

# The Evolution of Information Security at Wayne State University

**Nathan W. Labadie**

**ab0781@wayne.edu**

**Sr. Systems Security Specialist**

**Wayne State University**

# A Bit of Background

---

- Covers mid-2000 to present.
- Moved from virtually no information security infrastructure to a fairly modernized design.
- Discussion of growing pains and major steps taken along the way.
- Where we were, where we are, and where we are going.

# In The Beginning: 2001



# In The Beginning: 2001

---

- No real information security infrastructure.
- Monitoring primarily consisted of SNMP statistics and sniffing our Internet uplink if there was a problem.
- No major worms or DoS attacks, just the occasional email to the abuse address.
- Information security was 100% reactive.

# In The Beginning: 2001

---

- Network anomaly detection consisted of looking for spikes on MRTG graphs.
- A packet sniffer would be used against the uplink if anything seemed strange.
- Relatively simple to identify hosts that were using excessive bandwidth or causing problems.

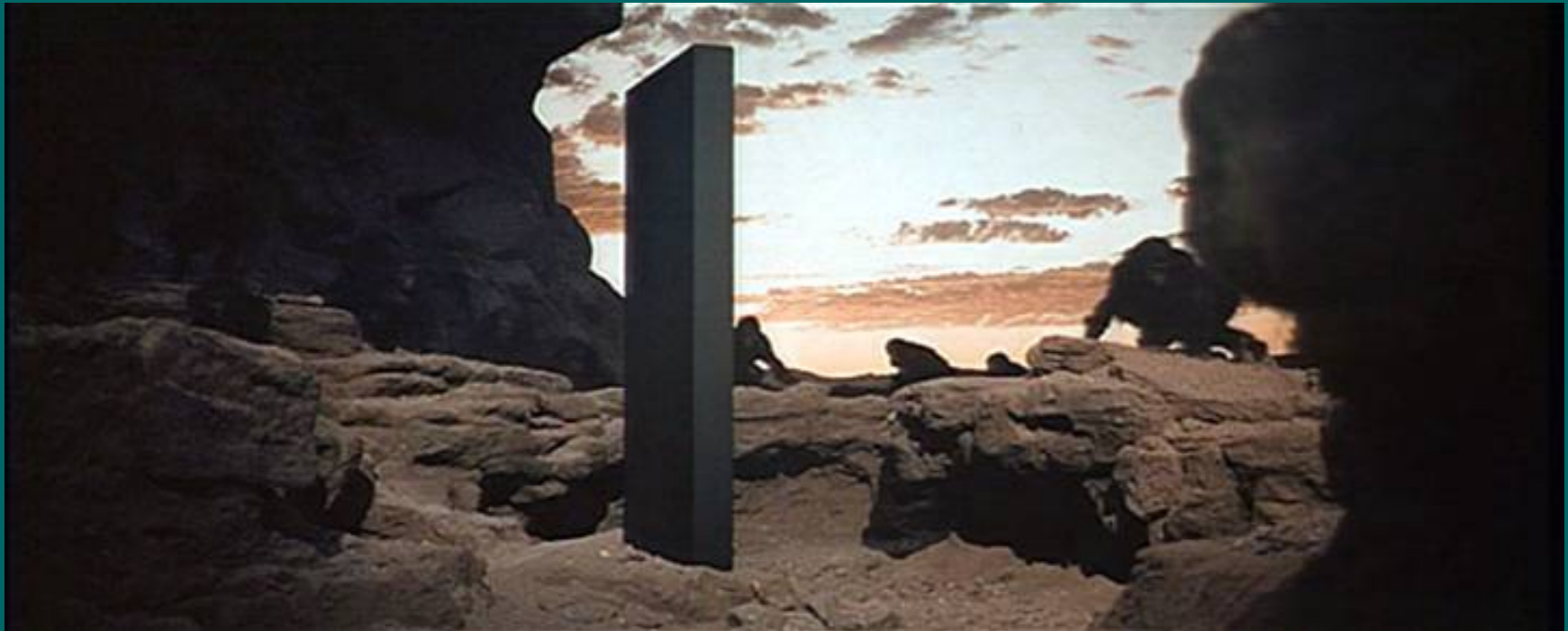
# In The Beginning: 2001

---

- Not a single network firewall on campus.
  - All information security was done on the host.
  - Editing inetd.conf and disabling telnet was considered “good” information security.
- When a host was hacked, it was restored from the last known good backup and put back online.
  - Wash, rinse, repeat.

# The First Step

---



# The First Step: 2001

---

- Began running a Snort IDS against a mirror of our Merit link “just to see”.
  - Much more malicious activity than we had anticipated.
    - Lots of IRC bots and FTP warez hosts.
    - No major Windows worms, yet.
- Most importantly, the IDS provided us with statistics and data that could be presented to management.
  - Allowed us to make a case for funding.

