

# The Past, Future & Evolution of IPS

Mike Swarm  
Security Solutions Engineer  
Juniper Networks  
mswarm@juniper.net



# Outline

---

- Introduction
  - Who am I?
  - Why am I qualified to talk about this topic?
- Remember the old days?
  - Network IDS 1.0
  - Host Based IDS 1.0
- Where we are now?
  - Network IPS 2.0
  - Host Based IPS 2.0
- What is the future?
  - Network IPS 3.0
  - Host Based IPS 3.0

# Introduction

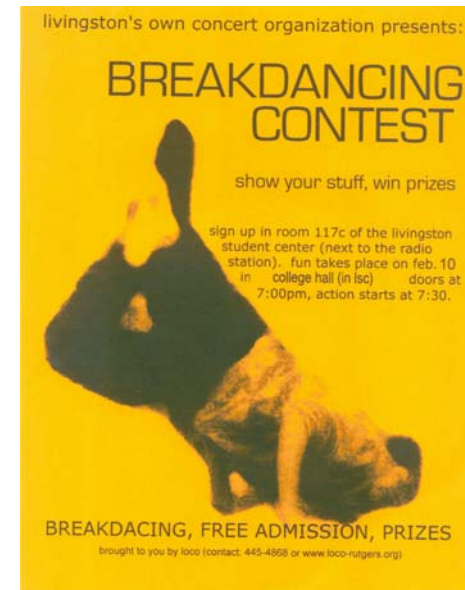
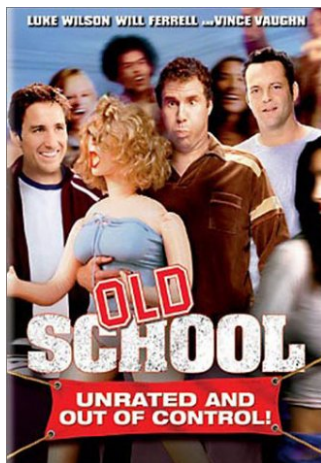
---

- Who am I?
  - Security Solutions Engineer, Juniper Networks
  - End customer consulting background
  - Published author
- Why am I qualified to talk about this topic?
  - 10+ years computer network security
  - Consult ~725 end customer opportunities
  - Volunteer InteropNet

# Remember The Old Days?



Going Old School



Juniper your Net

# Remember The Old Days?

---

- o Network Based IDS 1.0
  - o Detected attacks in real time
  - o False positive / management hell
  - o Bypassed easily
- o Remember 'GET /vuln.id%u0061 HTTP/1.0'
  - o IDS expected to see 'GET /vuln.ida HTTP/1.0'
- o Unicode
- o Hex encoding
  - o GET %65%74%63/%70%61%73%73%77%64
  - o GET etc/passwd
- o Really bad DoS Signatures
- o Night of a thousand //////////////////////////////////
- o Polymorphic shellcode

# Remember The Old Days?

---

- Session splicing
  - Attack string divided among multiple packets
    - Packet 1: G
    - Packet 2: E
    - Packet 3: T
    - Packet 4: /
    - Packet 5: v
    - Packet 6: u
    - Packet 7: l
    - Packet 9: n
    - And so on...

# Remember The Old Days?

---

- Fragmentation attacks
  - Fragmentation Overlap
    - Packet 1: GET vuln.idd
    - Packet 2: a? <big buffer>
  - Fragmentation Overwrite
    - Packet 1: GET vuln.id
    - Packet 2: <random characters>
    - Packet 3: a? <big buffer>
  - Lots of other examples.
- Great article from 2002
  - <http://www.securityfocus.com/infocus/1577>

# Remember The Old Days?

---

- Network Based IDS 1.0 "Cool Features"
  - IDS "signaling" to routers or firewalls
  - Connection dropping
  - Attack capture abilities
  - Remember counter attacking?

# Remember The Old Days?

---

- Network Based IDS 1.0 Usage Scenarios
  - Reactive alerting
    - "Something really bad happened on the network last night. It was horrible I saw the whole thing!"
  - Basic incident response assistance
    - Partial network traffic capture
  - Penetration tests or vulnerability assessments
    - Some service providers use these as validation of attacks sent

# Remember The Old Days?

---

- Host Based IDS 1.0
  - Basically log analysis + signatures
  - System resource intensive
  - No AV
  - Immature firewall capabilities if any
  - Bypassed easily
- Log Analysis
  - 1 event ok
  - 10 events alarm
  - So trip less events in your attack
  - Better yet, simply turn it off
- File Monitor
  - Doesn't cover temp directories

# Remember The Old Days?

---

- Obfuscation Attacks

- Very similar to Network IDS evasion plus some twists such as:
  - Double slashes: /winnt///repair///SAM.\_
  - Self referencing directories: /winnt/../../../../repair/../../../../SAM.\_
  - Reverse traversal: /temp/../../winnt/repair/SAM.\_

- Really loooooong commands

- Variables

- Old school Host IDS had issues
  - set hacked=c:\winnt\system32\  
set youare=\cmd.exe  
%hacked%%youare% /c copy  
c:\winnt\repair\sam.\_ c:\inetpub\www\public
  - This is really cmd.exe /c copy ...

