Introduction to IPS/IDS

Dr. Pipat Sookavatana

Network Security

Sans Institute Top 10 Cyber Threats for 2008

1. Increasingly sophisticated website attacks that exploit browser vulnerabilities
2. Increasing sophistication and effectiveness in botnets
3. Cyber espionage efforts by well-resourced organizations to extract large amounts of data for economic and political purposes
4. Mobile phone threats, especially against iPhones, Google's Android phones, and voice over IP systems
5. Insider attacks
6. Advanced identity theft from persistent bots
7. Increasingly malicious spyware
8. Web application security exploits
9. Increasingly sophisticated social engineering to provoke insecure behavior
10. Supply chain attacks that infect consumer devices

Top 9 Threat by Zdnet

- **100% growth in revenue for cyber crime**.
  - There are lots of estimates for just how big the cyber crime economy is. I peg it at over $1 bllion and under $10 billion. Whatever it is today I predict that the quest for financial gain will spur cyber criminals to a banner year, at least doubling their overall take.
- **DDoS in support of phishing attacks**.
  - A combined effort between the phishers and the DDoSers: an attack against a banking or ecommerce site along with a barrage of emails that claim the site is “down for maintenance, please log in here to access your account”, or some such social engineering attempt
- **Successful DDoS attack against a financial services firm**.
  - Zdnet believes that this is already going on, these types of organizations are not to quick to adit when they have had to pay extortion fees. 2007 will be the year of the first high profile attack against a large US or UK bank or trading desk.

- **Attacks against DNS are the threat of the year**.
  - DNS servers are part of the critical infrastructure of the Internet. They are also an easy target for DDoS attacks. Unfortunately the collateral damage could be devastating if an attack took our one of the root domain name servers.
- **No abatement in identity theft**.
  - As long as banks continue to essentially pay off cyber criminals, by covering their customers losses as a primary means of defense, identity theft will remain a threat. Markets are developing that make it easier to monetize stolen identities thus increasing the value of stolen IDs while decreasing the cost of “moving” them.
- **More attacks against wireless networks**.
  - 2006 saw the birth of new attacks against cell phones. These include a text message urging you to call a particular premium phone number (vishing), and malware that infects phones, particularly Symbian phones, and spreads via Bluetooth and even by MMS. And finally, MMS messages that generate calls to premium numbers; a short lived but lucrative exploit

- **MySpace grows up and gets secure**.
  - MySpace is riddled with opportunities for the entrepreneurial criminal. In 2007 the number of attacks from predators, criminals and hackers will get to the point that MySpace will tighten up its controls and monitoring. That will make it less appealing to its teenage audience will grow up and move on.
- **YouTube abuse threatens site**.
  - Like network news, email, and IM before it, the new popular service, video sharing, will succumb to spammers who post ads, ad backed videos, and stealth marketing exploits, ruining the experience for everybody.
- **Network infrastructure shows signs of overloading**.
  - The backbone providers have been resting on the excess bandwidth they invested in during the dot com bubble. But now that voice and video are really here their infrastructure is showing signs of weakness. That will manifest itself in outages, slowdowns, and a mad scramble to lay more fiber in 2007.

- Although 86 per cent of respondents use firewalls
- it is apparent that firewalls are not always effective against many intrusion attempts.
- *The average firewall is designed to deny clearly suspicious traffic - such as an attempt to telnet to a device* when corporate security policy forbids telnet access completely - ***but is also designed*** to allow some traffic through - **Web traffic to an internal Web server, for example.**

- The problem is, that many exploits attempt to take advantage of weaknesses in the very protocols that are allowed through our perimeter firewalls, and *once the Web server has been compromised, this can often be used as a springboard to launch additional attacks on other internal servers.*
- Once a "*rootkit*" or "*back door*" has been installed on a server, the hacker has ensured that he will have unfettered access to that machine at any point in the future.

- What is ROOTKIT
  - A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.
  - A rootkit is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.

Firewalls are also typically employed only at the network perimeter.

- However, many attacks, intentional or otherwise, are launched from within an organization. Virtual private networks, laptops, and wireless networks all provide access to the internal network that often bypasses the firewall.
- **Intrusion detection systems** may be effective at detecting suspicious activity, but do not provide protection against attacks. Recent worms such as Slammer and Blaster have such fast propagation speeds that by the time an alert is generated, the damage is done and spreading fast.

