SUMMARY

Using the mobile monitoring and network rack, the Cisco CSIRT provided secure and fast conference and management networks for the 20th annual FIRST conference in Vancouver, British Colombia in June 2008. Many Cisco security technologies were deployed that blocked thousands of malicious connections to and from Internet hosts and websites. The CSIRT managed the reliable, secure Cisco network along with a highly visible showcase of Cisco security products to hundreds of international security professionals.

BACKGROUND

FIRST (http://www.first.org) is the premier organization and recognized global leader in incident response. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. FIRST conferences promote worldwide coordination and cooperation among Computer Security Incident Response Teams (CSIRTs). The conference provides a forum for sharing goals, ideas, and information on how to improve global computer security. The Cisco CSIRT is a member of the FIRST organization, having participated as the Cisco representative for the last 10 years.

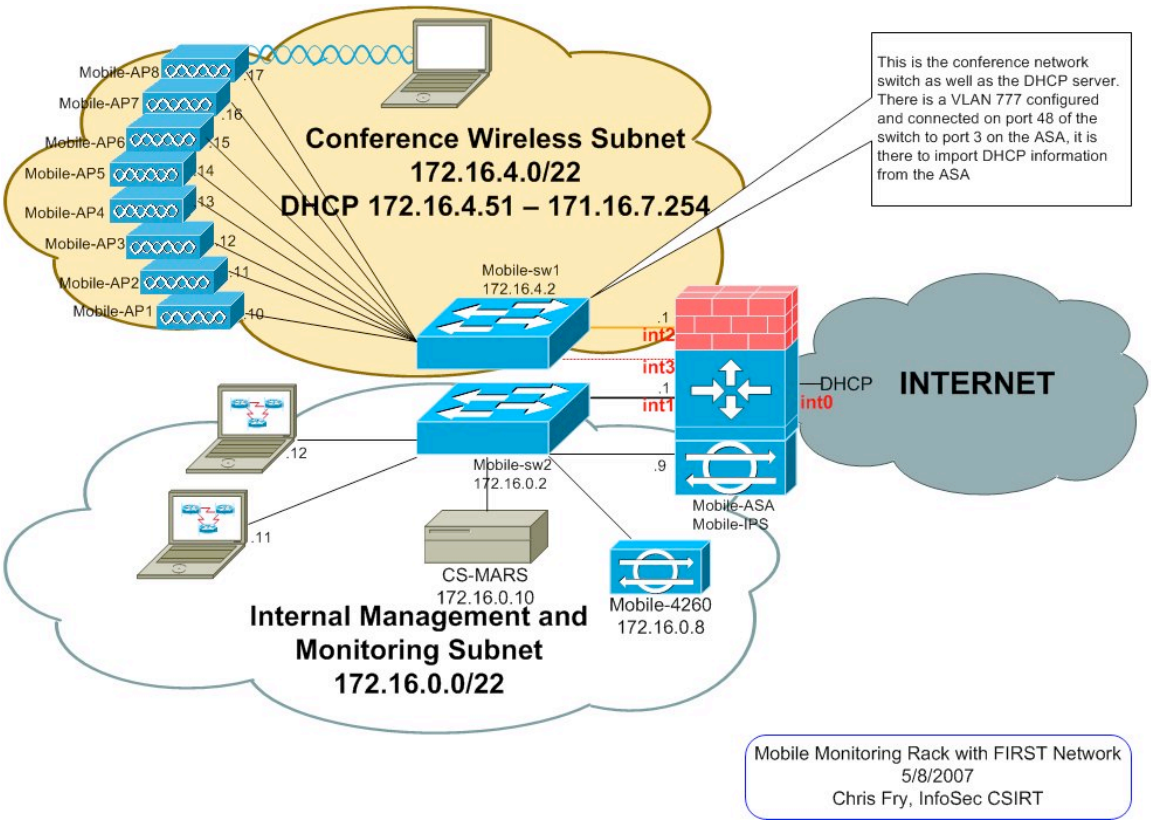
THE NETWORK

Recently, Cisco became the network sponsor with CSIRT team members providing secure network access and security services for the conference. This provides both a much appreciated service for the FIRST conference attendees and an opportunity for customers to see Cisco products in action including:

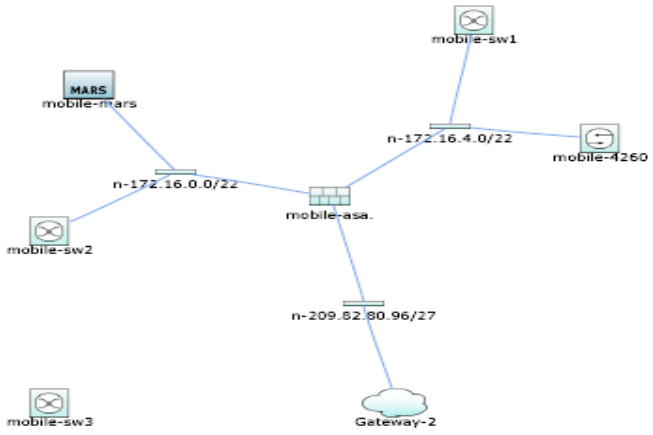
- Cisco 3750 series switches
- Cisco 1100 and 1200 series 802.11b/g/a wireless access points
- Cisco ASA 5510 with AIP module (IPS)
- Cisco IPS 4260
- Cisco CS-MARS
- Ironport 650 Series appliance

The conference hotel provided a 100 Megabit connection to the Internet where attendees experienced speeds of up to 80Mbps in both directions. Both a wired and wireless network was deployed using the hotel's existing CAT5 infrastructure. This network provided attendees with secure access via switched network as well as a wireless network available throughout the conference areas secured with WPA using 16 different Cisco wireless access points across four floors of the hotel. Extra switches for hardwired connections were also provided for the conference registration desk as well as the steering and planning committee boardrooms. The CSIRT mobile rack consists of two VLANs, one for management and monitoring and the other separate network for the conference attendees.

Here's a logical diagram of how the conference networks are setup using the mobile monitoring/networking rack:

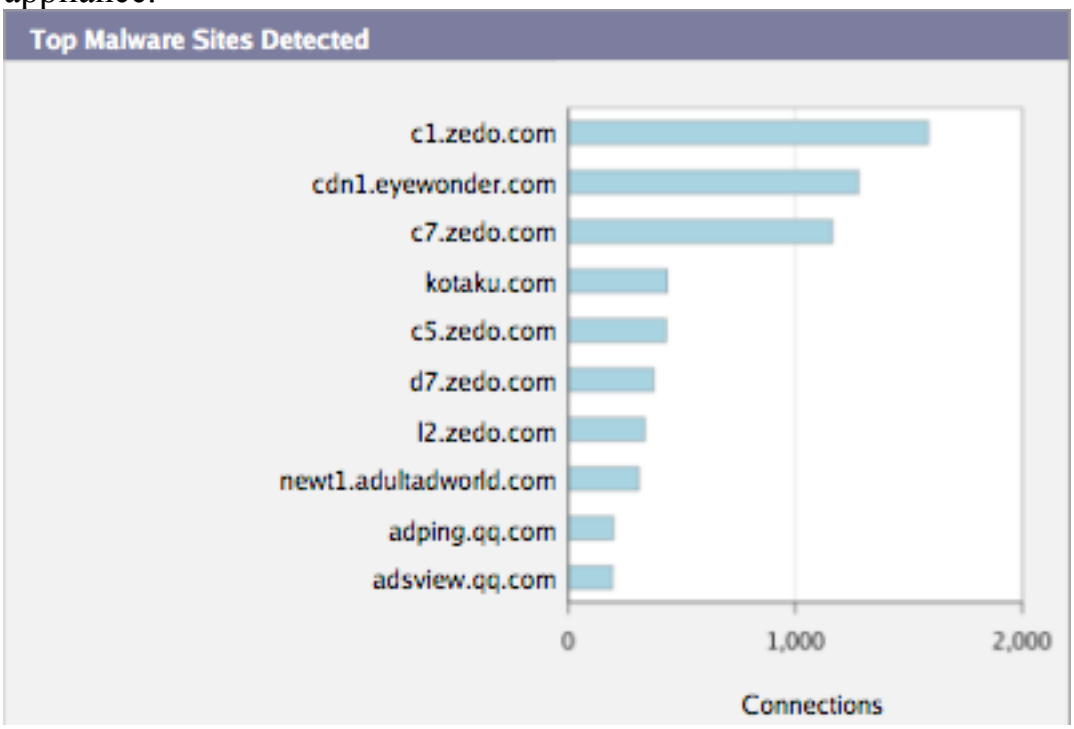


Here is the visualization created automatically by CS-MARS with all the security and network devices loaded:

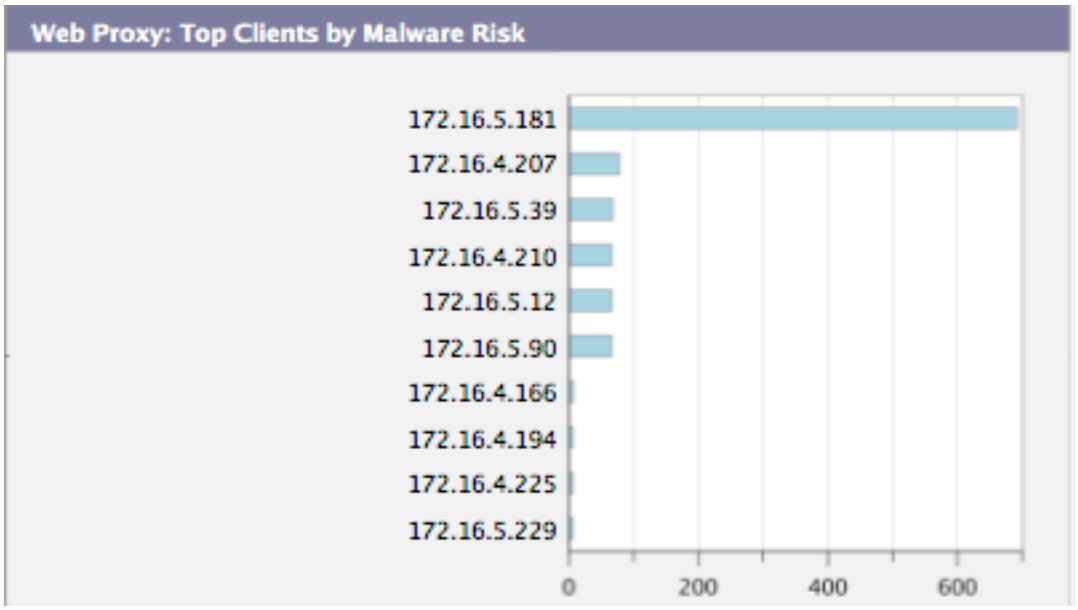


NETWORK SECURITY

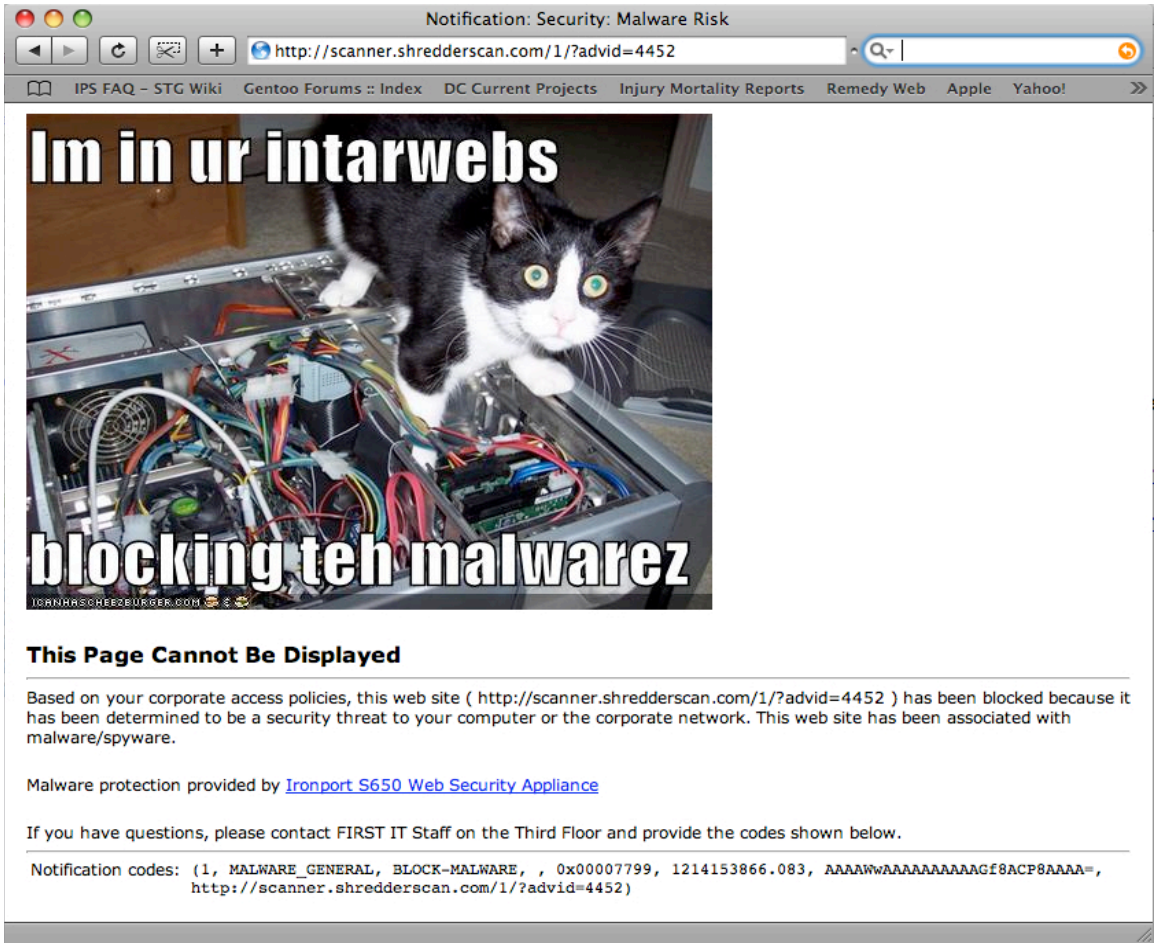
The CSIRT setup the Ironport Web Security Appliance to act as a secure web proxy for the attendees on the conference network. In order to maintain a high availability network and to avoid support issues, only the highest fidelity ratings for malware sites were set to "block" while the rest were simply set to "monitor" only. Here's a sample of one day's malware activity on the conference network as detected and blocked by the Ironport appliance:



We can also see the actual internal host addresses making connections to these malicious sites/domains through the web:



We detected quite a few connections to confirmed malicious sites that were automatically blocked by the WSA. We created a custom webpage for the attendees when they were redirected away from a known malware site, thus thwarting the malicious banner ads, javascript, active X, and trojans:



The WSA blocked several attempts by clients to download actual trojans from malicious websites. Sites hosting invisible "iframes" that load malicious javascript can force a browser to download a trojan backdoor onto their system. Without appropriate host based controls, conference attendees would have been infected without the protection of the Ironport web security appliance. We detected several attempts of sites trying to force malware onto client systems, like the Trojan-Downloader.Win32.Agent.ljx

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=144165

that were all dropped by the WSA.

