Defending Computer Networks
Lecture 13: NIDS

Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- Comment on scores so far
- Guest lecture feedback?
- HW3.
  - Will be out today
  - Will be due Friday October 18th.
- HW going forward.
  - Will be easier, no coding.
- Project descriptions
- IAP workshop

IAP | Industry-Academia Partnership

http://industry-academia.org/

Cloud Technology Workshop - Friday, October 18, 2013

"Meeting the Future Needs of the Data Center and Cloud"

Statler Amphitheater, 9AM–6PM (Registration at 8:30AM)

Network with Students, Professors and Industry Scientists and Engineers

Statler Amphitheater, Cornell

The IAP is a new association formed to address the revolutionary changes required for the underlying hardware and software as multi-core compute, storage and networking converge. Invited speakers from industry and academia will describe their research and development efforts underway to meet the future needs of the data center and cloud.

- *Keynote* - **Kiko Reis, Ubuntu**: "Demand and Challenges Facing the Future Data Center"
- **Dr. Shubu Mukherjee, Cavium**: "Multicore Processors for the Zettabyte Era"
- **Dr. Kim Hazelwood, Google**: "Scale-out Performance Challenges and Solutions"
- **Tom Fry, Samsung**: "The End of DRAM scaling; the Future of Cloud Memory Solutions"
- **Dr. John Busch, Sandisk**: "The Future of Cloud Storage"
- *Student Poster Session* - Cloud Research Projects by Undergrad and Grad Students
- **Prof. Hakim Weatherspoon, Cornell**: "Plug into the Supercloud"
- **Prof. José Martínez, Cornell**: "Toward Processor-Side Memory Scheduling"
- **Dr. Robbert van Renesse, Cornell**: "Driving Perf. of Large Fault Tolerant Services"
- **Dr. Robert Soulé, Cornell**: "Managing the Network with Merlin"
- *Expert Panel* - "An Exa-Op Data Center at < 10MW by 2020, Really?"

Lunch and a Reception after the sessions will be hosted for the Workshop Registrants.

Projects

40% class project. You will build a non-trivial piece of C code from scratch to do an interesting task in network security. You will write a document describing its algorithms and architecture (10% of total grade) and demonstrate how well it works at an interim milestone (10%) and towards the end of the course (20%).

Projects will be solo.

Project Description 1

Develop a working remote exploit for a previously unknown vulnerability in a widespread piece of software that works on a current 64 bit operating system with all defenses in place. Note that attacking software across the Internet (or Cornell's network) is generally illegal, so you should attack a piece of software for which you have local access. You should then notify the software vendor/development team of the vulnerability and provide them with your proof of concept exploit (keeping it secret in the meantime).

Intermediate milestone is to have selected your vulnerable application/OS, and demonstrate that you can crash it with malicious input.

The document should explain the nature of the vulnerability, how you worked around the various OS/compiler defenses, and what your shellcode/ROP chain/etc does.

Note that this project has hard-to-estimate risks of failure if you pick something that turns out not to be exploitable by you in the available time. But if you succeed, we know for sure that you are 31337.

Project Description 2

Build a simple network firewall from scratch in C. Your firewall should have the ability to handle transferring packets between multiple network interfaces (eg wireless and wired interfaces on your laptop), and also the ability to transfer packets between pcap files for testing purposes. Your firewall should be stateful, with the ability to keep track of TCP, UDP, and ICMP conversations going on in the network. You should implement a text-based rules language of your own design that includes the ability to block/pass/reject network conversations based on source/destination address ranges and port numbers. You should obtain multi-gigabyte pcap files online for testing, and be able to demonstrate that your algorithms do not crash or blow-up in time/space demands on large files.

Intermediate milestone is to demonstrate that you can pass packets between multiple interfaces and files, with a single rule of some kind.

The document should describe and give the rationale for: 1) your rules language, 2) the data structures/algorithms used in your code, and 3) your test plan and the results of your tests.

