Defending Computer Networks
Lecture 12: NIDS

Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- HW 2 due Midnight Monday (10/6)

Assigned Reading

- Roesch, M. Snort – *Lightweight Intrusion Detection for Networks*
- http://static.usenix.org/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf

Latest News

NEWS

Xen Project discloses serious vulnerability that impacts virtualized servers

By Lucian Constantin FOLLOW

IDG News Service | Oct 2, 2014 3:00 AM PT

The Xen Project has revealed the details of a serious vulnerability in the Xen hypervisor that could put the security of many virtualized servers at risk.

Xen is a free, open-source hypervisor used to create and run virtual machines. It is widely used by cloud computing providers and virtual private server hosting companies.

The security vulnerability, which is being tracked as CVE-2014-7188 and was privately disclosed to major cloud providers in advance, forced at least Amazon Web Services and Rackspace to reboot some of their customers' virtualized servers over the past week.

FEATURED RESOURCE

DESTINY AND CALL OF DUTY SERVERS TAKEN DOWN BY DDOS ATTACKS

Posted by: Crisan Mircea September 29, 2014 in NEWS, Playstation 4, Xbox One

Tweet 4 Share 3 +1 7 submit

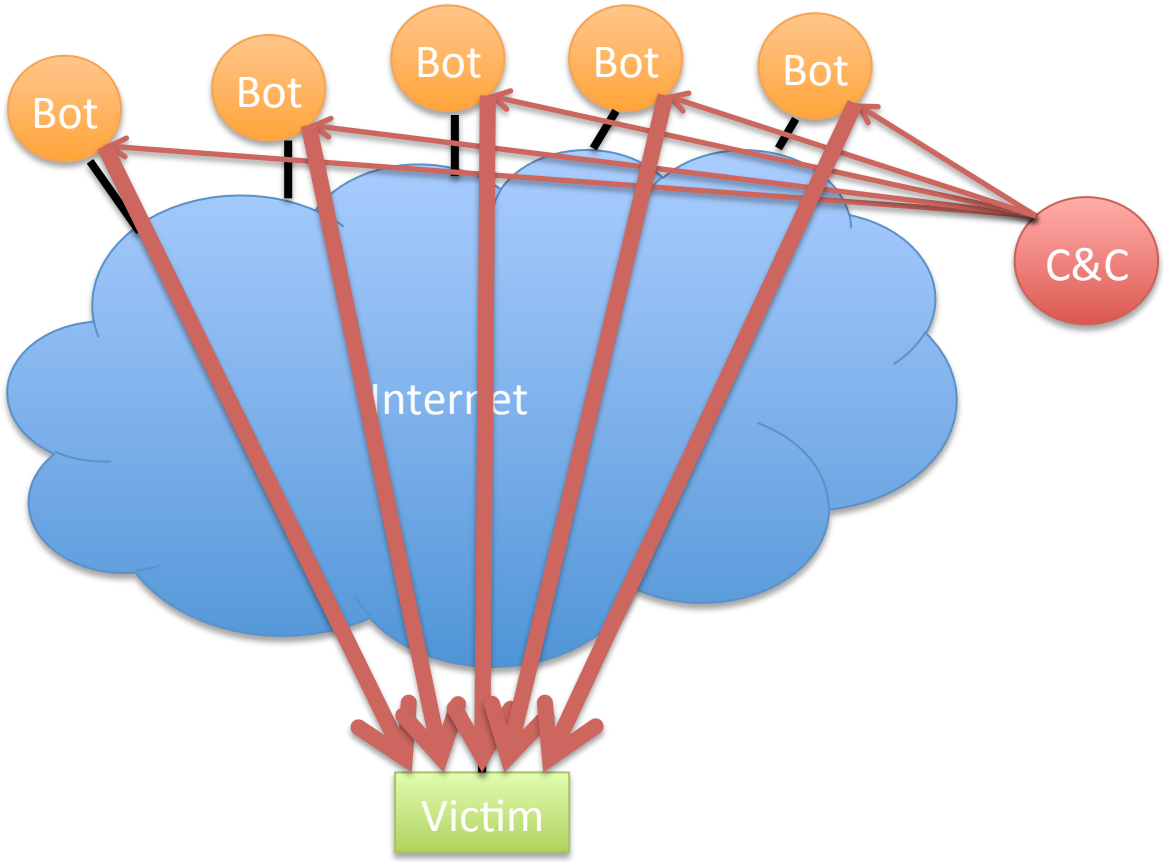
Over the past weekend, a hacker group known as “Lizard Squad” launched DDoS attacks to take down several game servers. The most affected were the North American servers of Destiny and Call of Duty: Ghosts, on all platforms.

