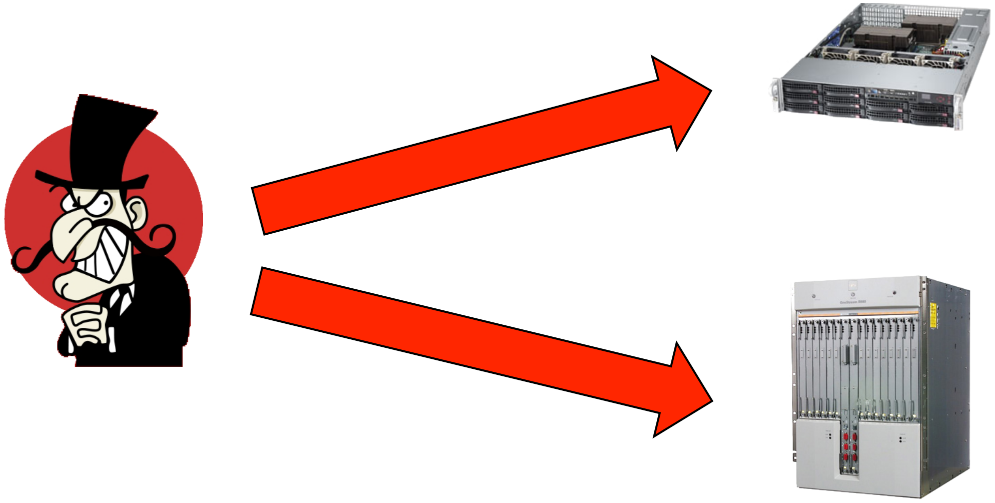
Fakrul Alam
fakrul@bdhub.com

Sometimes, Defenses Fail

- Our defenses aren't perfect
  - Patches weren't applied promptly enough
  - Antivirus signatures not up to date
  - 0-days get through
  - Someone brings in an infected USB drive
  - An insider misbehaves
- Now what?
- Most penetrations are never detected
  - This allows continuing abuse, and helps the attackers spread elsewhere