Project Description 3

Build a web-exploit scanner from scratch in C. Your code should be able to take a list of malicious domains, reach out to them via HTTP, replay the content in a virtual machine and perform some simple steps to determine if bad things have happened in the virtual machine (eg look for browser crashes or memory explosions). You should include code to obtain secondary downloads that the virtual machine asks for. Note that you must implement your own HTTP client/proxy that can handle all three major methods of length delineation. It's acceptable to use libraries to handle gzip decoding of content. You should demonstrate that your code can stay up on a list of at least hundreds of bad domains, and you should demonstrate that you can detect at least some malicious websites.

Intermediate milestone is to be able to get an HTML file off disk started in a virtual machine browser, and demonstrate the intercept and parsing of outbound HTTP requests from the VM.

The document should describe and give the rationale for: 1) how your code interacts with the VM/browser, 2) the data structures/algorithms used in your code, and 3) your test plan and the results of your tests, including the malicious domains you detected.

Project Description X

- Other. If you have a burning desire to do something else of similar scope to the above,
  - Put together a one paragraph description
  - Let me know.

Project Deadlines

- Interim milestone demonstration:
  - Friday November 1st
- Document Due
  - Friday November 29th
- Final implementation due:
  - Friday December 6th

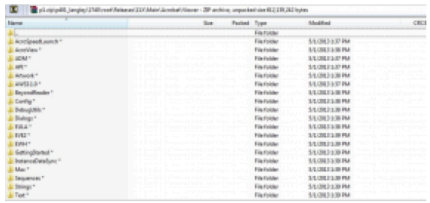
Assigned Reading

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

Latest News

03 OCT 13 Adobe To Announce Source Code, Customer Data Breach

Adobe Systems Inc. is expected to announce today that hackers broke into its network and stole source code for an as-yet undetermined number of software titles, including its **ColdFusion** Web application platform, and possibly its **Acrobat** family of products. The company said hackers also accessed nearly three million customer credit card records, and stole login data for an undetermined number of Adobe user accounts.



A screen shot of purloined source code stolen from Adobe, shared with the company by KrebsOnSec

KrebsOnSecurity first became aware of the source code leak roughly one week ago, when this author — working in conjunction with fellow researcher **Alex Holden**, CISO of Hold Security LLC — discovered a massive 40 GB source code trove stashed on a server used by the same cyber criminals believed to have hacked into major data aggregators earlier this year, including LexisNexis, Dun & Bradstreet and Kroll. The hacking team's server contained huge repositories of uncompiled and compiled code that appeared to be source code for ColdFusion and Adobe Acrobat.

Worst Day Ever for This Guy

Important Customer Security Announcement

POSTED BY BRAD ARKIN, CHIEF SECURITY OFFICER ON OCTOBER 3, 2013 8:08 AM IN EXECUTIVE PERSPECTIVES

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use of many of our products, Adobe has attracted increasing attention from cyber attackers. Very recently, Adobe's security team discovered sophisticated attacks on our network, involving the illegal access of customer information as well as source code for numerous Adobe products. We believe these attacks may be related.

Latest News

The Telegraph

Iranian cyber warfare commander shot dead in suspected assassination

The head of Iran's cyber warfare programme has been shot dead, triggering further accusations that outside powers are carrying out targeted assassinations of key figures in the country's security apparatus.

By Damien McElroy, and Ahmad Vahdat
8:00PM BST 02 Oct 2013

Mojtaba Ahmadi, who served as commander of the Cyber War Headquarters, was found dead in a wooded area near the town of Karaj, north-west of the capital, Tehran. Five **Iranian** nuclear scientists and the head of the country's ballistic missile programme have been killed since 2007. The regime has accused Israel's external intelligence agency, the Mossad, of carrying out these assassinations.