A few days before their attack, Lizard Squad posted a warning on Twitter, in which they stated that there were going to be a lot of mad gamers during the following weekend. The group took down the Destiny and Call of Duty servers through DDoS attacks, which basically means flooding a system with an overwhelming number of requests, and making the servers crash in the process.

Main Goals for Today

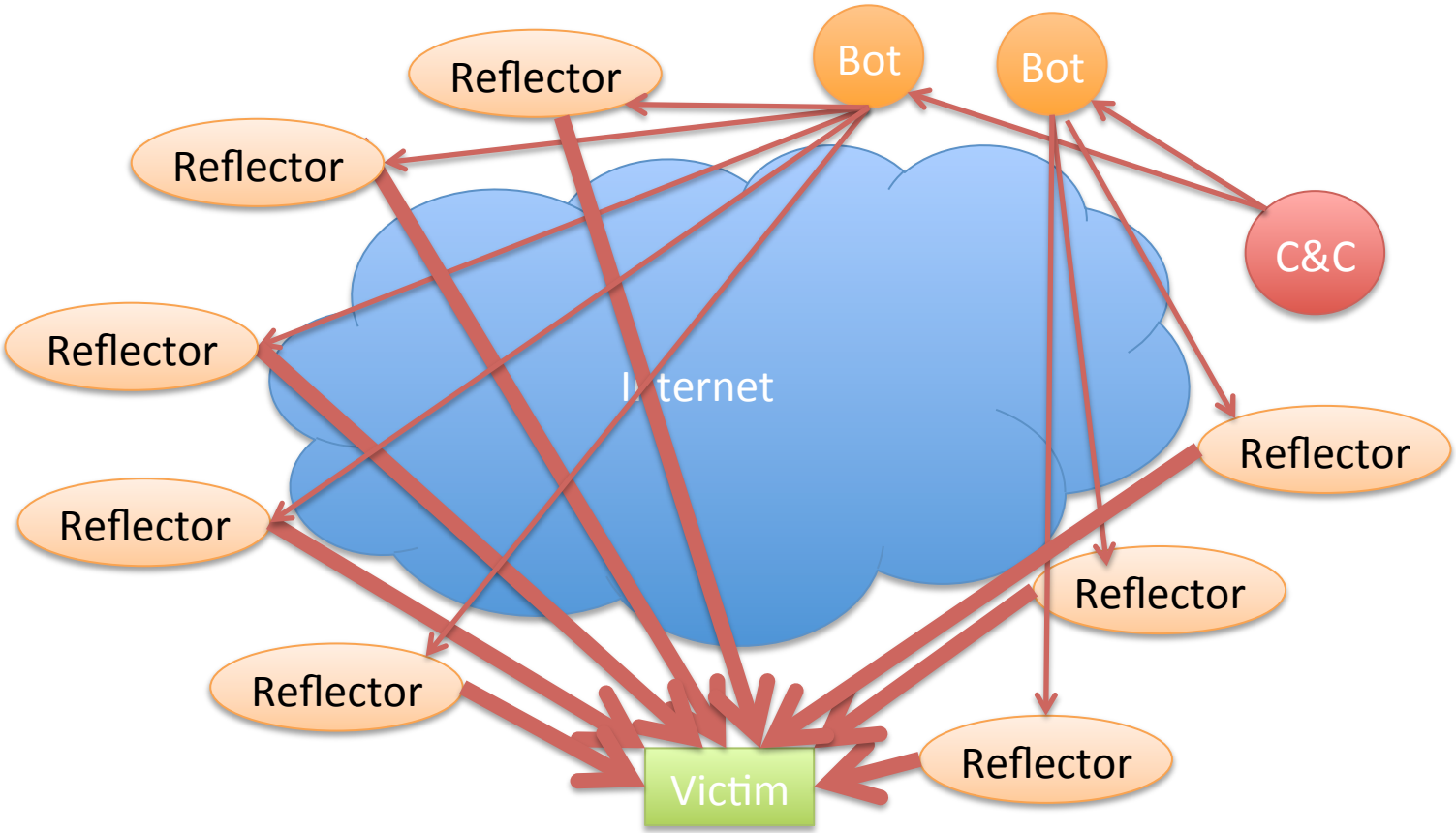
- Finish up DDOS.
- Start on Network Intrusion Detection

