IJCSI International Journal of Computer Science Issues, Volume 13, Issue 2, March 2016
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org http://dx.doi.org/10.20943/01201602.3843 

# A Survey on IPS Methods and Techniques

**Dr. K. Prabha[1], S. Sudha sree[2]**

**[1] Department of computer science, Periyar University PG Extension Centre Dharmapuri, Tamil Nadu, India**

**[2] Department of computer science, Periyar University PG Extension Centre Dharmapuri, Tamil Nadu , India**

**Abstract**

The quality and impact of attacks have been continuously increases; attackers continuously find vulnerabilities at various levels, from the network itself to operating system and applications, exploit to crack the system and services. Defence system and networking monitoring has becomes essential component of computer security to predict and present attacks. IPS can be termed as the extension of IDS with exercise of access control to protect computers from exploitation. IPS is an intelligent device that is capable of not only detecting malicious activities, but also to take preventive actions to secure both the host and the network attacks. An IPS works inline in the data stream to provide protection from malicious attacks in real time. This is called inline mode. In this paper the deeper analysis is the IPS identify, stop and block attacks that would normally pass through a traditional fire wall devices.

***Keywords:*** *IPS, firewall, Signature detection, Stateful Protocol, IP TTL, Security System.*

## 1. Introduction

Computer system security has become a major concern over the past few years. Attack, threat or intrusions, against computer system and network have become common place events, many system device and other tools are available to help counter the threat of these attack. wall, strengthen in implementing executing rules and policy, but The firewall can do nothing about attack from inside network and cannot clarify behavior or anomaly attack, antivirus software. Unfortunately, antivirus very limited ability to pattern recognition of new viruses before the anti-program created by corporate, and Intrusion Detection, only send the alert to trigger after attacked have entered the network, and do nothing to stop attacks. An IPS is best compared to a firewall. Firewalls and IPS are control devices. They sit in line between two networks and control the traffic going through them. But the basic difference between Firewall and IPS is the way they handle network traffic. Whereas a Firewall denies all the requests that do not match its safety definition, IPS accepts all the requests except those whose contents seem to be malicious and threatening to the system. Intrusion preventing system is a new approach system to defence networking system which proactive technique prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when attack is when an attack is identified, intrusion prevention block and log the offending data. Ghorbani [2], propose work in IPS filed, describes IPS uses to secure the system, the enterprise uses several technology security systems.

This document is set in 10-point Times New Roman. If absolutely necessary, we suggest the use of condensed line spacing rather than smaller point sizes. Some technical formatting software print mathematical formulas in italic type, with subscripts and superscripts in a slightly smaller font size. This is acceptable.

## 2. IPS APPROACHES

Some of the approaches being used are.

- *Software based heuristic approach*: This approach is similar to IDS anomaly detection using neural networks with the added ability to act against intrusions and block them.
- *Sandbox approach:* Mobile code like ActiveX, Java applets and various scripting languages are quarantined in a *sandbox* - an area with restricted access to the rest of the system resources. The system then runs the code in this *sandbox* and monitors it's behavior. If the code violate a predefined policy it's stopped and prevented from executing, thwarting the attack (Conry-Murray).
- *Hybrid approach:* On network-based IPS (NIPS), various detection methods, some proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router.
- *Kernel based protection approach:* Used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls access to system resources like memory, I/O devices, and CPU, preventing direct

user access. In order to use resources user applications send requests or system calls to the kernel, which then carries out the operation. Any exploit code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls.

## 3. TYPES OF IPS

### 3.1 Host based Intrusion Prevention (HIP)

1. *Storm watch*: OKENA's Storm Watch uses a kernel-based approach and works on servers and workstations. Policies - collections of access control rules based on acceptable behavior, is available out-of-the-box for common applications such as Microsoft SQL Server, Instant Messenger, and IIS Server. Policies control what resource is being used, what operation is being invoked, and which application is invoking it. Storm Watch hooks into the kernel and intercepts system calls (Okena).