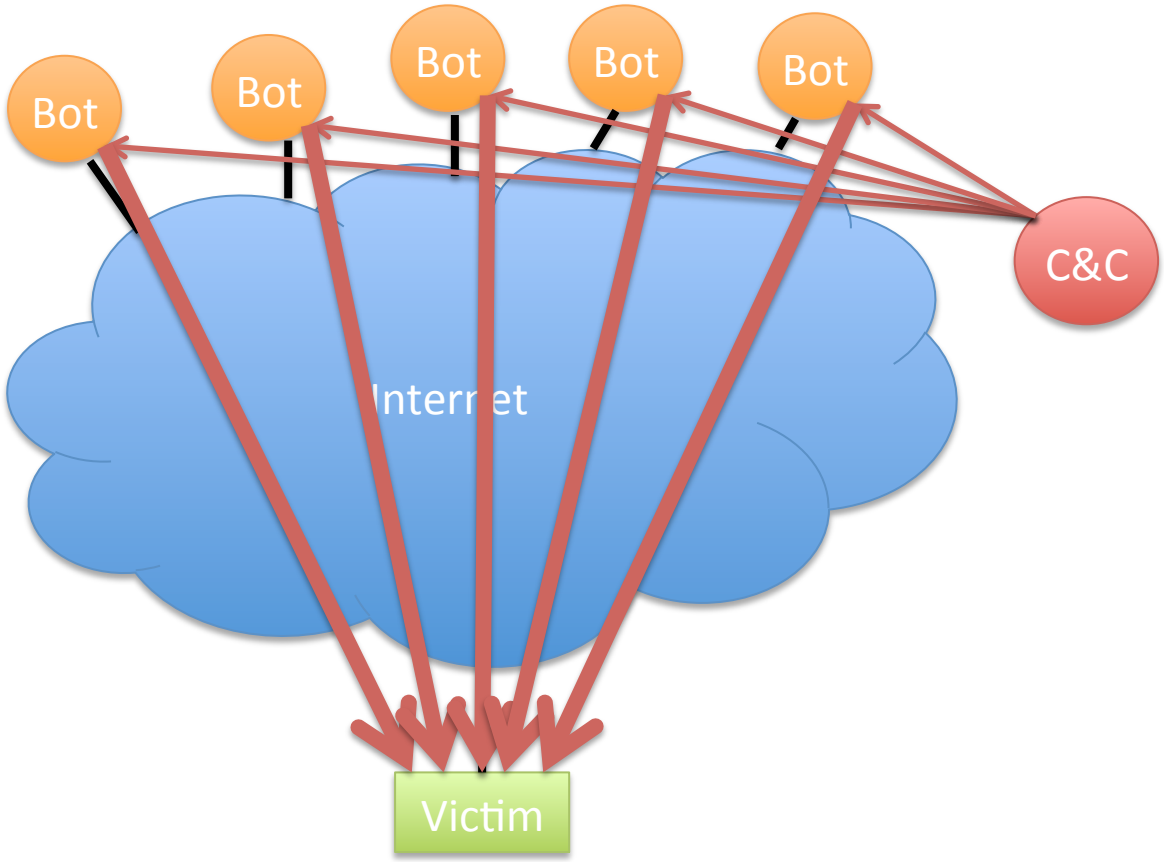
Ahmadi was last seen leaving his home for work on Saturday. He was later found with two bullets in the heart, according to Alborz, a website linked to the Revolutionary Guard Corps. "I could see two bullet wounds on his body and the extent of his injuries indicated that he had been assassinated from a close range with a pistol," an eyewitness told the website.

The commander of the local police said that two people on a motorbike had been involved in the assassination.