# Firewall Implementation: 2001

---

- Decided on Netscreen firewalls after evaluating performance and cost.
  - Implemented one at the perimeter and another for production services.
  - In many instances, security was still viewed as secondary to user convenience.
  - Most policies still left hosts behind the firewall wide open to attacks.

# Production Services Firewall: 2001

---

- Added the firewall as the default gateway for the production services network.
- Initial policy was set to default open.
  - Gained management's approval and worked through the list of hosts on the network.
  - All of the administrators were required to provide a list of rules for their hosts.
  - Required lots of cooperation between departments for successful implementation.

# Perimeter Firewall: 2001

---

- Operated in passive mode in front of 11,000 hosts on the University network.
- Initially served no major purposes.
  - Filters were added for compromised hosts.
  - Minor integration with the Snort IDS.
  - All ports were left open by default.
  - Rules were only added by requests from the department administrators.

# Worms Galore: 2001 - 2002

---

- A large number of worms and viruses plagued the network from 2001 – 2002.
  - Code Red, Code Red II, Sadmind, Nimda, etc.
  - Virtually all departments were impacted.
  - Served as a wake-up call to the overall state of security on the University network.
  - 200-250 infected hosts at one point.

# Worms Galore: 2001-2002

---

- Many of the hosts were backdoored with bots and denial-of-service agents.
  - Experienced DDoS attacks on a daily basis for several weeks.
    - Frequently crippled the network.
- Disruptions and downtime brought about a fundamental shift in policy.
  - Everyone agreed that changes needed to be made to prevent this from happening.

# The Next Steps

---



# Major Policy Change: 2002

---

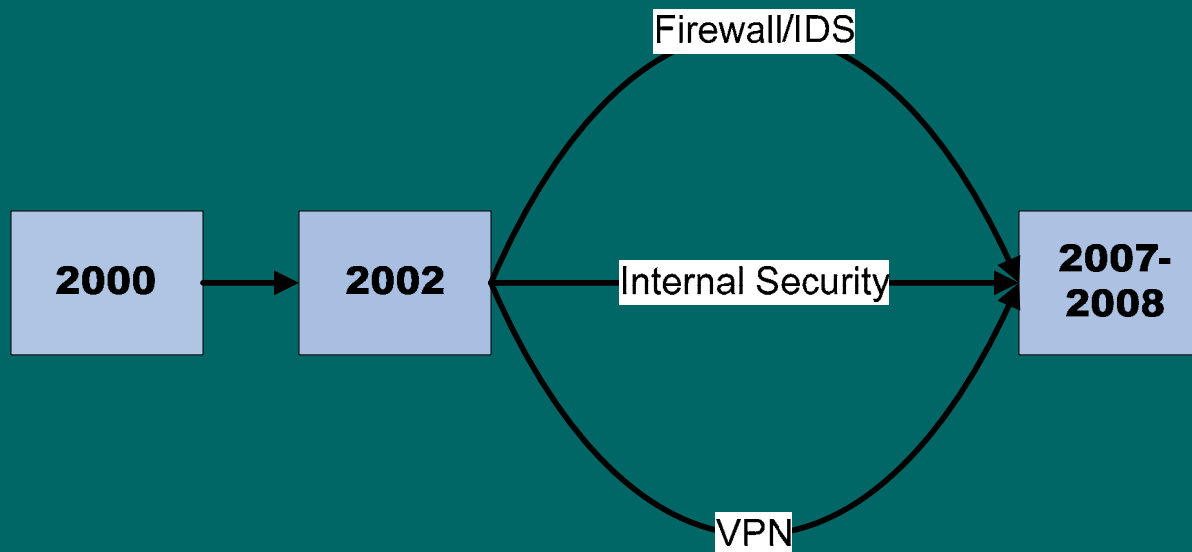
- Given a green light to block “problematic” services at the edge of the network.
  - Primarily included Windows services.
- Allowed us to focus on problems internal to the University network.
  - Implemented a Nessus server and conducted regular scans for specific vulnerabilities.
  - Administrators were notified of potential problems on their network.

# Information Security: 2002 - Present

---

- Growth and development in 3 major areas:
  - Firewall and IDS.
  - Internal Security.
  - VPN technology.
- Involved finding a balance:
  - Academic freedom.
  - Information security.
  - Ease of use.

# Information Security: 2002 - Present



# Firewall and IDS: 2002 - 2006

---

- Overall implementation was a success.
- New problem: where's *my* firewall?
  - Departments across campus decided they wanted their own departmental firewalls.
- Standardized on Netscreen firewalls.
  - No standardized process for deciding if a department-level firewall is required.
  - Cost forces many departments to reconsider.
  - Firewall management software allows responsibilities to be delegated.