Basic Setup of a DDOS Botnet



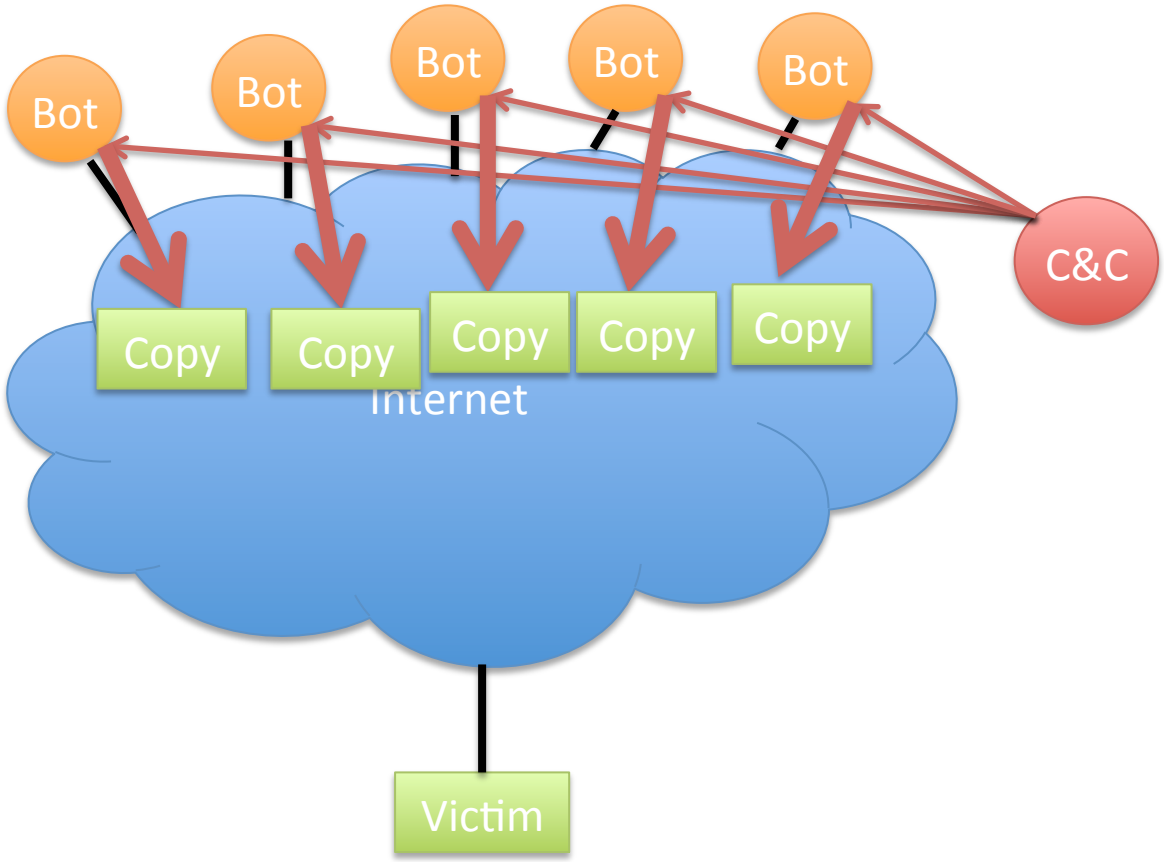
Illustrative only: practical attacks will have many more bots

