



Handling Security Incidents in your Network

Laura Kuiper

CTO Consulting Engineer - Security

Cisco Systems

Agenda

- Overview
- Preparation
- Detection
- Mitigation
- Lessons Learned

Normal part of an ISP's operations



- IR planning is about risk reduction and mitigation, and needs to be seen as such by top management
- It is not just a plan for technical staff to chase hackers and viruses, even though much of the work involved will have to be technology-oriented

Goals of Incident Response

- Confirm whether an incident occurred
- Provide accurate, relevant, and timely information
- Implement controls to Maintain Chain of Custody
- Protect individual rights established by policy and law
- Minimize downtime to business and network services
- Enable legal and law enforcement to prosecute malicious entities
- Provide recommendations to Sr. Management
- Understand correct priorities

Real Examples

- Computer Intrusion
 - System compromised (configuration, vulnerability)
 - Web Defacement
- Virus or worm outbreak
- Identification of unauthorized applications
- Denial-of-service attack
- Theft of intellectual property
- Unauthorized use of systems by employees or external entities
 - Launching ground for attacks
- Internal & External policy compliance
 - Government legislation
 - Corporate usage policy enforcement and containment

Problems with Incident Response Today

- Systems are taken off-line impacting services
- IR investigations which span different time zones
- Use of disjointed tools (Resource intensive)
- Various system and media types
- Foreign language support
- Hard to determine scope of compromise
- Restoration of systems and services
- Containment of potential compromise
- Controlling release of information about compromise

Preparation



Why is Preparation so important

- Why is preparation so important
 - Know what to do in a crisis situation
 - Know who to contact
 - Find out what may have happened
 - Information for tracking incident
- The problem—Most Organization's:
 - Do not have security plans
 - Do not have security procedures
 - Do not train in the tools or procedures
 - OJT (on the job training)—learn as it happens
 - Don't see it as important



The Preparation Problem

CEO, “Customer X just called and said they’ve been DOSed for the past 12 hours. What are we doing about it?”

Operations Chief, “We’re working on it.”

CEO, “How long before it is fixed?”

Operations Chief, “We’re working on it.”

CEO, “What exactly are we doing about it?”

Operations Chief, “We’re working on it.”

CEO, “Do you know how to get the customer up and running?”

Operations Chief, “It is all the vendor’s fault – they should fix the *DOS problem*.”

Prepare your tools

- Do you have Monitoring enabled?
- Do you have all your SNMP tools deployed?
- Do you have all your SYSLOG tools deployed?
- Do you have your ACLs created?
- Do you have your scripts created?
- Have you built and tested your sink hole and backscatter tools?

Do you know the answers?

- Q. Do you have the NOC and Security Contacts for every ISP you are peered?
- Q. Do you test the contact information every month (E-mail, Phone, Text)?
- Q. Have you agreed on the format for the information you will exchange?
- Q. Do you have Vendor contact information?
- Q. Do you have a customer security policy so your customers know what to expect from your Security Team?

Standards and Best Practices

FIRST: <http://www.first.org/resources/guides/>

ISO: ISO/IEC 27035 Security Incident Management

CISCO: <http://tools.cisco.com/security/center/serviceProviders.x?i=55>

SANS: http://www.sans.org/reading_room/whitepapers/incident/

Reporting

What to Report

- **Confirmed / Suspected Security Incident or Intrusions**
- **Denial of Service Attacks**
- **Malicious Logic / Mobile Code / Viruses**
- **Network Probes / Scans**
- **Attempts to Obtain Passwords**
- **Other Suspicious Behavior / Anomalies**

Incident Report Contents

- **Incident Date / Time (UTC)**
- **System Information (Location, IP, etc.)**
- **How the Attack was Identified**
- **Attack Success Evaluation**
- **Attack Impact**
- **Corrective Actions Attempted**
- **Points of Contact**

Okay—Tell Me Where to Start From?