# Firewall and IDS: 2006 - Present

---

- Port and host-based security was no longer sufficient enough.
- Migrated to Juniper firewalls with inline IDS capability.
  - Added for both perimeter and production.
  - Allows services to be exposed while still protecting from exploits.
  - Greatly reduced the amount of malicious traffic entering the campus network.

# VPN Implementation: 2002 - 2004

---

- VPN functionality was added to allow access restricted by the firewall change.
- Original VPN required a client install.
  - Terminated at the firewall.
  - Required a separate policy for each user.
  - Was painful to maintain and support.
  - Client only ran on Windows.

# VPN Implementation: 2004 - Present

---

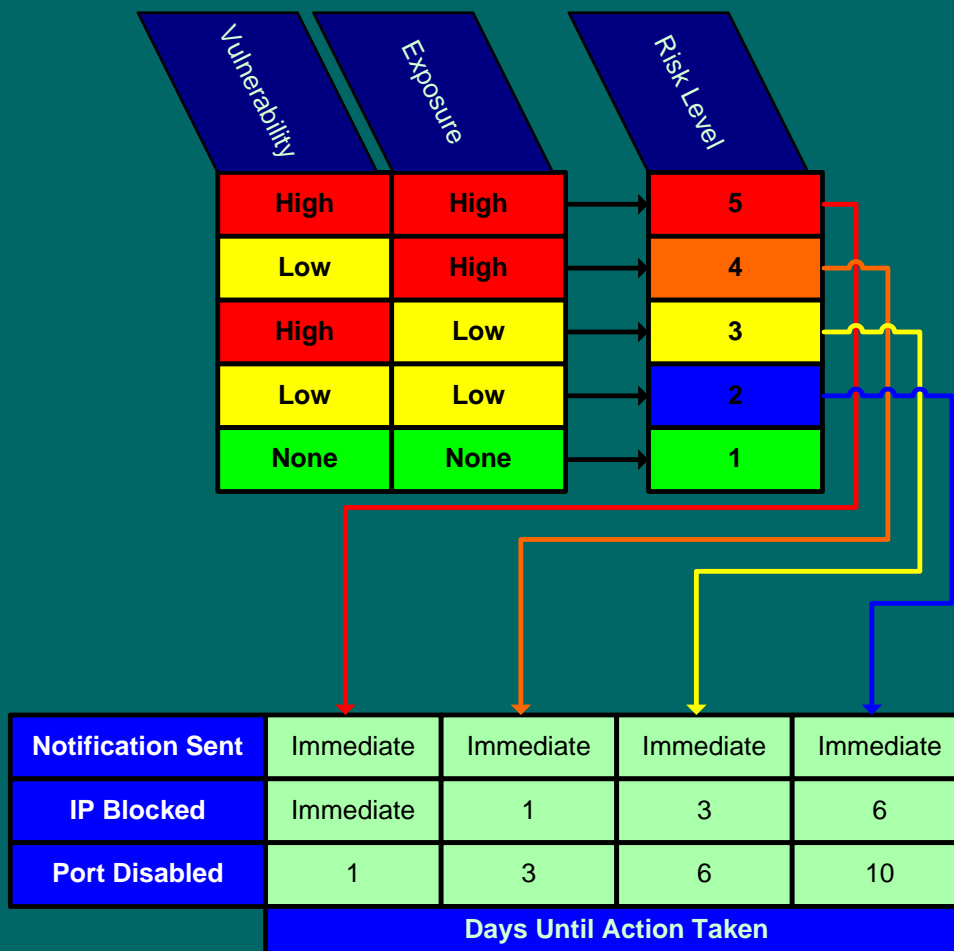
- Migrated from a client VPN solution to a web-based VPN solution.
  - Increased availability and lowered support costs for the VPN.
  - Supports all major operating systems.
  - Provides both a web interface and a Java-based IPSEC client.
  - Ties directly into our campus LDAP directory.
  - Used extensively by both staff and faculty.

# Internal Security: 2002 - Present

---

- Three recourses for compromised hosts on the campus network:
  - Notify the administrator of the problem.
  - Block the host at the edge of the network.
  - Disable the physical port for the host.
- Recourse depends on the severity of the problem and significance of the host.
- Process has not changed significantly.

# Internal Security: 2002 - Present



# Internal Security: 2003 - Present

---

- Nessus server available for internal use.
  - Essentially free to use.
  - Accounts are provided upon request to administrators across campus.
  - Usage is restricted to the admin's subnet.
  - Sweeps of the network are routinely conducted for specific vulnerabilities.
  - Comprehensive scans of production services are conducted every three weeks.