Reflection Attacks

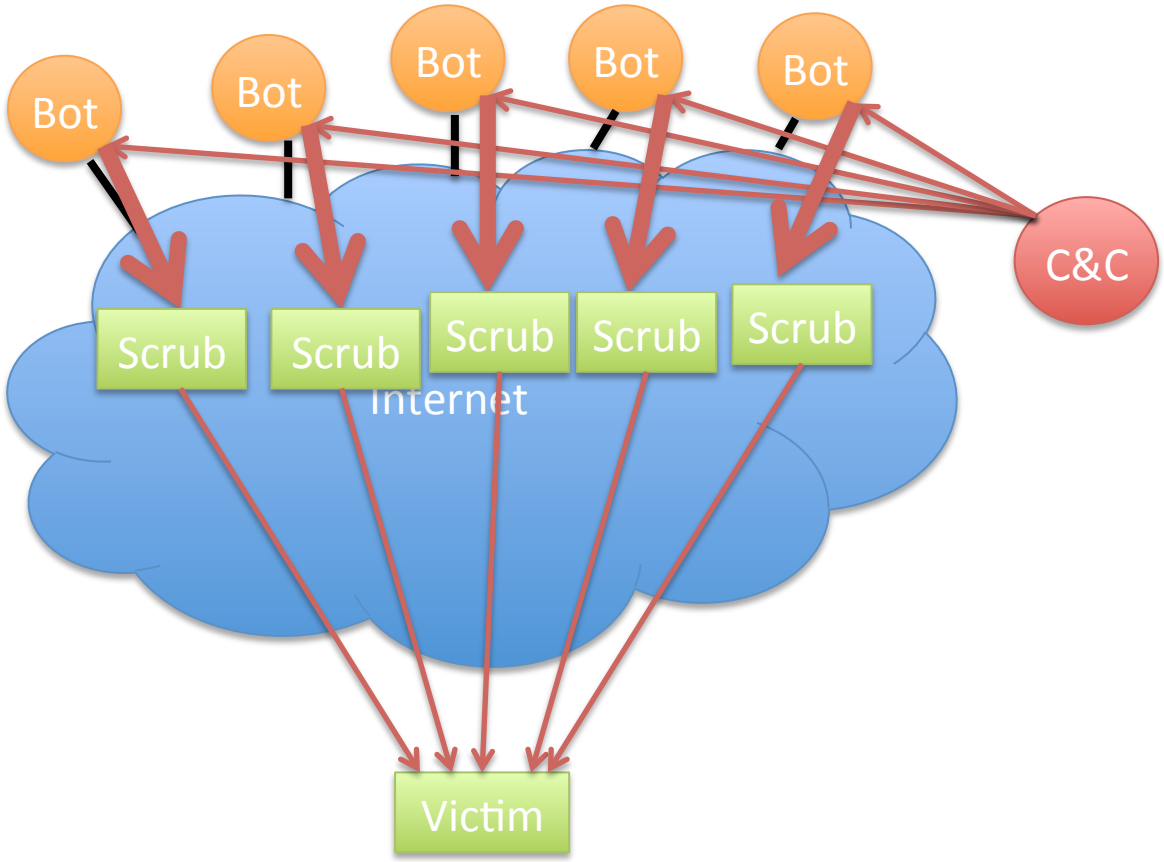


Illustrative only: practical attacks will have many more bots/reflectors

DDOS Defense: Content Distribution



DDOS Defense: Distributed Scrubbing



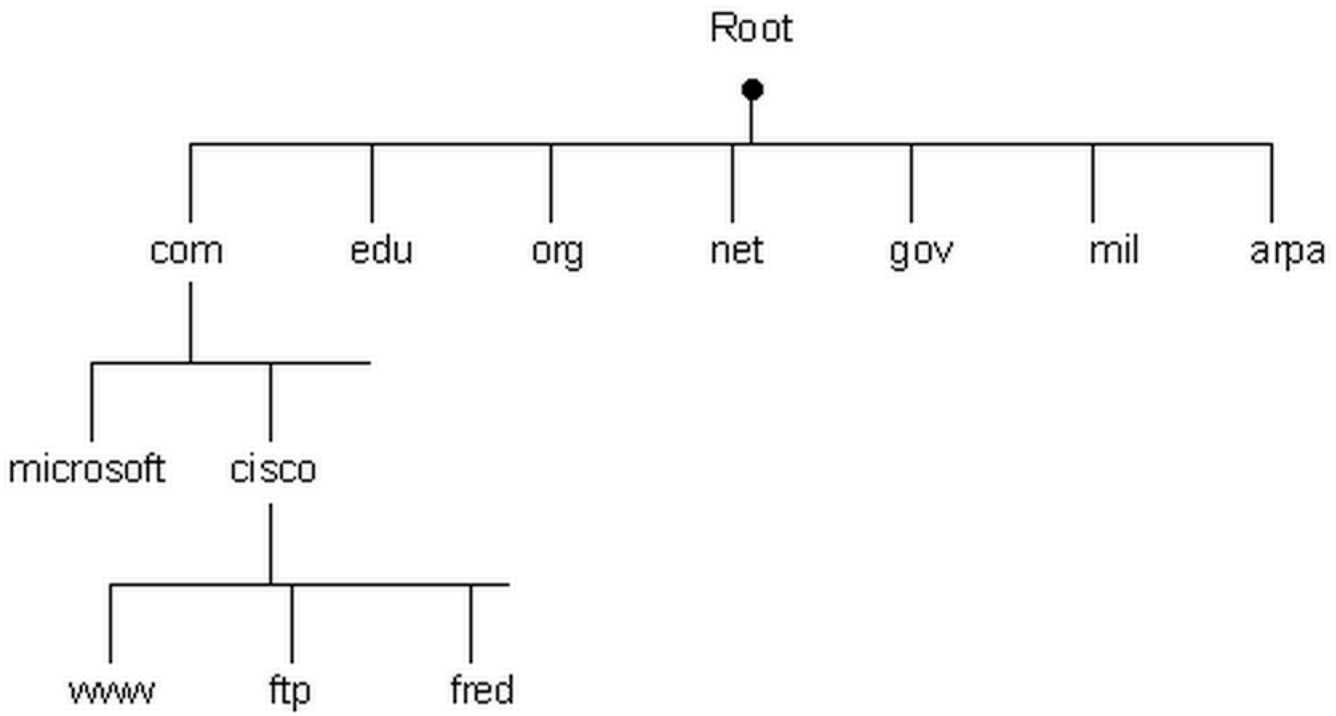
What Will Work as a Reflector?

- Any TCP host (send SA or R in response to S)
- ICMP (eg echo response to echo request)
- DNS – especially with recursion
  - Issue on campus recently
  - Let's look at this in more detail