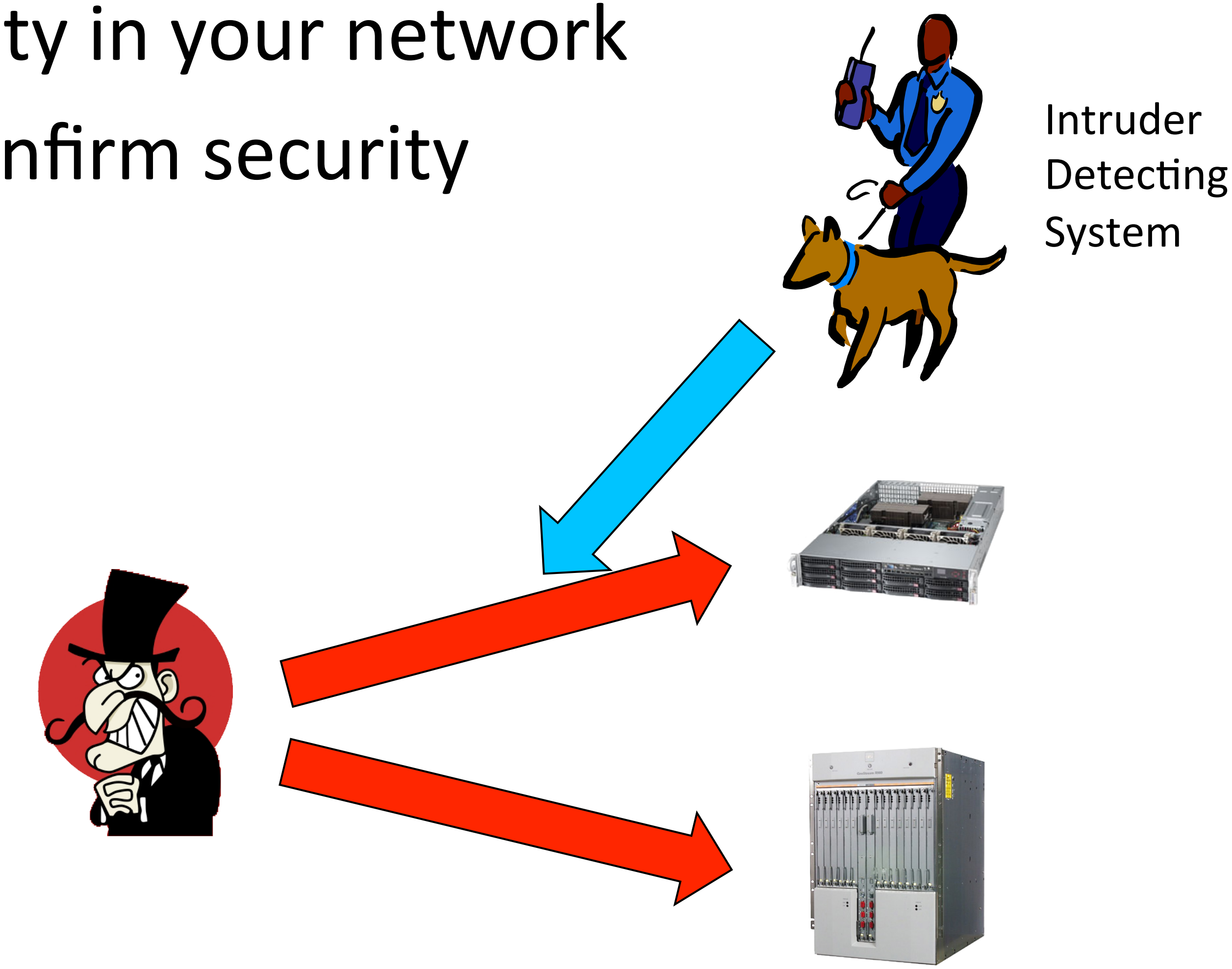
Unexpected Activity

- There could be an intruder even if you have security practice in place



Additional Monitoring

- Activity in your network
- To confirm security



Intruder Detecting System

What can IDS realistically do

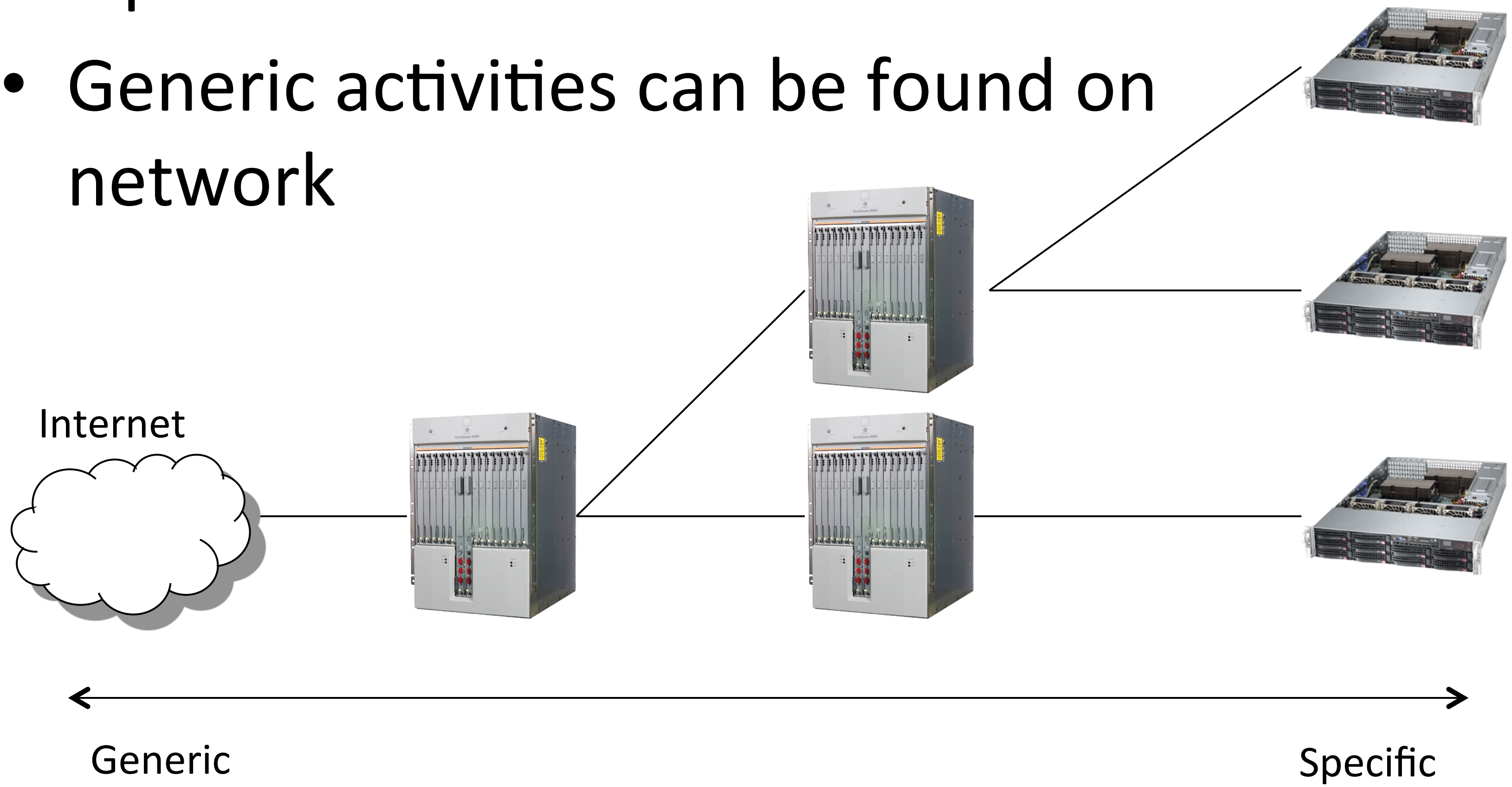
- Detect successful attacks
- Look for various things that shouldn't be there
  - Infected files
  - Attacks on other machines
  - Packets that shouldn't exist
  - Strange patterns of behavior
- Contain attacks before they spread further
- Clean up penetrated machines—because you'll know they're infected
- Recognition of pattern reflecting known attacks
- Statistical analysis for abnormal activites