It has four interceptors:

- File System interceptor - intercepts all file read and write requests.
- Network interceptor - intercepts packet events at the driver (NDIS) or transport (TDI) level.
- Configuration interceptor - intercepts read/write requests to the registry on Windows or to files on UNIX.
- Execution space (Run-time environment) interceptor - requests to write to memory not owned by the requesting application will be blocked by this interceptor.

2. ENTERCEPT's Standard: Entercept, a pioneer in kernel-based protection, proactively protects the host by intercepting system calls (Entercept). Unlike Okena's Storm Watch it uses both, signatures and behavior rules to stop and detect attacks. In an article by Ed Skoudis on "infosec's WORST NIGHTMARES", some Night mares that he mentions are stealthier attacks and "super" worms – "Fast spreading, multiplatform, multi-exploit, zero-day, metamorphic worms". He goes on to say that one way of preparing for these coming "super" worms is to, "Utilize host-based intrusion detection and prevention tools such as Entercept Security Technologies and OKENA's Storm Watch on critical systems to block or rapidly discover attacks.

### 3.2 Network based Intrusion Prevention (NIP)

NIPS are generally appliance-based systems that sit in line, and block suspicious traffic after detecting an attack. They utilize different detection methods, signature detection, anomaly detection, and some proprietary methods, to block specific attacks. Some of the methods adopted by vendors are

- Stateful Signature detection – It looks at relevant portions of traffic, where the attack can be perpetrated. It does this by tracking state and based on the context specified by the user detects an attack. It is not completely automatic, as the user needs to have some prior knowledge about the attack.
- Protocol anomaly detection - All vendors do detailed packet analysis with protocol decode engines to ensure packets meet protocol requirements. Traffic normalization is also done to remove protocol ambiguities and ensures that traffic interpreted by the NIPS.

## 4. IPS Advantages and Disadvantages

### 4.1 ADVANTAGES:

- One of the most common problems with an IPS is the detection of false positives or false negative, this occurs when the system blocks activity on the network because it is out of the normal and so it assumes it is malicious, causing denial of service to a valid users, trying to do a valid procedure; or in the case of a false negative, allowing a malicious to go.
- Considering that this problem found in IDS; however it should be one of the main goals of the network administrators and the manufacturers of IPSs to minimize this as much as they can [4].
- Other problem that occurred in IPS that it starts to be quite expensive. Also, if there are multiple IPSs on the network then every packet of data must make multiple stops from its original destination to get to the end user, this will cause loss of network performance and it's another problem [4].
- One of the IPS advantages that it has ability to act like antivirus software by detecting malicious signatures, stopping them then showing where are they coming from, and where they are trying to go. IPSs can prevent hackers to damage data on a users system or cause on overflow of network traffic [4].

### 4.2 DISADVANTAGE:

- Even these down sides the benefits of IPs that we receive lead us to protection that any one other security method can provide.

## 5. Methods used for Detection and Prevention:

### 5.1 Detection:

There are three methods used for detection [10],[6],[1]. They are Misuse detection or Signature detection (knowledge based), Anomaly detection (behavior based), Stateful protocol analysis method

- ***Misuse detection*** discovers attacks based on patterns extracted from known intrusions. Anomaly detection identifies attacks based on significant deviations from normal activities. Misuse detection has low false positive rate, but cannot detect novel attacks.
- ***Anomaly*** detection can detect unknown attacks, but usually has a high false positive rate. To combine the advantages of misuse and anomaly detection, many hybrid approaches have been proposed. Data mining is the analysis of large data sets to discover understandable patterns or models. Here there are some examples of Signatures given.
  - A telnet attempt with a username of "root", which is a violation of an organization's security policy.
  - An e-mail with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware.
  - An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled.
  - Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.
- ***Stateful protocol*** analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.

### 5.2 Prevention methods:

An IPS is a preemptive network security approach that uses advanced techniques to detect and block (or prevent) possible intrusion attempts into a computer system. An IPS thoroughly scans the traffic flowing to and from a computer system or computer network for security breaches. If a threat is detected, the system is able to take defensive actions such as dropping a particular data packet or dropping the whole connection. The scan captures details, the action report is logged in a file, and an alert is sent to the system or network administrator. IPSs differ in how they scan the data streams to detect a threat or intrusion. Some of the most popular methods are described below.