In addition to the Ironport malware filtering, we also showcased Cisco IDS to detect other types of network-based attacks on the conference network. Most attendee traffic on the conference network traversed individual secure VPN tunnels so much of the traffic was obfuscated from inspection. We did not detect any major malicious activity directed towards the conference

network protected by the Cisco ASA firewall. However we did see attempts by attendees to connect to each other internally using NetBIOS "exploits" as well as some file sharing traffic and a few instances of clear-text POP (email) logins.

In one case an attendee intentionally left their Windows file share "open". This open folder was apparently abused by some other attendees and was documented here:

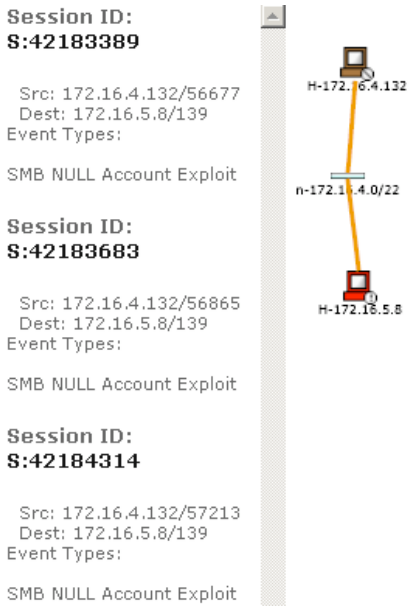
http://security.itproportal.com/articles/2008/06/25/youve-been-hacked-lessons-be-learnt/

We actually detected these attacks with our Cisco IDS as "SMB Login successful with Guest Privileges" (https://intellishield.cisco.com/security/alertmanager/signatureDetail.do?dispatch=4&signatureId=3303&signatureSubId=0)

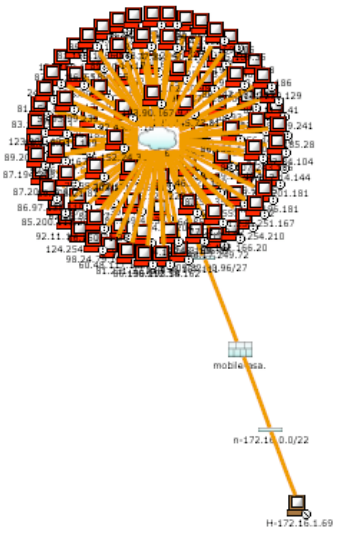
and "SMB NULL Account Exploit"

(https://intellishield.cisco.com/security/alertmanager/signatureDetail.do?dispatch=4&signatureId=5577&signatureSubId=0)

However we did not block these NetBIOS connections automatically as they do have some, albeit limited legitimate use in normal system/network environments, and its better not to block traffic on the diverse conference network without a clear-cut case of abuse or attack.

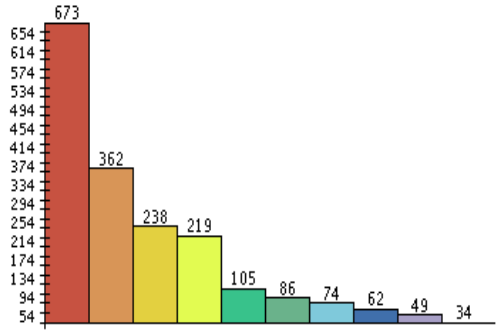


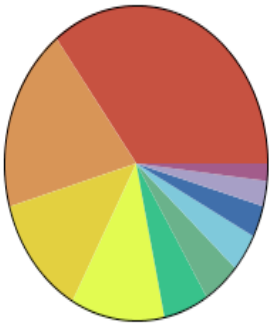
There was also a significant amount of peer-to-peer file sharing traffic on the network as well as is indicated in this MARS visualization:



The host towards the bottom (172.16.1.69) is connected to a Bittorrent swarm on the Internet (the large circle of interconnected hosts towards the top of the image.)