# Remember The Old Days?

---

- Host Based IDS 1.0 "Cool Features"
  - Immature generic detection
    - So what happens when it kills LSASS.EXE?
  - Trusted network concept
    - Should you really trust any network?
  - Provides detection for local vulnerabilities
    - Reactive signature based AV like technology
    - Helps protect users from themselves

# Remember The Old Days?

---

- Host Based IDS 1.0 Usage Scenarios
  - Forensic and Incident Response assistance
    - Great at collecting logs on large groups of workstations.
  - Some level of additional protection
    - Version 1.0 of most HIDS products were very immature and really offered minimal protection

# Where Are We Now?

---

## The State of IPS Today



# Where Are We Now?

---

- Network IPS 2.0
  - High speed devices
    - Multi-gig solutions
  - Can handle "hard things" like VOIP
    - Side note: Skype reversing = insanity
  - Can block attacks more accurately
    - More complex signatures
    - Detect pattern 123 but only if ABC exists
    - Detect object A look for function B

# Where Are We Now?

---

- Network IPS 2.0
  - Stateful signatures
    - IPS can maintain state and detect based on a sequence of packets
  - Less false positives
    - Some attacks are just too generic
  - Application decoding
  - Bypass still possible
    - But much harder today than ever
  - "Intelligent" network baselines
    - Artificial Intelligence will prove to fail (see next slide)

# Where Are We Now?

---

- Network IPS 2.0 - What's Missing
  - Bypass is still sometimes possible
    - Harder but still there in more complex protocols
  - False positives still happen
    - Some attacks are too generic and can appear legitimate. Complex signatures can fix this to a point.
  - Encryption still an issue
    - Won't it always be?

# Where Are We Now?

---

- Network IPS 2.0 - What's Missing
  - More integration needed with other technologies
  - "Intelligent" network baselines
    - Sasser story
    - Either fix it or kill it
  - IPv6 potential issues
    - Bypasses via IPv6 may be possible on some IPS
    - See Mark Dowd - Ruxcon 2006 - <http://www.ruxcon.org.au/2006-archive.shtml>

# Where Are We Now?

---

- Host IPS 2.0
  - Less system resource intensive
  - Better firewall capabilities - more flexible
  - Better generic detection of attack classes
  - Some AV protection
- Host IPS 2.0 - What's Missing
  - Bypass is still possible
  - False positives still happen
  - Integration into the network with better/smarter signaling
  - Better enterprise management capabilities
  - Integration into patch & systems management

# What Is The Future?

---

Crystal Ball Stuff



# What Is The Future?

---

- IPS is far from dead
  - As long as the technology evolves
    - Network based IPS is more mature today than ever
    - Host based IPS has a ways to go but can get there
- Host IPS 3.0 Should Do
  - Intelligently handles attacks
    - Stop crashing boxes!!!
  - Better file format decoding
    - Achilles heal of most HIPS

# What Is The Future?

---

- Host IPS 3.0 Should Do
  - Better enterprise management
    - This is the new pain point in security management
  - Zero day protection
    - Reactive on the host fails. Has AV not taught us this?
  - **Integration with Network Based IPS**
    - Can't we all just get along?

# What Is The Future?

---

- Network IPS 3.0 Should Do
  - Detect evasion attempts better
    - Research is ongoing but this is basically an arms race and very protocol dependant
  - Tighter integration with other technologies
    - IPS will eventually cease to be a separate technology but a feature of others
    - Network management type feature sets and control
  - Work with other security software
    - VA tool integration
  - Further reduce false positives
    - These will always exist but there can be even less than there are today
    - Some attacks are just too generic.

# What Is The Future?

---

- Network IPS 3.0 Should Do:
  - Better protocol decoding for application level protection
    - Ongoing research but some protocols are tougher than others
  - Better performance
    - 10gb links becoming more common with terabit+ devices
  - Simplify
    - Expertise is hard to find and maintain. Device management should cater to the JR. Infosec Professional
    - Maintenance should be minimal - this is one thing the AV industry has done right

# What Is The Future?

---

- Three essential goals
  - Fast
  - Simple
  - Embedded
- Caveats
  - Fast cannot be at the price of accuracy
  - Simple cannot be at the price of functionality
  - Embedded cannot be at the price of coverage

# ?? Questions ??

---

[mswarm@juniper.net](mailto:mswarm@juniper.net)

<http://security.juniper.net>