- false positive = an alarm that an attack has taken place whereas this was not the case
- false negative = the IDS does not detect and filter the attack

IDS/IDP

Most common used now a day
Network IPS only

- Host IDS/IPS (HIPS)
  - Application Base (Application Firewall or IPS)
- Network IDS/IPS (NIPS)
- Network Node IDS/IPS (NNIPS)
- Stack Base IDS/IPS
  - Honeypot
- Padded Cell Systems

HIPS

- As with Host IPS systems,
- The Host IPS relies on agents installed directly on the system being protected. It binds closely with the operating system kernel and services,
- Monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

- Since a Host IPS agent intercepts all requests to the system it protects, it has certain prerequisites
  - it must be very reliable, must not negatively impact performance, and must not block legitimate traffic.
- Any HIPS that does not meet these minimum requirements should never be installed in a host, no matter how effectively it blocks attacks.

Advantages: of HIDS/HIPS

- you "see" the impact of an attack and can react better on it
- you can recognize Trojan horses etc. better as the available information/possibilities are very extended
- you can detect attacks which cannot be detected by Network based IPS because traffic is often encrypted
- you can observe activities on your host exactly

Disadvantages: of HIDS/HIPS

- they are not good in recognizing scans
- they are more vulnerable to DoS attacks
- the analysis of operating system audit trails is very time-consuming because of its size.
- they stress the host's CPU performance (partly) immensely

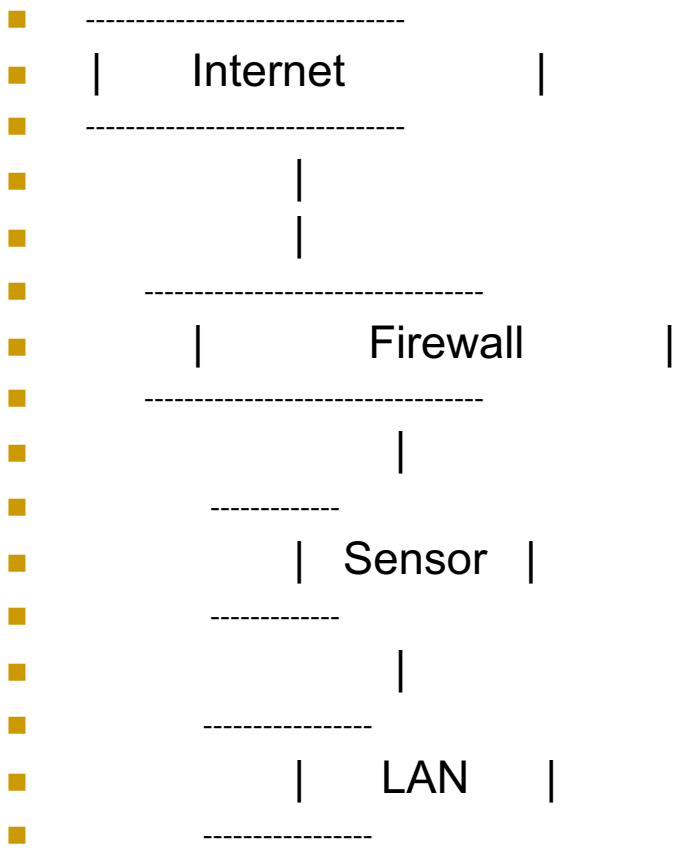
Network IDS/IPS (NIPS)

- The Network IPS combines features of a standard IDS, an IPS and a firewall, and is sometimes known as an In-line IPS or Gateway IPS (GIPS).
- The next-generation firewall - the deep inspection firewall - also exhibits a similar feature set, though we do not believe that the deep inspection firewall is ready for mainstream deployment just yet.

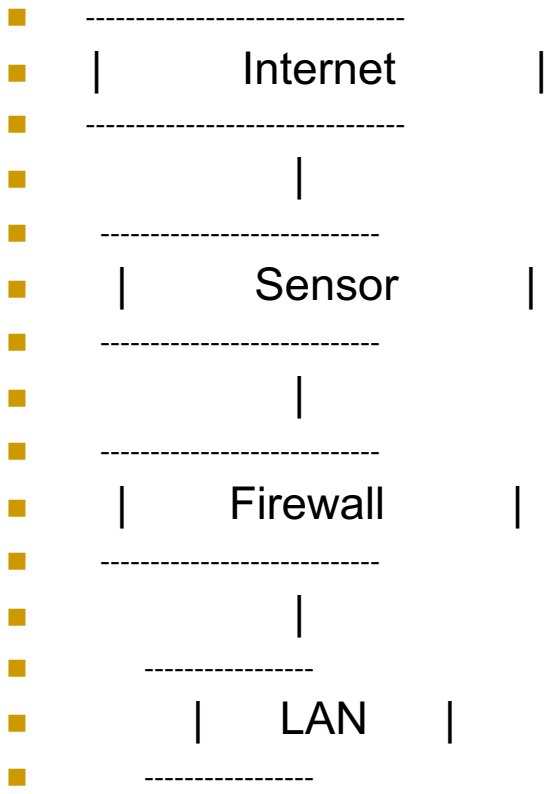
NIPS Sensor Location

- 1. With in the firewall
- 2. Outside the firewall

Within the firewall (simplified)