What IDS can't do

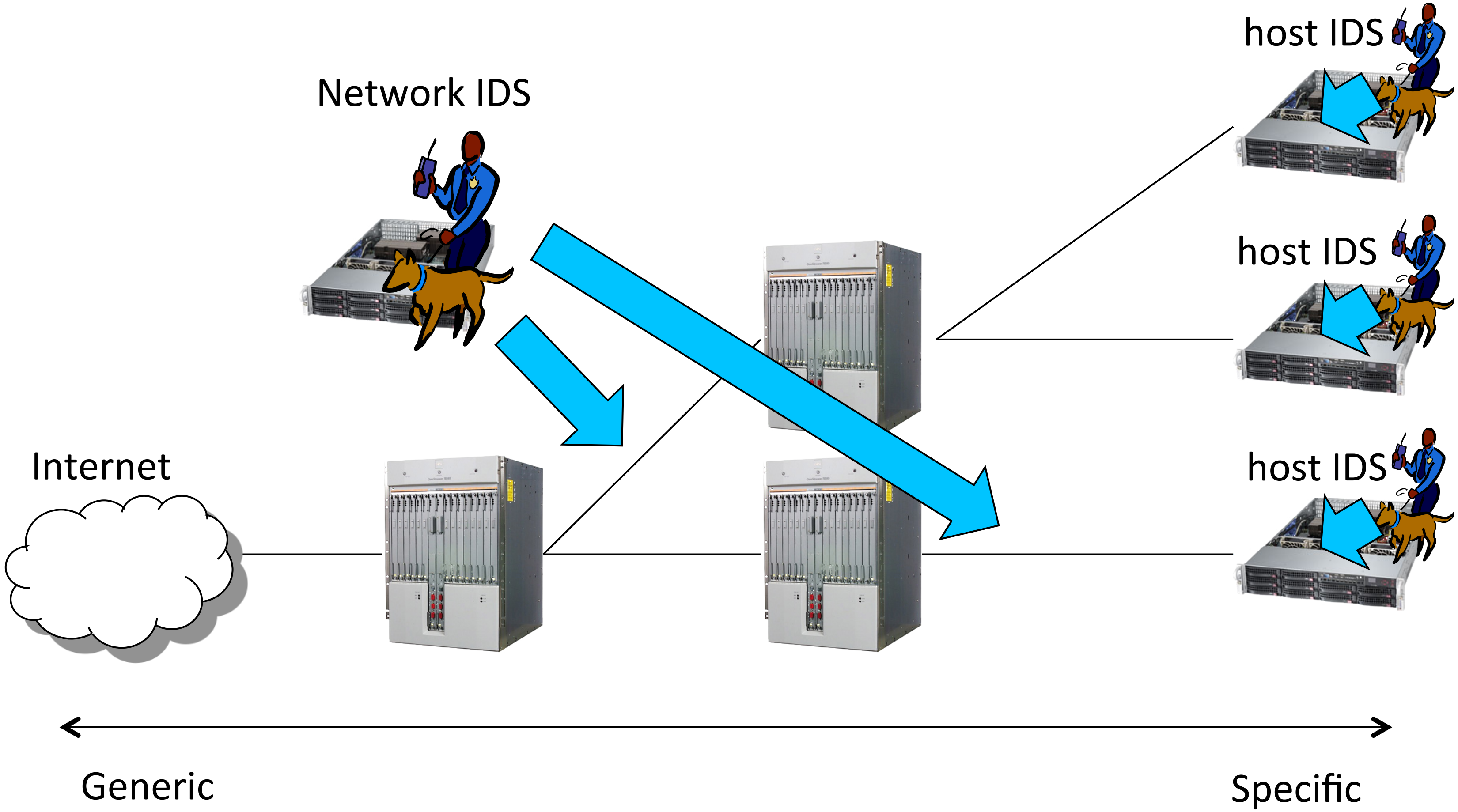
- Compensate for weak authentication & identification mechanisms
- Investigate attacks without human intervention
- Guess the content of your organization security policy
- Compensate for weakness in networking protocols, for example IP Spoofing