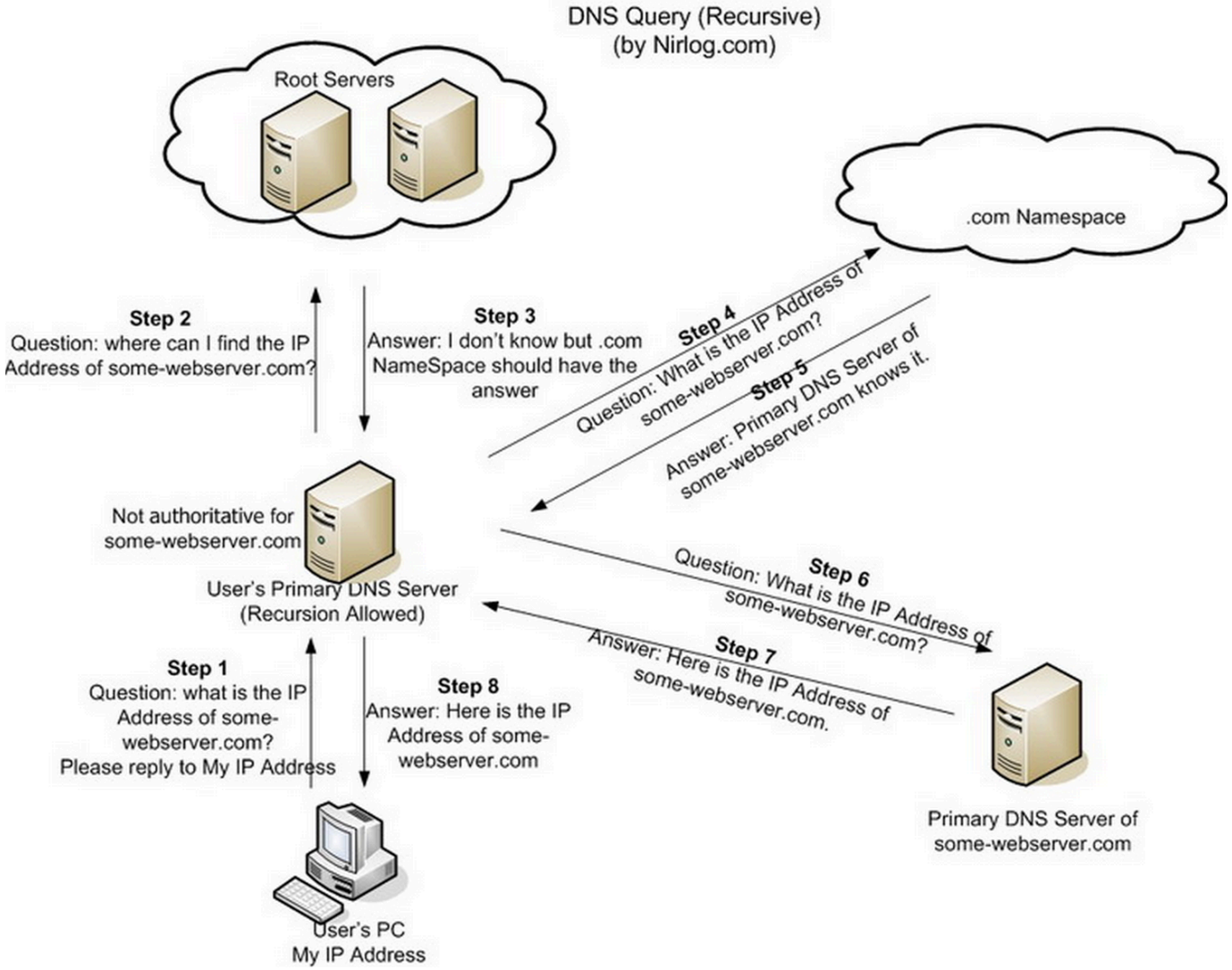
Domain Name Service

- Global Internet service to map names to IP addresses.
- Part of core TCP/IP suite of protocols
  - RFC 882 (1983) updated by RFC 1034 (1987)
  - Replaced manually maintained “hosts.txt” of all Internet connected computer’s IP addresses.
- Let’s do it
  - dig www.nytimes.com

The DNS Hierarchical Name Tree



How a DNS Query Works



Credit: http://securitytnt.com/dns-amplification-attack/

Egress Filtering

- Can have many purposes, but in DDOS case:
  - Don’t let spoofed packets out of our network
  - Eg through a pair of firewall rules on LAN interface
    - Allow 192.168.0.0/16:any -> any:allowed_ports
    - Deny any:any -> any:any

Network Intrusion Detection

- Basic idea:
  - Examine network traffic looking for evidence of attacks.
  - Idea is not to impose policy (firewall)
  - But specifically detect/id/block attacks.

Simple Example

- If we see a long string of 0x90 in the middle of a network packet, what should we think?