- Preparation

- Build and Prepare you CERT/FIRST Team

- Securing the router

- Securing the routing protocols

- Route filtering

- Black hole filtering

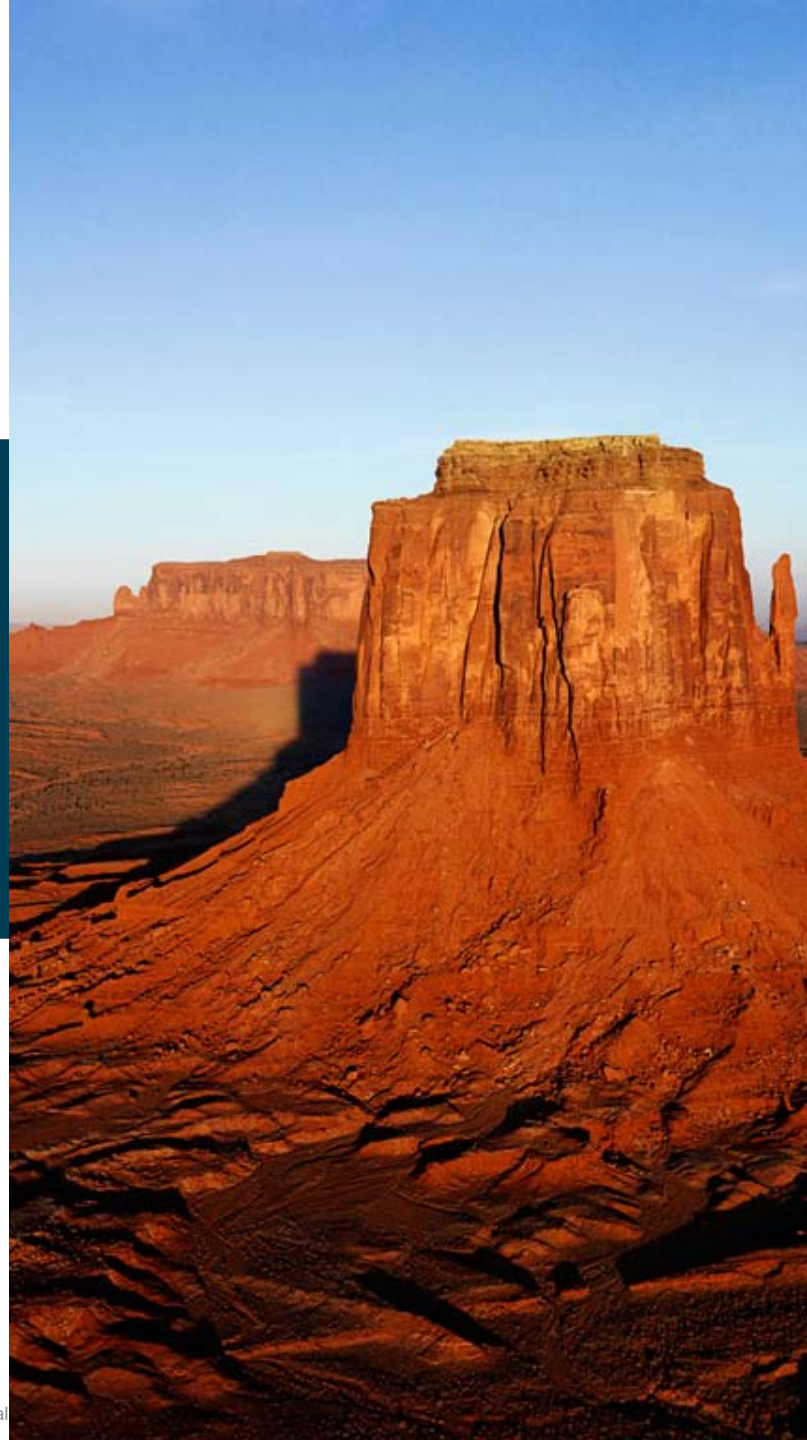
- Sink Hole routers/networks

- Packet filtering

- Securing the network

- Default routes, ISPs, and security

Detection



What should I look at?

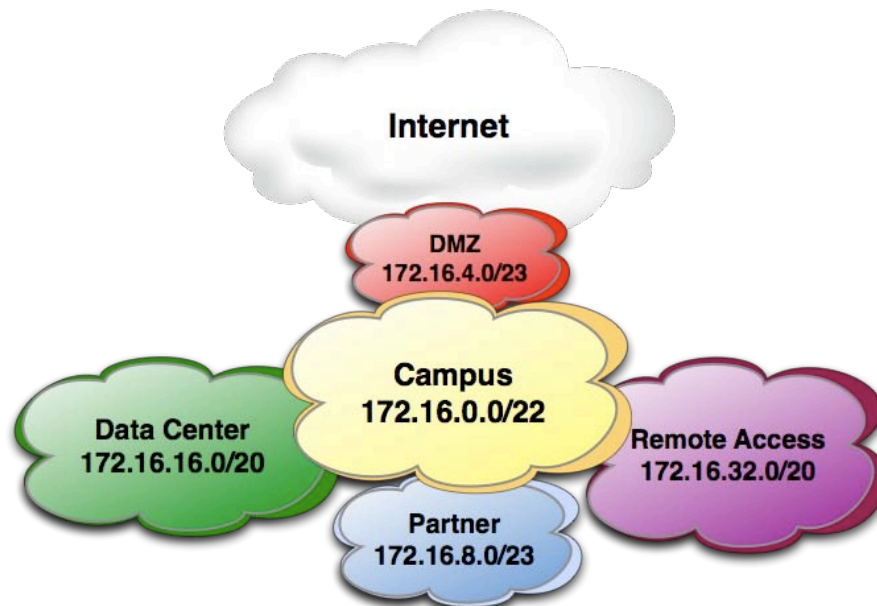
- File System Artifacts (Permissions, timestamps, etc)
- Logs (Operating System, Application, device)
- Deviations from Baseline
- IDS/IPS
- SNMP
- RMON
- BGP
- DNS
- IPFix

Network Baselines

- Network Management System (NMS) baselines
- Unexplained changes in link utilization
 - Worms can generate a lot of traffic, sudden changes in link utilization can indicate a worm
- Unexplained changes in CPU utilization
 - Worm scans can affect routers/switches resulting in increased CPU - process and interrupt switched traffic
- Unexplained syslog entries
- Changes don't always indicate a security event
- **Must know what's normal in order to identify abnormal behavior**