Main Goals for Today

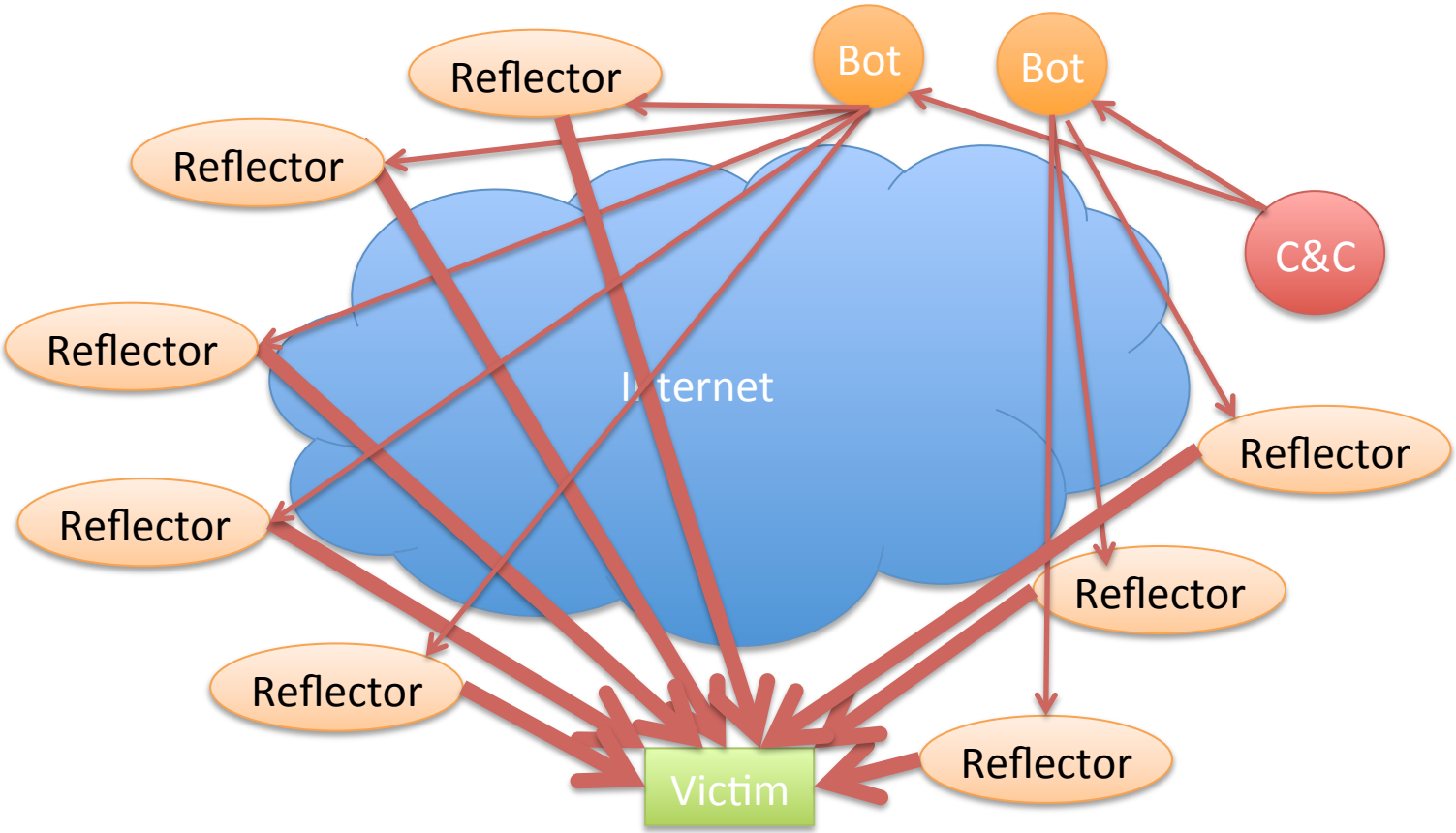
- Finish up DDOS.
- Start on Network Intrusion Detection

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

Latest News (9/27)

London schoolboy cuffed for BIGGEST DDOS ATTACK IN HISTORY

Bet his parents wish he'd been playing computer games

By Iain Thomson, 27th September 2013

RELATED STORIES

'Honker Union' sniffs 270 hacktivism targets

Tor traffic torrent: It ain't the Syrians, it's the BOTS

Chinese authorities say massive DDoS attack took down .cn domain

Bank man:

A British police investigation into the massive DDoS attack against internet watchdog Spamhaus has led to the arrest of a 16-year-old London schoolboy who, it is claimed, is part of an international gang of cyber-crooks.

"The suspect was found with his computer systems open and logged on to various virtual systems and forums," says the police document shown to the *London Evening Standard*. "The subject has a significant amount of money flowing through his bank account. Financial investigators are in the process of restraining monies."