Monitoring Point

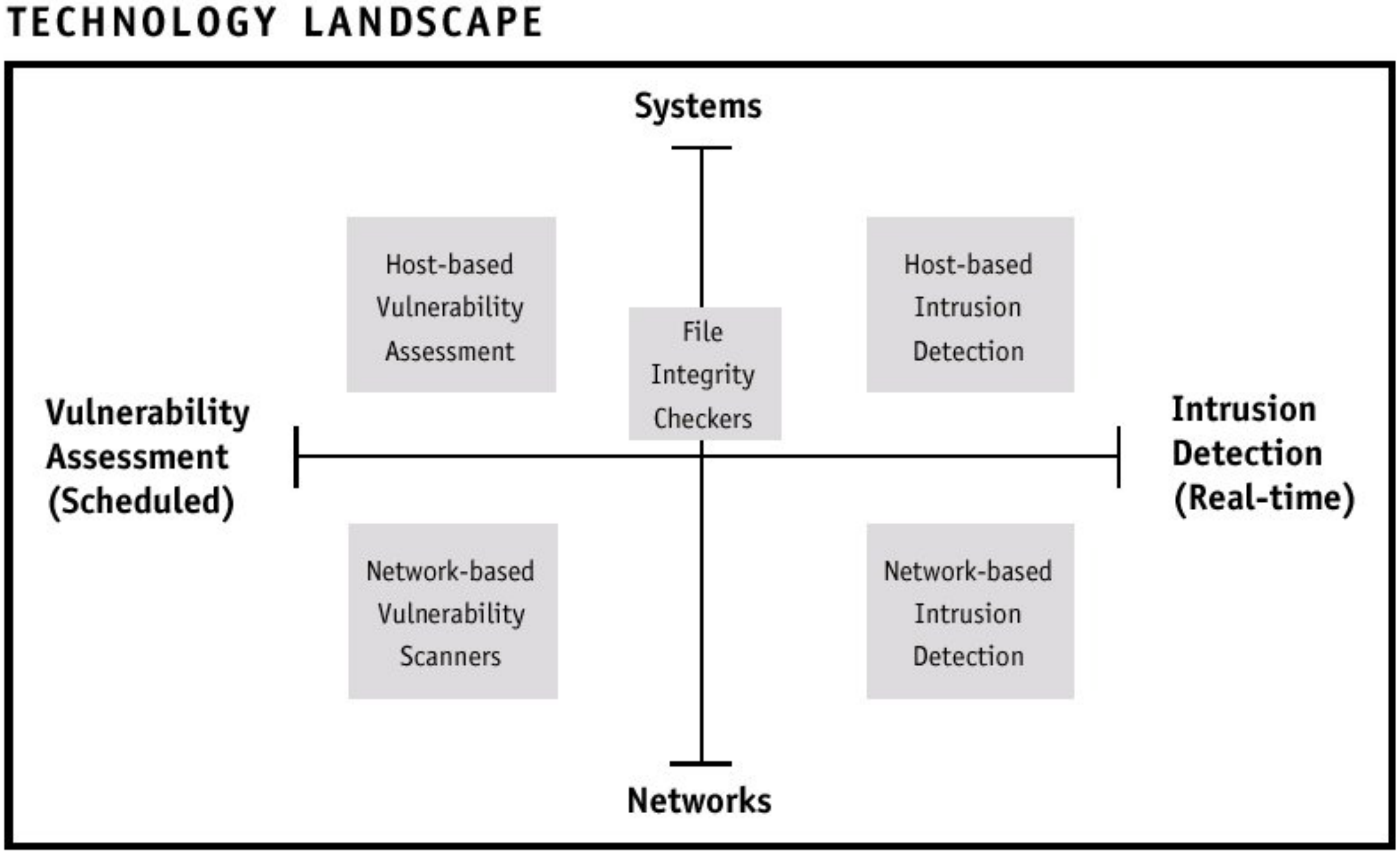
- More specific rules can be applied for a point close to end nodes
- Generic activities can be found on network