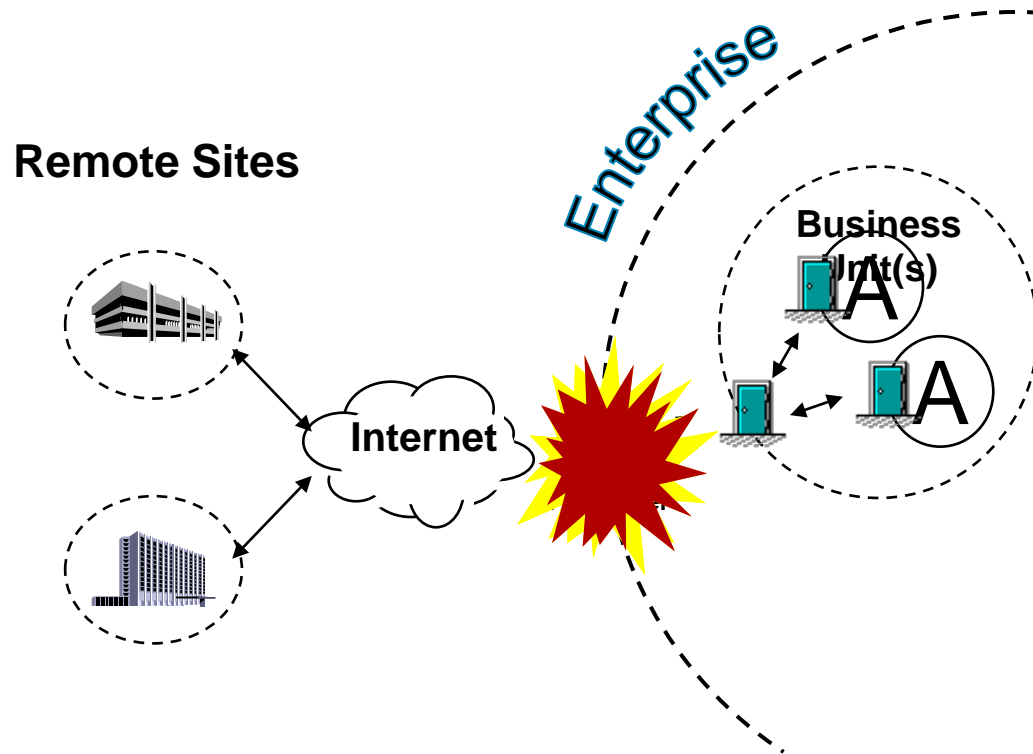
Know Your Addressing

- What Addresses are mine
- Provide context to an incident
 - What network was being attacked?
- Quickly able to identify known networks versus unknown



Intrusion Prevention/Detection Systems

IDS alert: Intruder detected Server hacked Data is altered



Should systems be taken offline?

What was accessed?

What was changed or left behind?

Where did it originate?

Syslog

- De facto logging standard for hosts, network infrastructure devices, supported in all Cisco routers and switches
- Many levels of logging detail available—choose the level(s) which are appropriate for each device/situation
- Logging of ACLs is generally contraindicated due to CPU overhead—NetFlow provides more info, doesn't max the box
- Can be used in conjunction with Anycast and databases such as MySQL (<http://www.mysql.com>) to provide a scalable, robust logging infrastructure
- **Different facility numbers allows for segregation of log info based upon device type, function, other criteria**
- Syslog-ng from http://www.balabit.com/products/syslog_ng/ adds a lot of useful functionality—HOW-TO located at <http://www.campin.net/newlogcheck.html>

Syslog—Sawmill

The screenshot shows the Sawmill 7.0.10 web interface. The browser address bar displays the URL: `http://sawmill.net/cgi-bin/sawmill7/samples/sawmill.cgi?dp+templates.profile.inde`. The page title is "Sawmill 7.0.10" and the profile is "Sawmill Sample Web Log Analysis". The user is logged in as "samples".

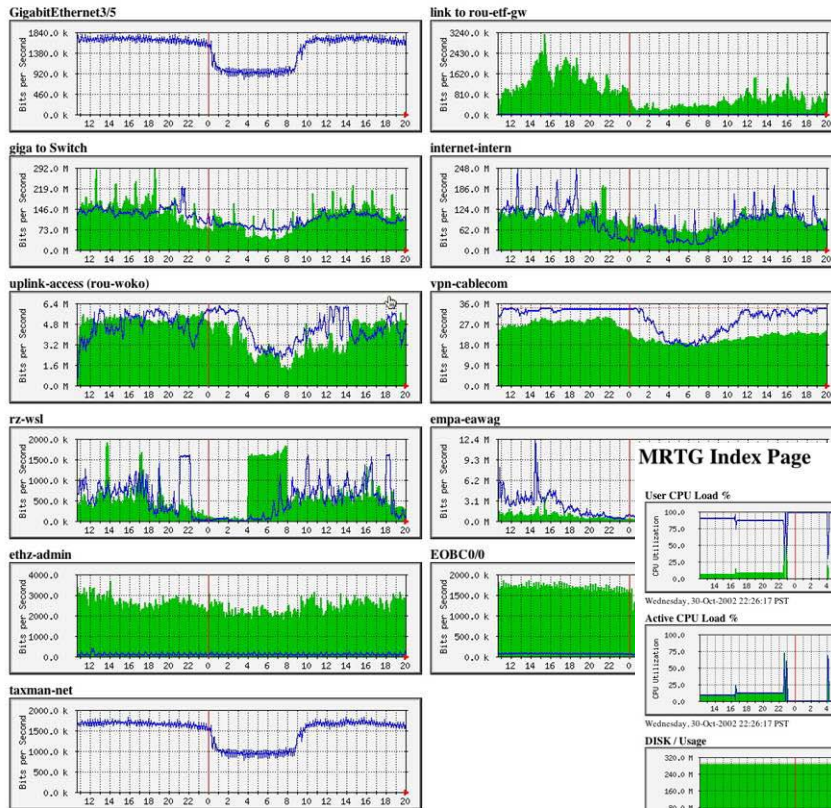
The main content area displays a "Worms" report for the date range "07/Apr/1998 - 31/Mar/2005, 2551 days". The report is circled in orange. The table below shows the statistics for various worms:

Worm	Hits	Page views	Visitors	Size	Percentage
1 Nimda	61,995	61,995	1,087	315.18 M	94.4 %
2 Code Red	4,589	4,589	2,142	17.89 M	5.4 %
3 SharePoint	708	708	274	468.90 k	0.1 %
4 Sasser	157	157	37	360.21 k	0.1 %
Total	67,449	67,449	-	333.87 M	100 %

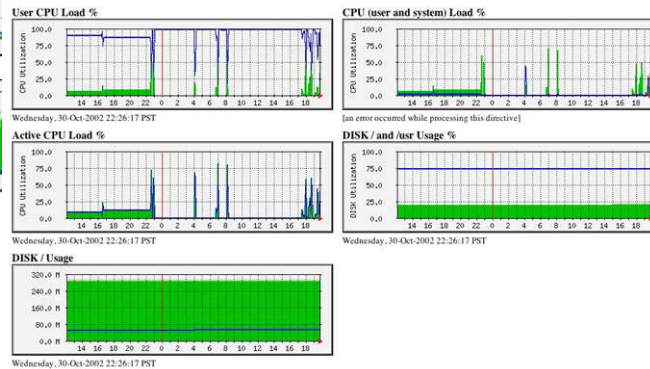
© 2005 Flowerfire

Powerful Visualization of SNMP with MRTG

MRTG Index Page



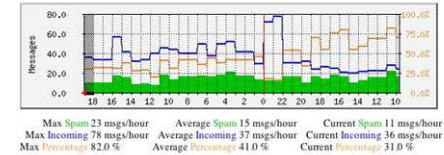
MRTG Index Page



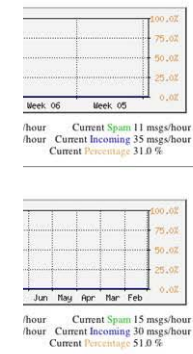
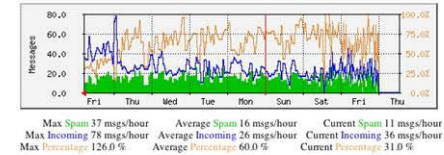
Incoming messages vs. spam per hour

The statistics were last updated Friday, 5 March 2004 at 19:00

'Daily' Graph (60 Minute Average)



'Weekly' Graph (30 Minute Average)