The young miscreant was arrested in April at the same time as a 35 year-old Dutchman (thought to be Sven Kamphuis – the owner of hosting firm Cyberbunker) as part of an investigation into the Spamhaus attack by British police dubbed Operation Rashlike. The

http://www.theregister.co.uk/2013/09/27/london_schoolboy_arrested_for_biggest_ddos_attack_in_history/

More News (10/1)

Latest 100 Gigabit Attack Is One of Internet's Largest

By Sean Michael Kerner | Posted 2013-10-01 Email Print

Quite possibly, the largest raw packet bandwidth attack in history slams a site for nine hours, but the site under attack stays afloat.

Unbeknownst to many people in the world, late last week one of the largest attacks in the history of the Internet was taking place—a massive nine-hour barrage that leveled an unrelenting 100 Gigabits of traffic at its peak.

The attack took place on Sept. 24, and to date the victim of the attack is remaining in the shadows, not wanting to be publicly identified. The target Website is protected by cloud security vendor Incapsula, which was able to withstand the massive distributed denial-of-service (DDoS) attack and keep the targeted Website up and running.

Incapsula co-founder Marc Gaffan explained to ***eWEEK*** that the attacked site is in an industry that is constantly under assault. The attack leveraged raw bandwidth under the control of the attacker and was not a DNS reflection or amplification attack, Gaffan said. In March of this year, another 100 Gigabit attack was reported that leveraged DNS reflection. With DNS reflection, the number of inbound connections to a target Website is amplified by taking advantage of poorly configured DNS servers.

http://www.eweek.com/security/latest-100-gigabit-attack-is-one-of-internets-largest.html

And From August 26th

Largest DDoS attack ever disrupts China's Internet

Posted on 26 August 2013.

BOOKMARK ...

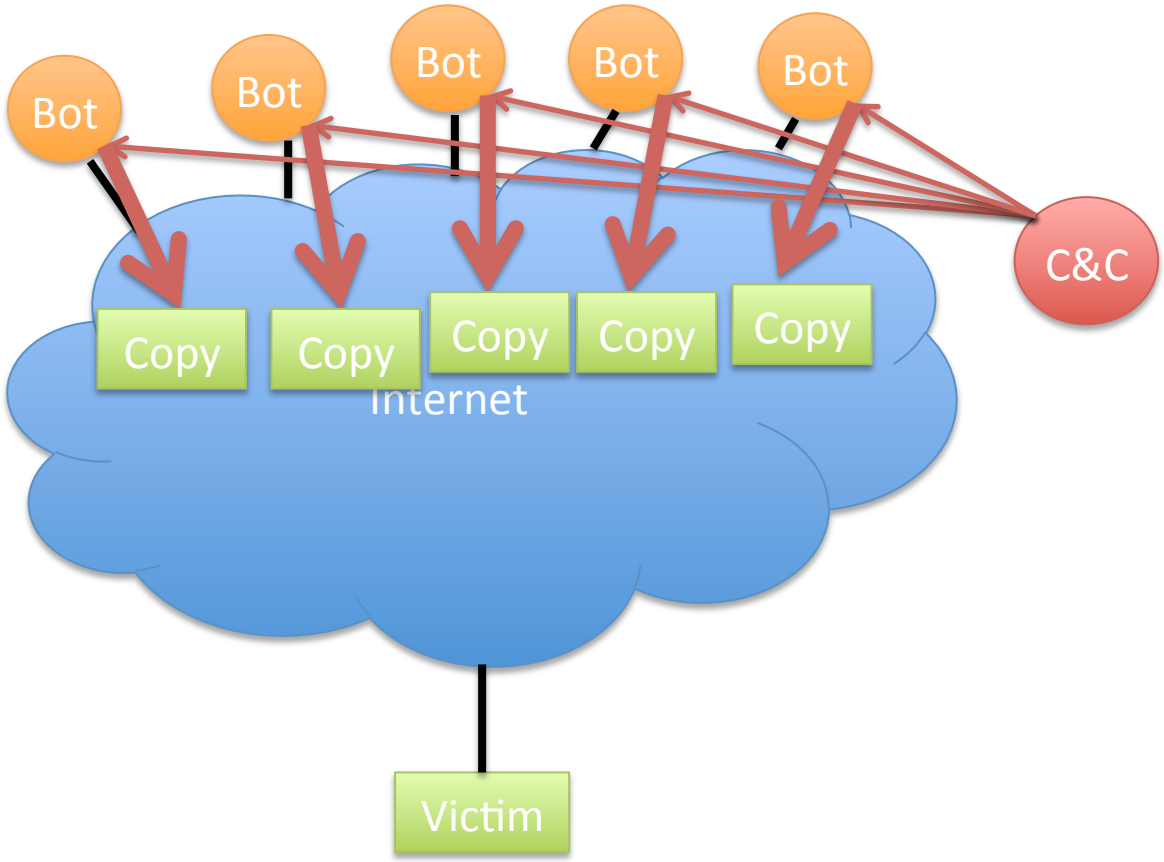
The China Internet Network Information Center (CNNIC), which maintains the registry for the *.cn*, China's country code top-level domain, has notified the public that two massive DDoS attacks have been aimed against the national Domain Name Service early on Sunday.

