

# Network Intrusion Prevention Systems

kamal hilmi othman



# Where are we ?

- Log Analysis - The Essential
- TCP/IP - Packet Analysis
- Network Security Monitoring - Using Snort
- Honeypot Systems - Tracking Intruder
- **Network Intrusion Prevention Systems**
- Intrusion and Vulnerability Management

\*\*\*\*\* Normally each topic is meant for 2 to 3 days, today - i'm taking only 30 mins!!

# Agenda

- Technologies
- Deployment
- Open Source Tools

# Some Timeline

- 1998 - 'TCP Rst' Technology
- 2001 - Hogwash
- June 2003 - "IDS is dead"
- 2003 - Honeywall
- .. ..been adopted into *perimeter ecosystem*.

# Intrusion

- Intrusion - policy violation of the systems
- Intrusion detection - detecting policy violations
- Intrusion prevention - prevent and/or defend attacks against violation of the systems

# Generic Intrusion Prevention Systems (IPS)

- Automatically detects and prevent attacks and/or misuse against protected systems / resources.
- 2 major classification - Network IPS , Host IPS

# Definition

- Network IPS

A system that monitors network traffic and attempts to control the flow of it based on decisions made through its analysis. This may include in-line systems that resemble firewalls, or systems that attempt to disrupt traffic through the application of TCP resets or ICMP control messages.

# Definition (cont'd)

- **Host IPS**

A program resident on a host that monitors its health and attempts to prevent unwanted (bad) behavior by system controls. Some of the latest technology monitors system calls and attempts to derive a baseline of “good” traffic based on a learned profile, while preventing system calls that are outside of the acceptable profile.

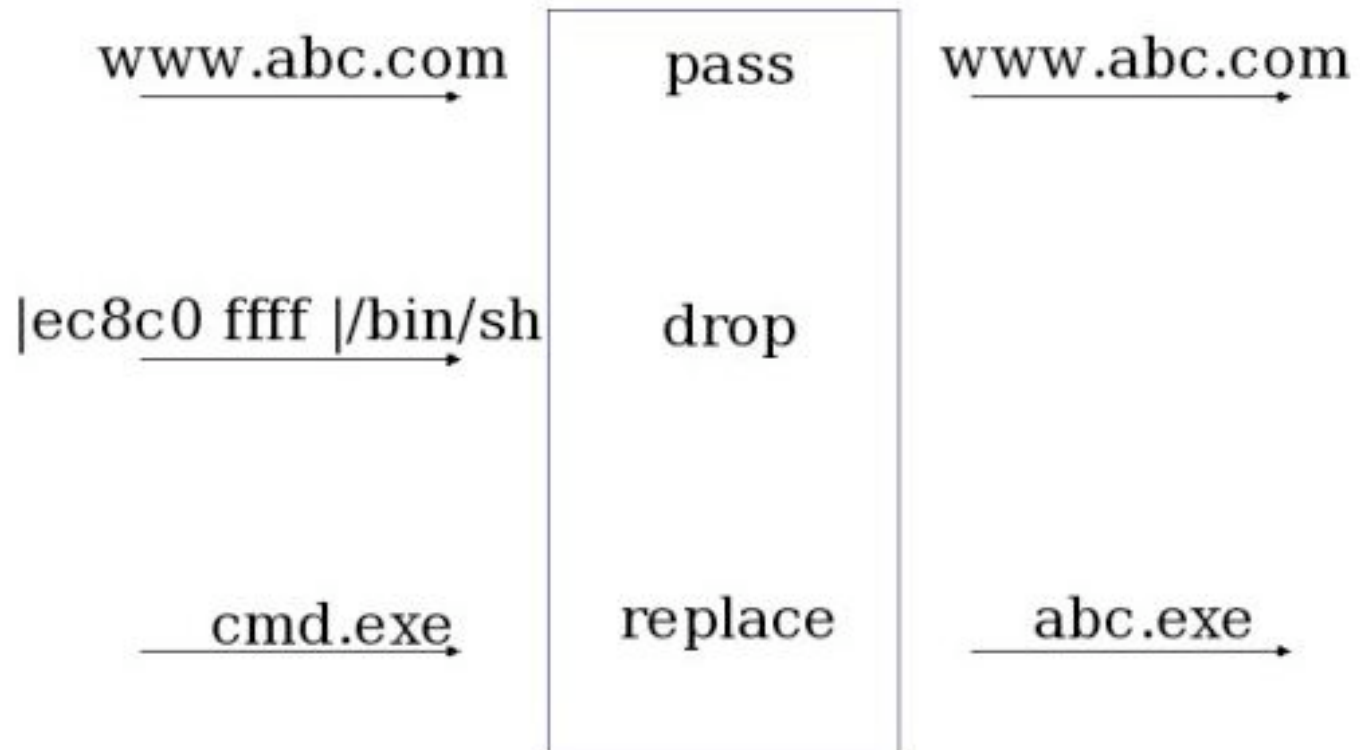
# IPS Mode

- Inline
  - Traffic stream
- Gateway Interaction
  - Dynamic interaction with router / firewall
- Session Snooping
  - TCP Rst
- Endpoint
  - IPC / System Call