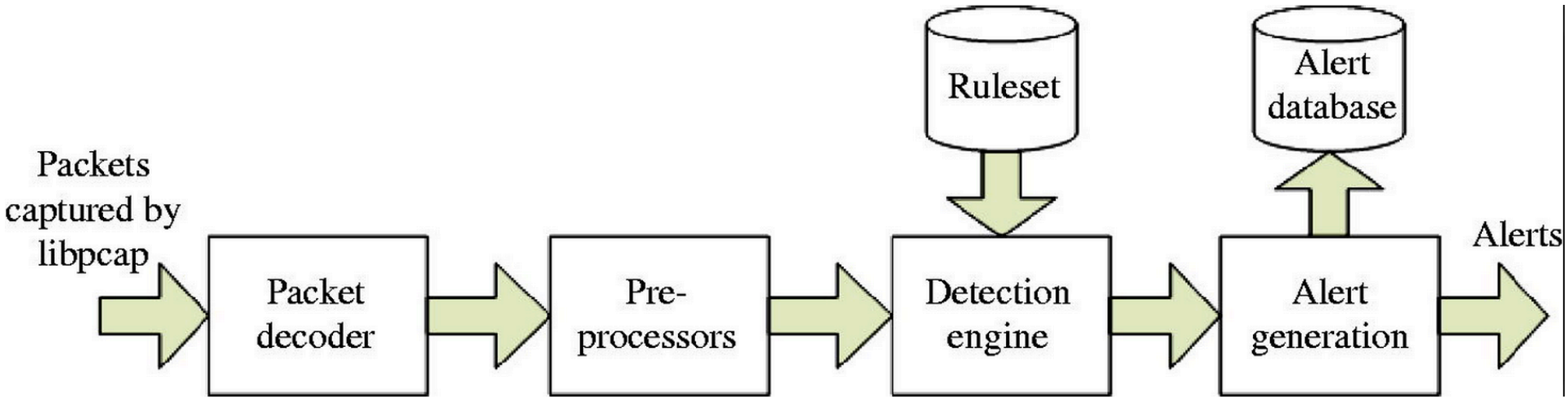
Example NIDS Rule

- alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"INDICATOR-SHELLCODE x86 NOOP"; content:"|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|"; fast_pattern:only; metadata:ruleset community; classtype:shellcode-detect; sid: 648; rev:14;)

High Points of NIDS History

- Heberlein et al NSM – 1989
- Wheelgroup NetRanger - 1995
- Snort – 1998
- Intruvert – 2000
- FireEye – 2004 (but really 2007)
- Focus on Snort here, as conveniently accessible.