Network and Host IDS



IDS Technology landscape


TECHNOLOGY LANDSCAPE
Systems
Host-based Vulnerability Assessment
File Integrity Checkers
Host-based Intrusion Detection
Vulnerability Assessment (Scheduled)
Intrusion Detection (Real-time)
Network-based Vulnerability Scanners
Network-based Intrusion Detection
Networks

Preventive

Real Time

Alert

- You may receive tons of millions of alerts
  - Depending on your detection rules
  - There are many suspicious activities in the Internet today
- You should notice a critical one at least
  - Detection rule is important!

Alert

- False Positive / Type I Error:
  - is the incorrect rejection of a true null hypothesis
  - is when a system raises an incorrect alert
- False Negative / Type II Error:
  - is the failure to reject a false null hypothesis
  - is when an attack pass undetected

Types of Detection

- Signature Based
  - Match patterns against known attacks
  - Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities
- Anomaly Based
  - Look for unusual behavior
  - Detect any action that significantly deviates from the normal behavior

Intrusion Detection for ISPs

- Monitor your own network—but that's no different than any other enterprise
- Monitor your customers
  - Good: you can help them by detecting problems
  - Good: you can prevent them from clogging your infrastructure
  - Bad: it can be privacy-invasive

SNORT

- Snort is an open source IDS, and one of the oldest ones
- Hundreds of thousands of users
- Active development of rules by the community make Snort up to date, and often more so than commercial alternatives
- Snort is fast! It can run at Gbit/s rates with the right hardware and proper tuning

Where to put SNORT?

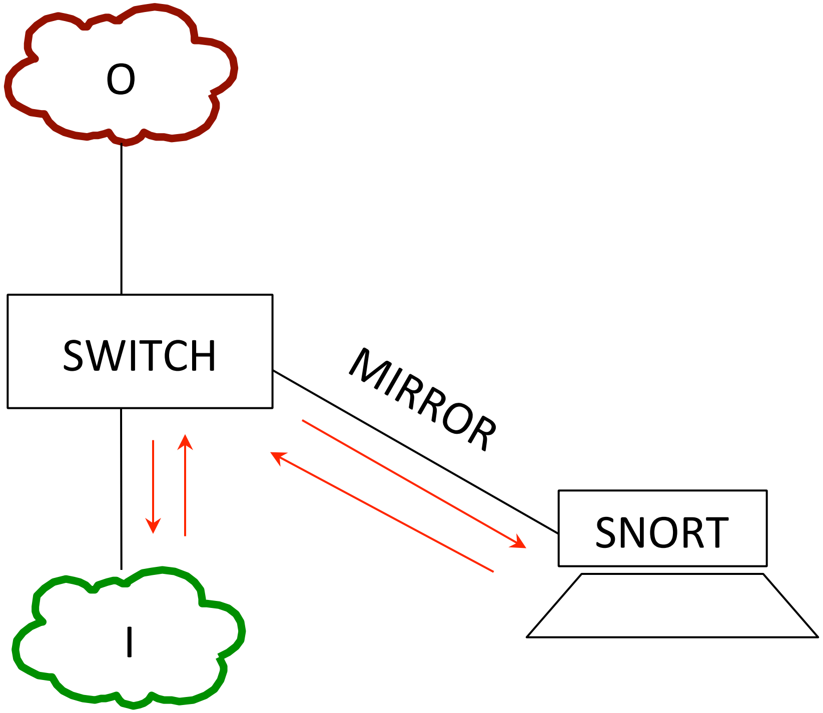
Where to put SNORT?