Outside the firewall (simplified)



Advantage of NIDS/IPS

- the sensors can be secured well as they "only" observe traffic
- you can detect scans better - on the basis of signatures... you can "filter" traffic (actually, we will show later that this is not always the case)

Disadvantage

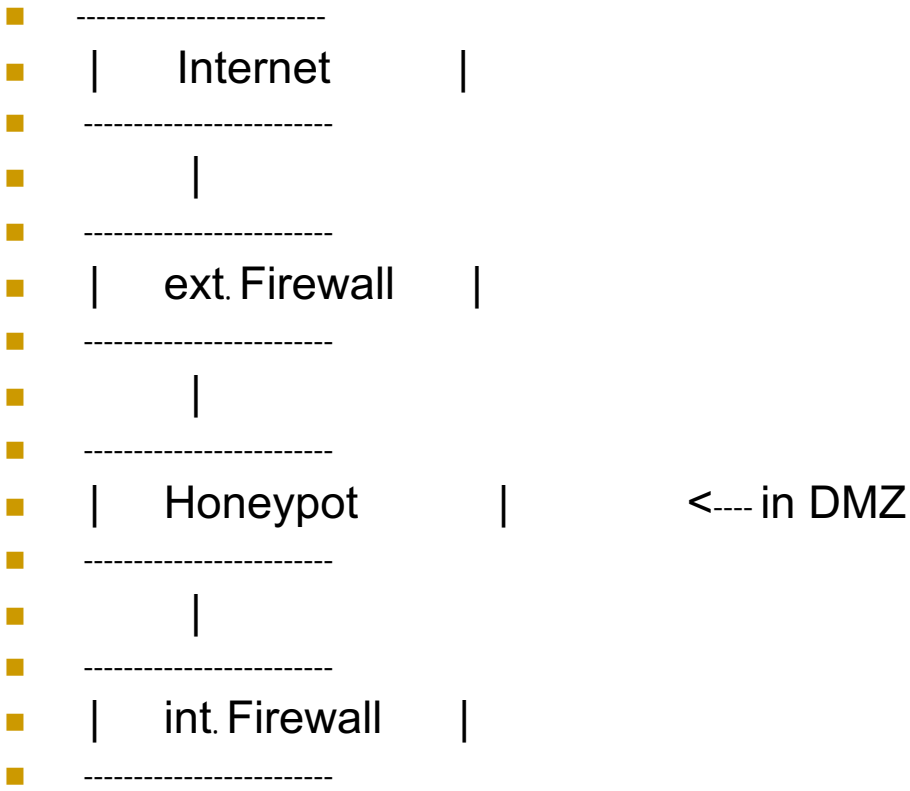
- the probability of so called false negatives (attacks are not detected as attacks) is high as it is difficult to control the whole network
- mostly, they have to operate on encrypted packets where analysis of packets is complicated
- as a difference to host-based IPS they do not see the impacts of an attack

Network Node IDS/IPS (NNIDS)

- Basically, this new type (NNIDS) works like typical NIDS, i.e., you take packets from network traffic and analyze them.
- But it only concerns packets which are addressed to the network node (this is where the name comes from).
- Another difference between NNIDS and NIDS is that NIDS run in promiscuous mode while NNIDS does not run in promiscuous mode.

Stack Based IPS

HoneyPot System



Padded Cell Systems

- Virtual Network System

Padded Cell Systems

- Advantages:
  - once in a padded cell host, attackers cannot do any more damage as it is only a "bogus“ environment
  - the admin can follow/log the activities of the attacker directly to get more information about the
  - attack and the target of the attack and so is able to initiate counteractive measures more easily

- Disadvantages:
  - eventually, usage of padded cell systems is not legal (the same as honeypots, in Europe this should be no problem)
  - the implementation of such a system is very difficult and requires some knowledge as the whole environment has to be simulated correctly.
  - If the admin makes a little mistake somewhere thissystem could by all means open additional security holes