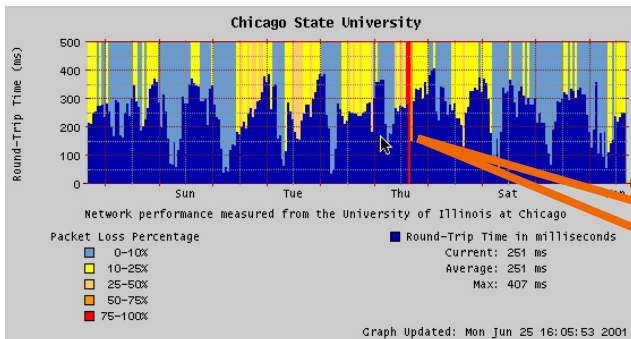
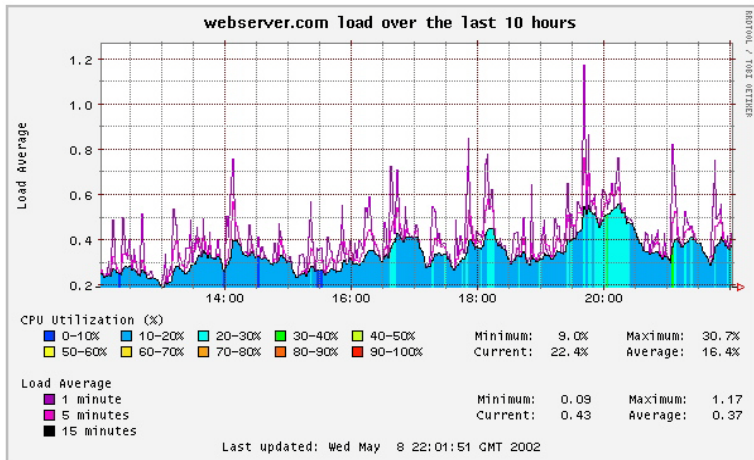
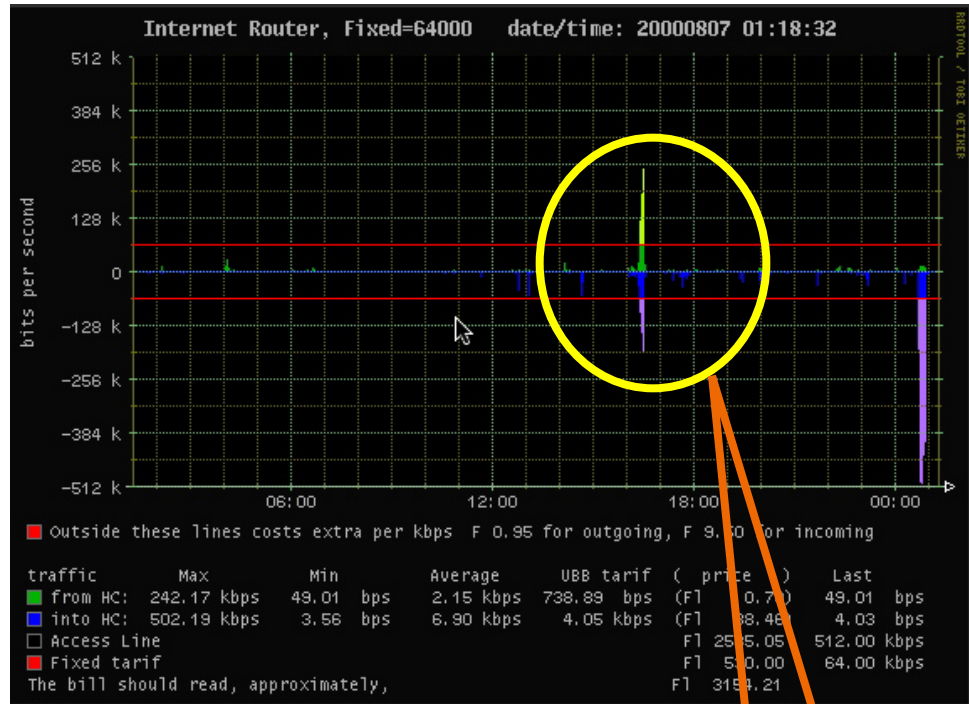
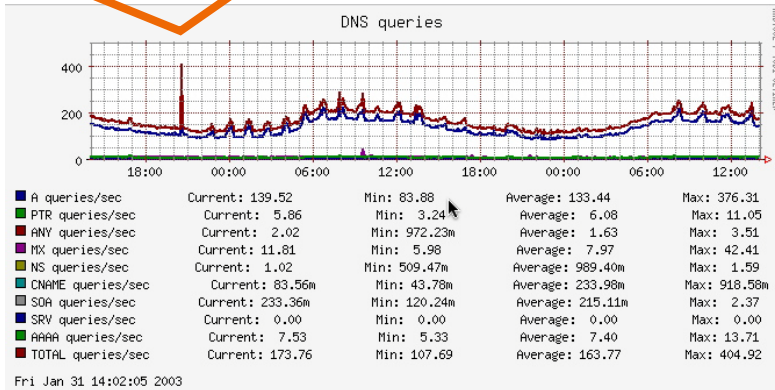
MRTG MULTI ROUTER TRAFFIC GRAPHER
 version 2.10.11
 Tobias Oetiker <oetiker@ee.ethz.ch>
 and Dave Rand <dir@bunji.com>

MRTG MULTI ROUTER TRAFFIC GRAPHER
 version 2.9.4
 Tobias Oetiker <oetiker@ee.ethz.ch>
 and Dave Rand <dir@bunji.com>

Source: <http://oss.oetiker.ch/mrtg/>

Other Visualization Techniques Using SNMP Data with RRDTool

Anomaly for DNS Queries



Thru'put Spike

RTT Spike

Source: <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

Mitigation



Mitigation

- Do Something to Counter the Attack
- Should you mitigate the attack?
 - Where?
 - How?
- No reaction is a valid form of reaction in certain circumstances
- Mitigation often entails more than just throwing an ACL onto a router