- Snort will need to be close to the “choke point” (the point where all traffic flows through on the way in or out of your network)
  - Inside of the border router or firewall, for example

Getting Snort to see the network

- You could run Snort in multiple ways
  - As a device “in line” behind or after the firewall/router
    - But this adds one more element that can fail in your connectivity
  - Or you could use a span/mirror port to send traffic to Snort
  - Or you can use an “optical splitter” to “mirror” or “tap into” traffic from a fiber optic link
    - This method and the previous are the most recommended

Getting Snort to see the network



Getting Snort to see the network

- Be careful not to overload your switch port – If you mirror a gigabit port to another gigabit port, the monitoring port (the receiving port) can drop packets if the total traffic exceeds 1 Gbit/s

Monitoring Port…

- On Cisco Catalyst, this is a “SPAN” port
- You can SPAN one port to another, a group of ports to one port, or an entire VLAN to a port
- Sample config:
- interface FastEthernet 0/1
- # port monitor FastEthernet 0/2
- This would copy any packet received on F0/2 to F0/1

Snort configuration file

- By default, /etc/snort/snort.conf
- It’s a long file – 900+ lines
- If you browse it, you will notice many “preprocessor” entries
- Snort has a number of “preprocessors” which will analyze the network traffic and possibly clean it up before passing it to the rules

Snort rules

- Snort rules are plain text files
- Adding new rules to snort is as simple as dropping the files into /etc/snort/rules/
- Groups of rules can be loaded from snort.conf using the “include” statement
- Rules can match anything
- Technical – web attacks, buffer overflow, portscan, etc…
- Policy/user oriented – URL filtering, keyword, forbidden applications, etc…

Tailoring the rules

- Not all rules will make sense in your network
- You will want to customize which rules you want to run
- Otherwise you will get many false positives, which will lead you to ignore Snort, or simply turn it of…
- It doesn’t help to have logs full of junk alerts you don’t want
- To avoid this, rules can be suppressed (disabled)

Updating Snort rules

- The commercially maintained snort rules are available for free with a 30 day delay from http://www.snort.org/start/rules
- Other rules are maintained by some volunteers at emerging threats: http://rules.emergingthreats.net/open/
- The updating of rules can be automated with a tool called “Pulled Pork”, which is located at http://code.google.com/p/pulledpork/