The first started around 0:00, Beijing time, and around 2 PM the service was restored to normal.

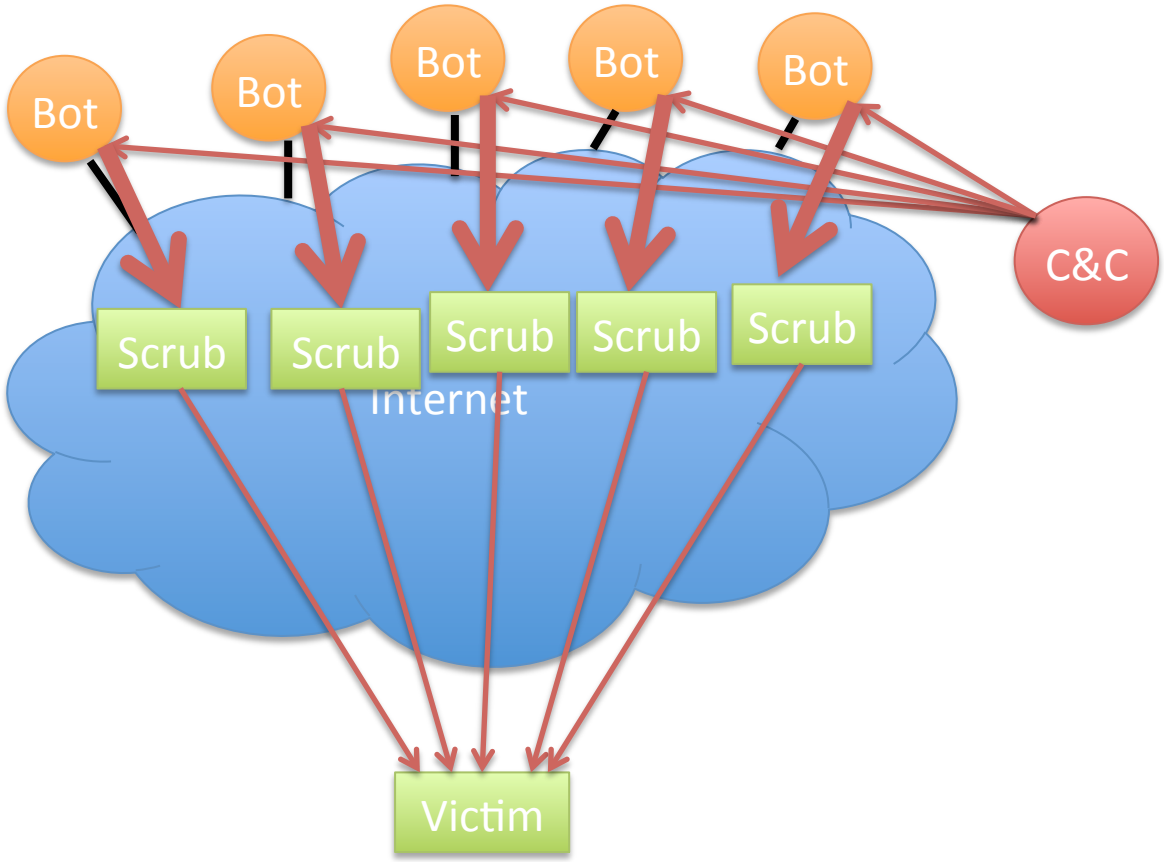
The second one hit around 4 PM, and according to the CNNIC, it was the largest ever denial of service attack to hit China's Internet, and led to many websites being completely inaccessible for a period of time or made them extremely slow to load.