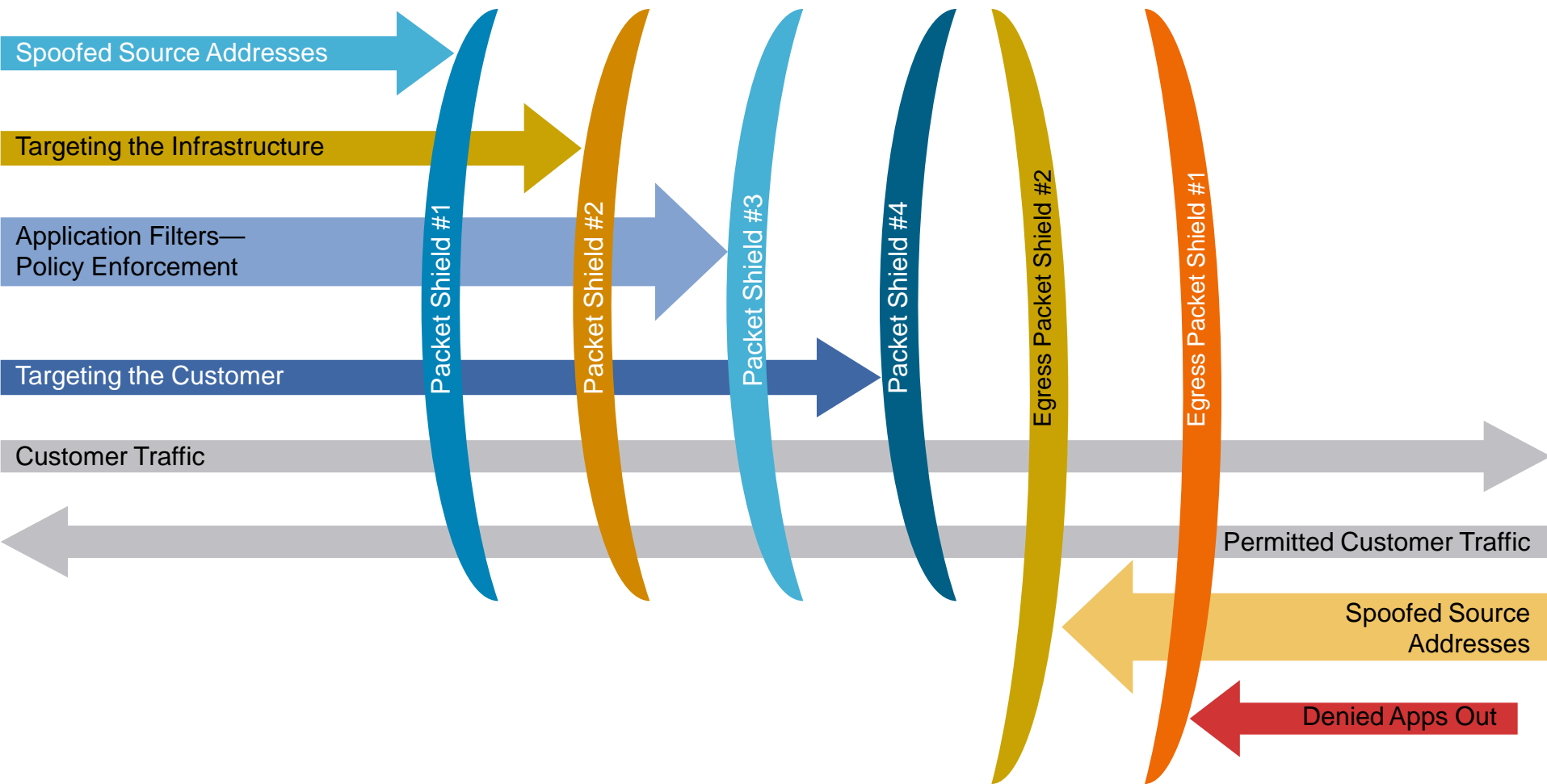
Mitigation Tools

- Access Control
- Spoofing Prevention
- Blackhole
- Sink Hole

Mitigating With ACLs

- Highly-effective deterrent to enforced boundary for Layer 3 and Layer 4 traffic
- Traditional method for stopping attacks
- Default deny ingress/egress will prevent a lot
- Filter as precisely as possible
 - Source and destination (Layer 3 and Layer 4)
- Filter as early as possible in the network

Modular and Phase-Based ACL Policy



Spoofing Prevention

- Minimize attacks that require spoofing
 - SYN Flood
 - Smurf attack
- Attack trace back simplified
- Multiple features exist
 - Access Control Lists (ACLs)
 - Unicast Reverse Path Forwarding (Unicast RPF)
 - TCP intercept (SYN cookies)
 - IP Source Guard (IPSG)*
 - DHCP snooping*

*Detailed Information About Layer 2 Security Is Available in [BRKSEC-2202](#)

Packet Conformance

Several Attacks Use Fuzzed or Irregular Packet Fields to Identify Hosts or Exploit Vulnerabilities or Evade Detection

- Fragmentation overwrite, overlap, short, long (teardrop, jolt, evasion)
- Nmap passive OS identification scanning
- Source routing to evade access control or cause other vulnerabilities
- Abnormal TCP flags, values, overwrite
- Time-to-live (TTL) abnormalities

Blackhole Filtering

- **Blackhole Filtering**, or **Blackhole Routing**, forwards a packet to a router's **bit bucket**

Also known as “route to Null0”

- Works only on destination addresses because it is really part of the forwarding logic
- Forwarding ASICs are designed to work with routes to Null0—dropping the packet with minimal to no performance impact
- Used for years as a way to blackhole unwanted packets

Remotely Triggered Blackhole Filtering

- Use BGP to trigger a network-wide response to attacks
- A simple static route and BGP will enable a network-wide destination address blackhole as fast as iBGP can update the network
- This provides a tool that can be used to respond to security related events and forms a foundation for other remote triggered uses
- Often referred to as RTBH