# Internal Security: 2006 - Present

---

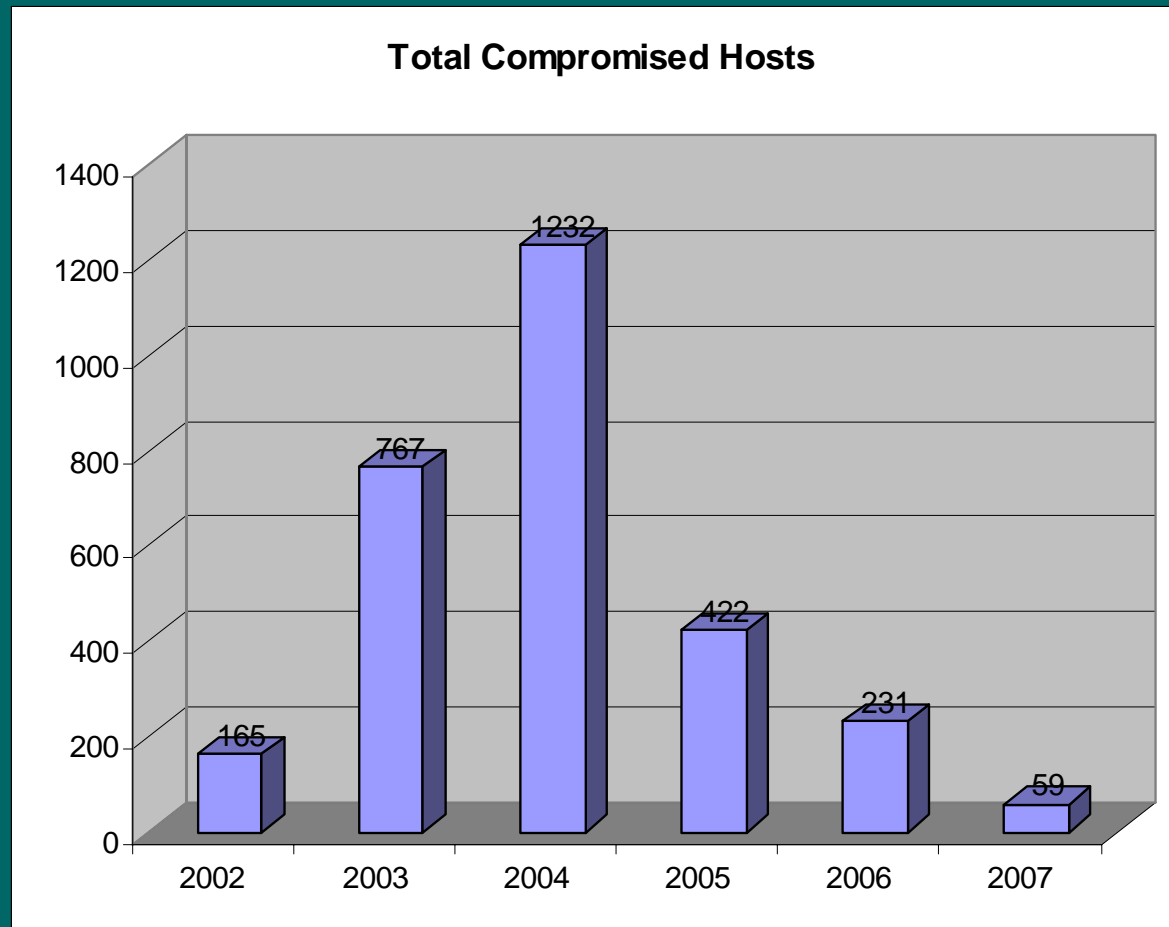
- Implemented a honeynet using honeyd.
  - One single host assumes the identity of ~60 different operating systems.
  - Given a /26 network of routable addresses.
  - Extremely useful for finding hosts on the internal network that are scanning.
  - Also useful for finding the “latest and greatest” when it comes to new worms and scans.
  - Firewall IDS rules are modified accordingly.

# Internal Security: Present

---

- In 2007 we began restricting incoming traffic at the perimeter of the network.
  - Still in progress.
  - Done on a subnet-by-subnet basis.
  - Administrators are give 2-4 weeks notification to register hosts that require external access.
    - Actively encourage users to utilize the VPN.
  - Created a web-based form for requesting rules that need to be added.

# Internal Security: The Results



# Information Security: Future Direction

---

- Focus is tying together large amount of information from multiple sources.
  - Logs from the honeynet, IDS, firewall, hosts, netflows, taps, etc.
- Quickly becoming impossible to manage all of the data and logs.
  - Only the most obvious is noticed.
  - Much of the data between 5:30PM and 9:00AM manages to slip through.

# Information Security: Future Direction

---

- Recently settled on QRadar by Q1 Labs.
  - Primarily used for network anomaly detection and security event management.
  - Provides the ability to “look back” at previous network traffic in the event of a compromise.
    - No longer have to assume worst-case scenario.
  - Ties together multiple information sources into a single interface.

# Questions?

---

## Contact information:

Nathan W. Labadie

ab0781@wayne.edu

313-577-2126