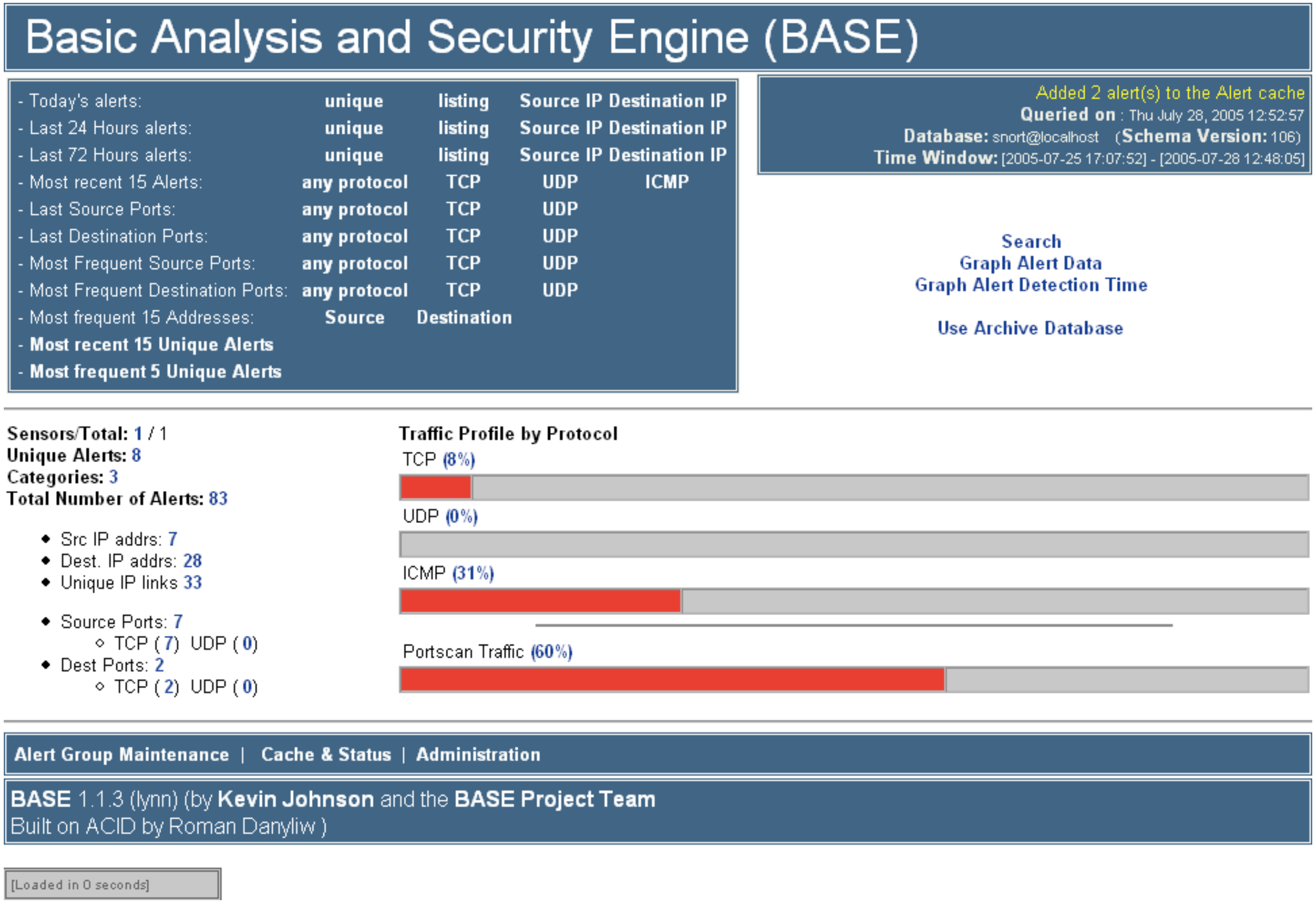
Sample rules

```
# These signatures are not enabled by default as they may generate false
# positive alarms on networks that do mysql development.

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL root login
attempt"; flow:to_server,established; content:"|0A 00 00 01 85 04 00 00 80|
root|00|"; classtype:protocol-command-decode; sid:1775; rev:2;)

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL show
databases attempt"; flow:to_server,established; content:"|0F 00 00 00 03|
show databases"; classtype:protocol-command-decode; sid:1776; rev:2;)

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL 4.0 root
login attempt"; flow:to_server,established; content:"|01|"; within:1;
distance:3; content:"root|00|"; within:5; distance:5; nocase;
classtype:protocol-command-decode; sid:3456; rev:2;)
```

Reporting and logging

- Snort can be made to log alerts to an SQL database, for easier searching
- A web front-end for Snort, BASE, allows one to browse security alerts graphically

BASE (Basic Analysis and Security Engine)



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 2 alert(s) to the Alert cache
Queried on : Thu July 28, 2005 12:52:57
Database: snort@localhost (**Schema Version:** 106)
Time Window: [2005-07-25 17:07:52] - [2005-07-28 12:48:05]

Search
Graph Alert Data
Graph Alert Detection Time

Use Archive Database

Sensors/Total: 1 / 1
Unique Alerts: 8
Categories: 3
Total Number of Alerts: 83

- Src IP addrs: 7
- Dest. IP addrs: 28
- Unique IP links 33

- Source Ports: 7
  - TCP (7) UDP (0)
- Dest Ports: 2
  - TCP (2) UDP (0)

Traffic Profile by Protocol

TCP (8%)

UDP (0%)

ICMP (31%)