Flipping RTBH Around

Triggered Source Drops

- Dropping on destination is important
 - Dropping on source is often what we really need
- Reacting using source address provides some interesting options:
 - Stop the attack without taking the destination offline
 - Filter command and control servers
 - Filter (contain) infected end stations
- Must be rapid and scalable
 - Leverage pervasive BGP again

Source-Based Remote Triggered

Blackhole Filtering

- What do we have?
 - **Blackhole Filtering**—if the **destination** address equals Null0, we drop the packet
 - **Remote Triggered**—trigger a prefix to equal Null0 on routers across the Network at iBGP speeds
 - **Unicast RPF Loose Check**—if the **source** address equals Null0, we drop the packet
- Put them together and we have a tool to trigger drop for any packet coming into the network whose source or destination equals Null0

Lessons Learned



Postmortem—the Forgotten Step

- Analyze what worked, what didn't, and what can be improved
- Learn how to protect against repeat occurrences
- Understand if the DoS attack was the real threat or a smoke screen for something else that just happened
- Learn how to make it faster, easier, and less painful in the future
- Gather and understand metrics
 - Resources, headcount, additional information

Summary

- Preparation... Preparation... Preparation...
The KEY to effective handling of Incidents
- Ability to identify anomalies in your network
 - Baselining
 - Monitoring
 - Telemetry
- Being ready with mitigation techniques
 - Access Control
 - Spoofing Prevention



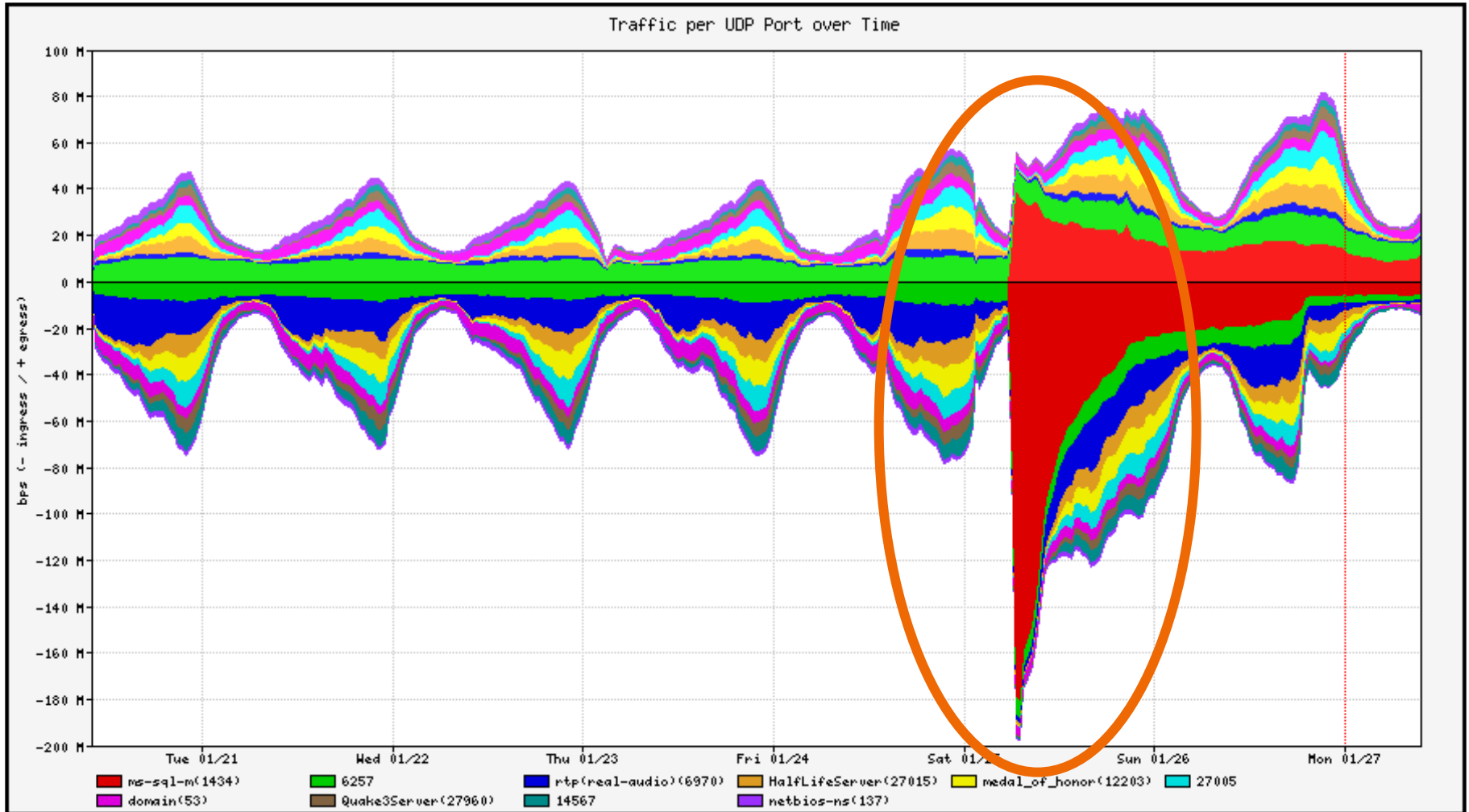
Case Study



Preparation

- People, processes, procedures, lines of communication, architecture, automation/tools all in place *prior to the event* (in the midst of a large attack is not the time to be figuring these things out).
- Security & networking teams work together as a well-oiled machine; no contention over authority, duty manager available 24/7/365 to make business decisions as needed, engineers empowered to do what it takes.
- Professional relationships with PSIRT, TAC/AES, ISPs/peers/customers who run other large networks, participation in FIRST, etc.
- Detailed communications/escalation plan in place and well-understood prior to the event (facilitated by Operations group, used daily).