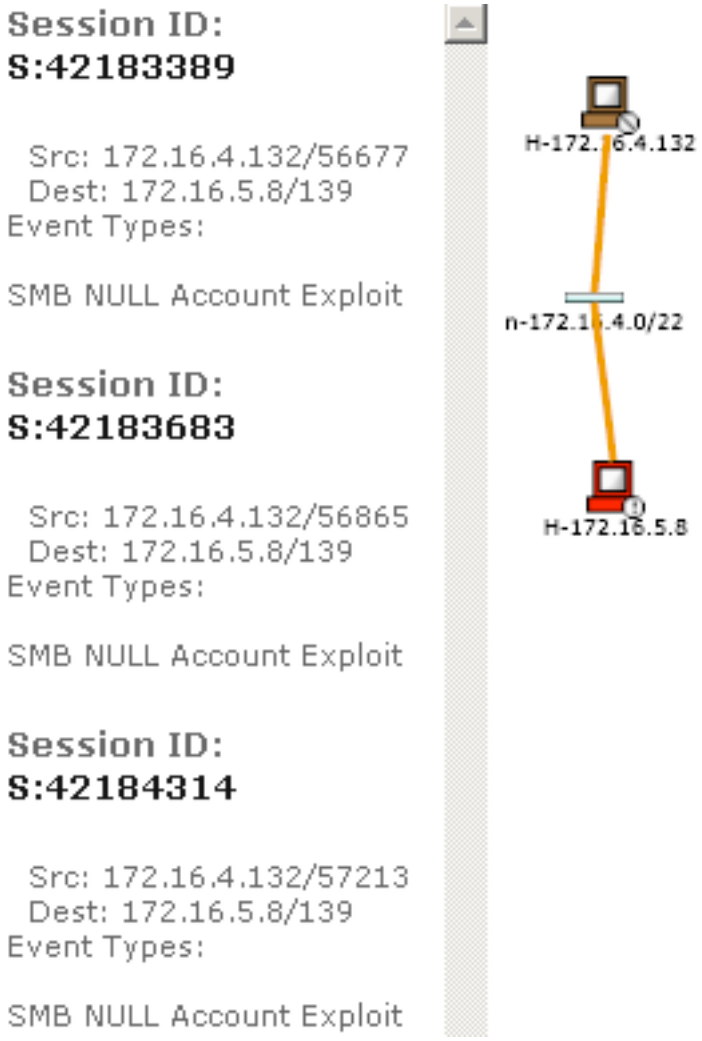
Here's an example of the conference network traffic as sampled directly from CS-MARS. Below are the top ten "rules" that fired during the duration of the conference:





Rank	Count (# of Incidents)	Name	Description
1	673	System Rule: Network Activity: P2P File Sharing - Active	This rule detects person-to-person file sharing activity via applications such as KaZaa, Napster, EDonkey, Gnutella, Bearshare et
2	362	System Rule: Server Attack: Misc. - Attempt	This correlation rule detects attacks on miscellaneous services (i.e. other than DNS, FTP, HTTP, Mail, FTP, RPC, Telnet, SSH, R-protocols) on a host, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial of service attempts etc.
3	238	System Rule: Network Errors - Likely Routing Related	This rule detects a large frequency of denied packets or ICMP destination unreachable events between the same source, destina pair - this may indicate a network routing error and may be caused by periodic retransmission attempts by TCP or the applicatio itself (e.g. DNS).
4	219	System Rule: Server Attack: RPC - Attempt	This correlation rule detects attacks on RPC services on a host, preceded by reconnaissance attempts targeted to that host, if ar The attacks include buffer overflows, remote command execution attempts, privilege escalation attempts to become root, denial service attempts etc.
5	105	System Rule: Server Attack: Web - Attempt	This correlation rule detects attacks on a web server, preceded by reconnaissance attempts targeted to that host, if any. The att include buffer overflows, remote command execution attempts, denial of service attempts etc.
6	86	System Rule: Client Exploit - Attempt	This rule detects a client workstation exploit - this means a workstation is either downloading executable content via Web or em or sending web requests that contain scripts or is the target of an (client side) exploit via protocols such as IRC, DHCP, DNS, P2 Worms.
7	74	System Rule: Password Attack: Mail Server - Attempt	This correlation rule detects a password guessing attack on a mail server (SMTP, POP, IMAP), preceded by reconnaissance attack the host, if any. A password guessing attack consists of multiple login failures and may sometimes be caused by a user forgettin the password.
8	62	System Rule: Misc. Attacks: Evasion	This correlation rule detects generic attempts by an attacker to bypass network IDS systems. The attempts may be preceded by reconnaissance attempts to that host.
9	49	System Rule: Network Activity: Chat/IM - Active	This rule detects person-to-person Chat or Instant Messenger protocol activity.
10	34	System Rule: Server Attack: Database - Attempt	This correlation rule detects attacks on a database server, preceded by reconnaissance attempts targeted to that host, if any. Th attacks include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.

Many of these events in the MARS reports were simply authentication failures, although there did appear to be some malicious activity on the conference network like the RPC overflows and NetBIOS attacks.



I:42876465	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 9:35:19 AM PDT - Jun 27, 2008 9:37:04 AM PDT
I:42876462	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 9:29:19 AM PDT
I:42876459	TOR Client Activity	System Rule: Misc. Attacks: Evasion		Jun 27, 2008 9:18:10 AM PDT - Jun 27, 2008 9:22:14 AM PDT
I:42876454	TOR Client Activity	System Rule: Misc. Attacks: Evasion		Jun 27, 2008 9:17:10 AM PDT
I:42876455	IE HTTPS Proxy Information Disclosure	System Rule: Server Attack: Web - Attempt		Jun 27, 2008 9:16:52 AM PDT
I:42876449	IE HTTPS Proxy Information Disclosure	System Rule: Server Attack: Web - Attempt		Jun 27, 2008 8:57:41 AM PDT
I:42876444	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 8:44:19 AM PDT - Jun 27, 2008 8:49:03 AM PDT
I:42876441	TOR Client Activity	System Rule: Misc. Attacks: Evasion		Jun 27, 2008 8:42:23 AM PDT - Jun 27, 2008 8:43:24 AM PDT
I:42876440	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 8:41:16 AM PDT - Jun 27, 2008 8:43:03 AM PDT
I:42876439	TOR Client Activity	System Rule: Misc. Attacks: Evasion		Jun 27, 2008 8:41:21 AM PDT
I:42876438	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 8:35:16 AM PDT - Jun 27, 2008 8:38:40 AM PDT
I:42876436	Microsoft Windows Vista DHCP Request Processing Denial of Service Vulnerability	System Rule: Server Attack: Web - Attempt		Jun 27, 2008 8:37:13 AM PDT
I:42876434	SMB NULL Account Exploit	System Rule: Server Attack: RPC - Attempt		Jun 27, 2008 8:33:30 AM PDT

Conclusion

In addition to the assurance of a secure network, these benefits can be attributed to CSIRT's monitoring of the 20th annual FIRST conference in Vancouver, BC:

- Showcasing some of CSIRT's highly effective security monitoring capabilities.
- Tested and learned capabilities of the Ironport web security appliance for the first time, providing us with eventual feedback to the business unit and for consulting on any potential internal deployments.
- Provided kiosk with read-only views into security reporting and detection from the conference network using CS-MARS, Ironport S650, Cisco IDS, ASA, etc. demonstrating how Cisco products can be used effectively for on-demand monitoring.
- Building and supporting a reliable and secure conference network in just days garnered many thanks and kudos from attendees from various companies and organizations around the globe.