http://www.net-security.org/secworld.php?id=15461

DDOS Defense: Content Distribution



DDOS Defense: Distributed Scrubbing



Egress Filtering

- Can have many purposes, but in DDOS case:
  - Don’t let spoofed packets out of our network
  - Let’s check the rules on our demo firewall setup

5 Minute Break

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?

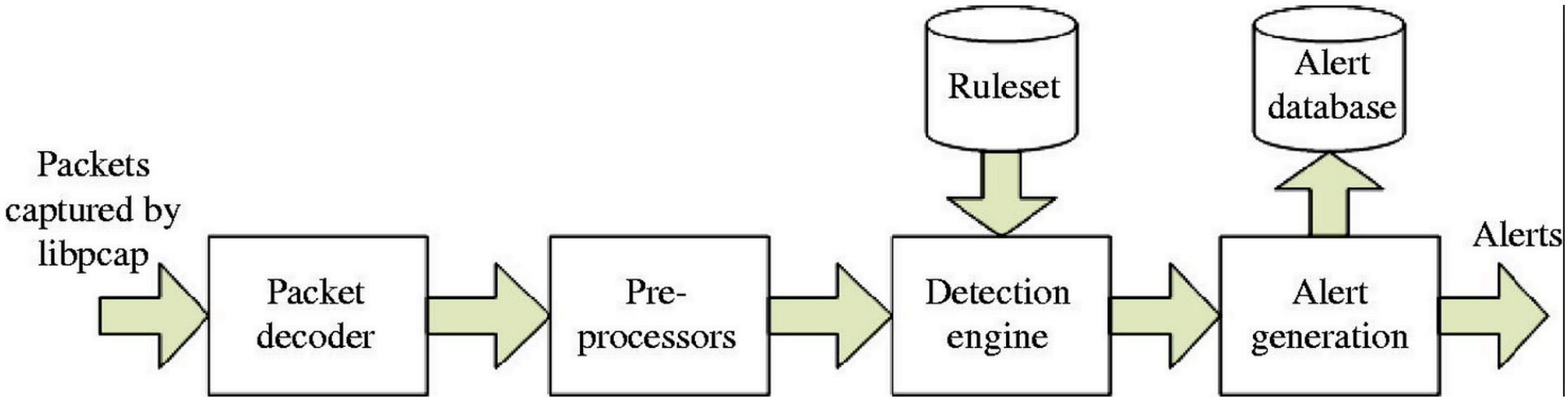