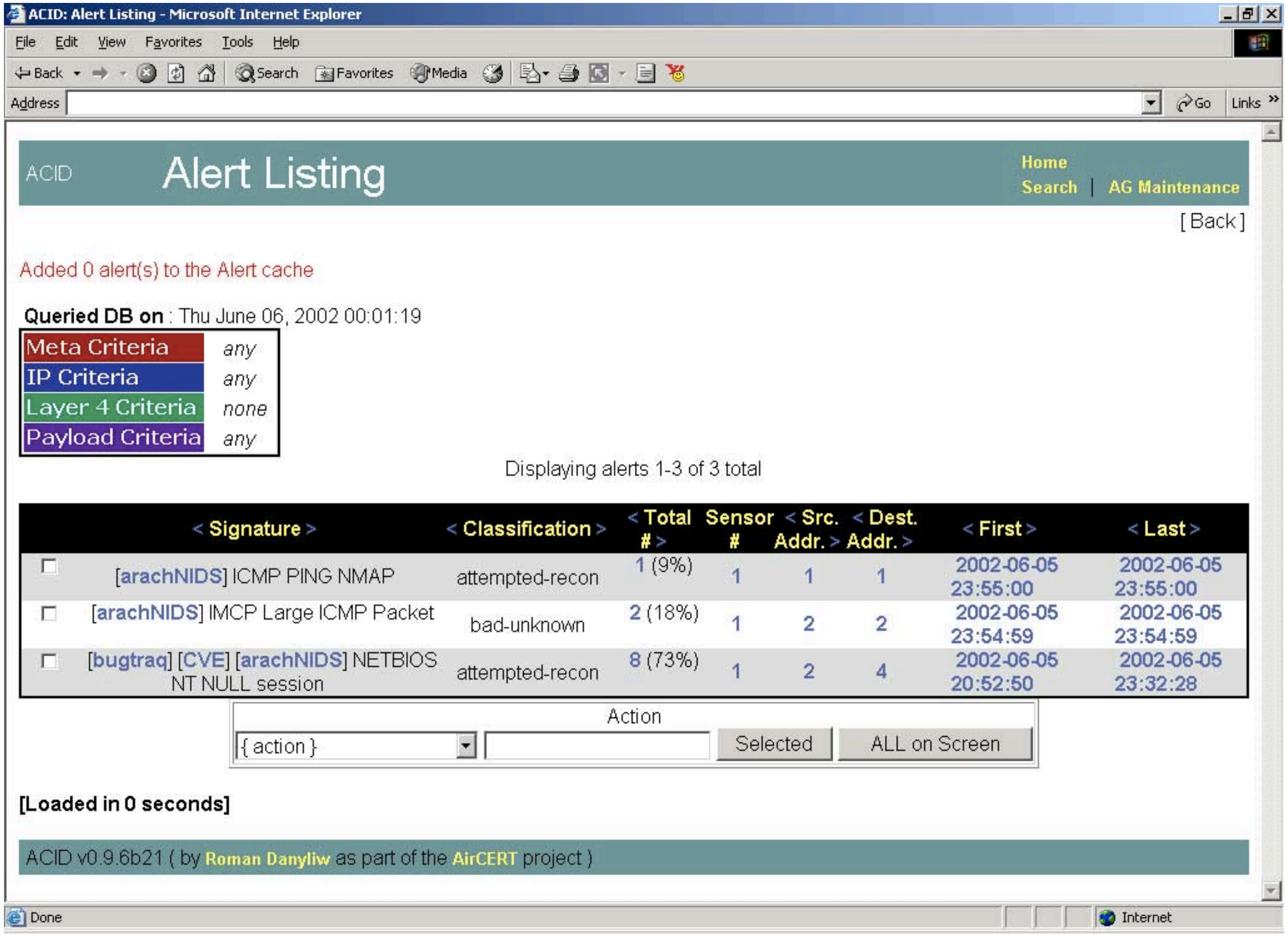
Portscan Traffic (60%)

Alert Group Maintenance | **Cache & Status** | **Administration**

BASE 1.1.3 (lynn) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 0 seconds]

BASE (Basic Analysis and Security Engine)


ACID: Alert Listing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Home
Search | AG Maintenance
[Back]
Done
Internet

ACID **Alert Listing**

Added 0 alert(s) to the Alert cache

Queried DB on : Thu June 06, 2002 00:01:19

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying alerts 1-3 of 3 total

	< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
□	[arachNIDS] ICMP PING NMAP	attempted-recon	1 (9%)	1	1	1	2002-06-05 23:55:00	2002-06-05 23:55:00
□	[arachNIDS] IMCP Large ICMP Packet	bad-unknown	2 (18%)	1	2	2	2002-06-05 23:54:59	2002-06-05 23:54:59
□	[bugtraq] [CVE] [arachNIDS] NETBIOS NT NULL session	attempted-recon	8 (73%)	1	2	4	2002-06-05 20:52:50	2002-06-05 23:32:28

Action

{ action } ▾ [ ] Selected ALL on Screen

[Loaded in 0 seconds]

ACID v0.9.6b21 (by Roman Danyliw as part of the AirCERT project)

References and documentation

- Snort preprocessors:
  - http://www.informit.com/articles/article.aspx?p=101148&seqNum=2
- Snort documentation
  - http://www.snort.org/docs
- An install guide for Ubuntu 10.04:
  - http://www.snort.org/assets/158/014-snortinstallguide292.pdf

DEMO