- ***Signature method:*** In the signature method, the IPS compares the real-time data stream patterns with a huge database of attack patterns that have already been detected. In this process, each data packet is scanned, byte by byte, for a particular pattern or string that represents complete or partial code associated with a known attack. The pattern or string could be anything, such as a command name or a specific set of characters. some examples of signature matching:
  - Matching the subject description or attachment name of an email with details of a known or detected malicious email.
  - Tracking the denial-of-service attack by counting the number of times a command is executed and matching it with known statistics of a similar kind of attack.
  - Matching a user activity prior to authentication or login with a known attack pattern.
- ***Profile method:*** In the profile method, the IPS collects a pattern of data stream flowing to and from a computer system (or computer network) in controlled or trusted conditions. This pattern is treated as a baseline profile and compared against the real-time data stream patterns. A real-time data stream pattern that is found to be suspiciously different from the baseline profile is treated as an attack, and preventive action is taken against it. A standard baseline profile can represent normal behavior of things such as network connections, applications, users, and hosts. For example, if a real-time data stream is observed to be accessing a crucial system file that wasn't accessed when the baseline profile was generated in the controlled environment, this attempt is treated as malicious stateful protocol method.
- ***State protocol method:*** Data packets are wrapped with various protocol headers. Each layer of the TCP/IP or Open Systems Interconnection (OSI) model adds the header of the protocol (the protocol being used for that layer, which is to the received packet. Protocols follow a standard document format known as Requests for Comments (RFCs). An RFC completely explains the protocol and describes how it should be used. The RFC forms the basis of the stateful protocol method. In this method, each protocol header is peeled apart and

scanned for its consistency with what its RFC specifies. A deviation from the RFC is considered alarming, and an alert is raised. For example, a TCP packet with only SYN and FIN flags on is a deviation from what the TCP RFC specifies. If a data packet with the TCP header contains both these flags on, then this needs to be reported.

## 6. IPS Evasion Techniques

As discussed in the previous section there are a number of methods to analyze attacks, but to better analyze and choose anti-evasion countermeasures it's important to understand the various evasion techniques used by attackers. Network attackers often use network IPS evasion techniques to attempt to bypass the intrusion detection, prevention, and traffic filtering functions provided by network IPS sensors. Some commonly used network IPS evasion techniques are listed below.

- Encryption and Tunneling
- Timing Attacks
- Resource Exhaustion
- Traffic Fragmentation
- Protocol-level Misinterpretation
- Traffic Substitution and Insertion

### 6.1 Encryption and Tunneling

One common method of evasion used by attackers is to avoid detection simply by encrypting the packets or putting them in a secure tunnel. As discussed now several times, IPS sensors monitor the network and capture the packets as they traverse the network, but network based sensors rely on the data being transmitted in plaintext. When and if the packets are encrypted, the sensor captures the data but is unable to decrypt it and cannot perform meaningful analysis. This is assuming the attacker has already established a secure session with the target network or host. Some examples that can be used for this method of encryption and tunneling are:

- Secure Shell (SSH) connection to an SSH server
- Client-to-LAN IPSec (IP Security) VPN (virtual private network) tunnel
- Site-to-site IPSec VPN tunnel
- SSL (Secure Socket Layer) connection to a secure website

There are other types of encapsulation that the sensor cannot analyze and unpack that attackers often use in an evasion attack. For example, GRE (Generic Route Encapsulation) tunnels are often used with or without encryption.

### 6.2 Timing Attacks

Attackers can evade detection by performing their actions slower than normal, not exceeding the thresholds inside the time windows the signatures use to correlate different packets together. These evasion attacks can be mounted against any correlating engine that uses a fixed time window and a threshold to classify multiple packets into a composite event. An example of this type of attack would be a very slow reconnaissance attack sending packets at the interval of a couple per minute. In this scenario, the attacker would likely evade detection simply by making the scan possibly unacceptably long.