Detection



Detection

- Using products and technologies such as Netflow and exporting to an anomaly detection systems
- Noted that there was an abnormal (lots of UDP/1434) traffic
- Determined that this was potentially hostile traffic

Mitigation

- Knowledge of our network allowed quick reaction
- Determined all potential vectors of attack (Internet, VPN, Extranet partners, labs, etc)
- Immediately placed a policy on all Internet connections to block UDP/1434 traffic
- Based on the knowledge of the virulence and threat-level caused ACLs to be pushed down to the desktop level in every single Cisco facility worldwide, along with strategically-placed ACLs in our WAN backbone, etc.
- This was all completed within 1 hour of seeing the initial anomaly.

Lessons Learned

- Follow-ups on a daily basis for two weeks to ensure that the threat was eradicated, and discuss lessons learned.
- Direction from management to prioritize & implement lessons learned in concrete, measurable ways, with meaningful follow-up to ensure future success.
- Preparation was key in the quick response.

QUESTIONS



Incident Response Resources -1

Incident Response, Electronic Discovery, and Computer Forensics

www.incident-response.org

Security Focus

www.securityfocus.com

SEI: Handbook for Computer Security Incident Response Teams

<http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf>

CERT/CC: Computer Security Incident Response

<http://www.cert.org/csirts/>

CERT/CC: Responding to Intrusions

<http://www.cert.org/security-improvement/modules/m06.html>

Incident Response Resources - 2

- CIAC: Incident Reporting Procedures
http://www.ciac.org/ciac/CIAC_incident_reporting_procs.html
- FIRST: Forum of Incident Response and Security Teams
<http://www.first.org/>
- IETF: RFC 2196 - The Site Security Handbook (Chapter 5)
<http://www.ietf.org/rfc/rfc2196.txt?number=2196>
- IETF: RFC 2350 - Expectations for Computer Security Incident Response
<http://www.ietf.org/rfc/rfc2350.txt>

Syslog—More Information

- Syslog.org

<http://www.syslog.org/>

- Syslog Logging w/PostGres HOWTO—

http://kdough.net/projects/howto/syslog_postgresql/

- Agent Smith Explains Syslog—

<http://routergod.com/agentsmith/>

- System Event Correlator (SEC)

<http://kodu.neti.ee/~risto/sec/>

- Cisco CS-MARS

<http://www.cisco.com/en/US/products/ps6241/index.html>

SNMP—More Information

- Cisco SNMP object tracker—

<http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4>

- Cisco MIBs and trap definitions

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

- MRTG

<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

DNS—More Information

- dnstop home—
<http://dns.measurement-factory.com/tools/dnstop/>
- dnslogger home—
<http://www.enyo.de/fw/software/dnslogger/>
- Kunamoto University Papers on DNS-based Detection
<http://www.cc.kumamoto-u.ac.jp/~musashi/musashicsec27.pdf>
<http://www.cc.kumamoto-u.ac.jp/~musashi/dsm32-12.pdf>
- Dan Kaminsky on DNS as a Covert Channel
http://www.doxpara.com/dns_bh
- DNS as an IDS
<http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf>
- Detecting Mass-Mailing Worms via DNS
<http://www.sigcomm.org/sigcomm2005/paper-IshToy.pdf>

NetFlow—More Information

- Cisco NetFlow home

<http://www.cisco.com/warp/public/732/Tech/np/NetFlow/>

- Linux NetFlow reports HOWTO

<http://www.linuxgeek.org/NetFlow-howto.php>

- Arbor Networks Peakflow SP and Peakflow/X

<http://www.arbornetworks.com>

- nfdump and nfsen

<http://nfdump.sourceforge.net>

<http://nfsen.sourceforge.net>

- Stager

<http://software.uninett.no/stager/>

BGP—More Information

- Slammer/BGP analysis—

http://www.nge.isi.edu/~masseyd/pubs/massey_iwdc03.pdf

- Team CYMRU BGP Tools—

<http://www.cymru.com/BGP/index.html>

- Packet Design Route Explorer—

<http://www.packetdesign.com/products/rex.htm>

- Team CYMRU BGP Tools—

<http://www.cymru.com/BGP/index.html>

spoofing References

- Understanding Unicast Reverse Path Forwarding
<http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html>
- Tracking Spoofed IP Addresses
<http://www.cymru.com/Documents/tracking-spoofed.html>
- Bogon Reference
<http://www.team-cymru.org/Services/Bogons>
- Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing, RFC2827
<http://tools.ietf.org/html/rfc2827>
- Ingress Filtering for Multihomed Networks, RFC3704
<http://tools.ietf.org/html/rfc3704>