Overall Snort Architecture



Anatomy of a Snort Rule

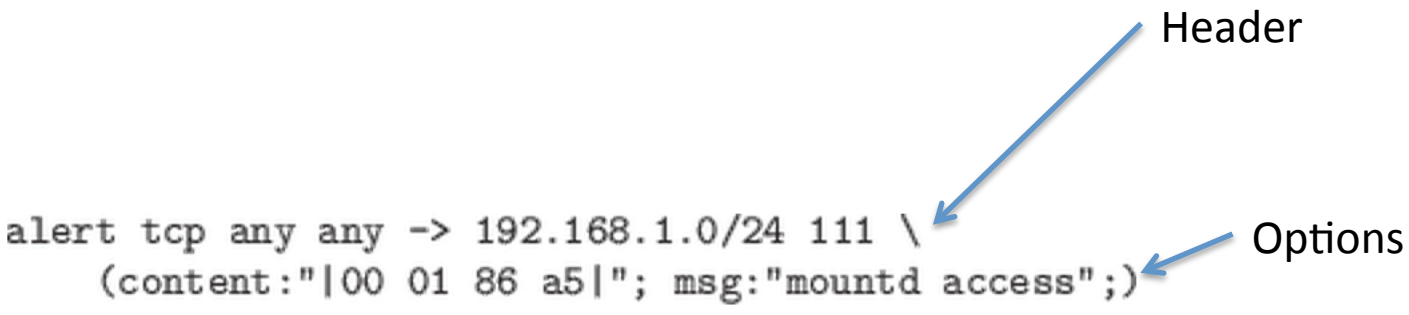


Figure: Sample Snort Rule

http://manual.snort.org/node28.html

Snort Detection Engine Data Structure

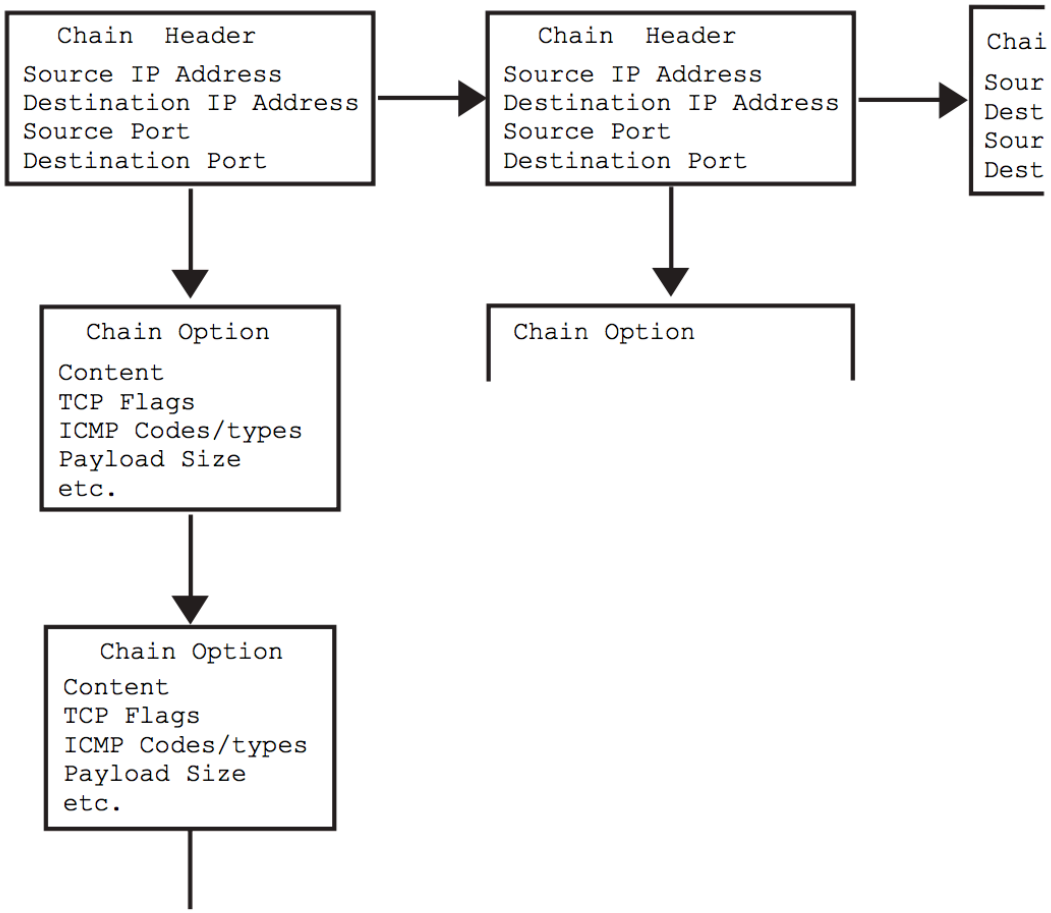


Figure 3: Rule Chain logical structure.

Snort Rule Example 1

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SERVER-WEBAPP HyperSeek hsx.cgi directory traversal attempt"; flow:to_server,established; content:"/hsx.cgi"; http_uri; content:"../../"; http_raw_uri; content:"%00"; distance:1; http_raw_uri; metadata:ruleset community, service http; reference:bugtraq,2314; reference:cve,2001-0253; reference:nessus,10602; classtype:web-application-attack; sid:803; rev:21;)

Snort Rule Example 2

alert tcp **$EXTERNAL_NET $HTTP_PORTS -> $HOME_NET** any (msg:"*EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe*"**; flow:to_client,established**; content:"**filename=";** http_header; content:**"readme.exe"**; within:12; fast_pattern; http_header; **content:"|0D 0A|"**; within:4; http_header; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:cve,2006-0003; reference:cve,2007-5659; reference:cve,2008-0655; reference:cve,2008-2992; reference:cve,2009-0927; reference:cve,2010-1885; reference:cve,2011-0559; reference:cve,2011-2110; reference:cve,2011-3544; reference:cve,2012-0188; reference:cve,2012-0507; reference:cve,2012-1723; reference:cve,2012-1889; reference:cve,2012-4681; reference:url,blog.webroot.com/2011/10/31/outdated-operating-system-this-blackhole-exploit-kit-has-you-in-its-sights/; classtype:trojan-activity; sid:25387; rev:3;)