### 6.3 Resource Exhaustion

A common method of evasion used by attackers is extreme resource consumption, though this subtle method doesn't matter if such a denial is against the device or the personnel managing the device. Specialized tools can be used to create a large number of alarms that consume the resources of the IPS device and prevent attacks from being logged. These attacks can overwhelm what is known as the management systems or server, database server, or *Out-of-Band (OOB)* network. Attacks of this nature can also succeed if they only overwhelm the administrative staff, which does not have the time or skill necessary to investigate the numerous false alarms that have been triggered.

Intrusion detection and prevention systems rely on their ability to capture packets off the wire and analyze them quickly, but this requires the sensor has adequate memory capacity and processor speed. The attacker can cause an attack to go undetected through the process of flooding the network with noise traffic and causing the sensor to capture unnecessary packets. If the attack is detected, the sensor resources may be exhausted but unable to respond within a timely manner due to resources being exhausted.

### 6.4 Traffic Fragmentation

Fragmentation of traffic was one of the early networks IPS evasion techniques used to attempt to bypass the network IPS sensor. Any evasion attempt where the attacker splits malicious traffic to avoid detection or filtering is considered a fragmentation-based evasion by:

- Bypassing the network IPS sensor if it does not perform any reassembly at all.

- Reordering split data if the network IPS sensor does not correctly order it in the reassembly process.
- Confusing the network IPS sensor's reassembly methods which may not reassemble split data correctly and result in missing the malicious payload associated with it.
- A few classic examples of fragmentation-based evasion are below:
- TCP segmentation and reordering, where the sensor must correctly reassemble the entire TCP session including possible corner cases, such as selective ACKs and selective retransmission.
- IP fragmentation, where the attacker fragments all traffic if the network IPS does not perform reassembly. Most sensors do perform reassembly, so the attacker fragments the IP traffic in a manner that it is not uniquely interpreted. This action causes the sensor to interpret it differently from the target, which leads to the target being compromised.

In the same class of fragmentation attacks, there is a class of attacks involving overlapping fragments. In *overlapping fragments* the offset values in the IP header don't match up as they should, thus one fragment overlaps another. The IPS sensor may not know how the target system will reassemble these packets, and typically different operating systems handle this situation differently.

## 6.5 Protocol-level Misinterpretation

Attackers also evade detection by causing the network IPS sensor to misinterpret the end-to-end meaning of network protocols. In this scenario the traffic is seen differently from the target by the attacker causing the sensor either to ignore traffic that should not be ignored or vice versa. Two common examples are packets with bad TCP checksum and IP TTL (Time-to-Live) attacks.

A bad TCP checksum could occur in the following manner: An attack intentionally corrupts the TCP checksum of specific packets, thus confusing the state of the network IPS sensor that does not validate checksums. The attacker can also send a good payload with the bad checksum. The sensor can process it, but most hosts will not. The attacker follows with a bad payload with a good checksum. From the network IPS sensor this appears to be a duplicate and will ignore it, but the end host will now process the malicious payload.

The IP TTL field in packets presents a problem to network IPS sensor because there is no easy way to know the number of hops from the sensor to the end point of an IP session stream. Attackers can take advantage of this through a method of reconnaissance by sending a packet that has a very short TTL which will pass through the network IPS fine, but be dropped by a router between the sensor and the target host due to a TTL equaling zero. The attacker may then follow by sending a malicious packet with a long TTL, which will make it to the end host or target. The packet looks like a retransmission or duplicate packet from the attacker, but to the host or target this is the first packet that actually reached it. The result is a compromised host and the network IPS sensor ignored or missed the attack.

## 6.6 Traffic Substitution and Insertion

Another class of evasion attacks includes traffic substitution and insertion. Traffic substitution is when that attacker attempts to substitute payload data with other data in a different format, but the same meaning. A network IPS sensor may miss such malicious payloads if it looks for data in a particular format and doesn't recognize the true meaning of the data. Some examples of substitution attacks are below.

- Substitution of spaces with tabs, and vice versa, for example inside HTTP requests.
- Using Unicode instead of ASCII strings and characters inside HTTP requests.
- Exploit mutation, where specific malicious shell code (executable exploit code that forces the target system to execute it) can be substituted by completely different shell code with the same meaning and thus consequences on the end host or target.
- Exploit case sensitivity and changing case of characters in a malicious payload, if the network IPS sensor is configured with case-sensitive signature.