Example NIDS Rule

- 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

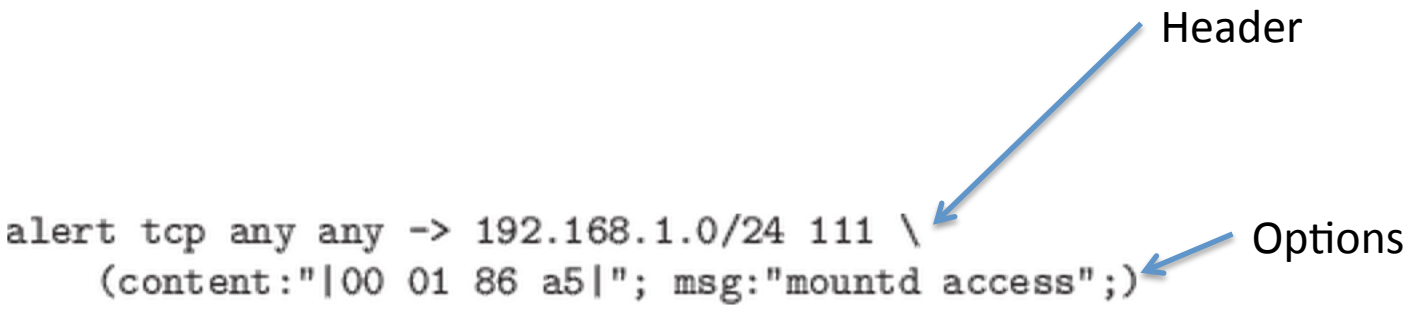


Figure: Sample Snort Rule

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

Snort Detection Engine Data Structure

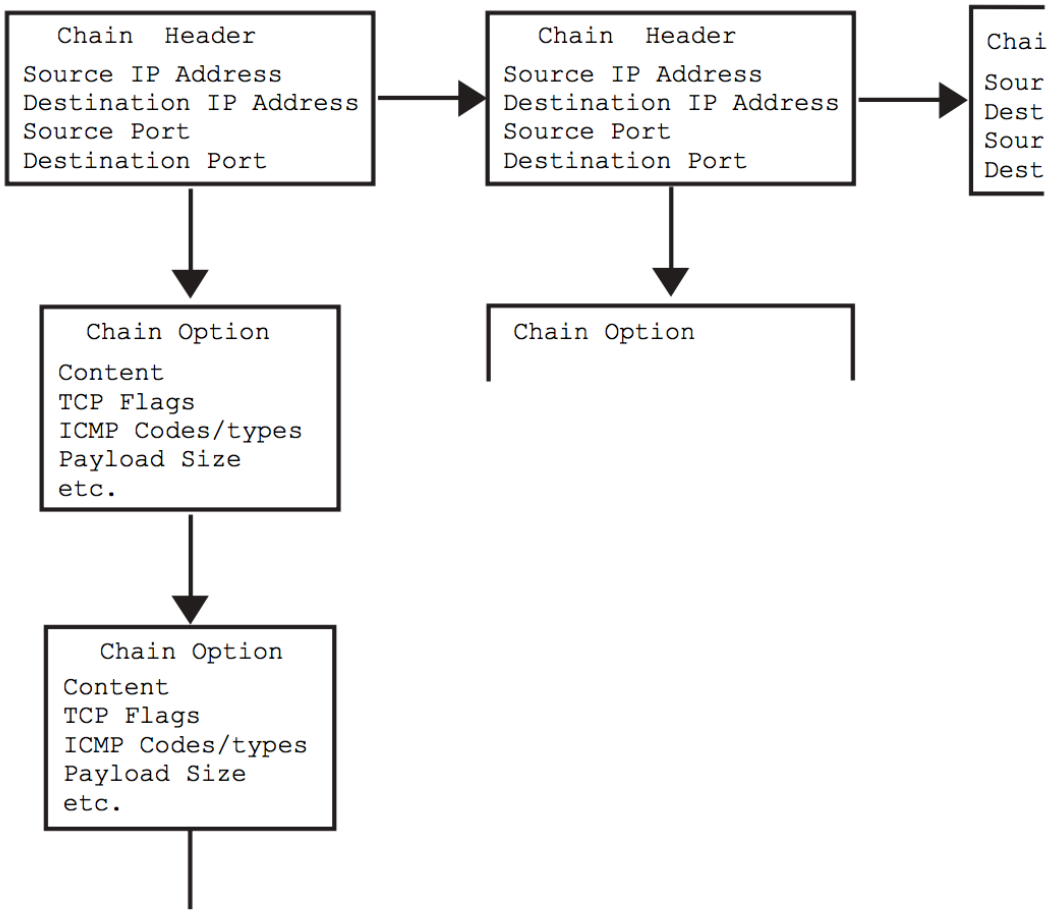


Figure 3: Rule Chain logical structure.

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;)