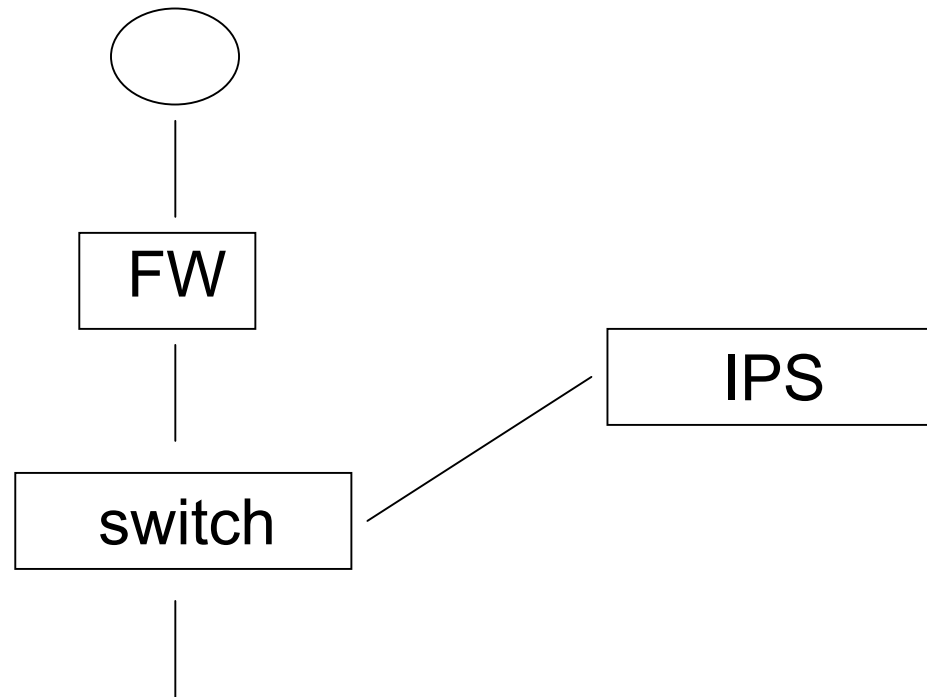
# NIPS

- A device
- Firewall + IDS
- Prevent intrusion

# NIPS Inline Concept



# NIPS “Active Response” Concept



# Requirements

- Fast
- Keep State
  - Knowledge in application protocols / behavior.
- Accurate and updated

# Challenges

- Detection capabilities
  - Encrypted ?
- Evasion resistance
  - Altered exploit ?
- Single point of failure
- High throughput
- Attack detection / update

# Hogwash 101

- No longer in maintenance ( works for me :))
- Gateway IDS and packet scrubber
- Keywords
  - drop - drop the packet, send TCP rst and log
  - Ignore - drop the packet
  - sdrop - drop the packet, send TCP rst
  - replace - replace detected string with another string

# Hogwash 101 (cont'd)

- drop icmp any any -> \$MYDMZ any (msg:"cyberkit drop pot"; content:"|aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa|"; itype:8; dsize:64;)
- drop udp any any -> \$MYDMZ 1434 (msg:"MS-SQL Worm attempt"; content:"|04|"; depth:1; content:"|81 F1 03 01 04 9B 81 F1 01|"; content:"sock"; content:"send";)
- drop tcp any any -> \$MYDMZ 445 (msg:"NETBIOS SMB-DS DCERPC attempt"; content:"|FF|SMB|25|";)

# Hogwash 101 (cont'd)

- Jun 19 03:57:26 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 151.9.116.99
- Jun 19 03:57:31 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 151.9.116.99
- Jun 19 03:57:36 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 140.112.38.9
- Jun 19 03:57:41 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 140.112.38.9
- Jun 19 03:58:37 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 151.9.116.99
- Jun 19 03:58:42 fw02 snort: [1:1855:2] Packet Dropped-DDOS  
Stacheldraht agent->handler (skillz) {ICMP} x.y.z.117 -> 151.9.116.99