Insertion attacks act in the same manner in that the attacker inserts additional information that does not change the payload meaning into the attack payload. An example would be the insertion of spaces or tabs into protocols that ignore such sequences.

TABLE 1: CISCO IPS EVASION TOOLS & ANTI-EVASION FEATURES

| Evasion Method | Evasion Tool | Cisco IPS Anti-Evasion Features |
|---|---|---|
| Traffic | Fragroute, | Full session |
| Traffic | Fragroute, | Full session |
| Traffic | Metasploit | Data |
| Protocol-level | | IP TTL |
| Timing Attacks | Nmap | Configuration |
| Encryption and | Any | GRE tunnel |
| Resource | Stick | Smart |

Table 6.1 above summarizes the evasion methods, tools, and the corresponding IPS anti-evasion features available on the Cisco IPS sensors. Though they are covered in the table the anti-evasion features are listed below.

- Smart and dynamic summarization of events to guard against too many alarms for high event rates.
- IP TTL analysis and TCP checksum validation to guard against end-to-end protocol-level traffic interpretation.
- Full session reassembly that supports the STRING and SERVICE engines that must examine a reliable byte stream between two network endpoints.
- Configurable intervals for correlating signatures, or the use of an external correlation that does not require real-time resources, such as Cisco Security MARS.
- Data normalization (de-obfuscation) inside SERVICE engines, where all signatures convert network traffic data into a normalized, canonical form being comparing it to the signature matching rules.
- Inspection of traffic inside GRE tunnels to prevent evasion through tunneling.

## 4. Conclusions

IPS system presents additional performance challenges because of its in-line nature. Misuse detection and anomaly detection have advantages and drawbacks. Major drawback of any IPS is very effective technique to protect databases and networks from unauthorized users. It is used in many organizations to keep its own data secure. Combining network and host IPS technology results in the most comprehensive and robust defensive posture. Implementing and deploying proactive IPS technologies g you avoid an attack. Combining IPS, IDS and Firewall technologies will provide a strong defense line to protect systems from any attack, for example firewall play as first defense line that connect to the second defense line IDS, and first and second lines connect to the third defense line IPS. Combining these three technologies will generate a great protection for any system. IPS is very useful to use in large networks. We expect to see more real world applications that use IPS in coming days.

## References

[1] A. Fuchsberger, "Intrusion Detection Systems and intrusion Prevention Systems," Information Security Technical Report, vol. 10, 2005, pp. 134-139.

[2] Charlie Kaufman, Radia Perlmon and Mike Speciner; "Network Security; Private Communication in a Public World", 2nd Edition, Prentice Hall of India.

[3] Intrusion Detection System using Sax 2.0 and wire shark 1.2.2.

[4] Ido Green, Tzvi Raz, Moshe Zviran, "Analysis of Active Intrusion Prevention Data for Prediction Hostile Activity In Computer Networks", Communications of the ACM April 2007/Vol. 50, No. 4.

[5] Jiong Zhang, Mohammad Zulkernine, and Anwar Haque (2008), "Random-Forests-Based Network Intrusion Detection Systems", IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol. 38, no. 5, September 2008.

[6] Nong Ye, Senior Member, IEEE, Syed Masum Emran, Qiang Chen, and Sean Vilbert (2002), "Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection", IEEE Transactions on Computers, Vol. 51, No. 7, July 2002.

[7] Nick Ierace, Cesar Urrution and Richard Bassett, "Intrusion Prevention System.

[8] Shaw n Conaway, "Using an Intrusion Prevention System as Part of a Layered Security Approach", Network Support, Technical Enterprises, October- 2006.

[9] T. Ghorbani, A.A., Lu, W., "Network Intrusion Detection and Prevention: Concepts and Technique", Springer, 2009.

[10] William Stallings, "Cryptography and Network Security: Principles and Practices", Pearson Education, 4th Edition, 2011.

[11] Y. Weinsberg, S. Tzur-David, D. Dolev, and T. Anker, "High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS)", High Performance Switching and Routing, IEEE, 2006, pp. 147-153.