# Snort Flexible Response

- Plug-in
- Keywords

- resp

- ```
resp: <resp_mechanism>[,<resp_mechanism>[,<resp_mechanism>]];
```

- react

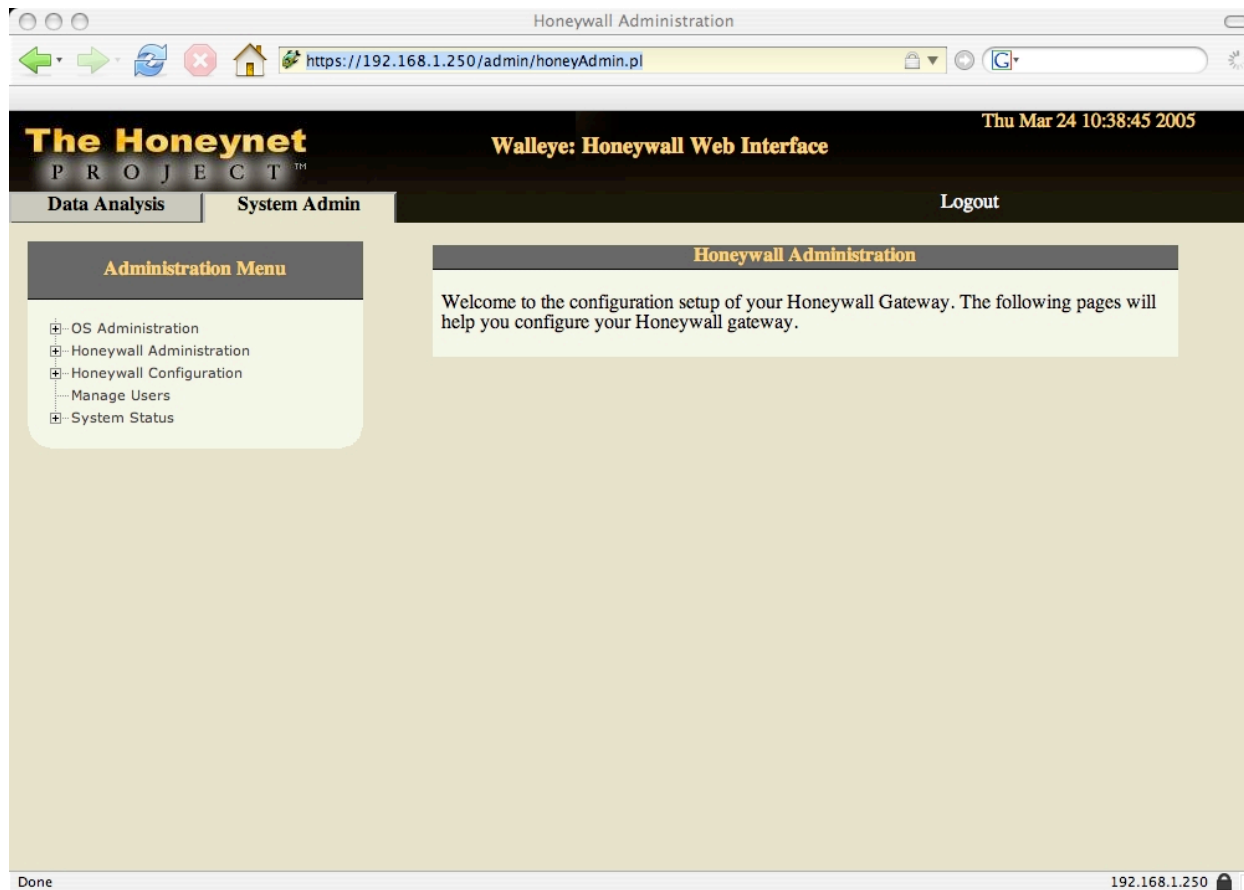
- ```
react: <react_basic_modifier[, react_additional_modifier]>;
```

# Snort Flexible Response (cont'd)

- alert tcp \$LAN any <> \$NET 80 (content: "mp3"; msg: "illegal music lah"; react: block, msg;)
- alert tcp \$DMZ any -> \$SWITCH 23 (msg:"telnet attempt"; flags:S; resp:rst\_all;)
- [http://www.snort.org/docs/snort\\_htmanuals/htmanual\\_233/node23.html](http://www.snort.org/docs/snort_htmanuals/htmanual_233/node23.html)

# Honeywall

- Based on Snort-Inline



# NIPS vs NIDS

## NIPS

- Acts as network gateway
- Stops suspect packets
- Prevents successful intrusions
- False positives are VERY bad

## NIDS

- Only observes network traffic
- Logs suspect packets and generates alerts
- Cannot stop an intruder
- False positives are not as big of an issue

Note: Taken from Jed Haile presentation at BlackHat02

# An Opinion

- Shall I ?
  - Understand your network
  - Understand your flow
  - Monitor - Firewall, NIDS, HIDS
- Then ... u are ready to fine tune your NIPS
- Wave of the future research

# URL

- Hogwash
  - <http://hogwash.sourceforge.net>
- Snort - Flexible Response
  - <http://www.snort.org>
- SnortSam
  - <http://www.snortsam.net>
- Snort-Inline
  - <http://www.snort-inline.sourceforge.net>
- Fwsnort
  - <http://www.cipherdyne.org/fwsnort/>
- LIDS
  - <http://www.lids.org>
- LAk
  - <http://lak-ips.sourceforge.net>

end()

khilmi @ {defenxis.com , hackinthebox.org}

see u @ HITBSecConf2005



<http://conference.hackinthebox.org>